COMENTÁRIOS AO PROVIMENTO Nº 134 DE 2022 DO CONSELHO NACIONAL DE JUSTIÇA: CONHECENDO IMPACTOS DA NORMATIVA NO REGISTRO DE IMÓVEIS

ARISP
Associação dos Registradores Imobiliários de São Paulo

FICHA CATALOGRÁFICA

DIRETORIA ARISP

George Takeda
Presidente

Frederico Jorge de Figueiredo Assad
Vice-Presidente

Ana Carina Pereira
Diretora de Prerrogativas, Enunciados e Emolumentos

Ricardo Alexandre Barbieri Leão
Diretor Financeiro

Ivan Jacopetti do Lago
Diretor Acadêmico

Fabio Costa Pereira
Secretário

Flaviano Galhardo
Diretor Institucional

Leandro Borrego Marini
Leandro de Lima Lopes
Coordenadores Institucionais

Conteúdo

Bernardo Chezzi
Daniel Ribeiro
Luis Acioly
Manuela Oliveira
Chezzi Advogados

Revisão

Ivan Jacopetti do Lago

Diagramação

Prefácio Comunicação

SUMÁRIO

Apresentação

A Lei Geral de Proteção de Dados Pessoais (LGPD) constitui diploma generalístico aplicável à toda e qualquer espécie de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, com o fim precípuo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Conceituando o que seria dado pessoal, estamos a falar de dado de pessoa natural, ou seja, dado atrelado à pessoa física, de modo que a legislação permeia tudo aquilo que é dado pessoal, independentemente do meio pelo qual se coleta, processa ou se compartilha.

Sua aplicação abrange o território nacional, ressalvadas as hipóteses de sua não incidência previstas no art. 4º do diploma normativo , bem como se aplica às operações realizadas em âmbito internacional, desde que os dados tenham sido coletados no Brasil ou tenham por objetivo o fornecimento de bens e serviços em território brasileiro.

Por conseguinte, as operações de tratamento de dados pessoais tocam tanto o setor privado, quanto o setor público, alcançando as atribuições promovidas pelas serventias extrajudiciais.

Os serviços públicos notariais e de registro, realizados em regime de delegação do poder público ao agente privado, recebem, por expressa previsão normativa disciplinada na LGPD (art. 23, §4º) , o mesmo tratamento dado à administração pública, ficando a cargo do Poder Judiciário a sua regulamentação, posto que competente constitucionalmente para tanto.

Ante seu caráter geral, **a norma precisa de regulamentação setorial**, a partir da necessidade da publicização de normas de regência por parte do Conselho Nacional de Justiça, para adequar as suas disposições à realidade jurídica esfera cartorial.

Relativamente aos ofícios notariais e de registros, as Corregedorias Gerais de Justiça do Poder Judiciário de diversos entes da federação têm atuado no sentido da regulamentação setorial da LGPD, editando Provimentos estaduais .

[1] Art. 4º, LGPD: Esta 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.

[2] Art. 23, § 4º, LGPD: (...) Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

Contudo, ante o pluralismo normativo que permeia um assunto de interesse nacional, o Conselho Nacional de Justiça (CNJ) tomou a dianteira para estabelecer parâmetros fixos de regulamentação do tema, a serem observados em todo território brasileiro.

A Corregedoria Nacional de Justiça do CNJ estabeleceu um Grupo de Trabalho para elaboração de estudos e de propostas voltadas à adequação dos serviços notariais e de registros à LGPD, através da Portaria nº 60, de 18 de dezembro de 2020. O referido Grupo apresentou minuta de um Provimento nacional submetido à consulta pública no período de 14 a 28 de fevereiro de 2022, recebendo propostas de alterações e adaptações.

De forma definitiva, a Corregedoria Nacional do CNJ publicou o Provimento nº 134, de 24 de agosto de 2022, estabelecendo medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais.

O cumprimento das diretrizes normativas será fiscalizado pelas Corregedorias Gerais de Justiça dos Estados e do Distrito Federal, a fim de atestar a sua observância pelas unidades do serviço extrajudicial.

Após a data de publicação citada, as serventias extrajudiciais passaram a possuir o dever de adequar os processos e procedimentos de tratamento de dados pessoais realizados em seus ofícios às balizadas diretivas contidas no Provimento.

Com o objetivo de apresentar a atualização normativa do CNJ, o presente documento explica os artigos que compõem o novel Provimento, tratando dos seus pressupostos, o sentido e alcance de sua interpretação e as consequências práticas para os delegatários, posto que diretamente afetados por suas disposições.

Cabe ressaltar que a LGPD elevou a importância da existência de uma boa gestão das informações dos titulares. O referido diploma estrutura-se na implementação de medidas organizacionais, técnicas e jurídicas que visam diminuir riscos à proteção de dados pessoais e promover um “ecossistema de privacidade” no âmbito das organizações. Espírito normativo reverberado no Provimento nº 134/2022.

O presente documento apresenta **cinco seções**, conforme a envergadura do Provimento do CNJ. A primeira seção diz respeito às disposições gerais do novel diploma e pressupostos normativos. A segunda seção adentra na estruturação de um Programa de Governança em Proteção de Dados Pessoais. A terceira trata especificamente dos instrumentos de adequação à LGPD. A quarta seção aponta as consequências na atividade finalística das **serventias de Registro de Imóveis** em função do Provimento. E a quinta seção traz os apontamentos finais da adequação à LGPD e ao próprio Provimento do CNJ.

[3] Como ressalta Chezzi (CHEZZI, B. A aplicação da LGPD ao Registro de Imóveis. In: GALHARDO, F.; PARO, J. P.; NALINI, J. R.; BRANDELLI, L. (orgs.). Direito Registral e Novas Tecnologias. Rio de Janeiro: Forense, 2021, p. 139-167), o **Provimento n. 23 da Corregedoria Geral de Justiça do Tribunal de Justiça de São Paulo**, de 03 de setembro de 2020, teve a primazia de inaugurar a regulamentação setorial da LGPD no âmbito das serventias extrajudiciais, influenciando, inclusive normas de CGJs de outros estados.

1ª seção Disposições gerais

Capítulo 1
Das disposições gerais

> ***Art. 1º*** *Os responsáveis pelas serventias extrajudiciais deverão atender às disposições da Lei Geral de Proteção de Dados Pessoais — LGPD (Lei n. 13.709/2018), independentemente do meio ou do país onde os dados estão localizados, obedecendo a seus fundamentos, princípios e obrigações concernentes à governança do tratamento de dados pessoais.*
>
> ***Parágrafo único.*** *Deverão ser cumpridas as disposições previstas na LGPD e nas diretrizes, regulamentos, normas, orientações e procedimentos expedidos pela Autoridade Nacional de Proteção de Dados Pessoais, com base nas competências previstas no artigo 55-J da LGPD.*

A redação em comento reproduz o ***caput*** do art. 3º da LGPD ao prever as hipóteses de aplicabilidade territorial e extraterritorial a partir dos incisos ali contidos.

O inciso I versa sobre a operação de tratamento realizada no território nacional, estendendo o dever de cumprimento da Lei aos agentes estrangeiros, mesmo sem sede no Brasil e que de qualquer forma operem dados pessoais no Brasil, incluindo-se, por exemplo, a coleta, produção ou recepção de dados pessoais.

Observa-se o espaço físico em que a operação de tratamento ocorre, não estando *in voga* se os dados foram coletados fora do Brasil, se são dados de brasileiros ou estrangeiros, residentes ou não no Brasil.

O inciso II do referenciado artigo, por sua vez, versa sobre a aplicação extraterritorial da LGPD.

De acordo com a previsão do Marco Civil da Internet, ao dispor sobre a aplicação da legislação brasileira para dados coletados em território nacional, a LGPD deverá ser cumprida mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, independentemente da sede física do responsável pela atividade de tratamento de dados pessoais, considerando que eventuais lesões aos titulares terão reflexo no Brasil.

Por fim, o inciso III versa sobre os dados pessoais objetos do tratamento que tenham sido coletados no território nacional.

Em atenção à disposição contida no parágrafo único, o Provimento nº 134/2022 da Corregedoria Nacional de Justiça, embora tenha o papel de orientar e disciplinar a aplicação da LGPD no âmbito específico das serventias extrajudiciais, **não exclui a observância de diretrizes, regulamentos, normas, orientações e procedimentos expedidos pela Autoridade Nacional de Proteção de Dados Pessoais - ANPD**, que tem suas funções estabelecidas no art. 55-J da LGPD.

[4] Art. 3º Esta Lei 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 (...)

[5] Art. 3º. 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;

O dispositivo da LGPD põe em foco o papel central da ANPD no universo regulatório da Proteção de Dados Pessoais, denotando a competência para a Autoridade "articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação" (inciso XXIII).

O art. 1º do Provimento nº 134/2022 confirma que este é um instrumento de regulamentação setorial da LGPD que compõe o universo jurídico da Proteção de Dados Pessoais, devendo ser aplicado de forma sistemática com outros regulamentos, normas e orientações já existentes sobre o tema e as consequentes atualizações normativas, especialmente quando formuladas pela Autoridade Nacional de Proteção de Dados – ANPD.

> **Art. 2º** *O tratamento de dados pessoais destinado à prática dos atos inerentes ao exercício dos respectivos ofícios, consistentes no exercício de competências previstas em legislação específica, será promovido de forma a atender à finalidade da prestação do serviço, na persecução do interesse público, e com os objetivos de executar as competências legais e desempenhar atribuições legais e normativas dos serviços públicos delegados.*

O Provimento se alinha à diretriz legal do art. 23, § 4º , da LGPD, ressaltando o caráter público do serviço prestado pelo delegatário, sendo-lhe imposto que o tratamento de dados para a atividade finalística do cartório deve atender à própria finalidade pública, no interesse público.

O atendimento das finalidades públicas por serventias extrajudiciais não se esgota no disposto na Lei Federal n. 8.935 de 1994, **mas pressupõe a observância do complexo normativo que norteia as diversas espécies de serviços prestados por delegatários**, entre eles, a Lei de Registros Públicos, as normas, provimentos e resoluções do CNJ ou de Corregedorias de Justiça dos Estados.

A necessidade de observância da finalidade pública do tratamento de dados traz repercussões na prestação do serviço delegado, incluindo os atos que envolvem a publicidade registral, conforme poderá ser observado nos capítulos que detalham os impactos da LGPD nas atribuições de notas e de registro e que serão abordados neste documento.

> **Art. 3º** *Fica criada, no âmbito da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça, a Comissão de Proteção de Dados — CPD/CN/CNJ, de caráter consultivo, responsável por propor, independentemente de provocação, diretrizes com critérios sobre a aplicação, interpretação e adequação das Serventias à LGPD, espontaneamente ou mediante provocação pelas Associações.*

O Provimento criou a Comissão de Proteção de Dados no âmbito da Corregedoria Nacional do CNJ, órgão de caráter consultivo, com função de propor diretrizes com critérios sobre a aplicação, interpretação e adequação dos cartórios extrajudiciais à LGPD, espontaneamente ou mediante provocação pelas **Associações**.

Observa-se, pois, o papel acentuado das associações de delegatários na busca do aperfeiçoamento normativo, pois lhes é deferida a prerrogativa de atuar como canal de comunicação das dúvidas alçadas pelos associados à Comissão de Proteção de Dados do

[6] Art. 3º. III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

[7] Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

CNJ, suprindo eventuais lacunas, bem como fornecendo modelos de documentos a serem utilizados no processo de conformidade à norma.

> **Art. 4º** *Os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, na qualidade de titulares das serventias, interventores ou interinos, são controladores no exercício da atividade típica registral ou notarial, a quem compete as decisões referentes ao tratamento de dados pessoais.*
>
> **Parágrafo único.** *Os administradores dos Operadores Nacionais de registros públicos e de Centrais de serviços compartilhados são controladores para fins da legislação de proteção de dados pessoais.*

O Provimento busca dar segurança jurídica na aplicação da LGPD deixando claro que Controlador de dados, no âmbito das serventias extrajudiciais, **são os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro**, na qualidade de titulares das serventias, interventores ou interinos, por lhes competir o poder decisivo sobre o tratamento de dados pessoais.

O controlador de dados pessoais é o agente de tratamento que se conceitua a partir do poder decisório (**"de controle"**) sobre elementos essenciais[8] da operação de tratamento de dados pessoais. Segundo o art. 5º, VI, da LGPD, o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

Seguindo essa linha, a ANPD, em seu Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[9], compreende que o delegatário é controlador dos dados atuando na qualidade de **Pessoa Natural**:

> **32.** *Uma pessoa natural poderá ser controladora nas situações em que é a responsável pelas principais decisões referentes ao tratamento de dados pessoais. Nessa hipótese, a pessoa natural age de forma independente e em nome próprio – e não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta.*
>
> **33.** *É o que ocorre, por exemplo, com os empresários individuais, os profissionais liberais (como advogados, contadores e médicos) e os* ***responsáveis pelas serventias extrajudiciais****.*

Da mesma forma, os administradores do **Operador Nacional do Registro (ONR) e de Centrais de serviços compartilhados** são considerados controladores, naquilo que lhes compete na tomada de decisões sobre o tratamento de dados.

