Provimento nº 134/2022

do Conselho Nacional de Justiça

COMENTADO

SUMÁRIO

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) já não é mais novidade, tampouco a necessidade de as serventias extrajudiciais se adequarem às suas exigências.

O ano de 2021 foi bastante profícuo em regulamentações sobre a LGPD, assim como o de 2022. Das 27 corregedorias gerais, 18 publicaram seus provimentos nesse período. Mas em 2022 enfim foi publicada a tão esperada regulamentação do Conselho Nacional de Justiça (CNJ): o Provimento 134/2022.

Seguindo o exemplo da Autoridade Nacional de Proteção de Dados (ANPD), o CNJ buscou ampliar o debate em torno dessa regulamentação, submetendo-a a prévia consulta pública. Ainda assim, não foram muitas as alterações realizadas.

Nesse contexto, a equipe do Instituto de Compliance Notarial e Registral (ICNR) comenta artigo por artigo do Provimento 134. A normativa está publicada no site oficial do CNJ, podendo ser consultada no seguinte link: https://atos.cnj.jus.br/atos/detalhar/4707.

Quer saber mais sobre como o ICNR pode ajudar sua serventia na adequação?

Clique aqui para falar com o ICNR!

CONSIDERANDO OS *CONSIDERANDA*

CONSIDERANDO que é missão do Conselho Nacional de Justiça (CNJ) desenvolver políticas judiciárias que promovam a efetividade e a unidade ao Poder Judiciário, incluindo-se as serventias extrajudiciais, para os valores de justiça e de paz social;

CONSIDERANDO a competência dos órgãos judiciários para exercerem função regulatória das atividades prestadas nas serventias notariais e registrais (CRFB, art. 236, § 1º);

CONSIDERANDO a necessidade de regulamentar as disposições da Lei n. 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, considerando as resoluções aplicáveis, como a Resolução CD/ANPD n. 02, de 27 de janeiro de 2022;

CONSIDERANDO o princípio da publicidade que orienta a prática dos atos registrais e notariais, possibilitando, inclusive, que a pessoa possa requerer certidão sem informar o motivo ou o interesse do pedido (Lei n. 6.015/73, art. 17; Lei n. 8.934/94, art. 1º);

CONSIDERANDO a obrigação das serventias extrajudiciais de cumprir as normas técnicas estabelecidas pelo Poder Judiciário (arts. 37 e 38 da Lei n. 8.935, de 18 de novembro de 1994);

CONSIDERANDO o fato de haver tratamento de dados pessoais, sensíveis ou não, na prestação das atividades notariais e registrais, sendo os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, no desempenho de suas atividades, controladores de dados pessoais;

CONSIDERANDO o compartilhamento de dados pessoais pelos responsáveis das serventias extrajudiciais com as centrais de serviços eletrônicos compartilhados, decorrente de previsões legais e normativas;

Comentários

Antes de adentrar os artigos, é importante atentar-se aos *consideranda.* Embora não possuam o mesmo valor normativo, revelam as intenções do legislador e auxiliam na interpretação das normas positivadas.

Os 3 primeiros *consideranda* do Provimento abordam a necessidade de regulamentar a LGPD e o dever institucional do CNJ em fazê-lo, no que tange às serventias extrajudiciais, a partir da competência descrita no 236, § 1º da Constituição Federal (CF).

Mais adiante, frisa a obrigação das serventias extrajudiciais de cumprir as normas técnicas estabelecidas pelo Poder Judiciário.

Até aí não há muita novidade, salvo pela previsão que a regulamentação do CNJ teve por base a Resolução CD/ANPD nº 02/2022.

Disso se pode extrair duas conclusões importantes.

A primeira é que **o CNJ atua alinhado com as demais autoridades regulamentadoras**, em especial com a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), seguindo preceito de cooperação previsto no art. 55-J, XXI da LGPD[1].

A segunda é que o CNJ considerou a **simplificação das exigências de implementação da LGPD conforme os recursos de cada serventia** nos termos da Resolução CD/ANPD n. 02/2022, que dispõe sobre os chamados "agentes de tratamento de pequeno porte".

Entende-se extremamente louvável essa simplificação, pois a LGPD não pode inviabilizar serventias menores. A população precisa da prestação de serviços notariais e registrais em todas as comarcas do país. Essa opinião, aliás, corrobora o que já havíamos dito na Audiência Pública realizada previamente à publicação da Resolução CD/ANPD n. 02/2022[2].

Outro considerando que merece atenção é o que prevê que os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, no desempenho de suas atividades, são **controladores de dados pessoais**. Fruto de detido trabalho interpretativo, o Provimento é preciso ao prever que são controladores os responsáveis pela serventia, termo que abrange titular, interino (respondente) e interventor.

[1] "Art. 55-J. Compete à ANPD: (...) XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação".
[2] ANPD. **Audiência Pública sobre a regulamentação da aplicação da LGPD para micro e empresas de pequeno porte**. Disponível em: https://www.youtube.com/watch?v=gkWYEHLaGTE, 2:47:36.

