Diretrizes Técnicas para o Programa de Proteção de Dados Pessoais da Prefeitura do Município de São Paulo

Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (SMIT/CGTIC)

NOV. 21 • VERSÃO 1.0

CIDADE DE SÃO PAULO
INOVAÇÃO E TECNOLOGIA

SUMÁRIO

INTRODUÇÃO 03
1. PAPÉIS DE CONTROLE DA LGPD 04
2. APLICAÇÃO DA LGPD 06
3. CICLO DE VIDA DOS DADOS PARA ATENDER A LGDP 09
4. ATIVOS ORGANIZACIONAIS 11
5. RELACIONAMENTO DO CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS 13
6. CASOS QUE A LGPD NÃO SE APLICA 15
7. MEDIDAS DE SEGURANÇA 16
8. PRIVACIDADE DESDE A CONCEPÇÃO 17
9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO 19
10. ADEQUAÇÕES DE SISTEMAS E DADOS JÁ COLETADOS 28
REFERÊNCIAS BIBLIOGRÁFICAS 30

INTRODUÇÃO

Este documento tem como objetivo atender o estabelecido no art. 8º do Decreto Municipal 59.767/2020 que regulamenta a aplicação da Lei Federal nº 13.709/2018 promulgada em 14 de agosto de 2018, tendo por objetivo **regular as atividades de tratamento de dados pessoais**. Ela introduz a **Governança de Dados** com o objetivo de **proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural** e exige que processos e tecnologias voltados para a segurança de dados, legitimidade dados e gestão de dados sejam definidos e implantados por todos aqueles que, de alguma forma, façam processamento de dados pessoais de terceiros.

Primeiramente, será demandado um esforço dos órgãos e entidades em relação à LGPD para iniciar uma nova cultura institucional que deve alcançar os níveis estratégico, tático e operacional da Prefeitura Municipal de São Paulo. Essa evolução na maturidade envolve: utilizar a abordagem de **Privacidade desde a Concepção** (visto com mais frequência em inglês, Privacy by Design), que considera a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução; e promover treinamentos e ações de conscientização de toda a força de trabalho no sentido de enraizar o respeito à privacidade dos dados pessoais nas atividades cotidianas e novos projetos.

Estas diretrizes têm por objetivo o contato inicial e a familiarização com o novo universo da LGDP e o tratamento de dados do ponto de vista da Tecnologia da Informação, complementando as diretrizes e boas práticas publicadas pela Controladoria Geral do Município, que podem ser encontradas em seu portal corporativo, neste link. Neste momento, o foco **não é apresentar uma metodologia de implementação da LGPD** ou abranger e esgotar todos os aspectos dessa Lei, principalmente porque algumas diretrizes de proteção de dados da LGPD ainda não tiveram todas as suas definições apresentadas de forma detalhada, em regulamentos e procedimentos próprios, que aguardam edição pela Autoridade Nacional de Proteção de Dados.

1. PAPÉIS DE CONTROLE DA LGPD

A Lei Geral de Proteção ao Dados define alguns atores (**Titular dos dados e Autoridade Nacional de Proteção de Dados - ANPD**) e faz referência aos agentes de tratamento de dados, estes são denominados: ***Controlador, Operador e Encarregado de tratamentos***. O tratamento dos dados pessoais pode ser realizado pelo Controlador e o Operador. A definição de cada ator está descrita abaixo:

Titular dos dados: Pessoa natural a quem se referem os dados pessoais que são objeto do tratamento, e tem garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

ANPD: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, além de aplicar sanções por descumprimento da lei, mediante processo administrativo.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (LGPD, art. 5º, VI). No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade com competência para decidir acerca do tratamento de tais dados.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador (LGPD, art. 5º, VII), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Encarregado de tratamento de dados: 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). A figura do Encarregado e suas atribuições são especificamente disciplinadas pelo art. 41 da LGPD.

1. PAPÉIS DE CONTROLE DA LGPD

No município de São Paulo, temos também o Decreto nº 59.767 de 2020, que **regulamenta a aplicação da LGPD no âmbito da Administração Municipal**. As definições de titular, controlador, operador e encarregado também aparecem nesse Decreto, no art. 2º, incisos V, VI, VII e VIII, respectivamente. Além disso, o decreto designa, no art. 5º, o Controlador Geral do Município como o encarregado da proteção de dados pessoais para os fins do art. 41 da LGPD e também complementa as atribuições do art. 41 da LGPD, no art. 6º do Decreto.

Outro conceito importante é o de "**tratamento de dados**", que abrange qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2. APLICAÇÃO DA LGPD

Antes do tratamento de dados pessoais, é necessário se certificar que a finalidade do tratamento de dados está clara e explicitamente registrada, seus propósitos são bem definidos e comunicados ao Titular dos dados.