Esse enquadramento atrela a figura do Controlador ao instituto da Responsabilidade Civil prevista no artigo 42 e seguintes da LGPD ao prever que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

8. A Autoridade Nacional de Proteção de Dados, em Guia Orientativo acerca dos agentes de tratamento, predispõe que os elementos essenciais do tratamento se circunscrevem ao cumprimento de sua finalidade, tornando desnecessário que todas as decisões sejam tomadas pelo controlador para que se configure como tal.

9. ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** "Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf>. Acesso em: 23 de outubro de 2022

A fim de assegurar a efetiva indenização ao titular de dados pessoais, o Operador será equiparado ao Controlador, respondendo solidariamente pelos danos causados pelo tratamento quando i) descumprir as obrigações da legislação de proteção de dados ou ii) quando não tiver seguido as instruções lícitas do controlador.

> **Art. 5º** *O operador, a que se refere o art. 5º da LGPD, é a pessoa natural ou jurídica, de direito público ou privado, externa ao quadro funcional da serventia, contratada para serviço que envolva o tratamento de dados pessoais em nome e por ordem do controlador.*

Outro agente de tratamento que também é detalhado pelo Provimento é o **Operador de Dados Pessoais**.

O Provimento, além de se alinhar à definição trazida pelo art. 5º, VII, da LGPD ("operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"), cuidou de dirimir previamente eventual dúvida conceitual, deixando claro que o Operador é **pessoa externa ao quadro funcional** da serventia.

Nesse ponto, o Provimento se compatibiliza com a orientação da ANPD, que define o Operador de Dados, quando pessoa física, como pessoa distinta da organização que é gerida pelo controlador:

> **59.** *Em caso de pessoa jurídica, importa destacar que a organização ou empresa é entendida como agente de tratamento, de forma que seus funcionários apenas a representam. Assim como explicado no tópico 2.2 e de forma análoga à definição de controlador,* ***a definição legal de operador também não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades****.*
>
> **60.** *Nesse cenário, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que* ***o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos****. (grifou-se)*

No cenário das serventias extrajudiciais, a figura do operador é recorrente quando atrelada ao cumprimento das atribuições gerenciais administrativas que envolvam compartilhamento de dados pessoais de seus colaboradores, com eventual contratação de empresa contábil (ou pessoa física contabilista) para gerir a folha de pagamento dos funcionários, ou empresa de tecnologia da informação que fornece software de automação dos processos da serventia, com assessoramento técnico informático.

A delimitação da figura de cada agente de tratamento é importante na medida em que o controlador detém o poder decisório sobre os dados tratados, **recaindo sobre ele a responsabilidade no entorno do tratamento de dados pessoais**.

Devem ser empregadas medidas técnicas e administrativas de preservação e segurança dos dados pessoais aptas a protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito podendo, inclusive, exigir do operador a tomada de precauções especiais e realizar auditorias.

Importa acentuar que o **Encarregado pelo Tratamento de Dados Pessoais**, embora também seja uma figura de grande importância para a LGPD e para o Provimento, não é agente de tratamento de dados pessoais, cuja abordagem se dará em capítulo próprio.

Capítulo 2
Da governança do tratamento de dados pessoais nas serventias

> ***Art. 6º*** *Na implementação dos procedimentos de tratamento de dados, o responsável pela serventia extrajudicial deverá verificar o porte da sua serventia e classificá-la, de acordo com o Provimento n. 74, de 31 de julho de 2018, da Corregedoria Nacional de Justiça (Classe I, II ou III), e observadas as regulamentações da Autoridade Nacional de Proteção de Dados ("ANPD"), fazer a adequação à legislação de proteção de dados conforme o volume e a natureza dos dados tratados, e de forma proporcional à sua capacidade econômica e financeira para aporte e custeio de medidas técnicas e organizacionais, adotar ao menos as seguintes providências:*
>
> ***I -*** *nomear encarregado pela proteção de dados;*
>
> ***II -*** *mapear as atividades de tratamento e realizar seu registro;*
>
> ***III -*** *elaborar relatório de impacto sobre suas atividades, na medida em que o risco das atividades o faça necessário;*
>
> ***IV -*** *adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais;*
>
> ***V -*** *definir e implementar Política de Segurança da Informação;*
>
> ***VI -*** *definir e implementar Política Intema de Privacidade e Proteção de Dados;*
>
> ***VII -*** *criar procedimentos internos eficazes, gratuitos, e de fácil acesso para atendimento aos direitos dos titulares;*
>
> ***VIII -*** *zelar para que terceiros contratados estejam em conformidade com a LGPD, questionando-os sobre sua adequação e revisando cláusulas de contratação para que incluam previsões sobre proteção de dados pessoais; e*
>
> ***IX -*** *treinar e capacitar os prepostos.*

O Provimento estabeleceu um efetivo passo a passo dos procedimentos a serem implementados pelas serventias extrajudiciais nos processos de adequação à LGPD, a partir da estruturação e do porte financeiro das serventias extrajudiciais.

São medidas que compõem o mínimo exigido para o cumprimento do Programa de ***Compliance*** em Privacidade e Proteção de Dados. O alinhamento da formulação de suas próprias regras e autorregulação estarão de acordo com as condições e peculiaridades da organização e a sua forma de funcionamento.

O Provimento reveste de caráter obrigatório as medidas de boas práticas por ele trazidas, por se tratar de providências estritamente necessárias para compatibilizar a Proteção de Dados Pessoais com a finalidade essencial dos serviços delegados.

Cada uma dessas medidas é desembrulhada no decorrer do provimento, que traz os parâmetros para a sua correta implementação.

3ª seção

Instrumentos e adequação em espécie

Capítulo 3
Do mapeamento das atividades de tratamento

> ***Art. 7º*** *O mapeamento de dados consiste na atividade de identificar o banco de dados da serventia, os dados pessoais objeto de tratamento e o seu ciclo de vida, incluindo todas as operações de tratamento a que estão sujeitos, como a coleta, armazenamento, compartilhamento, descarte, e quaisquer outras operações às quais os dados pessoais estejam sujeitos.*
>
> ***§ 1º*** *O produto final da atividade de mapeamento será denominado "Inventário de Dados Pessoais", devendo o responsável pela serventia:*
>
> ***I -*** *garantir que o inventário de dados pessoais contenha os registros e fluxos de tratamento dos dados com base na consolidação do mapeamento e das decisões tomadas a respeito de eventuais vulnerabilidades encontradas, que conterão informações sobre:*
>
> ***a)*** *finalidade do tratamento;*
>
> ***b)*** *categorias de dados pessoais, e descrição dos dados utilizados nas respectivas atividades;*
>
> ***c)*** *a identificação das formas de obtenção/coleta dos dados pessoais;*
>
> ***d)*** *base legal;*
>
> ***e)*** *descrição da categoria dos titulares;*
>
> ***f)*** *se há compartilhamento de dados com terceiros, identificando eventual transferência internacional;*
>
> ***g)*** *categorias de destinatários, se houver;*
>
> ***h)*** *prazo de conservação dos dados; e*
>
> ***i)*** *medidas de segurança organizacionais e técnicas adotadas.*

Alinhando-se com a disposição da LGPD que estabelece a necessidade do agente de tratamento **manter o registro de suas atividades que envolvam dados pessoais** (art. 37), o Provimento materializa a sistematização do registro na forma do **Mapeamento de Dados Pessoais**.

O provimento define o mapeamento como a "atividade de identificar o banco de dados da serventia, os dados pessoais objeto de tratamento e o seu ciclo de vida, incluindo todas as operações de tratamento a que estão sujeitos, como a coleta, armazenamento, compartilhamento, descarte, e quaisquer outras operações às quais os dados pessoais estejam sujeitos".

O inventário de dados, também conhecido como "mapeamento de dados" ou *"data mapping"*, é **um dos elementos fundamentais de um sistema de gestão de dados pessoais** tendo por função principal identificar o caminho dos dados, seja interna e ex-

ternamente, quando compartilhados com operadores, controladores e órgãos públicos.

Como medida de boa prática, sugere-se que o processo de mapeamento ocorra de forma setorizada, a fim de identificar claramente, à luz dos setores do gerenciamento administrativo-financeiro da serventia e da atividade finalística, o ciclo de vida dos dados pessoais (coleta, processamento, armazenamento e descarte).

Realizando o mapeamento é possível identificar: (i) Quais dados são coletados e para quais finalidades; (ii) Quais bases legais legitimam o tratamento; (iii) Quais categorias são tratadas; (iii) Quem tem acesso aos dados pessoais, com quem os compartilha e por quê; (iv) Se há transferência internacional de dados pessoais a partir da utilização de software ou dispositivos de armazenamento de informações em nuvem; (v) Quando os dados pessoais serão descartados ou mantidos de forma permanente e a forma de descarte e as considerações pertinentes ao Encarregado.

> ***Art. 7º** (...):*
>
> ***§ 1º** O produto final da atividade de mapeamento será denominado "Inventário de Dados Pessoais", devendo o responsável pela serventia:*
>
> ***I -** (...);*
>
> ***II -** elaborar plano de ação para a implementação dos novos processos, procedimentos, controles e demais medidas internas, incluindo a revisão e criação de documentos, bem como as formas de comunicação com os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), quando necessária;*
>
> ***III -** conduzir a avaliação das vulnerabilidades (gap assessment) para análise de lacunas em relação à proteção de dados pessoais no que se refere às atividades desenvolvidas na serventia;*
>
> ***IV -** tomar decisões diante das vulnerabilidades encontradas e implementar as adequações necessárias e compatíveis com a tomada de decisões;*
>
> ***V -** atualizar, sempre que necessário, não podendo ultrapassar um ano, o inventário de dados; e*
>
> ***VI -** arquivar o inventário de dados pessoais na serventia e disponibilizá-lo em caso de solicitação da Corregedoria Geral da Justiça, da Autoridade Nacional de Proteção de Dados Pessoais ou de outro órgão de controle.*

O Provimento nomeia o produto do mapeamento de dados como "Inventário de Dados Pessoais", cuja funcionalidade foi condicionada à possibilidade de fornecer subsídios para a construção de um **Plano de Ação** para conformidade à LGPD, que deve abarcar, tanto os novos processos quanto os antigos.

O Plano de Ação é um fluxo de trabalho capaz de contemplar todas as etapas do projeto de adequação, balizado de acordo com o nível de maturidade organizacional e de recursos financeiro e pessoal disponibilizado pela serventia.

Busca-se identificar num Plano de Ação pelo menos as seguintes informações: (i) o que será feito; (ii) por que será feito; (iii) onde será feito; (iv) quando será feito; (v) por quem será feito; (vi) como será feito; (vii) quanto custará para fazer.

Outro condicionante do inventário de dados é o fornecimento de subsídios para a realização da **avaliação de vulnerabilidades**, ou ***Gap Assessment***, como medida estritamente necessária para a concretização da prevenção, enquanto princípio da Proteção de Dados Pessoais.

A partir do *Gap Assessment*, o responsável pela serventia deve tomar as medidas necessárias para mitigar, erradicar ou conviver com os riscos inerentes às lacunas encontradas através das respectivas adequações.

Na prática, a análise de vulnerabilidades irá constar no **Relatório de *Gap Assessment*** após a verificação dos riscos inerentes a cada lacuna encontrada com base nos insumos coletados na planilha de mapeamento de dados pessoais.

Por sua vez, os riscos são parametrizados de acordo com a matriz de risco elaborada pela correlação entre a probabilidade de um evento ocorrer e o seu impacto ao titular, caso o evento venha a ocorrer.

Independentemente da denominação do documento, é importante que contenha, além dos itens mínimos definidos pela estrutura normativa da organização, os seguintes elementos: 1. Identificação dos ativos e/ou processos sujeitos ao documento em questão; 2. formas de comunicação na identificação de vulnerabilidades; 3. formas de documentação das vulnerabilidades encontradas; e 4. áreas de negócio envolvidas nas atividades de identificação das vulnerabilidades .

Para que se alcance a efetividade do inventário de dados é necessário que este seja atualizado sempre que houver alteração nas estruturas mapeadas que lhe consubstanciou. O Provimento resguarda o prazo de 1 (um) ano como base temporal para que seja realizada a atualização do inventário de dados podendo acontecer antes, caso ocorra alteração no fluxo de dados.

O Inventário de Dados deve ser arquivado na própria serventia e disponibilizado em caso de solicitação da Corregedoria Geral da Justiça, da Autoridade Nacional de Proteção de Dados Pessoais ou de outro órgão fiscalizatório.

[10] BISSOLI, L; SIQUEIRA, R. **Análise de Vulnerabilidades**. In: PINHEIRO, P.P. (org.). Segurança Digital: Proteção de Dados nas Empresas. São Paulo: Atlas, 2020. p. 117-131.