Por fim, os *consideranda* destacaram a necessidade de compatibilizar a proteção de dados com o Princípio Da Publicidade, concretizado pela expedição de certidões e com o uso compartilhado de dados. De sua importância prática, tais destaques deram azo a todo o Capítulo X do Provimento.

CAPÍTULO I - 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.

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.

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

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.

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.

Comentários

As disposições gerais buscam compatibilizar os conceitos da legislação com as peculiaridades da atividade notarial e de registro. Mesmo que seja inevitável a repetição de alguns termos da LGPD, o Provimento 134 não se limitou à simples cópia de dispositivos. Pelo contrário, desde seu primeiro artigo passou a dirimir controvérsias e fixar entendimentos importantes.

Ao destacar que deverão ser cumpridas as disposições previstas nas diretrizes, regulamentos, normas, orientações e procedimentos expedidos pela

ANPD, o CNJ extingue qualquer dúvida sobre a competência da Autoridade Nacional para regulamentar a LGPD também no âmbito notarial e de registro.

O art. 2º do Provimento correlaciona o conteúdo do caput e do art. 23 e do § 4º da LGPD, simplificando a interpretação da LGPD de maneira aplicada aos cartórios. Confira abaixo o texto da LGPD:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: (...) § 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.

Reforçando a previsão dos *consideranda*, o art. 4º de que os responsáveis pelas serventias extrajudiciais são controladores de dados, especificando que o termo "responsáveis" abarca titulares, interventores ou interinos. Para quem não se recorda, controladores são aqueles que tomam as decisões referentes ao tratamento de dados[3], definindo sua finalidade e meios de tratamento[4].

Outra previsão que merece destaque é do parágrafo único do art. 1º, segundo o qual também são controladores os operadores nacionais de registros públicos e as centrais de serviços compartilhados.

Tal previsão é acertada, já que de fato essas entidades utilizam os dados repassados pelos cartórios de maneira autônoma. Em outras palavras, os delegatários não têm ingerência sobre as finalidades do tratamento feito pelas centrais, que é realizado conforme previsões regulamentares específicas.

Adiante, o art. 5º delimita que os operadores de dados, pessoas naturais ou jurídicas, são **sempre externos** ao quadro funcional da serventia. Em

[3] LGPD: "Art. 5º Para os fins desta Lei, considera-se: (...) VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
[4] ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

conformidade com a orientação da ANPD[5], essa previsão afasta definitivamente a equivocada interpretação de que prepostos poderiam ser enquadrados como agentes de tratamento.

Optou-se por comentar ao final o art. 3º do Provimento tendo em vista a novidade que ele enseja. Esse artigo cria a **Comissão de Proteção de Dados** (CPD/CN/CNJ). Grosso modo, pode-se dizer que o CNJ criou uma "ANPD específica"[6] para a atividade notarial e registral, com atribuições consultivas, regulamentares e orientativas. A diferença é que o novo órgão não terá competências fiscalizatórias e sancionatórias, que permanecem com as corregedorias.

A criação do CPD/CN/CNJ é salutar para que a LGPD seja interpretada de maneira compatível com o complexo sistema normativo que regulamenta as atividades notariais e registrais. As consultas elevarão muito a segurança para aplicação prática da LGPD, pois permitirão que as serventias atuem com base numa "interpretação oficial" sobre a LGPD.

E não é demais lembrar: a existência de um órgão específico, dentro da Corregedoria Nacional, é reflexo da importância que as serventias extrajudiciais possuem para o ordenamento jurídico nacional, bem como da relevância que a proteção de dados tem para estas peculiares organizações.

[5] ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf.

[6] Considerando que o novo órgão possui várias das competências previstas no art. 55-J da LGPD.

CAPÍTULO II - 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 Interna 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.

Comentários

O caput do art. 6º retoma o que já foi dito nos *consideranda* do Provimento sobre a proporcionalidade das exigências à capacidade econômica de cada serventia, em atenção à isonomia e à regulamentação da ANPD sobre agentes de tratamento de pequeno porte (Resolução nº 2/2022). Assim, os responsáveis pela serventia devem-se adequar-se “de forma proporcional à sua capacidade econômica e financeira”.

Todavia, isso não significa ausência de adequação. Afinal, o art. 6º prevê um **conteúdo mínimo que todas as serventias devem adotar**. Neste capítulo, comentaremos com brevidade cada um desses itens[1], a saber:

Item	Comentário
I – nomear encarregado pela proteção de dados	É preciso nomear uma pessoa para exercer essa função. Pode ser interno (colaborador) ou externo (pessoa física ou jurídica). Pode haver indicação conjunta pelos cartórios de menor faturamento. Só não pode indicar o próprio delegatário! Note-se que a nomeação deve sempre ser por via contratual, por exigência expressa do Provimento.
II – mapear as atividades de tratamento e realizar seu registro	Mapear é analisar procedimentos de tratamento de dados e criar um documento a partir disso. Na prática, é uma planilha de Excel em que cada linha corresponde a um processo, e cada coluna uma informação sobre esse processo (dados tratados, finalidade, base legal, etc).
III – elaborar relatório de impacto sobre suas atividades, na medida em que o risco das atividades o faça necessário	O 00Relatório de Impacto serve para analisar atividades de tratamento que apresentam maior risco de dano aos titulares. Além de uma análise de riscos, esse relatório contém as medidas para sua mitigação.
IV – adotar medidas de transparência aos usuários sobre o tratamento de dados pessoais	As “medidas de transparência” são uma categoria na qual são inseridos: (i) canal de atendimento para titulares de dados; (ii) fluxo de atendimento aos direitos dos titulares; (iii) aviso de privacidade e proteção de dados; (iv) aviso de cookies; (v) aviso de privacidade para navegação no website.
V – definir e implementar Política de Segurança da Informação	Documento que estabelece as melhores práticas para garantir a confiabilidade das informações, por meio de diretrizes, princípios e divisão de funções e responsabilidades. Note-se que não basta escrever tal política, é preciso “definir e implementar”.
VI – definir e implementar Política Interna de Privacidade e Proteção de Dados	Documento que orienta o tratamento de dados pessoais, criando um amálgama entre todas as demais políticas e procedimentos. Além disso, contemplam o tratamento de dados dos colaboradores.
VII – criar procedimentos internos eficazes, gratuitos, e de fácil acesso para atendimento aos direitos dos titulares	O Provimento não especifica que procedimentos seriam estes, mas a princípio eles se confundem com o fluxo de atendimento aos direitos dos titulares, que é uma das medidas de transparência acima mencionadas.
VIII – zelar para que terceiros contratados estejam em conformidade com a LGPD, questionando-	A gestão de terceiros envolve medidas para garantir que os destinatários dos dados da serventia estejam também em conformidade. Ela se concretiza em duas frentes: (i) a jurídica, pela adequação de

os sobre sua adequação e revisando cláusulas de contratação para que incluam previsões sobre proteção de dados pessoais	contratos; e (ii) a procedimental, que são políticas e auditorias nos destinatários de maior risco.
IX – treinar e capacitar os prepostos	A adequação nunca é efetiva se a equipe da serventia (incluindo delegatários!) não estiver devidamente capacitada para "tirar do papel" as políticas de proteção de dados. As pessoas podem por "tudo a perder" ou podem ser o principal diferencial para garantir a adequação. Tudo depende de boa vontade e conhecimento.

Plano de ação

A partir desses itens, é possível montar um modelo básico de plano de ação aplicável a todas as serventias extrajudiciais. Para tanto, recomendamos criar um checklist resumido, como o que consta no exemplo abaixo:

	Item	Prazo estimado	Data de conclusão
	Nomeação do encarregado		
	Mapeamento de dados		
	Relatório de Impacto sobre suas atividades		
Medidas de Transparência	Elaborar e publicizar o canal de atendimento		
	Elaborar o fluxo de atendimento aos direitos dos titulares		
	Elaborar e publicizar o aviso de cookies		
	Elaborar e publicizar o aviso de privacidade e proteção de dados		
	Elaborar e publicizar o aviso de privacidade para navegação no website		
	Definir e implementar Política de Segurança da Informação		
	Definir e implementar Política Interna de Privacidade e Proteção de Dados		
Gestão de terceiros	Enviar comunicação exigindo adequação de terceiros		
	Revisar cláusulas de contratação com terceiros		
	Treinamentos para os prepostos		

No campo **DATA DE CONCLUSÃO** deve-se colocar a data exata em que a atividade foi concluída. Já no campo **PRAZO ESTIMADO**, é possível inserir uma data pré-fixada ou um período em dias/semanas.

Recomenda-se esta última modalidade, pois evita a necessidade de olhar calendários, feriado, períodos de férias, etc. Além disso, facilita com que o planejamento seja mais realista, na medida em que o avanço do projeto de implementação depende de uma série de atividades e múltiplos atores.

Diante disso, recomenda-se traçar prazos vinculados ao cumprimento da etapa anterior. Se a etapa atrasa, fica claro que não há possibilidade de seguir com o projeto. Veja o exemplo abaixo:

	Item	Prazo estimado
1	Nomeação do encarregado	7 dias, após início do projeto
2	Treinamentos para os prepostos	7 dias, após a etapa 1
3	Elaborar e publicizar o canal de atendimento	15 dias após a etapa 3
4	Elaborar o fluxo de atendimento aos direitos dos titulares	
5	Elaborar e publicizar o aviso de cookies	
6	Elaborar e publicizar o aviso de privacidade e proteção de dados	
7	Elaborar e publicizar o aviso de privacidade para navegação no website	
8	Enviar comunicação exigindo adequação de terceiros	7 dias após a etapa 3
9	Revisar cláusulas de contratação com terceiros	30 dias após a etapa 3
10	Definir e implementar Política de Segurança da Informação	
11	Definir e implementar Política Interna de Privacidade e Proteção de Dados	
12	Mapeamento de dados	120 dias após a etapa 1
13	Relatório de Impacto sobre suas atividades	30 dias após a etapa 12

Nesse ínterim, é bom ressaltar três questões.

Em primeiro lugar, o plano de ação acima contém etapas dispostas numa ordem lógica, com prazos que entendemos razoáveis. Contudo, trata-se de algo

meramente sugestivo. Cabe a cada serventia traçar o planejamento que melhor lhe convir.