Conforme art. 3º da LGPD a regra aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, 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 objetos do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

2. APLICAÇÃO DA LGPD

O objetivo primário do tratamento de dados no setor público está relacionado, geralmente, à implantação e execução de políticas públicas, com previsão legal, regulamentadas ou respaldadas em contratos, convênios ou outros instrumentos. Essas políticas públicas devem ser atribuições legais do órgão ou da entidade da administração pública responsável pelo tratamento dos dados. Outra finalidade, que podemos destacar, para o tratamento de dados no serviço público são as denominadas obrigações legais ou regulatórias do controlador. O consentimento do Titular dos dados deverá ser dispensado nessas duas hipóteses específicas. Para casos onde o tratamento de dados pessoais se faça necessário e não se enquadrem nas finalidades descritas anteriormente, o consentimento, bem como as outras possibilidades definidas no art. 7º da LGPD, poderão ser aplicadas.

As informações de mapeamento devem constar no Registro das Operações de Tratamento de Dados Pessoais (ROTDP), que conforme artigo 37 da LGPD, é uma obrigação tanto para controladores quanto operadores, especialmente quando esse tratamento é baseado no legítimo interesse.

A principal função da Lei Geral de Proteção de Dados é garantir que o tratamento de dados pessoais, seja ele no contexto e com a base legal que for, **não cause riscos e danos aos direitos e às liberdades individuais do titular de dados**.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) é uma ferramenta de gestão de riscos para evitar que ocorram violações de dados pessoais, especialmente de dados pessoais cujo impacto possa interferir nos direitos e liberdades do titular.

A autoridade nacional poderá solicitar ao controlador o Relatório de Impacto à Proteção de Dados Pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. Toda vez que o tratamento de dados pessoais tiver como base legal somente o interesse legítimo do controlador, sem partir de consentimento, cumprimento de contrato, entre outras bases legais, é necessário efetuar o RIPDP.

2. APLICAÇÃO DA LGPD

A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

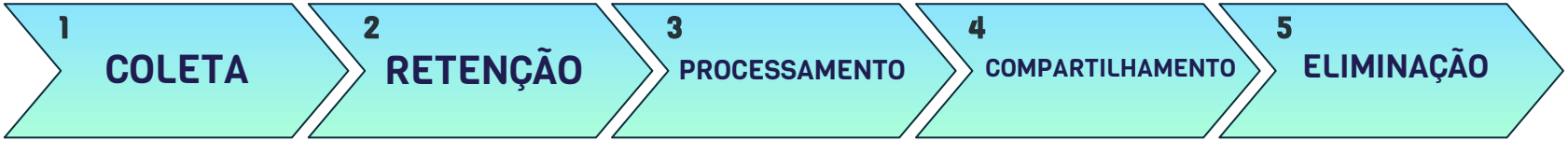
Apesar de a exigência legal pelo RIPDP só poder vir da ANPD, a sua elaboração é recomendada por cuidado e pró-atividade com a segurança de seus tratamentos de dados. Alguns motivos de relevância:

1. Avaliar o impacto do tratamento de dados
2. Obrigatório quando o tratamento for baseado no interesse legítimo ou resultar em risco elevado para os titulares
3. Mesmo sem obrigatoriedade, é uma boa prática de gestão de riscos
4. Visto com bons olhos por parceiros comerciais e pela população
5. Necessário para efetuar a transferência internacional de dados pessoais, uma vez que, devido à demora e incerteza jurídica sobre a LGPD e a ANPD, a posição do Brasil no ambiente internacional de proteção de dados ainda não é consolidada. Muitas Autoridades Nacionais de Proteção de Dados de países recipientes de dados brasileiros podem exigir um RIPDP para permitir a transferência.

3. CICLO DE VIDA DOS DADOS PARA ATENDER A LGPD

Todo dado possui um ciclo de vida. Para a implementação do tratamento de dados pessoais e medidas de segurança adequadas, o órgão precisa identificar os dados pessoais gerenciados e quais projetos, serviços, ativos e processos estão contemplados no ciclo de vida do tratamento dos dados pessoais, independente do meio utilizado (documento eletrônico, sistema de informação, planilhas etc.).

Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases[1]:



1. Fonte: Governo Federal, "Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)" <https://www.gov.br/defesa/pt-br/assuntos/hfa/acesso-a-informacao/encarregado-pelo-tratamento-de-dados-pessoais-dpo/arquivos/guialgpd-3.pdf/@@download/file/GuiaLGPD%203.pdf>

3. CICLO DE VIDA DOS DADOS PARA ATENDER A LGPD

FASE	TIPO DE OPERAÇÃO	OPERAÇÃO DE TRATAMENTO (LGPD ART. 5o, inciso X)
Coleta	Obtenção/Resgate	Refere-se à busca ou recepção de dados pessoais independente do meio utilizado - Mídia digital, Documento eletrônico, Sistema de informação, etc.
Retenção	Arquivamento ou armazenamento	Independente do meio utilizado - Mídia digital, documento eletrônico, banco de dados, arquivo de aço, etc.
Processamento	Operação	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
Compartilhamento	Operação	Envolve: - Transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.; - Distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido; - Comunicação; - Transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro; - Difusão e compartilhamento de dados pessoais telefônicos, radioelétricos, pneumáticos etc. - ato ou efeito de divulgação, propagação, multiplicação dos dados.
Eliminação	Operação	Apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

4. ATIVOS ORGANIZACIONAIS

A seguir, são apresentadas definições para os ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

BASE DE DADOS
Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.

