5ªEdição

Governo Aberto
RECOMENDA

Diretrizes para a **Implementação da Lei Geral de Proteção de Dados Pessoais**

CIDADE DE SÃO PAULO

Governo Aberto na Cidade de São Paulo

Sumário

Apresentação

A equipe de Governo Aberto tem como responsabilidade a promoção da abertura do governo municipal aos cidadãos. Para isso, engaja os servidores públicos municipais de todos os órgãos públicos na promoção da transparência, participação social, prestação de contas, tecnologia e inovação.

Sendo assim, a Coordenadoria de Governo Aberto (CGA) elabora documentos norteadores voltados para os servidores públicos, explorando temáticas relevantes para a promoção dos pilares de Governo Aberto no município através da coleção **"Governo Aberto Recomenda"**. Este quinto volume da coleção aborda a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito municipal. O presente documento foi idealizado e construído pela equipe da CGA, contando com o apoio da Coordenadoria de Proteção de Dados Pessoais (CPD) da Controladoria Geral do Município (CGM), além da sociedade civil por meio de entrevista com representante da área acadêmica.

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

CIDADE DE SÃO PAULO
CASA CIVIL

Introdução

Questões como privacidade e proteção de dados pessoais fazem parte, atualmente, de vários debates envolvendo a sociedade civil e o Estado, mas a preocupação com dados pessoais já era motivo de atenção nos anos 1960. Desde então, o desenvolvimento tecnológico crescente, somado à globalização, tem facilitado e permitido uma enorme acumulação de informações sobre cada um de nós. Em paralelo ao avanço tecnológico, cresceram também os questionamentos sobre privacidade e proteção de dados pessoais, armazenamento, circulação e uso das informações coletadas.

No Brasil, a regulação desse cenário veio com a promulgação da **Lei Geral de Proteção de Dados Pessoais (LGPD)**, a Lei Federal nº 13.709/2018, regulamentada na cidade de São Paulo a partir do Decreto Municipal nº 59.767/2020. Como o próprio nome já diz, a lei pretende normatizar a proteção de dados pessoais do cidadão, além de resguardar seus direitos fundamentais de liberdade, privacidade e não discriminação.

A rigor, a LGPD visa criar um procedimento padrão para o tratamento das informações, que pode ser compreendido no ciclo de tratamento dos dados pessoais, a saber: coleta, manipulação, compartilhamento, armazenamento, e eliminação de dados pessoais. A referida lei também pretende avaliar quando se aplica ou não a legislação e quais são as sanções específicas, além de definir quem são os agentes que participam do processo de tratamento de dados e os princípios a serem seguidos durante o ciclo de tratamento dos dados pessoais.

COLETA

MANIPULAÇÃO

COMPARTILHAMENTO

ARMAZENAMENTO

ELIMINAÇÃO

Importante mencionar que o novo ordenamento previsto na LGPD também se estende aos órgãos e entidades da administração direta e indireta, nos âmbitos municipal, estadual e federal, e nos poderes Executivo, Legislativo e Judiciário. A administração pública deve se adequar à nova prática e reformular os procedimentos de coleta, uso e compartilhamento de informações dos cidadãos para a realização de políticas públicas.

O órgão responsável por zelar, regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil é a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, e foi criada pela Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853, de 14 de agosto de 2019.

A ANPD foi criada como um órgão da administração pública federal direta. Entretanto, já se previa que sua natureza jurídica seria transitória e que poderia ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial, o que ocorreu em 2022, por meio da Medida Provisória nº 1.134, convertida na Lei nº 14.460, de 25 de outubro de 2022. A partir dessa transformação, a ANPD passou a possuir algumas características institucionais que lhe conferem maior independência, tais como a autonomia técnica e decisória e o mandato fixo dos Diretores.

Proteção de dados pessoais: Conceitos e antecedentes da LGPD

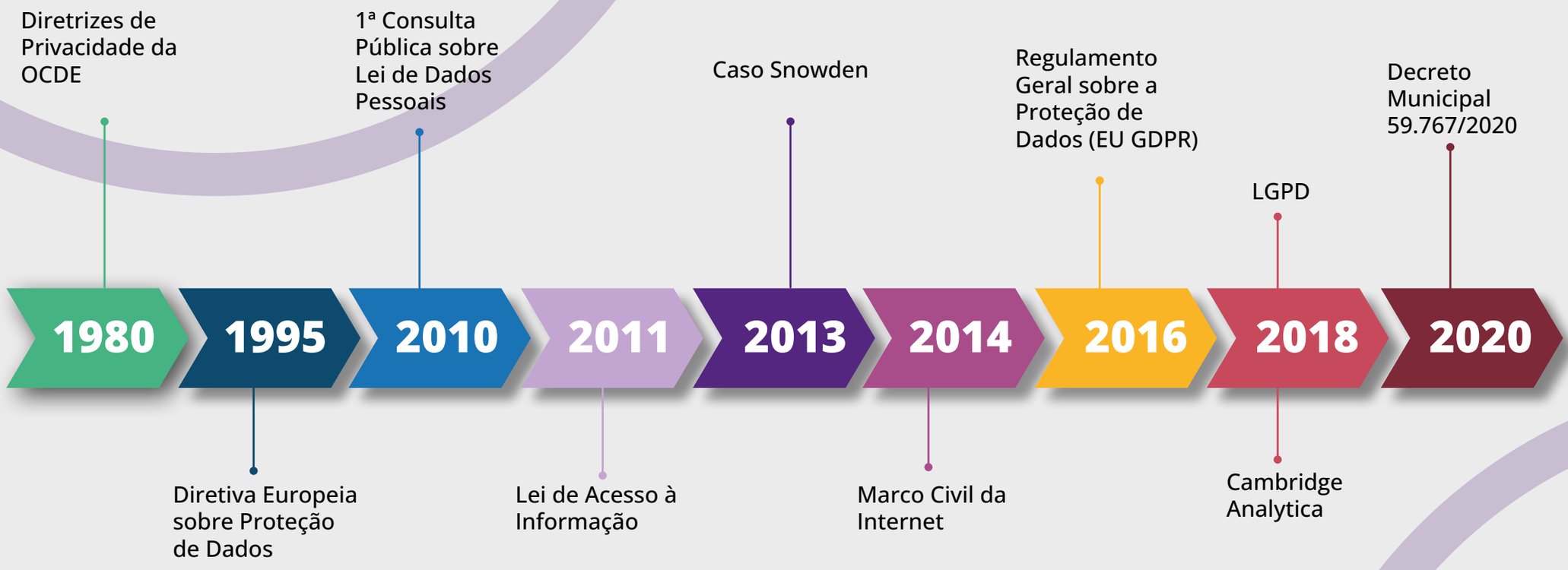
Segundo a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais –LGPD), dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável" (Art. 5º, I). A partir desta definição podemos conceituar a proteção de dados pessoais como o conjunto de medidas e práticas destinadas a salvaguardar a privacidade e a integridade das informações relacionadas a indivíduos.