4ª seção

Adequação da atividade finalística

Capítulo 4
Da revisão dos contratos

> ***Art. 8***º *A serventia deverá revisar e adequar todos os contratos que envolvam as atividades de tratamento de dados pessoais às normas de privacidade e proteção de dados pessoais, considerando a responsabilização dos agentes de tratamento prevista na lei, observando os seguintes procedimentos:*
>
> ***I -*** *revisar todos os contratos celebrados com os seus empregados, incluindo a obrigatoriedade de respeito às normas de privacidade e proteção de dados nos contratos ou em regulamentos internos;*
>
> ***II -*** *revisar os modelos existentes de minutas de contratos e convênios externos, que envolvam atividades de tratamento de dados pessoais, incluindo compartilhamento de dados;*
>
> ***III -*** *elaborar "Termos de Tratamento de Dados Pessoais" para assinatura com os operadores, sempre que possível, incluindo as informações sobre quais dados pessoais são tratados, quem são os titulares dos dados tratados, para quais finalidades e quais são os limites do tratamento;*
>
> ***IV -*** *incluir cláusulas de descarte de dados pessoais nos contratos, convênios e instrumentos congêneres, conforme os parâmetros da finalidade (pública) e necessidade acima indicados;*
>
> ***V -*** *elaborar orientações e procedimentos para as contratações futuras, no intuito de deixá-los em conformidade com a lei de regência;*
>
> ***VI -*** *criar procedimentos de auditoria regulares para realizar a gestão de terceiros com quem houver o compartilhamento de dados pessoais.*
>
> ***Art. 9º*** *Os responsáveis pelas serventias extrajudiciais deverão exigir de seus fornecedores de tecnologia, automação e armazenamento a adequação às exigências da LGPD quanto aos sistemas e programas de gestão de dados internos utilizados.*

OProvimento torna obrigatória a revisão de todas as relações com terceiros pautadas em **contratos**, seja para prestação de serviço, seja contrato de trabalho regido pela CLT, desde que correlatos a atividades que envolvam tratamento de dados pessoais.

A adaptação de contratos e demais instrumentos que impliquem no tratamento de informações é de extrema relevância para mitigar riscos e delimitar responsabilidades, uma vez que, de acordo com o art. 42 da LGPD, os agentes de tratamento são obrigados a reparar os titulares em razão de exercício de atividade que cause dano patrimonial, moral, individual ou coletivo em violação a norma brasileira de proteção de dados.

Os terceiros, muitas vezes, representam riscos do ponto de vista da proteção de dados e segurança da informação, caso os prestadores de serviços não possuam grau de conformidade adequado.

[11] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Não por outra razão, o Provimento determina que as serventias criem procedimentos de auditoria regulares para gerir a relação com terceiros que tenham acesso ao compartilhamento de dados pessoais, a fim de assegurar a vigilância das informações transferidas.

Em caso de contratos **com terceiros/operadores**, devem ser tomadas, pelo menos, as seguintes providências: 1. Regulamentar o compartilhamento dos dados pessoais; 2. Ressaltar obrigações relacionadas à segurança da informação e resposta a incidentes; 3. Delimitar responsabilidade; 4. Dever de confidencialidade; 5. Regular as ocasiões de eliminação e compartilhamento de dados pessoais; 5. Tratar sobre os direitos dos titulares; 6. Pontuar dever de cooperação e assistência; e 7. Prever a possibilidade de auditoria realizada pelo Controlador.

Em caso de contratos **com colaboradores**, deve-se adotar, ao menos, os seguintes procedimentos internos: 1. Dar ciência quanto aos dados do funcionário tratados pelo Controlador, bem como o contexto do tratamento e seus direitos com o titular; 2. Informar obrigação de seguir instruções e padrões de segurança adotados pelo Controlador; 3. Obrigação de tratar apenas os dados necessários ao exercício da função para a qual foi contratado; 4. Dever de notificar suspeita ou efetiva ocorrência de incidente de segurança com dado pessoal; e 5. Dever de confidencialidade.

Em tais contratos, deve-se, obrigatoriamente, constar **cláusulas de descarte de dados pessoais**, não podendo haver retenção de dados pessoais por prazo indefinido, salvo nas situações previstas no próprio contrato ou respaldadas em lei ou norma regulatória. Nesse sentido, há, inclusive, parâmetros fixados pelo **Provimento 50/2015 do CNJ** para descarte de dados contidos em documentos do acervo registral.

Em caso de fornecedores de sistemas de tecnologia, automação e armazenamento, o Provimento impõe que se exija o atendimento dos requisitos da LGPD, notadamente quanto às medidas técnicas de segurança, correlacionando-se com o **Provimento nº 74/2018 do CNJ**.

Por fim, a elaboração de orientações e procedimentos para as contratações futuras, no intuito de deixá-los em conformidade com a lei de regência, demonstra o nível de comprometimento e aculturamento organizacional quanto aos cuidados a serem empregados no tratamento de dados pessoais custodiados.

5.

Do Encarregado

> ***Art. 10.*** *Deverá ser designado o encarregado pelo tratamento de dados pessoais, conforme o disposto no art. 41 da LGPD, consideradas as seguintes particularidades:*
>
> ***I -*** *os responsáveis pelas Serventias Extrajudiciais poderão terceirizar o exercício da função de Encarregado mediante a contratação de prestador de serviços, pessoa física ou pessoa jurídica, desde que apto ao exercício da função;*
>
> ***II -*** *a função do Encarregado não se confunde com a do responsável pela delegação dos serviços extrajudiciais de notas e de registro;*
>
> ***III -*** *a nomeação do Encarregado será promovida mediante contrato escrito, a ser arquivado em classificador próprio, de que participarão o controlador na qualidade de responsável pela nomeação e o Encarregado; e*
>
> ***IV -*** *a nomeação de Encarregado não afasta o dever de atendimento pelo responsável pela delegação dos serviços extrajudiciais de notas e de registro, quando for solicitado pelo titular dos dados pessoais.*

O Provimento se alinha ao disposto na LGPD ao trazer a obrigatoriedade de nomeação de um Encarregado pelo Tratamento de Dados Pessoais, apontando ainda parâmetros para a sua efetivação.

É oportuno relembrar que se defere às serventias extrajudiciais o mesmo tratamento destinado ao Poder Público por expressa menção do art. 23, §4º da LGPD, de forma tal que não se aplica no âmbito dos serviços delegados a Resolução CD/ANPD n. 2 de 27 de janeiro de 2022 , que estabeleceu um Regulamento de aplicação da LGPD para agentes de pequeno porte. Dessa forma, também não se aplica a dispensa de Encarregado a que se refere a supracitada resolução.

À luz das determinações do art. 41, § 2º, da LGPD, as **principais obrigações do encarregado** são: a) dever de sigilo ou de confidencialidade no exercício das suas funções; b) administrar as reclamações e comunicações dos titulares de dados pessoais, incluindo o dever de prestar esclarecimentos e adotar as providências cabíveis; c) administrar as comunicações da ANPD e as demais entidades fiscalizadoras, a exemplo das Corregedorias de Justiça locais e o Conselho Nacional de Justiça (CNJ); d) orientar os funcionários do controlador quanto às melhores práticas para a proteção dos dados pessoais; e e) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O Provimento também se coaduna às múltiplas possibilidades de constituição e personalidade do Encarregado, podendo ser pessoa física interna ao quadro de colaboradores da serventia, ou ainda, pessoa física ou jurídica externa ao cartório, denominada ***DPO as a service.***

O Provimento se alinha ao disposto pela ANPD que, em seu Guia de Agentes de Tratamento dispõe: *"Considerando as boas práticas internacionais, o encarregado pode-*

[12] Art. 23. § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

[13] GOV.BR. **Resolução CD/ANPD, nº 2, de 27 de janeiro de 202**2. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 25 de outubro de 2022.

rá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica".

É obrigatória a constituição de Encarregado através de **contrato escrito** firmado entre o responsável pela delegação e a pessoa que figurará como DPO, arquivado em classificador próprio, diferentemente do que dispõe o Guia Orientativo da ANPD , que permite a nomeação por contrato de prestação de serviço ou ato administrativo.

Caso seja nomeada para a função pessoa que já é **funcionária da serventia**, deve ser feita a devida formalização contratual quanto exercício das suas novas atribuições, tarefas estas distintas da contratação inicialmente posta.

Os Encarregados internos com contratos regidos pelas normas da CLT deverão ter a qualificação registrada em livros e sistemas eletrônicos dos empregadores, em atenção às orientações do Ministério do Trabalho, com devida anotação em contrato de trabalho, ajuste contratual e anotação na CTPS, seguindo a orientação da CBO (Classificação Brasileira de Ocupações). Segundo esta Classificação, Encarregado é sinônimo de DPO.

A formalização contratual pode se dar por meio de aditivo contratual ou mediante a criação de um novo contrato de nomeação de Encarregado, o qual tece as atribuições vinculadas à função direcionada e evita a configuração de desvio de função.

Em relação à nomeação de **Pessoa Física ou Jurídica externa ao quadro da serventia** para função de Encarregado, a terceirização é possível mediante a contratação de prestador de serviços, pessoa física ou pessoa jurídica, desde que apta ao exercício da função, a exemplo de profissionais autônomos, escritórios de advocacia e consultorias em segurança da informação.

Não há necessidade legal de certificação específica para ser Encarregado. Trata-se de posição discricionária da organização no âmbito da prestação de contas e responsabilização (*accountability*). A LGPD não dispõe sobre critérios de restrição para nomeação de Encarregado e não define o nível necessário de competência de conhecimentos específicos para a realização de suas atribuições.

No direito comparado é comum a exigência de que a organização registre o seu Encarregado junto à autoridade supervisora, obrigação esta não prevista na LGPD, porém, nada impede que a ANPD ou o CNJ, setorialmente, venha a impor tal regra.

Como medida acautelatória, recomenda-se que o Encarregado, ao ser nomeado, seja uma pessoa que detenha conhecimento e experiência em Privacidade e Proteção de Dados Pessoais, a fim de evitar tratamento inadequado ou atuação não profissional no exercício de suas funções.

> ***Art. 10.*** *(...)*
>
> *§1° Serventias classificadas como "Classe I" e "Classe II" pelo Provimento n. 74, de 31 de julho de 2018, da Corregedoria Nacional de Justiça, poderão designar Encarregado de maneira conjunta.*
>
> ***§ 2°*** *A nomeação e contratação do Encarregado de Proteção de Dados Pessoais pelas Serventias será de livre escolha do titular da Serventias, podendo, eventualmente, ser realizada de forma conjunta, ou ser subsidiado ou custeado pelas entidades de classe.*

[14] Sobre o tema, é interessante ressaltar a visão extensiva da doutrina, que consubstanciou o Enunciado n. 680 da IX Jornada de Direito Civil do Conselho de Justiça Federal: "A Lei Geral de Proteção de Dados Pessoais não exclui a possibilidade de nomeação pelo controlador de pessoa jurídica, ente despersonalizado ou de mais de uma pessoa natural para o exercício da função de encarregado pelo tratamento de dados pessoais".

[15] ANPD. **Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em: 26 de outubro de 2022.

> ***§ 3º*** *Não há óbice para a contratação independente de um mesmo Encarregado por serventias de qualquer Classe, desde que demonstrável a inexistência de conflito na cumulação de funções e a manutenção da qualidade dos serviços prestados.*

Atentando-se à realidade econômica das serventias extrajudiciais, o Provimento flexibilizou as regras atinentes à nomeação de Encarregado pelo Tratamento de Dados Pessoais, facultando às serventias de Classe I e Classe II a sua **realização conjunta**.

À luz do Provimento nº 74, de 2018, do CNJ, são consideradas serventias de Classe I aquelas com arrecadação de até R$ 100 mil por semestre, e de Classe II aquelas com arrecadação entre R$ 100 mil e R$ 500 mil por semestre.

Outra possibilidade aberta pelo Provimento é o subsídio de Encarregado por entidade de classe, o que remete a participação ativa e relevante desse segmento no programa de adequação.

Por fim, há possibilidade de contratação conjunta de Encarregado por mais de uma serventia, desde que não haja conflito de interesses na cumulação de funções e a manutenção da funcionalidade do Encarregado.

6.

Do relatório de impacto

> ***Art. 11.*** *Ao responsável pela serventia incumbe cuidar para que seja realizado relatório de impacto à proteção de dados pessoais referente aos atos em que o tratamento de dados pessoais possa gerar risco às liberdades civis e aos direitos fundamentais do titular, de acordo com as orientações expedidas pela ANPD. A elaboração do Relatório deverá se atentar às seguintes instruções:*
>
> ***I –*** *adotar metodologia que resulte na indicação de medidas, salvaguardas e mecanismos de mitigação de risco;*
>
> ***II –*** *elaborar o documento previamente a contrato ou convênio que seja objeto da avaliação feita por meio do Relatório;*
>
> ***III –*** *franquear, a título de transparência, aos afetados a possibilidade de se manifestarem a respeito do conteúdo; e*
>
> ***IV –*** *elaborar o documento previamente à adoção de novos procedimentos ou tecnologias.*

Outro instrumento de adequação trazido pelo Provimento é o **Relatório de Impacto à Proteção de Dados Pessoais – RIPD**, que concretiza a documentação acerca dos riscos aos direitos fundamentais do titular eventualmente suportados em função do Tratamento de Dados Pessoais.

Como estabelecido na LGPD, o RIPD é a "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".