DOCUMENTOS
Unidade de registro de informações, qualquer que seja o suporte e formato (ex: Documento de texto, planilhas, imagens, plantas, etc.).

LOCAIS FÍSICOS
Determinação do lugar onde pode residir de forma definitiva ou temporária uma informação de identificação pessoal, por exemplo uma sala, um arquivo, um prédio, uma mesa, etc.

PESSOAS
Qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais.

SISTEMAS
Qualquer aplicação, sistema ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: Coleta, Retenção, Processamento, Compartilhamento e Eliminação de dados pessoais.

UNIDADES ORGANIZACIONAIS
Órgãos e entidades da Administração Pública.

4. ATIVOS ORGANIZACIONAIS

EQUIPAMENTOS[2]

Servidor de arquivos: Equipamento com a função de fornecer um sistema de arquivos ou partes dele para clientes conectados. O servidor de arquivos oferece aos usuários um local de armazenamento centralizado para que pastas, arquivos e objetos estejam disponíveis a todos os clientes autorizados. (ex: Network Attached Storage (NAS) da Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo - Prodam)

Mídia física portátil: Pen Drive, Mídia Óptica (CD/DVD/Blu-ray, etc.) e Disco Rígido (HD) externo, que estejam envolvidos com as fases do ciclo de vida do tratamento dos dados pessoais: Coleta, Retenção, Processamento, Compartilhamento e Eliminação de dados pessoais.

Nuvem: Qualquer serviço de computação em nuvem que esteja envolvido com as fases do ciclo de vida do tratamento dos dados pessoais: Coleta, Retenção, Processamento, Compartilhamento e Eliminação de dados pessoais.

2. Fonte: Orientações Técnicas de Tecnologia da Informação e Comunicação, Volume I <https://tecnologia.prefeitura.sp.gov.br/arquivos/ot-volumes/OT_vol1.pdf>

5. RELACIONAMENTO DO CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS

A identificação dos ativos organizacionais é uma atividade indispensável para a conformidade com a LGPD e deve ser realizada para **cada uma das fases do ciclo de tratamento de dados que estejam envolvidos**.

1. COLETA. Busca-se localizar os ativos responsáveis pela coleta de dados pessoais. Esses dados podem entrar no departamento através de formulários ou sistemas hospedados dentro do próprio órgão público responsável pelos dados. Alguns dados são coletados pela prestação de serviços externos ou prestados diretamente pelo órgão público nas unidades organizacionais.

2. RETENÇÃO. Os ativos utilizados para armazenar dados pessoais (bancos de dados, documentos eletrônicos, servidores de arquivos, sistemas, etc.) devem ser avaliados. É preciso considerar as unidades organizacionais responsáveis pela segurança e manutenção dos dados, bem como os locais físicos onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em "nuvem", por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

3. PROCESSAMENTO. Os ativos que realizam tratamentos de dados devem ser identificados individualmente. A realização do tratamento de dados poderá ser feita, por exemplo, em documento eletrônico, por um software interno ou contratado pelo órgão. Outro ponto indispensável é a identificação das pessoas (papéis organizacionais), unidades organizacionais e equipamentos envolvidos nesse tratamento. A localização física dessas unidades organizacionais e os equipamentos eletrônicos atuantes neste tratamento também são importantes.

5. RELACIONAMENTO DO CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS

4. COMPARTILHAMENTO. Deve-se mapear os ativos envolvidos no processo de divulgação dos dados pessoais, tanto para dentro, como também para fora do órgão público. Quais sistemas fazem interface e são usados para transmitir, exibir ou divulgar dados pessoais? Quais pessoas são destinatárias dessas informações? Quais unidades organizacionais, quais equipamentos são usados para tal?

5. ELIMINAÇÃO. Avaliam-se os ativos responsáveis pelo armazenamento dos dados pessoais que possam ser objeto de: solicitação de exclusão dos dados pessoais pelo seu titular; ou descarte dos dados quando necessário ao negócio da instituição. Os dados pessoais que devem ser eliminados, ao final do processo de tratamento de dados, deverão estar armazenados em ativos relacionados com bancos de dados, documentos eletrônicos, servidores ou Softwares. Também devemos considerar as unidades organizacionais encarregadas de armazenar e manter os dados que possam ser objeto de exclusão ou descarte, assim como suas localidades físicas onde os ativos estão alocados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em "nuvem", por exemplo, é preciso considerar o serviço de armazenamento contratado e/ou utilizado.

Após identificados todos os ativos, acessos e as relações com os dados pessoais, recomenda-se analisar as informações levantadas para identificar quais medidas técnicas de segurança (previstas na Orientação Técnica nº 13 – Diretrizes Básicas de Segurança da Informação) os ativos implementam de forma efetiva, almejando disponibilizar sempre uma adequada proteção aos dados pessoais conforme orientação da LGPD. Recomenda-se a utilização de algum framework (como o NIST, COBIT ou a implementação de uma política baseada na série de normas ISO 27000, por exemplo), boas práticas ou orientação técnica aplicável.