No Brasil, o tema da proteção de dados pessoais começou a se estruturar a partir da década de 1990. Um marco importante desse processo foi a Lei Federal nº 9.507, de 12 de novembro de 1997 (Lei do *Habeas Data*), que regulamentou aspectos do direito de acesso a informações tratadas pelo Poder Público e disciplinou o rito do *Habeas Data*.

A matéria sobre a proteção de dados ganha mais robustez depois de 2010, a partir da edição de uma série de normas destinadas à proteção de dados pessoais:

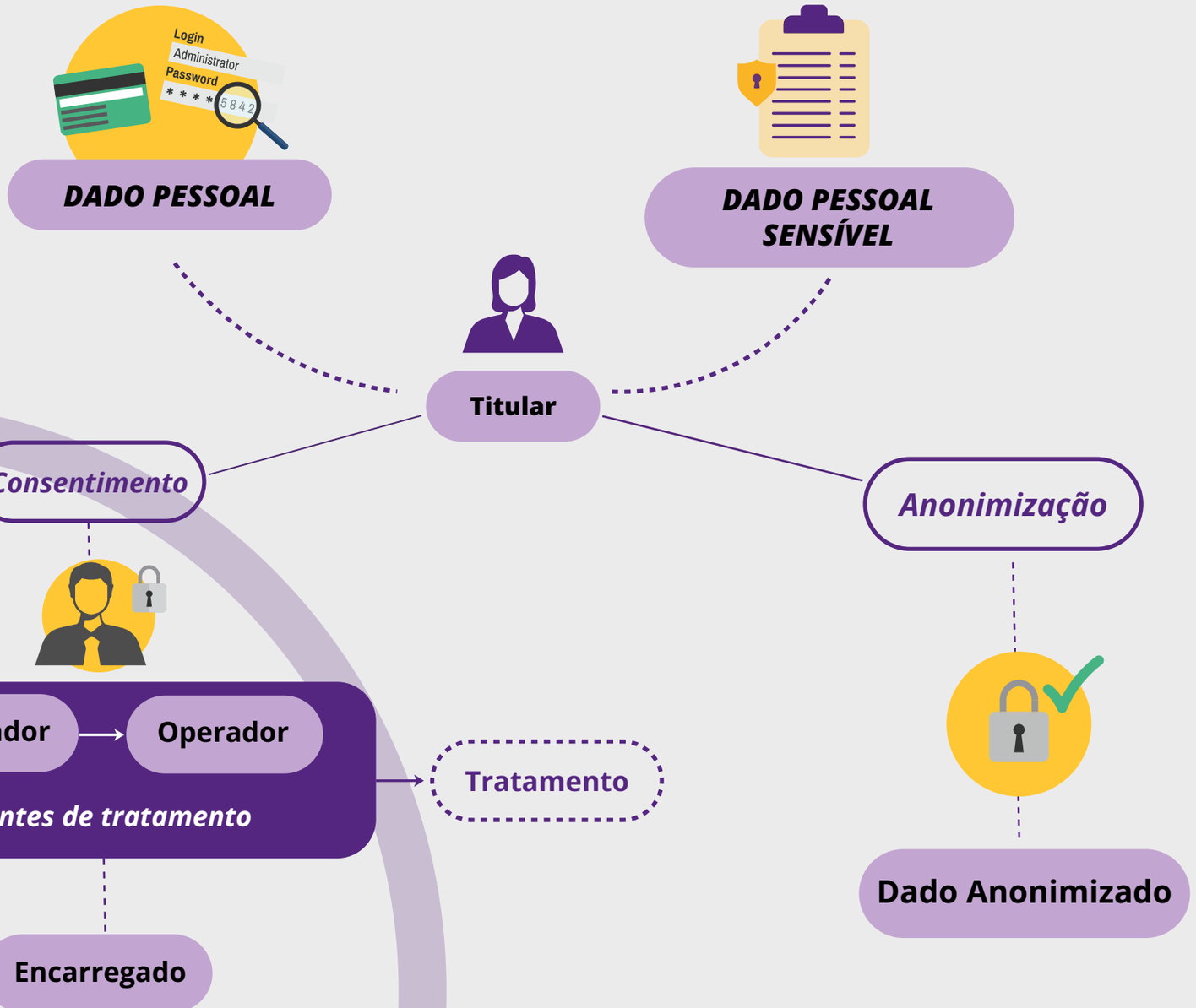
- Lei Federal n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI);
- Lei Federal n° 12.737, de 30 de novembro de 2012 (também conhecida como "Lei Carolina Dieckmann");
- Lei Federal n° 12.962, de 23 de abril de 2014 (Marco Civil da Internet - MCI);
- Lei Federal n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Decreto Municipal 59.767, de 15 de setembro 2020 (regulamentação da LGPD na cidade de São Paulo);
- Emenda Constitucional nº 115, de 10 de fevereiro de 2022 (EC nº 115/2022).