Em segundo lugar, o plano se refere aos itens MÍNIMOS de adequação, que são exigidos de todas as serventias. Para serventias de maior porte, o plano de ação precisa ser mais robusto.

Em terceiro lugar, o plano não contém o seu detalhamento completo. Por exemplo, a política de segurança da informação precisa ser definida e IMPLEMENTADA. Para a implementação, são necessárias várias medidas menores. Por isso, entende-se que o os itens acima devem ser destrinchados em diversos subitens.

CAPÍTULO III - 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.

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;

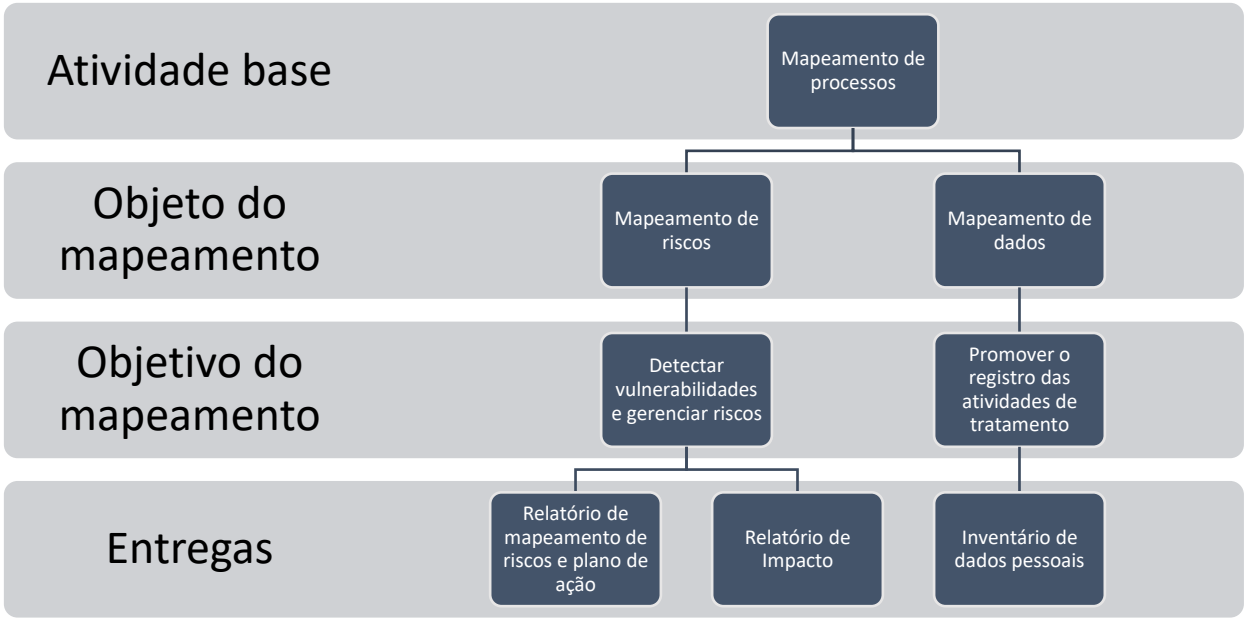
V – atualizar anualmente o inventário de dados;

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;

Parágrafo único. O responsável pela serventia extrajudicial poderá solicitar à associação de classe o fornecimento de formulários e programas de informática adaptados para cada especialidade de serventia para o registro do controle de fluxo, abrangendo a coleta, tratamento, armazenamento e compartilhamento de dados pessoais.

Comentários

É muito comum nos projetos de implementação da LGPD confundir o mapeamento de riscos com o mapeamento de dados pessoais. Ambos têm a mesma base, que é o mapeamento de processos, mas há diferença no objetivo de cada atividade. Para entender melhor, veja a figura abaixo.



A fim de que o leitor possa se aprofundar na temática, a tabela abaixo apresenta os fundamentos normativos de cada uma das atividades acima mencionadas:

Atividade	Provimento do CNJ
Mapeamento de processos	Art. 6º, II e art. 7º, caput
Mapeamento de dados	Art. 7, § 1º, I
Mapeamento de riscos	Art. 7, III
Relatório de mapeamento de riscos e plano de ação	Art. 7, § 1º II, IV
Relatório de Impacto	Art. 6º, III e art. 11
Inventário de dados pessoais	Art. 7, § 1º I, V, VI

Na LGPD, o **mapeamento de dados** e seu resultado concreto (Inventário de Dados) são requisitos do cumprimento da exigência de registro das atividades de tratamento (art. 37, LGPD).

Por sua vez, o **mapeamento de riscos** e o plano de ação decorrem do dever de estabelecer um plano de governança eficaz (art. 50, § 2º, LGPD).

Por fim, o relatório de impacto é previsto em diversos momentos da lei, bastando mencionar o conceito contemplado no art. 5º, XVII da LGPD.

Mapeamento na prática

Para o mapeamento recomenda-se três fontes de informação: (i) entrevistas com a equipe; (ii) questionários; e (iii) análise documental. Isso permite identificar as atividades de tratamento de dados pessoais sob diversos ângulos, que se complementam.