6. CASOS QUE A LGPD NÃO SE APLICA

Conforme estabelecido no **art. 4° da LGPD**, as disposições da Lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

I – Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II – Realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);

III – realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou 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 na LGPD.

7. MEDIDAS DE SEGURANÇA

Medidas de segurança aparecem diversas vezes na LGPD. A primeira delas vem no **art. 6º**, que coloca a segurança como um dos princípios a serem observados durante as atividades de tratamento. A definição, segundo o **inciso IV do art. 6º**, é que segurança se trata da "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". Fica claro que esse princípio tem uma relação direta com o conceito de Segurança da Informação, porém com foco no contexto de dados pessoais.

Posteriormente, esse princípio é reforçado pelo **art. 46**, porém com um quê a mais. Esse artigo determina que "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Até aqui não existem muitas novidades, apenas uma abrangência maior, visto que os dados devem ser protegidos de "qualquer forma de tratamento inadequado ou ilícito". Entretanto, "medidas de segurança" é um termo muito amplo e que deixa dúvidas sobre o que realmente é exigido por esse artigo.

O § 1º do art. 46 determina que a autoridade nacional poderá dispor sobre padrões técnicos mínimos a serem considerados, de acordo com a natureza das informações tratadas, características do tratamento e estado atual da tecnologia. No momento em que essas diretrizes técnicas estão sendo escritas, a Autoridade Nacional de Proteção de Dados ainda não publicou nenhuma disposição sobre o tema, mas cabe o acompanhamento de novas disposições da Autoridade Nacional de Proteção de Dados.

8. PRIVACIDADE DESDE A CONCEPÇÃO

O **§ 2º do art. 46** determina que "*as medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução*", trazendo o conceito de **Privacidade desde a Concepção**. Essa é uma abordagem que se baseia em **7 Princípios Fundamentais**, que serão explicados a seguir, e também possui forte correlação com os princípios definidos no **art. 6º** da LGPD.

1. Proativo, e não reativo; preventivo, e não corretivo. Esse princípio deixa claro que a abordagem de Privacidade desde a Concepção visa se antecipar e impedir que a privacidade seja corrompida sem que vazamento ou outro tipo de dano tenha ocorrido. A privacidade deve ser pensada desde o início do projeto, e não apenas durante a sua execução. Além disso, esse princípio conversa diretamente com o princípio da prevenção, previsto no inciso VIII do art. 6º da LGPD.

2. Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio. Esse princípio da Privacidade desde a Concepção conversa com os princípios da necessidade e da segurança, previstos nos incisos III e VII do art. 6º da LGPD, já que busca assegurar que a privacidade é flexibilizada apenas quando necessário e que todos os cuidados para proteger os dados pessoais são tomados.

3. Privacidade incorporada ao projeto. Esse princípio busca incorporar a privacidade às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa: holística porque contextos adicionais mais amplos devem ser considerados; integrativa porque todas as partes interessadas devem ser consultadas; e criativa porque incorporar a privacidade muitas vezes significa repensar as escolhas que se tornaram comuns em relação a dados pessoais.

4. Funcionalidade total. Esse princípio vem para lembrar que a abordagem de Privacidade desde a Concepção não se compromete apenas com a privacidade, mas busca entregar uma abordagem que satisfaça todos os objetivos do projeto. Ao incorporar privacidade dentro de um processo ou sistema, isso deve ser feito de maneira que não comprometa a plena funcionalidade do sistema, garantindo a privacidade em conjunto com as demais exigências do projeto.

8. PRIVACIDADE DESDE A CONCEPÇÃO

5. Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados. Como a abordagem de Privacidade desde a Concepção começa antes mesmo de a coleta do primeiro dado pessoal ocorrer, a privacidade e, para sua garantia, a segurança dos dados pessoais também deve ser assegurada desde a fase mais inicial do projeto. Desse modo, a segurança e proteção dos dados pessoais existem durante todo o ciclo de vida desses dados. Vale lembrar também que, como citado anteriormente, segurança também é um princípio previsto no inciso VII do art. 6º da LGPD, devendo ser garantida em todas as atividades de tratamento de dados pessoais.

6. Visibilidade e Transparência. Esse princípio busca garantir que as atividades de tratamento de dados pessoais operam de acordo com as premissas e objetivos declarados, sempre passíveis de verificação independente. Isso é fundamental para garantir responsabilidade e confiança no tratamento de dados pessoais, assegurando a devida responsabilização, abertura e conformidade das políticas e procedimentos relacionados ao tratamento de dados pessoais. Novamente, esse princípio conversa com outros definidos no art. 6º da LGPD, que são os princípios de livre acesso, transparência e responsabilização e prestação de contas, incisos IV, VI e X, respectivamente.