Confira a seguir uma linha do tempo com os principais marcos antecedentes à LGPD:



Glossário: Termos importantes

Dentro da LGPD, há a menção a vários termos específicos da área de proteção de dados que podem ser desconhecidos da maior parte da população. Confira na seguinte esquematização quais são os termos específicos mais recorrentes e suas respectivas definições conforme Art. 5º da Lei Geral de Proteção de Dados Pessoais:



Dado Pessoal: informação relacionada à pessoa natural identificada ou identificável, ou seja, são dados que permitem identificar de forma direta ou indireta a pessoa à qual os dados se referem. Por exemplo: CPF, RG, foto, endereço de e-mail, endereço de IP do computador, endereço residencial e/ou do local de trabalho etc.

Dado Pessoal Sensível: é uma categoria específica de dado pessoal que o relaciona aos contextos de 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.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Dado Anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

.

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.

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

Agentes de tratamento: o controlador e o operador.

Tratamento: 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.

Encarregado: 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 (ANPD).

Qual é a legislação aplicável

No âmbito nacional, a principal legislação definidora da política nacional de proteção de dados pessoais é a Lei nº 13.709/2018, a **Lei Geral de Proteção de Dados Pessoais (LGPD)**. A referida lei estabeleceu várias diretrizes básicas em relação à proteção de dados pessoais nos meios físicos e digitais, devendo ser observadas tanto por pessoas naturais quanto por pessoas jurídicas de direito público ou privado, e aplicadas a nível federal, estadual e municipal.

A LGPD foi disciplinada na administração pública da cidade de São Paulo a partir do Decreto Municipal nº 59.767/2020, sendo aplicável aos órgãos da Administração Direta e às entidades da Administração Indireta. Demais disposições sobre o tratamento de dados pessoais no âmbito da administração pública municipal estão presentes na Instrução Normativa CGM/SP nº 01/2022.

Como a LGPD é promovida na Prefeitura de São Paulo

Com a promulgação da LGPD pelo governo federal, em agosto de 2018, a Prefeitura de São Paulo começou um trabalho de implementação da lei no âmbito do Executivo municipal. Dois anos depois, em 15 de setembro de 2020, publicou o Decreto Municipal nº 59.767, que dispõe sobre a proteção de dados pessoais no campo de ação do poder municipal e alcance dos órgãos da administração pública direta e indireta.

De acordo com o decreto municipal, cabe à Controladoria Geral do Município (CGM) de São Paulo disciplinar a proteção de dados pessoais na esfera pública municipal. O Controlador Geral do Município é a pessoa que assume a atribuição de Encarregado pelo Tratamento de Dados Pessoais na Prefeitura de São Paulo, a quem compete editar diretrizes e orientações para a implementação da proteção

de dados pessoais no âmbito do Executivo municipal.

Outra atribuição do Controlador Geral do Município no papel de Encarregado é o de atuar como um canal de comunicação entre os órgãos da Prefeitura de São Paulo – que são os controladores de dados -, os titulares dos dados pessoais - que são o munícipes, residentes ou não na cidade de São Paulo -, e a Autoridade Nacional de Proteção de Dados (ANPD). Em outubro de 2023, com o Decreto Municipal nº 62.809/2023, a Prefeitura reorganizou a CGM. Entre as mudanças implementadas, criou a Coordenadoria de Proteção de Dados Pessoais (CPD), com o objetivo de subsidiar o Controlador Geral na atribuição de Encarregado pelo Tratamento de Dados Pessoais da Prefeitura de São Paulo.

A nova coordenadoria conta ainda com duas divisões: a de Conformidade em Proteção de Dados Pessoais e a de Normatização em Proteção de Dados Pessoais, responsáveis pela elaboração de estudos de conformidade dos órgãos com o tema e de propostas de atos normativos. Além disso, a CPD tem a atribuição de coordenar a política de governança em privacidade e em proteção de dados dos órgãos da Prefeitura, e de orientar agentes públicos e pessoas jurídicas sobre as práticas adequadas sobre o tema.

A Prefeitura Municipal de São Paulo segue subordinada à fiscalização da ANPD, a agência reguladora que atua nas esferas federal, estadual e municipal e nos poderes Executivo, Legislativo e Judiciário.