O mapeamento de processos se inicia com uma fotografia do organograma da serventia (setores, funções e equipe). Em seguida, passa pela descrição pormenorizada dos dados utilizados, estejam eles em documentos, softwares ou serviços de armazenamento. Por fim, descreve os diversos destinatários externos dos dados, e sua classificação como agentes de tratamento.

Com isso, é possível registrar o fluxo de utilização dos dados pessoais nos processos do cartório (*data mapping*), bem como os riscos envolvidos em cada etapa (*gap analylis*).

Abaixo serão analisadas as entregas provenientes da atividade de mapeamento de dados, com exceção do Relatório de Impacto, que tem capítulo específico no Provimento.

Relatório de mapeamento de riscos e plano de ação

O objetivo é indicar o grau de conformidade atual da serventia à LGPD, discriminando os principais riscos no tratamento de dados pessoais e recomendando as adequações necessárias para mitigá-los, através da análise jurídica, de segurança da informação e de processos.

É fundamental que a análise de riscos seja efetuada por meio deste diagnóstico tenha **metodologia** bem definida, que pode ser de natureza quantitativa (cálculos probabilísticos) ou qualitativa (análise interpretativa). Para um melhor resultado, recomenda-se o uso de ambas as modalidades.

A metodologia pode ser extraída de diversos **padrões de boas práticas** reconhecidos no mercado. Abaixo, constam aqueles que são utilizados pelo Instituto de Compliance Notarial e Registral (ICNR) em suas consultorias:

- ABNT NBR ISO/IEC[7] **27001:2013** – Sistemas de Gestão de Segurança da Informação (SGSI);
- ABNT NBR ISO/IEC **27002:2013** – Código de Prática para a Gestão de Segurança da Informação (SGPD);
- ABNT NBR ISO/IEC **27005:2011** – Gestão de Riscos em Segurança da Informação;
- ABNT NBR ISO/IEC **27701:2019** – Técnicas de segurança (extensão da ISO/IEC 27001);
- ABNT NBR ISO/IEC **27002:2020** – Sistemas de Gestão de Privacidade da Informação (SGPI);
- ABNT NBR ISO/IEC **29134:2020** – Avaliação de impacto de privacidade – diretrizes;
- ABNT NBR ISO/IEC **29184:2021** Aviso de privacidade online e Consentimento;
- COBIT 5 – *framework* de boas práticas em tecnologia e segurança da informação, sobretudo para elaboração de diagnóstico de riscos;
- Matriz RACI – *framework* de gestão de processos, sobretudo para definição de deveres e responsabilidades.

O plano de ação são as medidas a serem implementadas para mitigar os riscos detectados. Esse aspecto, porém, já foi abordado anteriormente.

[7] Por vezes, a ISO e a IEC publicam normas em conjunto. No caso do Brasil, a ABNT traduz essas normas, tendo propriedade das traduções.

Inventário de Dados Pessoais

Após o mapeamento de dados, é preciso extrair das informações coletadas, definir com precisão os processos de tratamento de dados e estruturar tais processos no Inventário de Dados Pessoais (IDP). Na prática, o IDP é uma **planilha de Excel** com campos pré-definidos, completados com as informações obtidas no mapeamento.

De acordo com o Provimento, o IDP deve conter uma série de informações. Abaixo listamos cada um desses campos com agrupamentos que didaticamente pensamos para facilitar a compreensão:

Processo de tratamento	Descrição os dados utilizados em cada atividade
	Categorias dos dados
	Categoria dos titulares
	Forma de coleta
Legitimação do tratamento	Finalidade do tratamento
	Base legal
Compartilhamento	Compartilhamento com terceiros
	Identificação de transferência internacional
	Categorias de destinatários
Armazenamento seguro	Prazo de conservação
	Medidas de segurança

Convém destacar que o IDP deve ser **atualizado** com periodicidade mínima anual, bem como sempre que houver novos processos de tratamento, uso de novos sistemas, trocas de fornecedores e adoção de medidas novas de segurança.

É muito importante realizar o IDP, pois o Provimento orienta que seja disponibilizado a qualquer tempo, em caso de solicitação da Corregedoria Geral da Justiça, da Autoridade Nacional de Proteção de Dados Pessoais ou de outro órgão de controle.

Glossário

ABNT – Associação Brasileira de Normas Técnicas: foro nacional de normalização, que desenvolve padrões em diversos segmentos.

COBIT – *Control Objectives for Information and Related Technologies*: organização internacional de normalização, com foco em governança de tecnologia da informação.

IEC – *International Electrotechnical Commission*: organização internacional de normalização nas áreas tecnológica, segurança e meio ambiente.

ISO – *Internacional Standard Organization*: organização internacional de normalização, que desenvolve padrões seguidos mundialmente em diversos setores.

RACI – *Responsible; Accountable; Consulted; Informed*: ferramenta que designa quatro papéis fundamentais para a realização de processos (Responsável, Aprovador, Consultado e Informado).