7. Respeito pela privacidade do usuário. Mais do que práticas de segurança e proteção dos dados pessoais, a abordagem de Privacidade desde a Concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso implica em empoderar os Titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais, garantido ao titular, por exemplo: a possibilidade de consentimento livre e específico, sendo apresentado de maneira clara e livre de erros; o acesso a seus dados pessoais e ao uso destes; a precisão dos seus dados pessoais e a pronta correção destes em caso de necessidade. Na LGPD, o consentimento é um fundamento de extrema importância, previsto no inciso I do art. 7º e detalhado no art. 8º, e o direito a acesso e precisão são definidos, junto a outros, nos incisos II e III do art. 18.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

A LGPD define no art. 5º os conceitos de dado anonimizado e anonimização, porém sem relacioná-los diretamente a critérios ou processos técnicos. As definições são as seguintes:

"*Art. 5º Para os fins desta Lei, considera-se:*
[...]
III - 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;
[...]
XI - 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;"

Por outro lado, este artigo não define o conceito de pseudonimização, que é definido apenas no art. 13, e é exigido apenas para estudos em saúde pública, sempre que possível. A definição é, na verdade, bem próxima à definição de anonimização:

"*Pseudonimização é o 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.*"

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

A diferença entre os processos de anonimização e pseudonimização é a reversibilidade do processo: na pseudonimização, a associação dos dados a um indivíduo ainda pode ser feita através de uma chave aleatória ou técnica semelhante; já o processo de anonimização deve ser, a princípio, irreversível. É importante ressaltar, porém, que é muito difícil afirmar inequivocamente que um processo de anonimização é irreversível, e a própria LGPD leva isso em consideração, em especial no art. 12:

"*Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.*

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios."

Então, de maneira resumida:

- A pseudonimização é um processo de tratamento de dados que retira a possibilidade de identificação do titular dos dados, exceto quando associados a um conjunto adicional de dados mantido separadamente pelo controlador, em ambiente seguro;
- A anonimização é um processo de tratamento de dados que impossibilita (o máximo possível, levando em conta custo, tempo e tecnologias disponíveis para a sua reversão) a identificação, direta ou indireta, do titular dos dados;
- Dados anonimizados são dados relativos a uma pessoa natural que passaram por um processo de anonimização e, por isso, deixam de ser considerados dados pessoais para os fins da LGPD.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

QUANDO UTILIZAR. No caso da pseudonimização, a LGPD deixa bem claro que este processo deve ser usado, sempre que possível, nos casos onde órgãos de pesquisa estejam realizando um estudo em saúde pública, além das demais condições exigidas pelo art. 13.

Já o processo de anonimização, é previsto em três situações. A primeira delas, já citada anteriormente, vem do art. 12, que deixa claro que dados que tenham passado por um processo razoável de anonimização deixam de ser considerados dados pessoais, o que facilita em grande medida o tratamento destes dados. A segunda vem do art. 16, que trata da eliminação dos dados pessoais ao término do tratamento, e deixa claro que a conservação dos dados é permitida, desde que estes sejam anonimizados e o uso seja exclusivo do controlador. A última situação é a prevista no art. 18, que determina que o titular dos dados tem direito a requisitar, entre outras coisas, a "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei". Vale ressaltar que essas requisições devem ser informadas a todos os agentes de tratamento com os quais tenha ocorrido o uso compartilhado desses dados.

Também deve ser levado em conta que à medida que a anonimização dos dados aumenta, a utilidade destes acaba diminuindo. A depender da técnica utilizada, é mais difícil (e, na verdade, desejável que o seja) afirmar se determinados registros se tratam de dados duplicados de um mesmo titular ou de titulares diferentes, mas similares. Portanto, a decisão de anonimizar ou não dados também deve considerar a criticidade e importância destes para o negócio.

Uma boa prática para anonimização de bases de dados utilizadas em testes e em sistemas em ambiente de produção é realizá-la de maneira gradual, preservando o máximo da utilidade dos dados.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

COMO FAZER. Existe uma variedade de técnicas conhecidas para se realizar um processo de anonimização de dados. Mas, reforçando o que já foi dito anteriormente, nenhuma dessas técnicas garante inequivocamente que a identificação, direta ou indireta, não possa ser realizada. Portanto, antes de falar especificamente das técnicas que podem ser utilizadas, vale um comentário sobre um modelo para a garantia de anonimato dentro do próprio conjunto de dados.

Um método relevante de garantia de anonimato é o modelo k-anonimato, onde se garante que cada registro de um conjunto de dados seja igual a, pelo menos, k-1 outros registros. Perceba, porém, que essa técnica pode comprometer a qualidade de tratamentos posteriores, principalmente em casos onde a garantia de unicidade de registros não exista antes do processo de anonimização. Além disso, esse método não garante que a identificação dos titulares não possa ocorrer através do relacionamento desse conjunto de dados a outros, inclusive conjuntos públicos.

Vamos, então, descrever algumas técnicas que podem ser utilizadas para aumentar a anonimização de dados pessoais. Vale ressaltar que existem outras técnicas não listadas aqui e que estas não são mutuamente exclusivas, podendo se utilizar várias técnicas de anonimização a um mesmo conjunto de dados. Para ilustrar melhor as técnicas, vamos assumir a tabela abaixo como nosso conjunto de dados contendo dados pessoais.