A proteção de dados pessoais na Prefeitura de São Paulo

A proteção de dados pessoais na Prefeitura de São Paulo está amparada no Decreto Municipal nº 59.767/2020, que regulamenta a aplicação da LGPD no âmbito da Administração Municipal Direta e Indireta. De acordo com o Decreto, fica designado o Controlador Geral do Município como o encarregado pelo tratamento de dados pessoais (Art. 5º, *caput*), além de caber aos Chefes de Gabinete das Secretarias e Subprefeituras o cumprimento, no âmbito dos respectivos órgãos, às ordens e recomendações do Controlador Geral do Município na qualidade de Encarregado pelo Tratamento de Dados Pessoais (Art. 7º, I).

CGM e a governança em privacidade e proteção de dados pessoais de São Paulo

No âmbito da LGPD, o Encarregado tem entre suas atribuições orientar os órgãos da Administração Pública Direta, como as secretarias municipais e as subprefeituras, e, em caráter subsidiário, as entidades da Administração Pública Indireta, como as autarquias, fundações, empresas públicas e sociedades de economia mista. Estas possuem seus próprios Encarregados, ou seja, há uma independência, uma autonomia na atuação das entidades da Administração Indireta em relação aos procedimentos e orientações do Encarregado e Controlador da CGM. No entanto, todos seguem as atribuições previstas na LGPD.

Também há uma certa autonomia com relação à Administração Direta. Para os efeitos da LGPD, cada secretaria e cada subprefeitura é considerada uma controladora de dados. Em relação às entidades da Administração Indireta, essas podem ser consideradas tanto controladoras de dados, no caso de estarem atuando em regime de concorrência, quanto ser consideradas operadoras de dados, isto no caso de estarem operacionalizando políticas públicas e no âmbito de execução delas. Nesse sentido, os controladores tomam as decisões sobre o tratamento de dados pessoais e os operadores atuam em nome dos controladores em relação ao tratamento de dados pessoais.

A autonomia mencionada acima, entretanto, segue obrigações legais e implica em uma série de responsabilidades, como, por exemplo, os direitos do titular dos dados. Previstos em vários artigos da LGPD, os direitos estão relacionados, por exemplo, à transparência no tratamento de dados pessoais, à confirmação sobre a existência de tratamento de dados pes-

soais, ao acesso aos dados pessoais tratados, à portabilidade e à revisão de decisões tomadas de forma automatizada (o que pode ser realizado com o uso de Inteligência Artificial).

Para auxiliar na efetiva aplicação da legislação, a CGM publicou, em janeiro de 2023, dois **guias orientativos** para a administração municipal sobre a privacidade e a proteção de dados pessoais, disponíveis no site da Coordenadoria de Proteção de Dados Pessoais (CPD). Um dos fatores que provocou a criação dos guias foi a necessidade de conscientizar a totalidade dos servidores sobre a importância da proteção de dados pessoais, informações que são a matéria-prima de trabalho dos agentes públicos. O foco é a sensibilização do servidor sobre a necessidade de adequar a sua rotina à proteção de dados pessoais.

Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo

Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo

Enquanto o primeiro guia (Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo) trata da sensibilização do servidor para importância da proteção de dados pessoais, o segundo (Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo) aborda como cada órgão - secretarias e subprefeituras -, pode desenvolver e implementar o seu próprio plano de adequação à LGPD. O plano de adequação compreende atividades como mapeamento de processos e de dados pessoais, e um plano de gestão de risco em segurança da informação, privacidade e proteção de dados. É entendido como um programa de governança, que se realiza de forma cíclica e contínua.

A partir do passo a passo orientado pelos guias da CGM, cada órgão elabora um relatório - Relatório de Impacto à Proteção de Dados Pessoais (RIPD) -, no qual estão mapeados dados pessoais, processos e plano de gestão de riscos. Este plano de adequação é uma etapa prévia que permite identificar, analisar e tratar os riscos relacionados à proteção de dados. Conhecer as vulnerabilidades de cada secretaria ou subprefeitura possibilita entender e atuar no ciclo de tratamento de dados pessoais de cada processo que existe nos órgãos.

Na avaliação da CGM, o plano de adequação, que é um programa de governan-

ça, é como um ciclo de conformidade: a partir das orientações do guia, o órgão busca a adequação, informa a CGM via relatório, e esta analisa a conformidade e envia novas diretrizes, numa atualização contínua. Desde 2020, a periodicidade do relatório é anual e obrigatória, pois se trata de um documento que pode ser solicitado pela ANPD.

A CGM entende que os atuais desafios que fundamentam as ações hoje realizadas são a conscientização sobre o tema e a especialidade de agentes públicos, no âmbito dos órgãos e das entidades, que possam realizar uma tarefa que não é de curta duração e sim uma tarefa contínua.

Em resumo, todo o procedimento tem a duração de quase um ano, uma trilha que vai ter variações dependendo do tamanho de cada órgão, mas que tem passos básicos. O primeiro passo é nomear a equipe designada para o plano de adequação. O segundo passo é realizar o mapeamento de processos; o terceiro passo é o mapeamento de dados pessoais com base no mapeamento de processos; o quarto passo é o plano de gestão de riscos em segurança da informação, privacidade e proteção de dados pessoais.

Ao final, se espera que o órgão tenha o controle sobre como tratar os riscos identificados, analisados e avaliados. E, após a etapa de controle, se passa ao quinto passo, que é a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. Esse relatório nada mais é do que a consolidação do trabalho realizado nas quatro etapas anteriores da trilha. O relatório deve demonstrar e documentar a situação do órgão ou da entidade perante a LGPD e, para alcançá-lo, a CGM trabalha em duas frentes: conscientização e capacitação dos agentes públicos.