CAPÍTULO IV - DA REVISÃO DOS CONTRATOS

Art. 8º 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 e adequação às exigências da LGPD quanto aos sistemas e programas de gestão de dados internos utilizados.

Comentários

A adequação contratual inicia-se internamente, com os colaboradores. Na prática, significa assinar instrumentos que contenham deveres referentes a proteção de dados (aditivo ao contrato de trabalho ou um termo autônomo). Essa é a parte mais importante da adequação contratual, pois os colaboradores são a extensão do delegatário (art. 20, § 3º da Lei nº 8.935/1994).

A principal diferença dessa adequação em comparação a feita para os contratos externos é a **posição dúplice** dos colaboradores: por um lado, eles são membros da equipe do cartório, e devem seguir as regras estabelecidas; por outro, são titulares de dados pessoais.

No que tange aos colaboradores **como membros da equipe**, é preciso que a disposição contratual preveja os seguintes requisitos:

(i) dever dos colaboradores de manter confidencialidade e seguir orientações de segurança da informação;
(ii) dever dos colaboradores de cooperação para atendimento de solicitações dos titulares de dados e de órgãos fiscalizadores (corregedorias e ANPD);
(iii) delimitação de responsabilidade civil e disciplinar em caso de descumprimento destes deveres.

No que tange aos direitos dos colaboradores **como titulares de dados**, o contrato deve prever os seguintes requisitos mínimos:

(i) delimitação dos dados dos colaboradores tratados, a finalidade do tratamento e a base legal que o autoriza (isso pode ser feito com referência à Política Interna de Proteção de Dados);
(ii) a duração do tratamento e o dever do delegatário em eliminar os dados (descarte);
(iii) as salvaguardas que a serventia oferece para os dados de seus colaboradores.

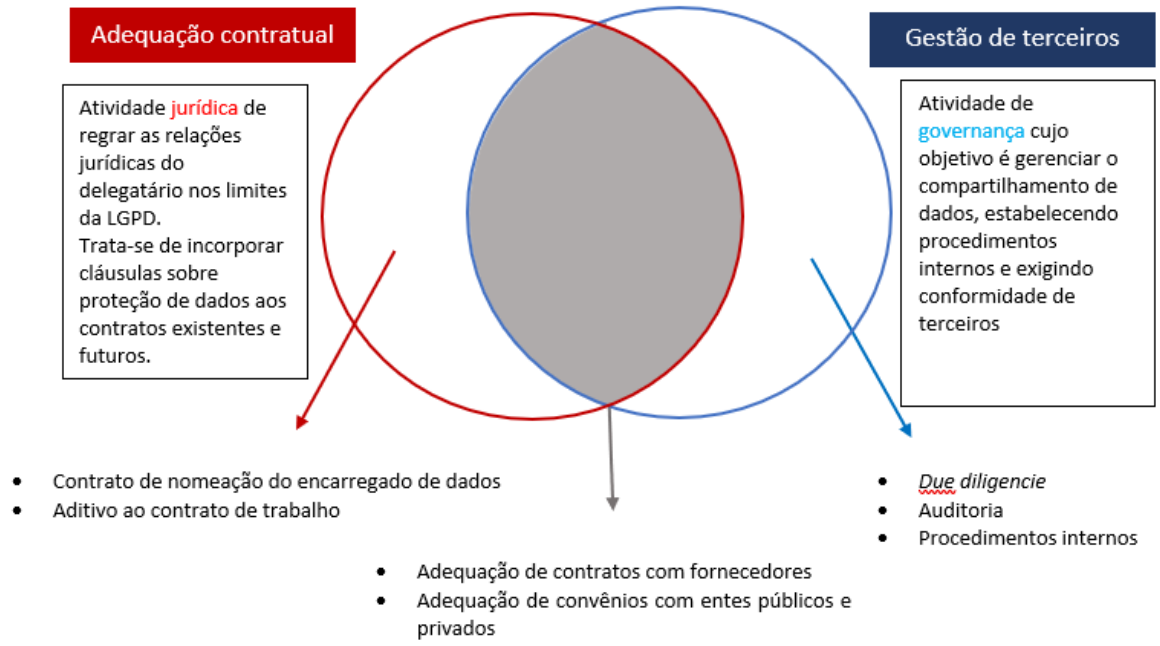
Essa adequação estende-se a todos os **demais instrumentos** de normatização internos, tais como código de ética, manuais de conduta, procedimentos operacionais, dentre outros.

Adequação contratual externa vs. Gestão de Terceiros

De igual modo, é preciso exigir conformidade das pessoas naturais ou jurídicas que tratam dados dos cartórios de maneira externa. Esses destinatários dos dados compartilhados pelo cartório são denominados no Provimento como “terceiros”.

O art. 6º, inciso VIII do Provimento prescreve que a serventia deve *"zelar para que terceiros contratados estejam em conformidade com a LGPD"*, fazendo isso de duas formas diferentes: **(a)** "*revisando cláusulas de contratação"* (adequação contratual); e **(b)** "*questionando-os sobre sua adequação"* (gestão de terceiros).