ID	NOME	ENDEREÇO	TELEFONE	IDADE
583	Arthur	Rua Harry Simonsen, 202	(11) 2409-5384	30
652	Bárbara	Rua Noel Rosa, 12	(11) 2860-1542	36
865	Jorge	Avenida Paulista, 3408	(11) 3386-2074	52
923	Marlene	Rua das Flores, 5	(11) 97254-8066	55

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

GENERALIZAÇÃO. Essa técnica consiste em substituir as informações por outras mais abrangentes, de modo que continuem corretas, mas sejam menos específicas e impossibilitem a identificação do titular. Entretanto, essa técnica não pode ser aplicada a todos os tipos de informação. No conjunto de dados da tabela 1, por exemplo, ela se aplica apenas às colunas de endereço e idade.

Vale notar que a generalização pode tomar formas bastante diferentes de acordo com o tipo de informação a ser substituída, portanto é necessária muita atenção a tentativas de automação desse processo.

ID	NOME	ENDEREÇO	TELEFONE	IDADE
583	Arthur	**Rua Harry Simonsen**	(11) 2409-5384	**30-40**
652	Bárbara	**Rua Noel Rosa**	(11) 2860-1542	**30-40**
865	Jorge	**Avenida Paulista**	(11) 3386-2074	**50-60**
923	Marlene	**Rua das Flores**	(11) 97254-8066	**50-60**

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

SUPRESSÃO. A supressão consiste em substituir os valores de uma informação por outra informação que não permita a identificação do titular. Podemos, usando a tabela 1 como exemplo, substituir as informações de id por "***" e de nome por "XXXXX".

ID	NOME	ENDEREÇO	TELEFONE	IDADE
***	XXXXX	Rua Harry Simonsen, 202	(11) 2409-5384	30
***	XXXXX	Rua Noel Rosa, 12	(11) 2860-1542	36
***	XXXXX	Avenida Paulista, 3408	(11) 3386-2074	52
***	XXXXX	Rua das Flores, 5	(11) 97254-8066	55

Entretanto, essa técnica torna essa informação inutilizável, devendo ser utilizada apenas em atributos considerados dispensáveis para usos futuros. Além disso, como dito anteriormente, as técnicas podem ser combinadas, como no exemplo abaixo, com as colunas de id e nome suprimidas e as colunas de endereço e idade generalizadas.

ID	NOME	ENDEREÇO	TELEFONE	IDADE
***	XXXXX	Rua Harry Simonsen	(11) 2409-5384	30-40
***	XXXXX	Rua Noel Rosa	(11) 2860-1542	30-40
***	XXXXX	Avenida Paulista	(11) 3386-2074	50-60
***	XXXXX	Rua das Flores	(11) 97254-8066	50-60

Essa técnica pode ser aplicada de maneira estática ou dinâmica. No caso da supressão estática, os dados são armazenados já na forma suprimida, podendo ser útil na utilização de bases de dados para desenvolvimento e testes de sistemas, por exemplo. Já a supressão dinâmica ocorre na operação de tratamento, sendo aplicado de acordo com políticas definidas para determinado consumidor dos dados.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

MASCARAMENTO. A técnica de mascaramento é semelhante à de supressão, porém pode conservar alguns dígitos da informação original, de forma a tornar parte dela utilizável, mas sem comprometer a privacidade do titular.

ID	NOME	ENDEREÇO	TELEFONE	IDADE
583	Arthur	**Rua Harry Simonsen, 202**	(11) 2XXX-XX84	**30**
652	Bárbara	**Rua Noel Rosa, 12**	(11) 2XXX-XX42	**36**
865	Jorge	**Avenida Paulista, 3408**	(11) 3XXX-XX74	**52**
923	Marlene	**Rua das Flores, 5**	(11) 97XXX-XX66	**55**

Assim como a supressão, essa técnica também pode ser aplicada de maneira estática ou dinâmica.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

TOKENIZAÇÃO. A tokenização é uma técnica que consiste na substituição do valor de um campo quando ele é carregado para uma aplicação ou uma nova base de dados. Normalmente, são utilizados algoritmos que garantem a unicidade e o mapeamento consistente entre os valores originais e o valor do token. Isso requer um cuidado especial na utilização dessa técnica, caso a reversão do token ao valor original não seja desejável, já que algoritmos que utilizam apenas o valor a ser tokenizado se tornam vulneráveis a ataques do tipo força bruta (brute force).

ID	NOME	ENDEREÇO	TELEFONE	IDADE
FYk	oT8iSne5	**Rua Harry Simonsen, 202**	(11) 2409-5384	**30**
7Mv	64mKadZR	**Rua Noel Rosa, 12**	(11) 2860-1542	**36**
Q4I	wLCFKMdS	**Avenida Paulista, 3408**	(11) 3386-2074	**52**
7xY	qCAq41jS	**Rua das Flores, 5**	(11) 97254-8066	**55**

Entre as várias formas possíveis de tokenização, destaco três principais:

Tokenização baseada em base de dados. Esse método de tokenização utiliza um serviço centralizado e armazena os pares de token e valor em uma base de dados. Essa forma permite a utilização de um mesmo token em diferentes conjuntos de dados, mas apresenta problemas de escalabilidade. Importante ressaltar que, no contexto da LGPD, essa técnica funciona apenas para a pseudonimização, visto que o dado pessoal e o token permanecem armazenados em um conjunto de dados separado.