O Relatório de Impacto à Proteção de Dados possui um rol não exaustivo de situações em que poderá ou será requerido:

- *para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º, LGPD);*
- *quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados, LGPD); e*
- *ao controlador, a qualquer momento, sob determinação da ANPD, quando se tratar de interesse legítimo ou dados pessoais sensíveis, referente a suas operações de tratamento de dados, observados os segredos comercial e industrial. (art. 38, LGPD).*

Além de tais situações, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer repercussão na privacidade dos dados pessoais, resultante de:

- *uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;*
- *rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);*

- *tratamento de dado pessoal sobre "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" (LGPD, art. 5º, II);*
- *processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);*
- *tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);*
- *tratamento de dados que possam resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);*
- *tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);*
- *tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);*
- *alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e*
- *reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.*

Alinhado com o disposto no Provimento, o RIPD tem seu escopo estruturado em: 1. descrever a natureza, escopo, contexto e finalidades do processamento; 2. avaliar a necessidade, proporcionalidade e medidas de conformidade; 3. identificar e avaliar riscos para indivíduos; e 4. identificar quaisquer medidas adicionais para mitigar esses riscos.

A par da considerações citadas, cumpre-nos dar conhecimento do teor do enunciado 679 aprovado na IX Jornada de Direito Civil, segundo o qual: "O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de *accountability* para qualquer operação de tratamento de dados considerada de alto risco, tendo sempre como parâmetro o risco aos direitos dos titulares".

Essa orientação preenche lacuna da redação da LGPD ao não disciplinar o momento de realização do citado relatório: se antes ou após a solicitação emitida pela ANPD. A elaboração antecipada desse documento evidencia a boa-fé do agente de tratamento (Controlador) ao tratar informações que gerem ao titular relevante risco.

O texto deixa dúvidas a respeito da possibilidade franqueada aos afetados pelo tratamento, a título de transparência, de se manifestarem sobre o conteúdo do RIPD. Não está claro o tipo de manifestação, nem a extensão, objetivamente, da sua influência no Relatório. Espera-se que a Comissão de Proteção de Dados do CNJ venha a regulamentar tal ponto.

7.

Das medidas de segurança, técnicas e administrativas

> ***Art. 12.*** *Cabe ao responsável pelas serventias implementar 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, nos termos dos arts. 46 e seguintes da LGPD, por meio de:*
>
> ***I –*** *elaboração de política de segurança da informação que contenha:*
>
> ***a)*** *medidas de segurança técnicas e organizacionais;*
>
> ***b)*** *previsão de adoção de mecanismos de segurança, desde a concepção de novos produtos ou serviços (security by design) (art. 46, § 1º, da LGPD); e*
>
> ***c)*** *plano de resposta a incidentes (art. 48 da LGPD).*
>
> ***II –*** *avaliação do sistemas e bancos de dados em que houver tratamento de dados pessoais e/ou tratamento de dados sensíveis, submetendo tais resultados à ciência do Encarregado pelo tratamento de dados pessoais da serventia;*
>
> ***III –*** *avaliação da segurança de integrações de sistemas;*
>
> ***IV –*** *análise da segurança das hipóteses de compartilhamento de dados pessoais com terceiros; e*
>
> ***V –*** *realização de treinamentos.*

Seguindo-se nos instrumentos de adequação, o Provimento também prevê a obrigatoriedade de tomada de medidas técnicas e administrativas que preservem a segurança dos dados contra qualquer tipo de **tratamento irregular**.

São exemplos de tratamentos irregulares os acessos não autorizados ou desalinhados com o ecossistema de proteção de dados pessoais, bem como as situações acidentais ou voluntárias de deterioramento ou alteração substancial dos dados pessoais. Essas situações representam o incidente de segurança.

A concretização do princípio da Segurança (art. 6º, VII, LGPD) pressupõe a **integridade, disponibilidade e confidencialidade** dos dados, de forma tal que estes devem estar sempre hígidos, íntegros, sem alteração na sua substância, disponíveis para a operação a que se destina e confidenciais, isto é, devem apenas ser acessados por pessoa autorizada.

A redação e os incisos do artigo em comento se alinham à orientação publicizada pela ANPD no Guia sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte . Ao traçar o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação, o Guia já traz à baila o entendimento da ANPD a respeito das boas práticas na área. Esse conjunto de ações impacta todo o ambiente institucional, com objetivo de prevenir, detectar e combater as ameaças digitais.

[16] ANPD. **Guia Orientativo "Segurança da Informação para Agentes de Tratamento de Pequeno Porte"**. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 28 de outubro de 2022.

Setorialmente, o Provimento nº 74/2018 do CNJ dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil.

Nessa normativa, há a determinação de criação de plano de continuidade de negócios que preveja ocorrências nocivas ao regular funcionamento dos serviços e atendimento às normas de interoperabilidade, legalidade e recuperação a longo prazo na prática dos atos e comunicações eletrônicas.

Nesse esteio, a Política Interna de Segurança da Informação é o instrumento que consubstancia as diretrizes necessárias para o atendimento da segurança dos dados, no escopo do tripé supramencionado, coordenando as medidas, responsabilidades e prerrogativas na preservação desse princípio.

A adequação efetiva dos requisitos previstos na LGPD exige a instalação de um Sistema de Gestão apropriado às finalidades da Lei Geral e ao estágio organizacional e econômico de cada instituição, configurando assim o **Sistema de Gestão de Cibersegurança e Segurança da Informação (SGCSI)**.

A Política de Segurança da Informação, ou **Sistema de Gestão de Cibersegurança**, pressupõe o ordenamento em quatro grupos de controles, a saber: 1. Estruturação do SGCSI; 2. Implantação do SGCSI; 3. Manutenção do SGCSI e; 4. Execução do SGCSI.

Faz-se necessário realizar uma estruturação inicial antes que se possa realizar a sua implantação. Esta deve ser faseada no tempo, respeitando os direcionadores de negócio da instituição.

A manutenção do SGCSI é uma demanda natural, porque a instituição se altera em: novas estruturas organizacionais, novos negócios e novas práticas que precisam ser incorporadas. Para os processos ou áreas em que o SGCSI já está implantado, deve-se executar conforme previamente estabelecido .

O Provimento também traz à luz a necessidade de atendimento a mecanismos de segurança desde a concepção, denominado ***Privacy By Design*** *(Privacidade por Desenho). O privacy by design é uma metodologia preventiva, pela qual a privacidade se parametriza no tripé de: (i) gestão dos sistemas de tecnologia informação (IT systems); (ii) práticas negociais responsáveis (accountable business practices); e (iii) gestão do design físico e infraestrutura de rede (physical and networked infrastructure).*

A adoção do *Privacy By Design* se apresenta conjuntamente com as necessárias avaliações dos sistemas informáticos de uso interno e de compartilhamento de dados, levando a privacidade em conta durante todo o processo de implementação e execução de atividades.

Outro instrumento concernente à segurança dos dados é o **Plano de Resposta a Incidentes** envolvendo dados pessoais. Este documento integra o rol de exigências coadunadas à Política de Segurança da Informação e se caracteriza por estabelecer procedimentos para preparar a organização em caso de ameaças ou violações aos dados pessoais dos titulares. É utilizado nas situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Recomenda-se que o Plano preveja a criação de um **Comitê de Resposta a Incidentes (CRI)**, bem como formas de detecção dos indícios de ocorrência de um incidente de segurança envolvendo dados pessoais, de informação ao controlador e de notificação do Encarregado, para que este possa acionar o Comitê.

[17] GARCIA, L.R.; AGUILERA-FERNANDES, E.; GONÇALVES, R.A.M.; PEREIRA-BARRETO, M. R. **Lei Geral de Proteção de Dados: Guia de Implementação.** São Paulo: Blucher, 2020, p. 48.

[18] VAINZOF, Rony. **Artigo 6º**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 135-178.

Caso a serventia não possua recursos humanos para estruturação do CRI, a apuração interna do incidente se dará pelo Encarregado, que poderá acionar os colaboradores do setor afetado para compreensão da extensão do suposto incidente de segurança.

O CRI exercerá as seguintes atribuições, sob supervisão do Encarregado: 1. Coordenar o cumprimento e a evolução da maturidade do processo de gestão de incidentes de segurança da organização; 2. Propor medidas de aperfeiçoamento dos p rocessos e de proteção dos ativos envolvidos em operações de tratamento de dados pessoais; e 3. Zelar, sempre que lidar com a ocorrência de incidentes de segurança da informação, pela restauração dos serviços afetados com a maior brevidade possível, de forma a minimizar os prejuízos à serventia e demais envolvidos.

O Plano descreve também a metodologia de apuração do incidente, as hipóteses e prazo de comunicação do evento ao Juiz Corregedor Permanente, às Corregedorias de Justiça e à Autoridade Nacional de Proteção de Dados (ANPD).

Há instruções para que sejam adotadas as providências pertinentes à contenção e erradicação do incidente, viabilizando as medidas técnicas necessárias para limitar o dano e evitar mais prejuízos aos titulares dos dados pessoais.

A preparação refinada dos colaboradores em situações envolvendo segurança da informação perpassa pelo processo de implementação de campanhas de conscientização e treinamento direcionadas a todos da serventia, sendo medida de boa prática a participação, nesse projeto, de terceiros e fornecedores externos.

> ***Art. 13.*** *O plano de resposta a incidentes de segurança envolvendo dados pessoais deverá prever a comunicação, pelos responsáveis por serventias extrajudiciais, ao titular, à Autoridade Nacional de Proteção de Dados, ao Juiz Corregedor Permanente e à Corregedoria Geral da Justiça, no prazo máximo de 48 horas úteis, contados a partir do seu conhecimento, de incidente que possa acarretar risco ou dano relevante aos titulares, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.*
>
> *O Provimento uniformizou os prazos de comunicação de incidentes envolvendo dados pessoais, definindo o lapso de 48 horas úteis como tempo máximo para a referida comunicação às autoridades competentes. Muitos dos provimentos das Corregedorias Gerais do Tribunais dos estados determinavam que o juiz corregedor permanente e a Corregedoria-Geral da Justiça deveriam ser informados em até 24 horas úteis.*

A previsão do Provimento se coaduna com a orientação da ANPD[19] , uma vez que a LGPD não definiu expressamente o prazo máximo, mas apenas que a comunicação deve acontecer em prazo razoável.

[19] GOV.BR. **Comunicação de Incidente de Segurança**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em: 30 de outubro de 2022.

[20] ARTICLE 29 WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> Acesso em 22 de novembro de.2022.

[21] ANPD. Comunicação de Incidente de Segurança. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>. Acesso em 22 de novembro.2022.

[22] Ibidem.

[23] Ibidem.

Pela leitura atenta do artigo *in voga*, a proteção dos dados pessoais não se destina a quaisquer incidentes de segurança, mas tão somente àqueles que, de fato, configurem "violações de dados pessoais", terminologia esta utilizada pelo GDPR.

Bebendo da fonte da Opinião do *Working Party* [29], as violações de dados pessoais podem ser classificadas de acordo com os tradicionais princípios de segurança: (i) violação da confidencialidade - em que há acidental ou não autorizada divulgação ou acesso de dados pessoais; (ii) violação de integridade - em que há incidental ou não autorizada alteração de dados pessoais; e (iii) violação de disponibilidade - em que há acidental ou não autorizada perda de acesso ou destruição de dados pessoais .

A ANPD em seu sítio eletrônico qualifica incidente de segurança envolvendo dados pessoais como:

> *(...) qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulta 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*[22].

Sendo assim, não havendo risco ou dano relevante, não há necessidade de comunicação aos autores mencionados no artigo, embora seja medida de boa prática o registro do incidente de segurança.

Agora, estando-se diante de violação que efetivamente acarrete prejuízo aos titulares e que estarão sujeitas ao dever de notificação, tal providência deverá ser adotada. Nesse tocante, posicionou-se a ANPD:

> *Critérios mais objetivos serão objeto de futura regulamentação e não poderão ser aqui exigidos sob pena de se inovar na LGPD. De toda forma, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados*[23].

Com base na experiência internacional, o GDPR afere os potenciais prejuízos decorrentes de violações de dados pessoais, cuja probabilidade e gravidade variam, de acordo com a Consideranda 85:

> *Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar* ***danos físicos, materiais ou imateriais*** *às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. (Grifos nossos)*

> ***Art. 14.*** *A inutilização e eliminação de documentos em conformidade com a Tabela de Temporalidade de Documentos prevista no Provimento n. 50/2015, da Corregedoria Nacional de Justiça, será promovida de forma a impedir a identificação dos dados pessoais neles contidos.*
>
> ***Parágrafo único.*** *A inutilização e eliminação de documentos não afasta os deveres previstos na Lei n. 13.709, de 14 de agosto de 2018, em relação aos dados pessoais que remanescerem em índices, classificadores, indicadores, banco de dados, arquivos*

> *de segurança ou qualquer outro modo de conservação adotado na unidade dos serviços extrajudiciais de notas e de registro.*
>
> ***Art. 15.*** *O responsável pela serventia extrajudicial, sempre que possível:*
>
> ***I –*** *digitalizará os documentos físicos ainda utilizados; e*
>
> ***II –*** *armazenará os documentos físicos que contenham dados pessoais e dados pessoais sensíveis em salas ou compartimentos com controle de acesso.*
>
> ***Parágrafo único.*** *Após a digitalização, o documento físico poderá ser eliminado, respeitados as disposições e os prazos definidos no Provimento n. 50, de 28 de setembro de 2015, da Corregedoria Nacional de Justiça.*

O Provimento aborda a possibilidade de descarte de dados pessoais nas situações contempladas no Provimento nº 50/2015 do CNJ, sinalizando o ciclo de vida deles dentro da serventia extrajudicial.