Essas atividades correspondem a elementos distintos do projeto de implementação da LGPD que, embora diferentes, complementam-se. Para entender com mais clareza, veja o diagrama abaixo:



A diferença fica clara ao se compararem as determinações previstas nos incisos do art. 8º: **(a)** os incisos II, III e IV abordam adequação eminentemente jurídica (revisar modelos, elaborar termos e incluir cláusulas); e **(b)** os incisos V e VI se referem a atividades de governança (elaborar orientações criar procedimentos).

Análise de riscos

É evidente que nem todos os fornecedores do cartório precisam ser exigidos da mesma maneira, que deve ser proporcional ao **risco do tratamento** de dados envolvido e ao porte do fornecedor.

O risco na atividade prestada por um fornecedor pode ser aferido pelos critérios estabelecidos pelo artigo 4º da Resolução CD/ANPD nº 2/2022, a saber:

(i) **volume de dados** tratados: tratamento em larga escala apresenta mais risco que o de menor escala;

(ii) **natureza dos dados** tratados: dados sensíveis e/ou sigiloso apresentam mais risco;

(iii) **categoria dos titulares** aos quais os dados se referem: dados de crianças, adolescentes ou outros grupos vulneráveis apresentam mais risco.

Para delimitar o risco, esses critérios devem ser analisados em conjunto. É diferente o risco de uma empresa que trata dados sensíveis de *um colaborador* (ex: fornecedor de vigia terceirizado) do que aquela que trata dados sensíveis de *diversos colaboradores* (ex: fornecedor de ponto eletrônico). No primeiro caso, o risco existe apenas na natureza dos dados; no segundo, pela natureza e pelo volume.

Pelo destaque dado no art. 9º, o Provimento considera de antemão que os **fornecedores de tecnologia, automação e armazenamento** devem ser mais exigidos. É comum que as serventias possuam *todo seu acervo* indexado a sistemas fornecidos por esses terceiros, o que representa tratamento de grande volume de dados, vários deles sensíveis. Logo, o tratamento de dados realizado por tais empresas apresenta maior risco, conforme os critérios acima mencionados.

Por fim, entende-se recomendável fazer exigências **proporcionais ao porte** de cada fornecedor. Em primeiro lugar, porque o porte delimita o grau de exigência que o próprio sistema de proteção de dados brasileiro impõe a cada agente de tratamento, conforme critérios da Resolução CD/ANPD nº 2/2022. Em segundo lugar, porque exigências excessivas podem criar entraves à prestação de serviços.

Note-se: dada a "gestão em caráter privado" da serventia, os delegatários podem criar as exigências que acharem mais convenientes, indo além das disposições legais. Todavia, exigir do fornecedor algo que a própria lei não prevê pode impedir a continuidade do contrato.

Gestão de Terceiros

A gestão de terceiros envolve a criação de procedimentos internos para governança de dados, incluindo atividades periódicas de auditoria.

Uma das formas mais básicas de auditoria é a solicitação de **evidências de adequação,** que vão além de simples declaração formal de estar adequado. Isso significa pedir que o fornecedor envie provas concretas da realização da implementação, tais como certificados de treinamento, cópias de políticas internas, cópia de aditivos contratuais assinados com colaboradores e fornecedores, etc.

Essa solicitação pode ser feita através de comunicado enviado por e-mail. Seu conteúdo deve abranger os requisitos mínimos de adequação pertinentes ao próprio cartório, os quais são descritos nos incisos do art. 6º do Provimento.

O Provimento também se refere à necessidade de elaborar "procedimentos de auditoria regulares" e "procedimentos para as contratações futuras" (art. 8º, V e VI). Para tanto, recomenda-se a confecção de uma **Política de Gestão de Terceiros**, na qual sejam previstos os critérios para contratação e as auditorias periódicas. Com o tempo, tal Política pode se desdobrar em procedimentos e protocolos específicos, para detalhar tais atividades de maneira mais concreta.

Adequação Contratual Externa

Na prática, a adequação contratual é a inclusão de cláusulas sobre proteção de dados nos instrumentos jurídicos da serventia. Para todos os contratos externos, o conteúdo mínimo deve abranger:

(i) delimitação dos dados tratados, a finalidade do tratamento e a base legal que o autoriza;
(ii) a duração do tratamento e o dever de eliminação de dados (descarte);
(iii) deveres de confidencialidade e requisitos mínimos de segurança da informação exigidos;
(iv) autorização (ou não) para a contratação de suboperadores;
(v) dever de comunicação de incidente de segurança;
(vi) dever de cooperação para atendimento de solicitações dos titulares de dados e de órgãos fiscalizadores (corregedorias e ANPD);
(vii) delimitações de responsabilidade civil e administrativa (e trabalhista, se for o caso).

Em seguida, é importante classificar os destinatários dos dados do cartório de acordo com as categorias previstas na LGPD (art. 5º, VI e VII), a saber: **(i) operadores** recebem os dados e utilizam para finalidades delimitadas pelo cartório; ou **(ii) controladores** recebem os dados e utilizam para as finalidades próprias, fora do controle do cartório.