Como promover a governança em privacidade e proteção de dados pessoais

Basicamente, a LGPD se refere à proteção e tratamento de dados pessoais, sendo uma lei que se aplica às organizações públicas e/ou privadas que coletam, armazenam, processam ou compartilham dados pessoais no Brasil. No caso do Poder Público, é possível adotar a privacidade e a proteção de dados como base para a criação de todas as iniciativas de políticas públicas - seja ação, projeto e/ou programa desenvolvidos. E entre as boas práticas que podem ser incorporadas estão:

- Ser proativo, não reativo;
- Ser preventivo, não corretivo;
- Ter a privacidade como padrão, ou seja, *privacy by default;*
- Ter a privacidade incorporada ao design;
- Prover segurança de ponta a ponta e proteção durante todo o ciclo de vida dos dados; e
- Limitar o tratamento ao mínimo necessário para a realização de suas finalidades.

Assim, a LGPD visa proteger ao máximo todos os envolvidos no tratamento de dados. Tal legislação busca avançar no sentido protetivo dos atores envolvidos, estabelecendo princípios e definindo os direitos do titular dos dados pessoais, além de estabelecer sanções administrativas nos âmbitos privado e público (sendo que no último há diferenças na aplicação de algumas sanções).

Ficou interessado em conhecer mais sobre o processo de criação da LGPD no Brasil, sua aplicação na administração pública e demais boas práticas relacionadas à proteção de dados pessoais? Então confira a entrevista realizada pela CGA com o pesquisador e acadêmico Rafael Mafei Rabelo Queiroz, disponível no Anexo deste guia.

Princípios da proteção de dados pessoais

Você sabia que, além da boa-fé, o tratamento de dados pessoais deve obedecer a uma série de princípios elencados pela LGPD? Alguns desses princípios guardam profunda semelhança com os pilares da agenda de Governo Aberto, como a transparência e o accountability (responsabilização e prestação de contas), permitindo assim um maior controle do munícipe sobre os seus dados pessoais por meio da **autodeterminação informativa**. Confira, a seguir, os princípios a serem observados pelos agentes de tratamento de dados, conforme o Art. 6º da LGPD:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e

não excessivos em relação às finalidades do tratamento de dados;

- **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos Dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **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, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

.

Hipóteses legais que autorizam o tratamento

A LGPD também definiu os requisitos, ou a base legal, para o tratamento dos dados pessoais. Quer dizer, além da boa-fé e dos princípios gerais (presentes no Art. 6º da LGPD), o tratamento de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e adolescentes **só poderá ocorrer** se estiver previsto nas hipóteses listadas no **Art. 7º (sobre dados pessoais) e Art. 11 (sobre dados pessoais sensíveis)**. Além disso, demais regras estão dispostas no **Art. 14 da LGPD quando é realizado o tratamento de dados pessoais de crianças e adolescentes**. Confira a seguir as principais hipóteses autorizadoras do tratamento de dados pessoais e de dados pessoais sensíveis:

Dado Pessoal (Art. 7º, LGPD)	**Dado Pessoal Sensível (Art. 11, LGPD)**
Mediante o fornecimento de consentimento pelo titular	Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
Sem consentimento explícito: Para o cumprimento de obrigação legal ou regulatória pelo controlador; Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; Para a proteção da vida ou da incolumidade física do titular ou de terceiro; Entre outras hipóteses.	Sem consentimento explícito: Cumprimento de obrigação legal ou regulatória pelo controlador; Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis Proteção da vida ou da incolumidade física do titular ou de terceiro; Entre outras hipóteses.

Direitos do titular

Além do enquadramento em uma das hipóteses legais listadas anteriormente, é essencial garantir que os direitos dos titulares sejam considerados ao tratar dados pessoais e dados pessoais sensíveis. Veja, a seguir, quais são alguns desses direitos:

Art. 9º - O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de **forma clara, adequada e ostensiva** acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - **finalidade** específica do tratamento;

II - **forma e duração do tratamento**, observados os segredos comercial e industrial;

III - **identificação** do controlador;

IV - **informações de contato** do controlador;

V - **informações acerca do uso compartilhado** de dados pelo controlador e a **finalidade**;

VI - **responsabilidades** dos agentes que realizarão o tratamento; e

VII - **direitos do titular**, com menção explícita aos direitos contidos no art. 18 desta Lei.

Art. 18º - O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - **confirmação da existência** de tratamento;

II - **acesso aos dados**;

III - **correção de dados** incompletos, inexatos ou desatualizados;

IV - **anonimização, bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - **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;

VI - **eliminação dos dados pessoais tratados com o consentimento do titular,** exceto nas hipóteses previstas no art. 16 desta Lei;

VII - **informação das entidades públicas e privadas** com as quais o controlador realizou **uso compartilhado de dados**;

VIII - **informação sobre a possibilidade** de não fornecer consentimento e sobre as consequências da negativa;

IX - **revogação do consentimento**, nos termos do § 5º do art. 8º desta Lei.

Sanções administrativas

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável pela aplicação de sanções administrativas em caso de descumprimento da LGPD, seja por organização privada ou pública. Instituição do setor público, entretanto, não está sujeita ao pagamento de multa (incisos II e III do Art. 52 da LGPD). As sanções previstas na LGPD são:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples (até 2% do faturamento até o limite de R$ 50 milhões);
- Multa diária;
- Publicização da infração;
- Bloqueio dos dados pessoais envolvidos;
- Eliminação dos dados pessoais envolvidos;
- Suspensão parcial, por até seis meses, do banco de dados envolvido;
- Suspensão do exercício da atividade de tratamento dos dados pessoais pelo período de seis meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

.