O descarte é, portanto, uma medida técnica e organizacional que assegura que os dados não terão um uso secundário em dissonância às expectativas dos seus respectivos titulares ou a realização de tratamento por tempo indeterminado, quando assim não deva ocorrer, excepcionando-se a guarda por tempo permanente legalmente prevista.

O término do tratamento de dados se compatibiliza com o disposto no art. 15 da LGPD, que expõe:

> ***Art. 15.*** *O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:*
>
> ***I -*** *verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;*
>
> ***II -*** *fim do período de tratamento;*
>
> ***III -*** *comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou*
>
> ***IV -*** *determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.*

O término do tratamento de dados pessoais contidos em arquivos físicos se subsome à "verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada".

Importante lembrar que o acervo físico das serventias possui prazos de guarda de documentos regidos pelo Provimento nº 50/2015. Dessa forma, não existindo mais obrigatoriedade de guarda, uma vez que ultrapassado os prazos dispostos no citado Provimento nº 50/2015, exaure-se a finalidade do tratamento.

A guarda do acervo da serventia é também reforçada pelo Provimento, que constitui medida técnica de observância obrigatória, consubstanciada no estabelecimento de controle de acesso aos arquivos físicos do cartório e na digitalização de tais documentos.

Essa segmentação de acesso traduz medida impeditiva de acesso aos colaboradores ou terceiros contratados que não necessitam ter o conhecimento das informações ali armazenadas para o ofício de suas atribuições ou funcionalidades.

8.

Do Treinamento

> ***Art. 16.*** *As serventias deverão realizar treinamentos para implementação da cultura de privacidade e proteção de dados pessoais, bem como para a capacitação de todos os envolvidos no tratamento dos dados pessoais sobre os novos controles, processos e procedimentos, observando o seguinte:*
>
> ***I –*** *capacitar todos os trabalhadores da serventia a respeito dos procedimentos de tratamento de dados pessoais;*
>
> ***II –*** *realizar treinamentos com todos os novos trabalhadores;*
>
> ***III –*** *manter treinamentos regulares, de forma a reciclar o conhecimento sobre o assunto e atualizar os procedimentos adotados, sempre que necessário;*
>
> ***IV –*** *organizar, por meio do Encarregado e eventual equipe de apoio, programa de conscientização a respeito dos procedimentos de tratamento de dados, que deverá atingir todos os trabalhadores; e*
>
> ***V –*** *manter os comprovantes da participação em cursos, conferências, seminários ou qualquer modo de treinamento proporcionado pelo controlador aos operadores e Encarregado, com indicação do conteúdo das orientações transmitidas.*
>
> ***Parágrafo único.*** *O responsável pela serventia extrajudicial poderá solicitar apoio à entidade de classe para capacitação de seus prepostos.*

Seguindo-se no passo a-passo aduzido no art. 6º do Provimento, este também cuidou de ressaltar os parâmetros em que se dará por efetiva a obrigação de "treinar e capacitar os prepostos".

A cultura organizacional em Proteção de Dados Pessoais deve ser implantada desde a base, treinando-se os colaboradores a respeito de todas as técnicas e medidas necessárias à correta implementação da LGPD.

Os treinamentos de equipe em qualquer Programa de *Compliance* em Proteção de Dados são fundamentais para percepção, absorção e aplicação das alterações organizacionais promovidas. Faz-se necessário fortalecer a cultura organizacional de conformidade para que o Programa seja, de fato, efetivo.

Os valores e as linhas gerais sobre as políticas e os procedimentos adotados pela organização devem ser claros e acessíveis a todos os colaboradores. A organização deve ter um plano de capacitação estruturado com o objetivo de treinar os funcionários e gestores acerca da aplicação de regras de medidas de segurança da informação, bem como elucidar os conceitos legais e deveres previstos na LGPD.

Deve-se investir em materiais educativos, a exemplo de cartilhas, guias e folders para absorção do conteúdo e materialização do Programa pelos colaboradores, com o objetivo de fortalecer a cultura de privacidade desde a concepção dos processos e procedimentos internos (*privacy by design*).

O Provimento também torna obrigatório o registro dos treinamentos e dos materiais educativos elaborados, visto que este é um mecanismo de comprovação dos esforços e das evidências de implementação do Programa de *Compliance* em Proteção de Dados acaso correições ou investigações sejam realizadas pela ANPD, Corregedorias, Juízes Corregedores ou autoridades de fiscalização.

9.

Das medidas de transparência e atendimento a Direitos de Titulares

> ***Art. 17.*** *Como medida de transparência e prezando pelos Direitos dos Titulares de dados, deverá o responsável pela serventia elaborar, por meio do canal do próprio Encarregado, se terceirizado, e/ou em parceria com as respectivas entidades de classe:*
>
> ***I –*** *canal eletrônico específico para atendimento das requisições e/ou reclamações apresentadas pelos titulares dos dados pessoais; e*
>
> ***II –*** *fluxo para atendimento aos direitos dos titulares de dados pessoais, requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.*

Outra medida eleita pelo Provimento na aplicação da LGPD nas serventias extrajudiciais é o atendimento de solicitações e requerimentos dos titulares. À luz desse artigo, a serventia deve dispor de fluxo de trabalho específico para o atendimento de requisições dos titulares de dados no tocante aos **direitos por eles titularizados por força da LGPD**.

A LGPD e o Provimento não trouxeram a forma quanto à operacionalização do processamento de solicitações feitas pelos titulares de dados pessoais, de modo que a indicação de um canal eletrônico específico para atendimento das requisições ou reclamações se espelha na prática adotada pelo GDPR.

A prática internacional sinaliza a criação de um canal próprio para a coleta de solicitações a partir da disponibilização de formulário no sítio eletrônico da organização, endereço postal ou eletrônico dedicado ou, mesmo, linha telefônica.

Após essas providências, o processo ocorre de forma manual e semiestruturada, contando com buscas e efetivação de ações de forma manual em sistemas e bases. Estimando-se alto volume de solicitações, busca-se por ferramentas de mercado que automatizam e aumentam a capacidade de gestão do atendimento de solicitações dessa natureza .

Quanto aos Direitos dos titulares de Dados, estes se encontram fixados no art. 18 da LGPD:

> ***Art. 18.*** *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;*

[24] PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. ***Compliance* Digital e LGPD**. Coleção *Compliance*, Volume V, São Paulo: Thomson Reuters Brasil, 2021, p.262/263.

> ***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.*

É importante ressaltar que esses direitos não são aplicados em sua integralidade aos **serviços públicos notariais e de registro**, merecendo a necessária mitigação de alguns deles, a citar, o direito de acesso, de portabilidade ou exclusão de informações, dada a natureza pública de sua atividade finalística.

> ***Art. 18.*** *Deverão ser divulgadas em local de fácil visualização e consulta pelo público as informações básicas a respeito dos dados pessoais e procedimentos de tratamento, os direitos dos titulares dos dados, o canal de atendimento disponibilizado aos titulares de dados para que exerçam seus direitos e os dados de qualificação do encarregado, com nome, endereço, e meios de contato.*
>
> ***Art. 19.*** *Deverão ser disponibilizadas pelos responsáveis pelas serventias informações adequadas a respeito dos procedimentos de tratamento de dados pessoais, nos termos do art. 9º da LGPD, por meio de:*
>
> ***I –*** *aviso de privacidade e proteção de dados;*
>
> ***II –*** *avisos de cookies no portal de cada serventia, se houver; e*
>
> ***III –*** *aviso de privacidade para navegação no website da serventia, se houver.*

O Provimento instrumentaliza a publicização de elementos essenciais sobre o tratamento realizado pela serventia e os meios de comunicação para exercício dos Direitos dos Titulares.

Prestigiou-se a transparência, eleita como princípio da Proteção de Dados Pessoais, bem como o princípio da autodeterminação informativa do titular de dados pessoais (controle pessoal do trânsito de dados sob sua titularidade). A publicização da figura do Encarregado também se coaduna com o disposto expressamente pela LGPD (art. 41 § 1º).

Ainda em atenção ao paradigma da transparência, o Provimento torna obrigatória a elaboração de instrumentos de política interna de privacidade, avisos de privacidade e de cookies voltados ao público externo da serventia.

A Política de Privacidade e Proteção de Dados Pessoais (*Privacy Policy*) visa nortear todo o tratamento de dados pessoais que ocorrer no âmbito da organização sendo fruto da materialização do processo de mapeamento de dados, com o objetivo assegurar o princípio da transparência e permitir o exercício dos direitos dos titulares dos pessoais, nos termos do art. 6º, VI e art. 18 e seguintes da LGPD.

A Política interna tem **função organizacional**, disposta a direcionar ações no contexto das atividades de uma organização por meio da definição de princípios, regras, obrigações, proibições, responsabilidades, funções, procedimentos, protocolos e guias.

No contexto da privacidade, a Política tem por escopo direcionar ações no sentido da adequação à LGPD, e conformidade. A própria LGPD estabelece a Política como inserto em um programa de governança em privacidade, desde que elaborada com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, §2º, I, "d", LGPD).

A Política deve contemplar as principais categorias de dados pessoais tratados pela organização, as atividades desempenhadas que envolvam utilização de dados pessoais e as suas finalidades específicas, bem como o contexto das operações, os respaldos legais e a duração do tratamento das informações.

Precisa se debruçar, também, sobre os direitos dos titulares, além de explicar as hipóteses de compartilhamento e eliminação dos dados, atentando-se, para tanto, às regras estabelecidas pela própria LGPD e pelas legislações específicas que regulam a atividade.

Com o objetivo de permitir a ciência dos titulares acerca do tratamento das suas informações pessoais, deve-se ter em mente os seguintes questionamentos no momento da elaboração deste documento:

- *Quais são as principais categorias de dados tratados pela organização e as suas finalidades específicas?*
- *Quais são as bases legais que norteiam o tratamento dos dados pessoais?*
- *Qual é o tempo de guarda das informações tratadas pela organização?*
- *Existe coleta de cookies? Em caso positivo, quais?*
- *Quais direitos os titulares de dados podem exercer perante a organização?*
- *Existe compartilhamento de dados pessoais dos titulares com outras organizações? Em caso positivo, quais dados são compartilhados e para quais finalidades específicas?*
- *Existe transferência internacional de dados pessoais?*
- *Quais são as boas práticas e orientações de segurança da informação realizadas pela organização para proteção dos titulares?*

O Aviso de Privacidade (*Privacy Notice*), a seu turno, tem por escopo a comunicação com indivíduos externos à organização quando se vincularem como Titulares de Dados Pessoais tratados pelo controlador.

Trata-se da concretização do princípio da Transparência (art. 6º, VI, LGPD), apontando substancialmente as operações que demandam tratamento de dados pessoais, os direitos dos titulares e como exercitá-los, o compartilhamento de dados, e demais detalhes que se fizerem pertinentes.

A construção do Aviso de Privacidade pouco difere da Política de Privacidade, uma vez que ambas compartilham do dever de transparência, com o fito de informar o titular sobre elementos essenciais do tratamento realizado com os seus dados pessoais, e viabilizar o exercício dos seus direitos.

Contudo, a Política de Privacidade (*Privacy Policy*) **possui um espectro mais amplo de funções** e mais robusto em suas abordagens e informações ali contidas, destinando-se a organizar e dirigir a tomada de decisões e o fluxo de informações no que se refere aos processos internos à instituição que envolvam dados pessoais.

O Aviso de Privacidade (*Privacy Notice*), por sua vez, destina-se a ser mais sucinto e objetivo, com linguagem simples e clara, tendo em vista o público amplo e diverso que pretende atingir.

> ***Art. 20.*** *A gratuidade do livre acesso dos titulares de dados (art. 6º, IV, da LGPD) será restrita aos dados pessoais constantes nos sistemas administrativos da serventia, não abrangendo os dados próprios do acervo registral e não podendo, em qualquer hipótese, alcançar ou implicar a prática de atos inerentes à prestação dos serviços notariais e registrais dotados de fé-pública.*
>
> ***§ 1º*** *Todo documento obtido por força do exercício do direito de acesso deverá conter em seu cabeçalho os seguintes dizeres: "Este não é um documento dotado de fé pública, não se confunde com atos inerentes à prestação do serviço notarial e registral nem substitui quaisquer certidões, destinando-se exclusivamente a atender aos direitos do titular solicitante quanto ao acesso a seus dados pessoais".*
>
> ***§ 2º*** *A expedição de certidões deverá ser exercida conforme legislação específica registral e notarial e taxas e emolumentos cobrados conforme regulamentação própria.*
>
> ***§ 3º*** *Mantém-se o disposto quanto aos titulares beneficiários da isenção de emolumentos, na forma da lei específica.*
>
> ***§ 4º*** *O notário e/ou registrador coletarão as informações necessárias para identificação segura do solicitante, com o objetivo de garantir a confidencialidade.*

A Lei Geral de Proteção de Dados estabelece em seu art. 18, § 5º, a **gratuidade** do exercício de direitos do titular, "nos prazos e nos termos previstos em regulamento". A esse respeito, o Provimento trouxe a regulamentação desse exercício, relacionando-o à diferenciação de tratamento de dados pela serventia em suas atribuições administrativas e finalísticas.