Tokenização baseada em algoritmo. Esse método também utiliza um serviço centralizado, porém não armazena os pares de token e valor. Nesse caso, o serviço também deve ser capaz de transformar o token novamente no dado original, o que gera uma nova possibilidade de engenharia reversa para a exposição do titular dos dados.

Criptografia com preservação de formato executada localmente. A criptografia com preservação de formato processa o valor de entrada de modo a produzir um valor de saída de mesmo formato. Um telefone que passe por esse método, por exemplo, produziria uma cadeia de dez ou onze números aleatórios, no formato que estamos acostumados. A diferença nessa abordagem é a execução local da técnica, que possui melhor escalabilidade dada a distribuição de carga de processamento em cada sistema, porém gera um trabalho maior no gerenciamento desses tokens, visto que um mesmo valor pode ser representado por vários tokens diferentes, a depender do sistema.

9. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Dada a variedade de técnicas que foi apresentada, listamos na tabela[3] abaixo diferentes cenários, de acordo com o fim desejado.

ATRIBUTO	TÉCNICAS PARA MAIOR ANONIMIZAÇÃO	TÉCNICAS POSSÍVEIS
ID	Supressão Tokenização Mascaramento	Supressão Generalização Tokenização
NOME	Supressão	Supressão Tokenização
ENDEREÇO	Supressão Tokenização	Generalização Supressão Tokenização
TELEFONE	Supressão Tokenização Mascaramento	Supressão Mascaramento Tokenização
IDADE	Supressão Generalização Tokenização	Generalização Supressão Tokenização

3. Tabelas adaptadas de XU, Dennis et al, 2020

10. ADEQUAÇÕES DE SISTEMAS E DADOS JÁ COLETADOS

Bancos de dados já existentes

Depois de compreender as exigências e conhecer algumas técnicas possíveis para atender à LGPD, fica a dúvida sobre o que fazer com dados e sistemas já existentes. Felizmente, a própria LGPD já faz menção a esse tipo de dado, no seu art. 63., onde determina que a Autoridade Nacional de Proteção de Dados estabelecerá normas sobre a adequação progressiva de bases já existentes, considerando "a complexidade das operações de tratamento e a natureza dos dados". Novamente, até o momento em que esse documento foi elaborado, não existe nenhuma norma publicada pela ANPD sobre o tema, portanto é necessário realizar o acompanhamento frequente às possíveis publicações da autoridade nacional e, caso as normas entrem em conflito com o conteúdo dessas diretrizes, devem ser respeitadas as normas publicadas pela autoridade nacional.

Isso nos leva à primeira alternativa de adequação, que é a estratégia de Wait and See: simplesmente não realizar novos tratamentos nas bases de dados pessoais já existentes até que as normas de adequação sejam publicadas. Os pontos negativos dessa estratégia são a inutilização desses dados por tempo indeterminado, visto que não existe uma previsão de data para a publicação dessas normas, e o risco de não conseguir seguir essas normas a tempo, quando publicadas, levando a uma possível exclusão de todos esses dados.

10. ADEQUAÇÕES DE SISTEMAS E DADOS JÁ COLETADOS

Esses pontos negativos podem ser contornados usando uma estratégia mais ativa de adequação desses dados, mesmo que ainda não existam normas de como isso deve ser feito. Nessa abordagem, existem basicamente três passos:

- Verificar a existência de consentimentos já fornecidos e a adequação destes à LGPD, em especial ao art. 8º, e catalogar esses dados com consentimentos válidos para a utilização;
- Verificar a aplicação de uma das outras nove bases legais para o tratamento de dados pessoais, previstas também no art. 7º da LGPD, e catalogar os dados de acordo com a base legal;
- Finalmente, nos dados restantes, decidir se é mais viável a busca ativa de consentimento, a reserva desses dados até a publicação das normas previstas no art. 63., ou mesmo a exclusão desses dados.

É importante fazer a ressalva de que, para que essa estratégia possa ser tomada, o mapeamento prévio das atividades de tratamento de dados pessoais e suas finalidades é fundamental, pois somente com as finalidades bem demarcadas se torna possível solicitar o consentimento ou avaliar a aplicação das bases legais previstas na LGPD.

10. ADEQUAÇÕES DE SISTEMAS E DADOS JÁ COLETADOS

Sistemas em funcionamento

Sobre sistemas em operação, por outro lado, a LGPD não especifica o que deve ser feito e nem prevê a publicação de norma ou diretriz específica sobre o tema. Porém, diversos aspectos da lei sinalizam que a complexidade e a boa-fé dos agentes à adequação a ela sejam levadas em conta em casos de infração, de modo que não parece ser necessário nenhum radicalismo, como a suspensão de utilização de algum sistema existente, desde que exista um plano para a adequação deste tipo de sistema.