Fatores de sucesso

Com a entrada em vigor da LGPD, criou-se a necessidade de estabelecer e seguir parâmetros mínimos de governança digital de dados pessoais para a plena proteção dos munícipes de nossa cidade e êxito na execução da lei. Muitos destes parâmetros mínimos são atendidos por meio da conscientização tanto dos servidores e demais agentes públicos municipais quanto dos cidadãos, aumentando o conhecimento das boas práticas relacionadas ao tratamento de dados pessoais e dos deveres da administração pública e os direitos da sociedade civil.

Como mencionado, uma das frentes de trabalho da CGM é a conscientização de todos os servidores sobre a lei. Atualmente, a Controladoria realiza uma campanha ativa por meio do envio de um e-mail, semanal (às quintas-feiras), com informações sobre temas relacionados à LGPD. No total, são 50 publicações, que foram consolidadas posteriormente no guia "Robô e a Turma da LGPD no Controle dos Seus Dados Pessoais". As 50 postagens formam um guia prático destinado a ajudar os servidores a entender o que é a LGPD e os principais pontos sobre os quais todo servidor municipal deve ter conhecimento.

Ainda no campo da conscientização, além da campanha ativa de envio sema-

nal de *e-mails*, a CGM tem elaborado cursos sobre proteção de dados pessoais que se relacionam aos contextos de atuação dos servidores. Já foram realizados dois cursos: *LGPD no contexto da Lei de Acesso à Informação (LAI)*, destinado aos servidores que atuam com e-SIC (Sistema Eletrônico de Informação ao Cidadão); e *LGPD no contexto do Sistema Municipal de Bibliotecas (SMB)*, para os servidores que atuam na gestão documental das bibliotecas. Um terceiro curso, em elaboração, será destinado aos servidores municipais que trabalham na área da saúde.

Outra frente da CGM é o programa de capacitação de agentes públicos. A capacitação é destinada aos servidores que vão promover a governança em privacidade e proteção de dados pessoais nos seus respectivos órgãos ou entidades. A tarefa inclui desde a escolha da equipe para realizar o mapeamento de processos até a realização do Relatório de Impacto à Proteção de Dados Pessoais. É um programa de capacitação específico, baseado na Instrução Normativa CGM nº 01, de 2022, e no Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo.

Entretanto, é importante ressaltar que a governança em privacidade e em proteção de dados pessoais também precisa de amparo legal e institucional para ser plenamente efetivada. Na esfera legal, tanto o Decreto Municipal nº 59.767/2020 quanto a Instrução Normativa CGM/SP nº 01/2022 representaram passos importantes na consolidação dos preceitos da LGPD à nível local. Já na esfera institucional, a criação e condução de um amplo programa de governança se faz por meio da figura da CGM, que organiza diversas ações voltadas para os servidores da Prefeitura de São Paulo - como é o caso dos dois guias orientativos para a proteção de dados pessoais e a análise de conformidade dos órgãos com relação aos seus respectivos programas de governança.

Desafios

Atualmente, todos os usuários dos serviços públicos oferecidos direta ou indiretamente pelo Município de São Paulo podem ter seus dados pessoais tratados durante a utilização desses serviços. Esse cenário, naturalmente, apresenta diversos desafios, sendo que fatores de sucesso, como os programas de conscientização e capacitação implementados pela CGM, têm o potencial de destacar e lidar com as dificuldades inerentes às atividades administrativas do dia a dia em relação à proteção de dados pessoais.

A superação de obstáculos requer uma mudança da cultura organizacional, ou seja, ter como prática cotidiana a atenção sobre a importância da proteção de dados pessoais e a privacidade. Isso aponta para a necessidade de rever processos operacionais internos, para que fiquem em conformidade com as demandas da LGPD. Outro desafio decorrente da legislação é adotar o monitoramento dos processos como medida de rotina.

E, em função do volume de atendimento diário pela máquina administrativa municipal, fazer o mapeamento de dados pessoais tratados é outro desafio, pois inclui identificação da origem, fluxo, armazenamento e finalidade dos dados de cidadãos, funcionários e outras partes relacionadas. Por fim, mas não menos importante, a consolidação da governança em privacidade e em proteção de dados pessoais no setor público requer o comprometimento da alta administração. O apoio e o envolvimento das chefias são elementos essenciais para a implementação e efetiva prática da LGPD e seus respectivos instrumentos regulamentadores, num ciclo contínuo de revisão e atualização.

Conclusão

A proteção de dados pessoais é um mecanismo essencial para garantir os direitos relativos à privacidade e à autodeterminação informativa dos munícipes, possuindo vários instrumentos regulamentadores que criam uma verdadeira base legal e institucional à nível nacional e local. Entretanto, mesmo com esse aparato legislativo e institucional, o engajamento de servidores se faz crucial para a plena manutenção da governança em privacidade e proteção de dados pessoais em nossa cidade.

Nesse aspecto, programas de conscientização e capacitação fornecidos pela CGM são de grande importância para a promoção da cultura de proteção de dados pessoais na administração pública municipal, além de uma perspectiva abrangente, que envolva todas as partes interessadas no contínuo aprimoramento da execução da LGPD.