Como bem ressaltado pelo Provimento, a gratuidade do livre acesso dos titulares de dados será restrita aos dados pessoais constantes nos sistemas administrativos da serventia, quais sejam, por exemplo, informações utilizadas para contratação de colaboradores e prestadores de serviço, banco de currículos ou para envio de newsletter para usuários dos serviços da serventia.

Como visto alhures, esses direitos guardam particularidades e mitigações em seu exercício, dada a natureza pública das informações levadas a registro, inclusive no que diz respeito à gratuidade de seu exercício. A prestação de serviços delegados continua submetida às normas próprias quanto à cobrança de emolumentos.

Neste sentido, não poderá o titular dos dados pessoais se valer da regra, por exemplo, para pedir uma cópia de seu indicador pessoal. Isso porque o livro 5 (indicador pessoal) está previsto como um dos livros da atividade fim do registro de imóveis, conforme art. 173, V da Lei de Registros Públicos.

A informação desses dados pessoais é obtida através de certidão, pois implica em busca no acervo cartorial relacionada à sua atividade fim, a qual, por força da legislação de regência dos emolumentos, deverá ter as custas recolhidas.

Pondo-se em foco essa diferenciação, cabe ao notário e registrador, ao fornecer documentos relacionados aos direitos dos titulares de dados (quando gratuitamente permitida informação), explicitar que *"este não é um documento dotado de fé pública, não se confunde com atos inerentes à prestação do serviço notarial e registral nem substitui quaisquer certidões, destinando-se exclusivamente a atender aos direitos do titular solicitante quanto ao acesso a seus dados pessoais"* em cabeçalho.

4ª seção

Adequação da atividade finalística

Capítulo 10
Das certidões e compartilhamento e dados com centrais e órgãos públicos

> ***Art. 21.*** *Na emissão de certidão o Notário ou o Registrador deverá observar o conteúdo obrigatório estabelecido em legislação específica, adequado e proporcional à finalidade de comprovação de fato, ato ou relação jurídica.*
>
> ***Parágrafo único.*** *Cabe ao Registrador ou Notário, na emissão de certidões, apurar a adequação, necessidade e proporcionalidade de particular conteúdo em relação à finalidade da certidão, quando este não for explicitamente exigido ou quando for apenas autorizado pela legislação específica.*
>
> ***Art. 22.*** *Em caso de requerimento de certidões por via telemática, havendo necessidade de justificação do interesse na certidão, o solicitante será identificado por meio idôneo, reconhecido pela entidade responsável pela tramitação do serviço eletrônico compartilhado da respectiva especialidade cartorial.*

O Provimento também altera alguns aspectos da própria atividade finalística da serventia ante a imperiosidade de atendimento dos princípios norteadores do tratamento de dados pessoais esculpidos na LGPD.

A atividade cartorária é precipuamente uma atividade de manipulação de dados pessoais em função do cumprimento de obrigações legais assumidas pelo serventuário.

Dessa forma, a atuação do notário e registrador também necessita da pertinente observância dos princípios para tratamento de dados pessoais, notadamente quanto à **finalidade**[25] , à **adequação**[26] e à **necessidade**[27].

O Provimento orienta ao delegatário que na emissão de certidão cujo conteúdo não seja expressamente definido em norma, ou meramente autorizado, sem atribuição de obrigatoriedade, seja realizado um exame de adequação, necessidade e proporcionalidade do conteúdo à finalidade do documento, com o fito de atendimento ao espírito protetivo da LGPD.

Foi estabelecida a obrigatoriedade de identificação do solicitante de certidão em meio eletrônico, quando também for obrigatória a justificação do seu interesse, em função do fundamento de autodeterminação informativa que orienta a disciplina de proteção de dados pessoais, pelo qual o titular tem a prerrogativa de ver os seus dados serem tratados de maneira condizente com as suas expectativas.

No âmbito do **Registro de Imóveis**, a expedição de certidão por via eletrônica, em serviço eletrônico compartilhado, fica a cargo do **SREI – Sistema de Registro Eletrônico de Imóveis**, que teve sua origem ligada ao Fórum de Assuntos Fundiários - dado através do

[25] "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" - art. 6º, I, LGPD

[26] "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" - art. 6º, II, LGPD

[27] "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" - art. 6º, III - LGPD

Provimento nº 110/2010 do CNJ, regulamentado no Provimento nº 47, de 2015, do CNJ, com posterior atualização no Provimento nº 89 de 2019.

É importante ressaltar que o SREI tem sua criação e inspiração intimamente ligadas à atuação da Associação de Registradores Imobiliários do Estado de São Paulo (ARISP), que em 2013 lançou a **Central Registradores**, integrando todas a unidades de Registro de Imóveis do estado e disponibilizando serviços online.

A seu turno, a Lei Federal nº 13.465, de 2017, instituiu o Operador Nacional do Registro (ONR), pessoa jurídica de direito privado, responsável pela implantação do SREI em todo país.

O Sistema de Registro Eletrônico de Imóveis, com o advento da Lei nº 14.382, de 2022, passa a ser integrado ao **SERP - Sistema Eletrônico dos Registros Públicos**, nos termos do seu art. 7º, V e na forma do Provimento nº 139/2023 do Conselho Nacional de Justiça.

> ***Art. 23.*** *O compartilhamento de dados com centrais de serviços eletrônicos compartilhados é compatível com a proteção de dados pessoais, devendo as centrais observar a adequação, necessidade e persecução da finalidade dos dados a serem compartilhados, bem como a maior eficiência e conveniência dos serviços registrais ou notariais ao cidadão.*
>
> ***Parágrafo único.*** *Deverá ser dada preferência e envidados esforços no sentido de adotar a modalidade de descentralização das bases de dados entre a central de serviços eletrônicos compartilhados e as serventias, por meio do acesso pelas centrais às informações necessárias para a finalidade perseguida, evitando-se a transferência de bases de dados, a não ser quando necessária para atingir a finalidade das centrais ou quando o volume de requisições ou outro aspecto técnico prejudicar a eficiência da prestação do serviço.*

Buscando dirimir eventuais dúvidas sobre o **uso compartilhado** de dados pessoais pela Administração Pública , no tocante aos serviços notariais e de registro, o Provimento clarifica que o compartilhamento de dados com centrais eletrônicas de serviços **não contraria** a LGPD, desde que atendido os princípios de finalidade, adequação e necessidade, em atenção ao aprimoramento e eficiência administrativa.

Como orienta a ANPD , o compartilhamento de dados pessoais deve atender, para além dos princípios supracitados, a **segurança e prevenção**, em vistas a atenuar os riscos decorrentes da operação.

A essa feita, o Provimento faz eleição pelo sistema de compartilhamento descentralizado de base de dados, evitando-se a transferência integral do acervo da serventia às centrais de serviço compartilhado, exceto se for estritamente necessário.

Especificamente quanto ao compartilhamento de dados com o Operador Nacional do Registro (ONR), **por ser pessoa jurídica de direito privado**, o compartilhamento de dados não se submete ao expresso regimento do caput art. 26 da LGPD, mas ao artigo 27:

> ***Art. 27.*** *A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:*
>
> ***I -*** *nas hipóteses de dispensa de consentimento previstas nesta Lei;*
>
> ***II -*** *nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do* caput *do art. 23 desta Lei; ou*

> ***III -*** *nas exceções constantes do § 1º do art. 26 desta Lei.*
>
> ***Parágrafo único.*** *A informação à autoridade nacional de que trata o* caput *deste artigo será objeto de regulamentação.*

Portanto, aplica-se o disposto no § 1º do art. 26:

> ***Art. 26.*** *(...)*
>
> ***§ 1º*** *É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:*
>
> ***I -*** *em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação); (...)*
>
> ***IV -*** *quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;*

Dessa forma, o ONR trata dados das serventias fundamentado na **hipótese de execução descentralizada de atividade pública** (in ciso I), em que se exige a transparência e o dever de conservação funcional dos dados registrais.

Ao aduzir que "o compartilhamento de dados com centrais de serviços eletrônicos compartilhados é compatível com a proteção de dados pessoais", o Provimento oferece subsídio para a previsão legal (inciso IV) de transferência de dados entre os ofícios de registro de imóveis e o Operador Nacional do Registro.

> ***Art. 24.*** *O compartilhamento de dados com órgãos públicos pressupõe lei ou ato normativo do órgão solicitante, ou convênio ou outro instrumento formal com objeto compatível com as atribuições e competências legais da atividade notarial e registral.*
>
> ***§ 1º*** *O compartilhamento deverá ser oferecido na modalidade de fornecimento de acesso a informações específicas adequadas, necessárias e proporcionais ao atendimento das finalidades presentes na política pública perseguida pelo órgão, observando-se os protocolos de segurança da informação e evitando-se a transferência de bancos de dados, a não ser quando estritamente necessária para a persecução do interesse público.*
>
> ***§ 2º*** *Caso o registrador ou notário entenda haver desproporcionalidade na solicitação de compartilhamento de dados pelo órgão público, deverá consultar a Corregedoria Nacional de Justiça, no prazo de 24 horas, oferecendo suas razões, à luz do disposto neste artigo.*
>
> ***Art. 25.*** *O responsável pela serventia extrajudicial efetuará, sempre que possível, aplicável e compatível com a finalidade perseguida e o tipo de tratamento, a criptografia ou a pseudonimização de dados pessoais para o acesso a informações ou transferência dos dados para terceiros, inclusive centrais de serviços eletrônicos compartilhados e órgãos públicos.*

No rol de hipóteses autorizativas do tratamento de dados pessoais (arts. 7º e 11, LGPD), a base legal de "execução de política pública" se aplica em uma gama de atribuições do Poder Público, conforme inciso III do art. 7º da LGPD:

> ***Art. 7º*** *O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
>
> *(...)*
>
> ***III -*** *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, observadas as disposições do Capítulo IV desta Lei;*

Observa-se, na leitura do dispositivo, a imperiosidade de **previsão normativa** em lei, regulamento, contrato, convênio ou instrumentos congêneres para o uso compartilhado de dados entre entes determinados. É **condição geral de legalidade** do uso compartilhado de dados pessoais pelo Poder Público.

Em se tratando de dados **pessoais sensíveis** , a condição de legalidade do tratamento compartilhado de dados é **ainda mais restrita**, porquanto a LGPD restringe a previsão normativa às espécies **"Lei"** e **"Regulamento":**

> ***Art. 11.*** *O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*
>
> *(...)*
>
> ***II -*** *sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:*
>
> *(...)*
>
> ***b)*** *tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;*

Seguindo-se a diretriz da LGPD, o Provimento reverbera a mesma exigência para o tratamento compartilhado de dados, de que seja previsto em ato normativo, convênio ou instrumento formal, compatível com as particularidades dos serviços notariais e de registro.

Ainda que não haja expressa menção no Provimento, entende-se que se aplica o disposto na LGPD quanto à **Legalidade Estrita** do compartilhamento de **dados pessoais sensíveis** à realidade cartorária, exigindo-se previsão normativa em Lei ou Regulamento, exclusivamente.

O compartilhamento de dados pessoais da serventia com órgão do Poder Público também deve atender aos princípios de finalidade, adequação, necessidade, segurança e prevenção, além dos demais nortes axiológicos da LGPD, de forma tal que também se elegeu o sistema de compartilhamento descentralizado de base de dados, evitando-se a transferência integral do acervo cartorário.

Quando do compartilhamento de dados com órgão público ou central eletrônica de serviço compartilhado, recomendam-se precauções adicionais, entre as quais a **criptografia** e **pseudonimização** .

[28] Art. 26, LGPD – "O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei"

[29] ANPD. **Guia Orientativo "Tratamento de Dados Pessoais pelo Poder Público"**. <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 de novembro de 2022.

Nessa toada, verificando o delegatário que o compartilhamento de dados pessoais com órgão do Poder Público é desproporcional, e não observa o dever de legalidade nos termos acima explicados, este possui a **prerrogativa de consultar o CNJ**, oferecendo suas razões no prazo de 24 horas, para avaliação da Corregedoria Nacional.

> ***Art. 26.*** *Os registradores e notários remeterão dados com a finalidade da formação de indicadores estatísticos às entidades previstas em lei ou regulamento, garantindo que sejam anonimizados na origem, nos termos da Lei Geral de Proteção de Dados Pessoais.*
>
> ***Art. 27.*** *Na correição anual será verificada pelo corregedor permanente a adaptação de suas práticas de tratamento de dados pessoais à Lei Geral de Proteção de Dados Pessoais (LGPD) e a este Provimento.*

O Provimento também dimensiona o compartilhamento de dados pessoais do acervo da serventia com finalidade de indicador estatístico dos serviços prestados pelas serventias na ótica da segurança e prevenção, prezando pela **anonimização** dos dados .