E, nesse ponto, o esforço é semelhante ao de novos sistemas e processos desenvolvidos sob a vigência da LGPD. Novamente, é necessário acompanhar a atuação da Autoridade Nacional de Proteção de Dados sobre o tema e, caso exista divergência entre disposições e normas publicadas pela autoridade nacional e esse documento, deve-se respeitar o posicionamento da autoridade nacional. De todo modo, como exemplo de ações a serem tomadas, seguem algumas dicas de passos a serem seguidos na adequação de sistemas:

- Avaliar todas as atividades relacionadas ao sistema que demandem o tratamento de dados pessoais e determinar a finalidade de tais tratamentos;
- Depois, com base nessa finalidade, avaliar o embasamento legal, de acordo com o art. 7º da LGPD, e manter um catálogo dessas informações;
- Para as atividades que necessitem de consentimento, é necessário se adequar o sistema para se comunicar com um sistema central de controle desses consentimentos ou, quando não for viável uma integração, realizar esse controle de maneira independente;
- Paralelamente, trabalhar em uma política de segurança da informação que garanta a observação do princípio da segurança, previsto no inciso VII do art. 6º da LGPD, e adequar o sistema em estudo de acordo com essa política.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Gervânia. Ciclo de Vida dos Dados e LGPD. In: XPOSITUM. Produtos e serviços da Xpositum. São José dos Pinhais, entre 2018 e 2021. Disponível em: https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd. Acesso em: 5 nov. 2021.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei geral de proteção de dados, Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 abr. 2021.

BRASIL. Ministério da Economia. Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD): Guia de Boas Práticas para Implementação na Administração Pública Federal. Brasília: [s. n.], 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 5 nov. 2021.

CARVALHO, Luiz Paulo; OLIVEIRA, Jonice; CAPPELLI, Claudia. Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações. In: BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING (BRASNAM), 9. , 2020, Cuiabá. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 73-84.

COSTA, Juliana. Como adaptar os dados antigos de sua empresa à Lei Geral de Proteção de Dados Pessoais. In: Jus navigandi: Tudo de direito e justiça. Teresina, 2020. Disponível em: https://jus.com.br/artigos/84625/como-adaptar-os-dados-antigos-de-sua-empresa-a-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 10 maio 2021

FAGUNDES, Jorge A. O tratamento de dados do setor público e privado diante da LGPD e suas hipóteses. In: JUSBRASIL. Jusbrasil: Conectando Pessoas à Justiça. São Paulo, 2020. Disponível em: https://jorgealexandrefagundes.jusbrasil.com.br/artigos/1108221736/o-tratamento-de-dados-do-setor-publico-e-privado-diante-da-lgpd-e-suas-hipoteses. Acesso em: 5 nov. 2021.

KRIKKEN, Ramon; FRITSCH, Joerg. Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization. [S. l.]: Gartner, 15 mar. 2018. Disponível em: https://www.gartner.com/document/code/343738. Acesso em: 29 abr. 2021.

LEGALCLOUD CONSULTORIA. Tratamento de dados na LGPD: O que é e Como Fazer?. In: LEGALCLOUD CONSULTORIA. Legalcloud: Contagem de prazo processual com software jurídico. Rio de Janeiro, 30 out. 2020. Disponível em: https://legalcloud.com.br/tratamento-de-dados-lgpd/. Acesso em: 5 nov. 2021.

REFERÊNCIAS BIBLIOGRÁFICAS

MAGRATHEA LABS; SILVA, SANTANA & TESTON ADVOGADOS. LGPD na prática. Joinville, 28 jan. 2021. Disponível em: http://lgpd.magrathealabs.com/. Acesso em: 5 nov. 2021.

MURTHY, Suntherasvaran et al. A Comparative Study of Data Anonymization Techniques. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS), [s. l.], p. 306-309, 2019.

O CICLO de vida dos dados previstos na LGPD. In: SOFTWARESUL TECNOLOGIA. Softwaresul. Curitiba, 2020. Disponível em: https://softwaresul.com.br/o-ciclo-de-vida-dos-dados-pessoais-previstos-na-lgpd/. Acesso em: 5 nov. 2021.

SANT'ANA, Ricardo. LGPD: Atores envolvidos e seu impacto na gestão arquivística de dados. In: CÂMARA MUNICIPAL DE SÃO PAULO. Escola do Parlamento. Escola do Parlamento. São Paulo, 2018. Disponível em: https://www.saopaulo.sp.leg.br/escoladoparlamento/wp-content/uploads/sites/5/2018/11/apresenta%C3%A7%C3%A3o-Ricardo.pdf. Acesso em: 5 nov. 2021.

TOTVS, Anonimização de dados e LGPD: Conheça melhor. Blog TOTVS, [S. l.], 29 mai. 2020. Gestão de Negócios, p. 100. Disponível em: https://www.totvs.com/blog/negocios/anonimizacao/. Acesso em: 30 abr. 2021.

VIDIGAL, Paulo. LGPD e o enigma da Esfinge: o que fazer em relação à base legada?. In: CryptoID: Tudo sobre o universo da identificação digital. São Paulo, 30 set. 2019. Disponível em: https://cryptoid.com.br/protecao-de-dados/lgpd-e-o-enigma-da-esfinge-o-que-fazer-em-relacao-a-base-legada/. Acesso em: 10 maio 2021.

XU, Dennis et al. Guide to Data Security Concepts. [S. l.]: Gartner, 9 out. 2020. Disponível em: https://www.gartner.com/document/3991573. Acesso em: 29 abr. 2021.