Se ainda tem dúvidas em relação à proteção de dados pessoais no âmbito do município de São Paulo, entre em contato com a equipe da Coordenadoria de Proteção de Dados Pessoais (CPD) através do email privacidade@prefeitura.sp.gov.br ou com a equipe de Governo Aberto pelo e-mail governoaberto@prefeitura.sp.gov.br.

Para saber mais

- **Entrevista com Rafael Mafei Rabelo Queiroz**, disponível no Anexo deste guia
- **Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo**, disponível no site da Prefeitura
- **Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo**, disponível no site da Prefeitura
- **Revista Robô e a Turma da LGPD no Controle dos Seus Dados Pessoais**, disponível no site da Prefeitura
- Guia Orientativa sobre o Tratamento de Dados Pessoais pelo Poder Público (versão 2.0), disponível no site do Governo Federal
- **Como se adequar à LGPD?**, artigo disponível no site do SERPRO

Anexo

Entrevista com Rafael Mafei Rabelo Queiroz

Confira a seguir os principais tópicos abordados em entrevista realizada pela equipe da Coordenadoria de Governo Aberto (CGA) com o acadêmico Rafael Mafei Rabelo Queiroz, pesquisador na área de "Privacidade e Proteção de Dados Pessoais".

CGA: Na sua visão, qual foi o principal impulsionador para a elaboração e sanção da LGPD aqui no Brasil?

RAFAEL: A Lei Geral de Proteção de Dados (LGPD) não é um fenômeno exclusivamente brasileiro, pois leis similares existem globalmente. Isso decorre do desenvolvimento tecnológico, principalmente ligado à computação, que permitiu a acumulação, acesso e tratamento massivo de dados pessoais desde os anos 60. A preocupação inicial surgiu devido a experiências de governos totalitários que praticavam vigilância e espionagem, ameaçando os direitos dos cidadãos.

A globalização econômica intensificou o acúmulo de dados por empresas atuando internacionalmente, levando a situações de risco, como a transferência de operações para países com padrões mais baixos de proteção de dados. A década de 70 marcou um período de transformações tecnológicas e econômicas, despertando a atenção de governos, sociedade civil e acadêmicos para os riscos associados ao amplo acúmulo de dados.

Países como a Alemanha adotaram precocemente medidas de proteção de dados, enquanto a Comunidade Econômica Europeia (atual União Europeia) pressionou pela harmonização das legislações. No contexto brasileiro, dois fatores foram determinantes para a LGPD: a influência da legislação europeia, que protege os titulares de dados europeus, e o escândalo de Edward Snowden, que revelou uma espionagem sistemática dos Estados Uni-

dos, gerando uma percepção ampliada da importância da proteção de dados.

Eventos como o escândalo da Cambridge Analytica e casos de avaliações injustas por inteligência artificial reforçaram a importância de uma legislação protetiva. À medida que o uso massivo e opaco de dados impacta diversos aspectos da vida, a necessidade de controle e compreensão sobre a origem e uso dos dados torna-se fundamental, justificando a emergência da LGPD no contexto brasileiro.

CGA: Ao longo dos 5 anos de existência da LGPD você enxerga alguma necessidade de revisão ou aperfeiçoamento desta lei?

RAFAEL: A LGPD é uma legislação principiológica que serve como base para o direito de proteção de dados. No entanto, sua abordagem geral demanda leis mais específicas para compor o ecossistema normativo. Atualmente, no Senado, tramita uma legislação específica para regular o uso de inteligência artificial, destacando-se como um complemento necessário à LGPD. Assuntos como segurança pública e defesa nacional, embora não excluídos, carecem de regulamentação mais detalhada.

O uso significativo da tecnologia em atividades como policiamento e investigação criminal exige legislação clara. Complementos à LGPD surgirão naturalmente, moldados pela prática, jurisprudência e a atuação da Autoridade Nacional de Proteção de Dados (ANPD). Algumas áreas, explicitamente descobertas pela LGPD, como segurança pública e inteligência artificial, necessitam de legislação adicional. Já há tramitação no Congresso para regulamentar esses temas, envolvendo comissões de juristas e avanços legislativos.

A complexidade desses assuntos requer um processo legislativo cuidadoso, envolvendo debates entre empresas, organizações da sociedade civil e órgãos governamentais, como Ministério Público e órgãos de investigação. Embora esse processo demande tempo para maturação, discussões detalhadas são essenciais para criar legislações específicas e eficazes, mostrando a importância de um de-

senvolvimento gradual e bem fundamentado.

CGA: No âmbito da administração pública quais são os desafios do gestor público na aplicação da LGPD

RAFAEL: A LGPD redefine as práticas em relação aos titulares de dados no setor público e privado. Historicamente, a administração pública buscava coletar o máximo de dados possível, adotando uma postura oposta à LGPD, que prioriza a coleta mínima necessária. A nova abordagem exige que órgãos públicos justifiquem o motivo da coleta, indiquem um fundamento legal e detalhem como os dados serão utilizados e protegidos.

A mudança de paradigma na administração pública envolve uma reavaliação de procedimentos, incluindo o estoque de dados acumulados ao longo do tempo. A LGPD demanda uma revisão criteriosa, questionando a necessidade de informações antigas. Além disso, os procedimentos tradicionais, como a solicitação de dados pessoais, devem ser reestruturados para atender aos novos princípios.

O compartilhamento de dados entre órgãos públicos também enfrenta desafios, exigindo uma formalização rigorosa para garantir segurança e conformidade com a lei. A transparência, um dever do setor público, é reavaliada à luz da privacidade do titular dos dados. O exemplo da divulgação da remuneração de servidores destaca a necessidade de equilíbrio entre transparência e proteção da privacidade, desafiando a administração pública a determinar quais informações são relevantes para a transparência e como proteger dados sensíveis.