O conjunto de técnicas de segurança e prevenção, bem como de atendimento às medidas organizacionais de adequação à LGPD, deve ser objeto de fiscalização pelos órgãos competentes, em **correição anual**.

[30] MARANHÃO. Juliano Souza de Albuquerque. **Proteção de Dados e Registro Imobiliário**. In: Boletim IRIB em Revista. N. 362. P. 4-45.

[31] Art. 5º, II, LGPD – "dado pessoal sobre 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"

[32] Art. 13, §4º, LGPD – "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"

[33] Art. 5º, XI, LGPD – "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"

11.

Do registro de imóveis

> ***Art. 45.*** *Dependem de identificação do requerente e independem de indicação da finalidade os pedidos de certidão de registros em sentido estrito, averbações, matrículas, transcrições ou inscrições específicas, expedidas em qualquer modalidade.*
>
> ***§ 1º*** *Também dependem de identificação do requerente e independem de indicação da finalidade os pedidos de certidão de documentos arquivados no cartório, desde que haja previsão legal ou normativa específica de seu arquivamento no registro.*
>
> ***§ 2º*** *Pedidos de certidão de documentos arquivados em cartório para a qual não haja previsão legal específica de expedição dependem de identificação do requerente e indicação da finalidade, aplicando-se a regra do § 4º deste artigo.*
>
> ***§ 3º*** *Pedidos de certidão, busca e informações apresentados em bloco, ainda que instruídos com a numeração dos atos a serem certificados, dependem de identificação do requerente e indicação da finalidade.*
>
> ***§ 4º*** *Na hipótese do parágrafo anterior, caracterizada tentativa de tratamento de dados em desacordo com as finalidades do Registro de Imóveis e com os princípios da Lei Geral de Proteção de Dados Pessoais, poderá o oficial recusar o fornecimento em nota fundamentada, do que caberá revisão pelo juízo competente.*

A Publicidade Registral, estatuída por ocasião do art. 1º da Lei de Registros Públicos, tem por escopo o deferimento de autenticidade, segurança e eficácia aos atos jurídicos, possuindo natureza **constitutiva**[34] .

Assim, os atos tornados públicos através do Registro de Imóveis descortinam interesses de natureza privada, afastando-se qualquer compreensão equivocada sobre se tratar de dados públicos. Os dados tratados pelo Registro de Imóveis se relacionam diretamente com o Direito à Propriedade e com o Direito ao Livre Desenvolvimento da Personalidade dos sujeitos envolvidos.

A Lei Geral de Proteção de Dados, a esse respeito, tem a primazia de pôr o titular no centro das atribuições e regulamentações que dizem respeito aos seus dados, inclusive em face da utilização pelo Poder Público, instrumentalizando medidas que garantam o respeito à sua autodeterminação informativa.

Portanto, inexiste rivalidade entre a Publicidade Registral e a Proteção de Dados porque **ambas as espécies tratam da tutela de interesses de natureza privada**.

O Provimento dispôs acerca de medidas que garantam o respeito à autodeterminação informativa do titular dos dados tratados pelo Registro de Imóveis, bem como o alcance de sua finalidade precípua, qual seja, a de conferir autenticidade, segurança e eficácia *erga omnes* dos atos jurídicos neles consubstanciados.

Assim, uma face da solidificação da atividade do Registro de Imóveis – expedição de cer-

[34] MARANHÃO. Juliano Souza de Albuquerque. **Proteção de Dados e Registro Imobiliário**. In: Boletim IRIB em Revista. n. 362. p. 4-45.

tidão dos atos ali registrados – também recebe novos contornos a partir da garantia de atendimento às legítimas expectativas dos titulares dos dados pessoais.

A esse respeito, merece comedimento e interpretação sistemática o *caput* do art. 17 da Lei de Registro Públicos, que determina: "Qualquer pessoa pode requerer certidão do registro sem informar ao oficial ou ao funcionário o motivo ou interesse do pedido".

A aplicação desse dispositivo se restringe aos atos tipicamente realizados pelo Registro de Imóveis, para os quais há expressa previsão legal. São exemplos de atos típicos do Registro de Imóveis a **Certidão de Inteiro Teor, a Certidão de Relatório, a Certidão por Quesitos** (art. 19, *caput*, LRP) e a **Certidão de Situação Jurídica** (art. 19, § 9º, LRP).

A outro giro, não há na LRP menção ao anonimato do requerente de certidões de registro. O Provimento 134/2022 do CNJ clarifica eventuais dúvidas sobre a necessidade ou não de registro da identidade do requerente, apontando por sua **obrigatoriedade,** em todo caso.

O espírito desta determinação está ancorado na necessidade de proporcionar o exercício do direito à autodeterminação informativa ao titular inscrito no fólio real, nos termos do art. 2º, II e do art. 9º, da LGPD, conferindo condições mínimas de controle do fluxo das informações compartilhadas, a partir da identificação de quem as solicitou.

A **certidão em sentido estrito**, a que se refere o *caput* do art. 45 do Provimento, pode ser entendida por meio da análise da Lei de Registros Públicos (LRP), norma regulamentadora do sistema de registro. Nesse sentido, é possível admitir que "certidão de registro em sentido estrito" se refere às certidões típicas de atribuição do ofício de Registro de Imóveis. Com base no *caput* do dispositivo, observa-se que a publicidade ampla permanece como regra, existindo, assim, nítida consonância com a disposição do art. 17, da LRP.

Em se tratando de Certidão de documento arquivado em cartório, o Provimento aponta diferentes regramentos:

De acordo com o § 1º art. 45 do Provimento 134, desde que haja **previsão legal ou normativa** específica de arquivamento de documentos no acervo registral, a exemplo dos títulos registrados , a indicação da finalidade da solicitação será dispensada, devendo o registrador anotar, tão somente, a identificação do solicitante.

Quanto aos títulos registrados, é importante ressaltar que a alteração do art. 194, da Lei nº 6.015/1973, realizada por meio da Lei nº 14.382/2022, prevê a desobrigação de arquivamento da via física dos títulos levados a registro, conforme regulamentação a ser implementada pela Corregedoria Nacional do CNJ. Tal medida, além de agasalhar o princípio da necessidade do tratamento (ou minimização dos dados), repercute na noção de "previsão legal de arquivamento", posto que deixará de haver normativa que imponha ao delegatário o dever de armazenamento da via física do título.

No § 2º art. 45 há previsão de que, diante de pedidos de certidão de documentos arquivados para a qual não haja previsão legal específica de expedição, o registrador deverá anotar a identificação do requerente e a **finalidade da solicitação**, podendo o oficial, nos termos do § 4º do mesmo artigo, recusar o atendimento por meio de nota fundamentada. Trata-se, neste caso, de **certidão atípica**, uma vez que não possui base normativa que a vincule às funções do Registro de Imóveis.

Esse segundo contexto, pode se descortinar em específicas situações: (i) Documentos arquivados sem previsão legal ou normativa: situação em que o documento foi arquivado para mero controle do cartório, mas não foi utilizado para prática do ato pela serventia; (ii) Documentos arquivados com respaldo legal ou normativo: situação em que o documento foi utilizado para prática do ato e foi arquivado no cartório por regra que o obriga.

Na situação apontada no item (i), uma vez que não há previsão legal ou normativa de arquivamento do documento no cartório, havendo solicitação de certidão sobre o docu-

mento, entende-se pela aplicação dos §§ 2º e 4º, do art. 45.

No tocante à situação condizente ao item (ii), o cartório pode receber solicitação de certidão de documentos que foram arquivados para a prática de ato específico, mas cuja expedição de certidão individualizada, em princípio, não se relaciona com as funções típicas do Registro de Imóveis (ex.: certidão de documentos pessoais e procurações que foram arquivadas junto com um instrumento particular). Ponderando a finalidade da norma, compreende-se que, também nessas situações, é possível aplicar os §§ 2º e 4º, do art. 45 do Provimento.

Explica-se: mesmo na expedição de certidão de documento arquivado por força de lei, é necessário levar em conta a existência de propósito legítimo, que é a regra prevista na Lei Geral de Proteção aos Dados.

Necessário verificar se o documento em si é o título propriamente dito, ou se o solicitante apenas busca ter acesso a documentos e dados pessoais de terceiros via Registro de Imóveis, sem relação com a razão que levou à sua inclusão no acervo.

Dessa forma, caso na avaliação realizada pelo delegatário fique constatada violação às finalidades do Registro de Imóveis e à LGPD, poderá o Oficial recusar seu fornecimento, por nota fundamentada, cabendo ao juiz competente a sua revisão, aplicando-se a disposição contida no § 4º, do art. 45 do Provimento, combinada com o art. 6º, I, da LGPD (princípio da finalidade).

O cuidado dispensado à expedição de certidão de documento arquivado se relaciona diretamente com o dever do delegatário de garantir a **segurança** e **adequação** do serviço registral, na forma da Lei Federal nº 8.935/1994 , bem como em respeito aos fundamentos da privacidade, inviolabilidade da intimidade, honra e imagem e os demais princípios previstos na Lei nº 13.709/2018.

O mesmo regime se aplica ao requerimento de certidões, de busca ou de informações apresentados ***"em massa"***, ou ***"em bloco"***, caso em que dependerá de, além de identificação do requerente, da justificação de sua finalidade, ficando ao cargo de juízo de adequação à finalidade do Registro de Imóveis e aos princípios da LGPD pelo delegatário.

O conceito de ***"requerimentos em bloco"*** não é definido pelo Provimento, pois a norma do CNJ não traz parâmetros para definição de uma régua volumétrica para enquadramento de solicitações dessa natureza.

Em princípio, ante o caráter protetivo que consubstancia a mens legis do dispositivo, é possível entender que, para que os requerimentos sejam considerados em bloco, eles precisam ser feitos por um mesmo solicitante, de uma só vez, com o objetivo reproduzir grande volume do acervo.

Também é possível vislumbrar a existência de ***"requerimentos em bloco"*** quando da ocorrência da **fragmentariedade da solicitação**. Isto é, quando há recorribilidade de pedidos sobre informações constantes no acervo da serventia, por um mesmo solicitante, de forma que contextualmente se depreenda a reprodução em massa da base de dados do ofício.

Ante a ausência de parâmetros claros para interpretação do conceito discutido, espera-se que a Comissão de Proteção de Dados da Corregedoria Geral de Justiça, venha pacificar o entendimento em relação ao tema. Enquanto não houver definição de métricas para o assunto, não há caráter vinculativo que imponha ao delegatário a forma de

[35] Lei nº 6.015/73: "Art. 194. Os títulos físicos serão digitalizados, devolvidos aos apresentantes e mantidos exclusivamente em arquivo digital, nos termos estabelecidos pela Corregedoria Nacional de Justiça do Conselho Nacional de Justiça".

[36] LGPD: "art. 6º (...) III - 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".

aplicação do § 3º do art. 45 do Provimento.

Como aduzido anteriormente, a finalidade do Registro Público é o deferimento de autenticidade, segurança e eficácia aos atos jurídicos (art. 1º, LRP).

A eficácia e publicidade *erga omnes* de direitos reais, seja de propriedade, seja em coisa alheia, atende a um interesse do proprietário ou titular de ônus real de **opor contra a sociedade o seu direito**, e dela esperar o dever absoluto de não violação.

A publicização de informações constante em negócios privados atende a um interesse social de **conhecer os riscos e consequências** da realização de eventual negócio jurídico .

Observa-se nesse caso, que a Publicidade Registral tem por consequência elucidar questões essenciais para o livre desenvolvimento da personalidade quanto à **liberdade e autonomia negocial do indivíduo**.

Tamanha é a importância da Publicidade Registral que o ordenamento jurídico pátrio lhe confere a condição de validade para transferência de propriedade de bens imóveis (art. 1.245, Código Civil).

O Provimento buscou atender a esses interesses privados, do proprietário ou titular do ônus real e do indivíduo que busca conhecer os riscos e consequências de firmamento de um negócio jurídico, balizando-os com os direitos dos titulares dos dados arquivados em cartório.

O Ofício de Registro de Imóveis cumpre, portanto, papel singular nesse complexo sistema de ponderação de bens e interesses, não podendo terceirizar sua função a outrem e evitando compartilhar sua base de dados com órgão público (art. 24, Provimento nº 134/2022) ou ente privado (art. 23, Provimento nº 134/2022) sem a prévia existência de norma regulamentadora ou para finalidade diversa da atribuição finalística do seu mister.

Por essa razão, o Provimento veda o compartilhamento de base de dados pessoais do acervo da serventia, ainda que parcialmente, a título das denominadas “certidões em bloco” .

A esse respeito, o art. 26, §1º da LGPD, explicitamente aponta a vedação do compartilhamento de bases de dados do acervo público com entidade privada, senão nas situações ali excepcionadas.