A LGPD impõe uma transformação profunda na cultura de coleta e tratamento de dados, abordando desde o primeiro contato com o cidadão até o compartilhamento entre entidades públicas. Países europeus, com experiência na implementação de legislações semelhantes, fornecem insights valiosos sobre como conciliar transparência e privacidade. O desafio consiste em garantir a conformidade legal, promover a transparência e proteger a privacidade dos titulares de dados, exi-

gindo uma revisão abrangente de práticas estabelecidas.

CGA: Quais são os principais casos em que não há necessidade de aplicação da LGPD?

RAFAEL: A aplicação da LGPD pela administração pública é a regra, excetuando-se, de acordo com a lei, os tratamentos realizados por pessoas naturais (para fins exclusivamente particulares e não econômicos), ou tratamentos de dados com finalidades exclusivamente jornalísticas, artísticas, acadêmicas, de segurança pública, de defesa nacional, e de investigação penal. Tratamento envolvendo dados de pessoas jurídicas e dados anonimizados também estão isentos da aplicação da LGPD. Contudo, mesmo em investigações, o direito à proteção de dados permanece, e a Autoridade Nacional de Proteção de Dados atua em casos de violação. Registros detalhados de acesso, alteração e compartilhamento de dados são cruciais, garantindo conformidade com a lei, que busca coibir excessos, limitar tratamentos desnecessários e proteger contra incidentes de segurança.

CGA: Por que é tão importante essa questão de limitar o tempo em que a informação fica com o poder público ou com o poder privado?

RAFAEL: A LGPD exige que os dados sejam mantidos apenas enquanto necessário para a finalidade original da coleta. Se uma lei determina retenção por 20 anos, após esse prazo, o dado deve ser anonimizado, removendo a identificação pessoal. O não cumprimento configura violação. O rigor da LGPD visa limitar o tratamento de dados após o término de sua relevância, mitigando riscos, especialmente em incidentes de vazamento. O princípio é evitar acumulação desnecessária de informações, respeitando a finalidade específica da coleta de dados.

CGA: Sobre o aparente dilema entre a transparência de dados e a proteção de dados, você enxerga muitos pontos de atrito entre a LGPD e a LAI (Lei de Acesso à Informação)? Você enxerga alguma complementaridade entre as duas legislações?

RAFAEL: A LGPD não deve ser utilizada como desculpa para negligenciar deveres de transparência, mas o cumprimento desses deveres deve respeitar a privacidade e, principalmente, a intimidade das pessoas. A distinção entre privacidade e intimidade é crucial; enquanto a privacidade se refere a dados pessoais, a intimidade é algo que afeta apenas a pessoa em questão. Em situações complexas de conflito de direitos, a resolução prática se dará por meio de debates específicos em casos concretos. Por exemplo, a divulgação da agenda pública de autoridades não é considerada uma violação à intimidade, pois há um interesse público em conhecer as atividades de figuras públicas durante o expediente. Casos difíceis serão refinados por meio do debate circunstancial. Em situações excepcionais, informações sensíveis sobre a saúde de uma autoridade podem ser consideradas de interesse público, como no caso de presidentes em cirurgia ou tratamento médico. Exemplos como estes demonstram que, mesmo em assuntos pessoais e delicados, a exposição da condição de autoridades públicas pode não ser uma violação de privacidade, quando há um interesse público relevante, como a saúde de uma figura pública que impacta diretamente a governança.

Sobre o Entrevistado:

Rafael Mafei Rabelo Queiroz é bacharel, mestre, doutor e livre-docente em direito, sendo professor associado da Faculdade de Direito da Universidade de São Paulo (Departamento de Filosofia e Teoria Geral do Direito) e advogado. Atualmente atua em linhas de pesquisa envolvendo o direito à livre expressão no contexto brasileiro e a privacidade e proteção de dados pessoais. Também é colunista na revista Piauí e produtor do canal e podcast Direito e Sociedade.

Ficha Técnica

PREFEITO
Ricardo Nunes

SECRETÁRIO CHEFE DA CASA CIVIL
Fabricio Cobra Arbex

CHEFE DE GABINETE DA CASA CIVIL
Denise Soares Ramos

SECRETÁRIO EXECUTIVO DE RELAÇÕES INSTITUCIONAIS
Enrico Misasi

COORDENADORIA DE GOVERNO ABERTO
Coordenadora
Patrícia Marques dos Santos
Equipe Técnica
Bianca Talarico Botta
Bruno Venâncio de Abreu Costa
Daniela Matos Nascimento
Derek Ferreira Melo
Maria Luiza Vilella

Estagiários
Airam Magalhães Muniz
Amanda Raynara Quintana Theodoro
Beatriz Vogel Bordignon
Bruno Gomes Ponciano
Giovanna Ribeiro Castelo Branco
Isabela Nascimento de Massena

Residentes
Josefina Maria Pasquato
Luan Santos de Araujo
Matheus Henrique Furtado
Pedro Henrique Junqueira Martins

Parceria 5ª edição:

CONTROLADOR GERAL DO MUNICÍPIO DE SÃO PAULO
Daniel Falcão

COORDENADOR DE PROTEÇÃO DE DADOS PESSOAIS
Kelvin Peroli dos Reis

Entrevistado 5ª edição:
Rafael Mafei Rabelo Queiroz