A atribuição de um **juízo de adequação à finalidade da Publicidade Registral**, quando em face de um requerimento de certidões ou informações em massa, serve justamente para verificar a intenção de, por meios oblíquos, reproduzir parcialmente, de forma indevida, o acervo registral, estando o delegatário impedido de realizar esse compartilhamento de base de dados.

A abstração do conceito “em bloco” é, assim, o meio de viabilizar a aplicação contextual dessa diretriz, não se atendo a critérios formais que poderiam respaldar eventual abuso de direito pelo requerente de má-fé.

Portanto, **a partir da análise do contexto**, se o delegatário entender que a intenção do solicitante é a reprodução do acervo cartorial sem justificativa e fora da finalidade da publicidade registral, não lhe restará outra alternativa senão negar o requerimento, por ser seu dever funcional.

Não se pode esquecer que o Provimento exige a identificação do requerente de expedi-

[37] Art. 1º Serviços notariais e de registro são os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, **segurança** e eficácia dos atos jurídicos. (...) Art. 4º Os serviços notariais e de registro serão prestados, **de modo eficiente e adequado**, em dias e horários estabelecidos pelo juízo competente, atendidas as peculiaridades locais, em local de fácil acesso ao público e que ofereça segurança para o arquivamento de livros e documentos.

ção de toda certidão, facilitando a tarefa e identificar solicitações reiteradas de informações e obstar o compartilhamento indevido de base de dados do acervo.

A outro giro, visualizando-se que o requerimento de certidões ou informações em bloco se alinha às finalidades do Registro Público, ora delimitadas, poderá o Oficial autorizar o seu fornecimento.

Pode-se citar como exemplos de finalidade legítimas para a expedição de certidão em bloco: (i) levantamento de incorporadora imobiliária sobre a situação jurídica de imóveis já transferidos aos adquirentes; (ii) levantamento de titulares de imóveis em área atingida por determinado evento natural; (iii) levantamento da incorporadora de imóveis de área adjacente à construção de um determinado imóvel.

Como se mostra, a visualização de finalidade legítima para emissão de certidões em bloco somente se dará no caso concreto, partindo-se da premissa de adequação aos objetivos da Publicidade Registral.

> ***Art. 46.*** *Ressalvadas as hipóteses que tenham previsão legal ou normativa expressa, como as certidões de filiação de imóveis, ou de propriedade com negativa de ônus e alienações, ou outras compatíveis com as finalidades dos registros de imóveis e com os princípios da Lei Geral de Proteção de Dados, não serão expedidas certidões cujo conteúdo envolva informações sobre dados pessoais extraídos de mais de uma matrícula, assentamento do registro auxiliar, transcrição ou inscrição.*

Ainda em relação à emissão de certidão e a ponderação entre a Publicidade Registral e a Proteção de Dados Pessoais, o Provimento já revela uma **presunção** de emissão em desacordo com as finalidades do Registro de Imóveis, consubstanciada em **certidão sem previsão normativa expressa com conteúdo plural**.

São, portanto, dois os elementos eleitos pelo Provimento como fundantes da presunção supramencionada: **(1)** Inexistência de previsão expressa em Lei ou outra espécie normativa acerca da certidão; **(2)** conteúdo plural, isto é, que envolva informações sobre dados pessoais extraídos em mais de um registro.

Para casos em que se presencie ambos os elementos, aplica-se o disposto no § 2º do art. 45 do Provimento, ante a inexistência de previsão legal da espécie de certidão (elemento 1), com a consequente juízo de finalidade e possibilidade de negativa fundamentada pelo oficial do serviço.

> ***Art. 47.*** *As certidões dos imóveis que já forem objeto de matrícula eletrônica, após a "primeira qualificação eletrônica", serão expedidas, independentemente de indicação de finalidade, em formato nato-digital estruturado, contendo a situação jurídica atual do imóvel, ou seja, sua descrição, titularidade e os ônus reais não cancelados.*
>
> ***Parágrafo único.*** *A expedição de certidão de atos anteriores da cadeia filiatória do imóvel depende de identificação segura do requerente e de indicação da finalidade.*

A primeira qualificação eletrônica é procedimento previsto expressamente no art. 10, III, do Provimento 89/2019 do CNJ, e estabelece a migração de um registro de imóvel existente efetuado no livro em papel, seja transcrição ou matrícula, para o formato de registro eletrônico denominado matrícula eletrônica.

[38] LOUREIRO, Luiz Guilherme. Registros públicos: teoria e prática. São Paulo: Editora Método, 2020, p. 594; PASSARELLI, Luciano. Os livros 4 e 5 do registro imobiliário: os indicadores real e pessoal. Revista Jus Navigandi. ISSN 1518-4862, Teresina, ano 14, n. 2013, 4 jan 2009.

As certidões de imóveis solicitadas no escopo SAEC/SREI, que se coadunam com a finalidade do Registro de Imóveis e estejam previstas expressamente em Lei ou regulamento, independem de apresentação de justificativa, como estabelece o *caput* do art. 45 do Provimento 134/2022 do CNJ.

Por conseguinte, a certidão de situação jurídica, instituída pela Lei nº 14.382 de 2022, prevista expressamente no § 9º do art. 19 da Lei de Registros Públicos, nos casos em que a matrícula for eletrônica, submete-se a essa normativa, devendo ser fornecida em **formato nato-digital estruturado**, contendo a descrição, titularidade e os ônus reais não cancelados de imóvel cujo registro já tenha passado pelo procedimento de "primeira qualificação eletrônica".

Excepcionalmente, as **certidões de relatório**, ou de cadeia filiatória, de imóvel que já tenha passado pela primeira qualificação deve ser fornecida **mediante apresentação de justificativa**, caso em que o delegatário procederá ao arquivamento desta para eventual solicitação do titular.

Sendo certidão prevista legalmente, não se aplica a essa situação o disposto nos §§ 2º e 4º do art. 45 do Provimento 134/2022 do CNJ, **não podendo o delegatário negar a sua expedição**, mas apenas registrar sua finalidade.

Essa justificativa deve ser armazenada em prontuário digital, juntamente com a identificação do requerente, estando à disposição do titular dos dados tratados na certidão de cadeia filiatória, para eventual requisição junto ao registrador.

> ***Art. 48.*** *O atendimento a requisições de buscas fundadas exclusivamente no indicador pessoal ou real pressupõe a identificação segura do solicitante, bem como a indicação da finalidade, de tudo mantendo-se o registro em meio físico ou virtual.*
>
> ***Art. 49.*** *O fornecimento, pelo registrador, por qualquer meio, de informações sobre o registro não veiculadas por certidão dependerá da segura identificação do solicitante, e da indicação da sua finalidade, exceto nos casos em que o solicitante figure no registro em questão.*

Seguindo-se o vetor orientativo da autodeterminação informativa, o Provimento traz um regramento específico para as buscas fundadas exclusivamente no indicador pessoal ou real.

Como se observa, em face de um direcionamento exclusivo para a pesquisa em face de informação vinculada diretamente ao titular do bem ou do direito real constante no acervo registral, o Provimento exige a identificação segura do solicitante, bem como o arquivamento de uma justificativa de finalidade.

Tal exigência se mantém ainda que não se encontrem informações nos respectivos Livros do Registro de Imóveis, pois não se busca identificar o receptor da informação, mas aquele que requereu o serviço de busca. Portanto, a expedição de **Certidão Negativa de Busca** deve ser precedida de pedido, cuja motivação e identificação do requerente tenham sido registradas.

[39] Art. 1.245. Transfere-se entre vivos a propriedade mediante o registro do título translativo no Registro de Imóveis.

§ 1 o Enquanto não se registrar o título translativo, o alienante continua a ser havido como dono do imóvel.

§ 2 o Enquanto não se promover, por meio de ação própria, a decretação de invalidade do registro, e o respectivo cancelamento, o adquirente continua a ser havido como dono do imóvel.

[40] MARANHÃO. Juliano Souza de Albuquerque. Proteção de Dados e Registro Imobiliário. In: Boletim IRIB em Revista. N. 362. P. 4-45.

O Provimento não faz diferença se a busca fundada em indicador pessoal se refere à pessoa física ou jurídica, dispondo, em princípio, o mesmo regramento para ambas as situações. Contudo, entende-se que, ante o caráter protetivo da LGPD, que busca tutelar a autodeterminação informativa e livre desenvolvimento da personalidade através de informações pessoais, razão pela qual se protege o dado pessoal relacionado à pessoa natural identificada ou identificável, deve-se restringir o elemento protetivo do dispositivo comentado às buscas fundadas em indicador pessoal de **pessoa física**.

Não há menção expressa à possibilidade de o oficial negar, mediante nota fundamentada, o fornecimento dessa informação, mas **tão somente** acerca do seu dever de arquivar a justificativa do solicitante. Ressalta-se que o serviço de busca fundada em indicador pessoal ou real **não se confunde** com o direito de acesso, deferido ao titular na forma do art. 18 da Lei nº 13.709/2018, submetendo-se ao regime de emolumentos.

O mesmo raciocínio é aplicável quando em face de solicitação de informações do Registro de Imóveis **não veiculadas** por certidão, caso em que o delegatário procederá ao arquivamento da justificativa para eventual solicitação do titular.

É importante ressaltar, nesse contexto, que a previsão legal de visualização eletrônica dos atos dos registros públicos pelo Serp , estatuída no § 8º do art. 19 da LRP com redação dada pela Lei 14.382/2023, constitui medida de compartilhamento de informações do acervo registral não veiculadas por certidão. Nesse sentido, a não ser que o requerente figure no registro objeto de visualização, caberá o armazenamento da finalidade e a identificação do solicitante desse serviço, em vista ao atendimento do art. 49 do Provimento 134/2022 do CNJ pelas serventias de Registro de Imóveis conectadas ao Serp.

> ***Art. 50.*** *Serão formados prontuários físicos ou digitais contendo os dados de identificação e indicação de finalidade em todas as hipóteses em que estas tenham sido exigidas.*
>
> ***Parágrafo único.*** *O titular dos dados pessoais solicitados terá direito a requisitar as informações contidas nos prontuários formados em virtude de buscas ou pedidos de informações e certidões para os quais foi exigida a identificação do solicitante e a indicação de finalidade.*

Nos casos delimitados neste capítulo - em que é exigida a identificação da finalidade da solicitação de informações, buscas e certidões junto ao Registro de Imóveis -, há o deferimento da obrigação de guarda das respectivas justificativas e identidade dos solicitantes no formato de **prontuário**, físico ou digital.

Insta rememorar que tais justificativas também se consubstanciam **dados pessoais,** na medida em que apontam informações sobre a pessoa do solicitante, razão pela qual também se lhes aplica o ecossistema de proteção de dados a que se refere a LGPD e o presente Provimento.

Igualmente, não há dúvidas que a identidade dos solicitantes também é dado pessoal. Tais informações constarão no inventário de dados, bem como devem atender ao prisma de segurança, qualidade e prevenção, entre outras diretrizes.

Esses dados **somente** poderão ser fornecidos ao titular do dado pessoal a qual se referiu a busca ou solicitação realizada pelo requerente ou a este próprio, e **não poderão ser eliminados** a pedido deste, posto que é parte do próprio acervo registral da serventia.

[41] O Sistema Eletrônico dos Registros Público – Serp constitui medida de modernização e simplificação das atividades de serventias extrajudiciais de Registros Públicos, com regulamentação dada pela Lei nº 14.382/2022, que tem como um dos seus objetivos o atendimento remoto dos usuários dos serviços registrais por meio da internet.

5ª seção

Apontamentos finais

Capítulo 12
Disposições finais

> ***Art 58.*** *As Corregedorias Gerais da Justiça dos Estados e do Distrito Federal fiscalizarão a efetiva observância das normas previstas neste Provimento pelas unidades do serviço extrajudicial, expedindo as normas complementares que se fizerem necessárias, bem como promoverão, no prazo estabelecido no art. 59, a adequação das normas locais que contrariarem as regras e diretrizes constantes do presente provimento.*
>
> ***Art. 59.*** *Este provimento entra em vigor na data de sua publicação, observado o prazo de 180 (cento e oitenta) dias para adequação das serventias extrajudiciais às disposições contidas neste documento.*

O Provimento também estabeleceu um prazo de *vacatio legis* de 180 dias, a fim de que as serventias pudessem adequar o seu funcionamento às suas diretrizes normativas, registrando todos os passos já realizados, em atenção ao princípio da ***accountability*** (responsabilização e prestação de contas), posto que serão fiscalizados.

Os delegatários também devem se atentar às diretrizes constantes em normas editadas pelas Corregedorias Gerais de Justiça dos Estados e Distrito Federal, ressaltando que estas possuem o dever de adequar eventual Provimento Estadual sobre o tema ao que está disposto no diploma da Corregedoria Nacional.

Às Corregedorias Gerais de Justiça dos Estados e Distrito Federal que já tiverem editado normas que contrariem o disposto na norma da Corregedoria Nacional, também foi dado o prazo de 180 dias para ajuste, ante a necessidade de uniformização da aplicação da LGPD, lei federal, no âmbito das serventias extrajudiciais em todo território nacional.


ARISP
Associação dos Registradores
Imobiliários de São Paulo