Em regra, todos os fornecedores são operadores de dados. Podem existir situações, contudo, em que os cartórios compartilhem dados com outros controladores, como as associações de classe, os operadores nacionais e as centrais de serviços[8].

O uso de modelos é bem-vindo como forma de agilizar o processo de adequação, mas a verdadeira adequação contratual demanda uma análise

[8] Esse tema, porém, será retomado quando comentarmos o Capítulo X do Provimento

casuística. É recomendável **analisar todos os contratos** vigentes e propor **adequações específicas** àqueles cujo objeto envolver tratamento de dados de maior risco.

CAPÍTULO V - 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.

§ 1º 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.

§ 2º 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.

§ 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.

Comentários

Nas empresas, a indicação do encarregado de dados não necessariamente é obrigatória. A Resolução CD/ANPD nº 2/2022 relativiza esse dever para os chamados agentes de tratamento de pequeno porte:

Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.
§ 1º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.
§ 2º A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD.

Contudo, para as serventias extrajudiciais a indicação do encarregado de dados é **sempre obrigatória**, pois o Provimento é enfático ao dizer que *"deverá ser designado o encarregado"* (art. 10, *caput*) e que *"a função do Encarregado não se confunde com a do responsável pela delegação"* (art. 10, II).

A nomeação do encarregado tem forma prescrita: **contrato bilateral**. O Provimento não deixa espaço para dúvidas, ao dispor que a nomeação *"será promovida mediante contrato escrito, a ser arquivado em classificador próprio"* (contrato escrito), *"de que participarão o controlador na qualidade de responsável pela nomeação e o Encarregado"* (bilateral).

Evidentemente, na situação em que o encarregado seja colaborador da serventia, é cabível tal nomeação por meio de aditivo ao contrato de trabalho. O que não é adequado é a nomeação de encarregados por meio de termos, portarias e outros instrumentos.

Modalidades de encarregado de dados

Faculta-se ao agente delegado a escolha de um encarregado em três modalidades: (i) colaborador; (ii) pessoa natural externa; (iii) pessoa jurídica.

A primeira coisa que se percebe é que o encarregado de dados não é um cargo de pouca importância; assim fosse, o Provimento não teria "gastado" um capítulo inteiro para regulamentar essa função. Além disso, trata-se de uma questão prática. Em grande medida a conformidade do cartório e o respeito aos direitos dos titulares depende da indicação de um bom encarregado. Por isso, o primeiro critério para escolher é que seja alguém comprometido com a função e capaz de exercê-la.

A contratação de **encarregados externos** deve ser feita com as cautelas aplicáveis a quaisquer fornecedores da serventia. A respeito, o Provimento exige que seja "demonstrável a inexistência de conflito na cumulação de funções e a manutenção da qualidade dos serviços prestados" (art. 10, § 4º).

Questão “espinhosa” é a da independência do **encarregado de dados interno** em relação ao agente delegado. A função do encarregado é indicar as melhores soluções, com independência. Logo, caso seja um colaborador celetista, pode haver certo “conflito de interesses” no exercício dessa função.

Mesmo quando subordinado, o encarregado deve estar **realmente livre para alertar** quanto às atitudes do controlador, pois isso o ajudará a evitar danos a terceiros e a si mesmo. O desafio é o encarregado possuir, na prática, essa autonomia, mesmo sendo um colaborador celetista. Afinal, é realmente difícil ser consultor e subordinado ao mesmo tempo.

O risco é de que essa tensão subordinação-independência resulte na omissão do encarregado em situações nas quais precise orientar o controlador a mudar de atitude. Essa omissão prejudicará o delegatário (que poderá sofrer sanções e condenações), mas também o próprio encarregado. Afinal, em havendo irregularidades, a omissão por culpa e dolo, o encarregado implicará sua responsabilização (art. 42, § 4º da LGPD).

Além do que se disse sobre o *conflito de interesses*, deve-se compatibilizar as atribuições antigas com as novas. Não adianta, por exemplo, indicar um substituto que já esteja sobrecarregado com as funções notariais e registrais, pois ele pode não possuir *tempo hábil* para trabalhar como encarregado, mesmo que possua competência técnica para tal.

Por fim, é preciso tomar cuidado com a “questão trabalhista”. A soma de funções, sem substituição das antigas e sem aumento de salário, pode implicar infração às regras que regem a relação laboral.

Particularidades conforme o faturamento da serventia

É fato que nem todos os cartórios possuem recursos para contratar (interna ou externamente) um *expert* como encarregado de dados. Nesse sentido, tendo por base os critérios estabelecidos na Resolução CD/ANPD nº

2/2022, o CNJ trouxe relativizações ao dever de indicação de DPO para serventias Classe I e II. Para entender, veja a tabela abaixo:

Classe	Faturamento	Opções	Provimento 134
I	Até 100 mil/semestre	Encarregado individual ou indicado conjuntamente	Art. 10, § 1º e § 3º
II	Até 500 mil/semestre		Art. 10, § 1º
III	Acima de 500 mil/semestre	Encarregado Individual	Art. 10, § 2º

Em todo caso, há possibilidade de solicitar subsídios à entidade de classe.

A primeira conclusão que se pode tirar a partir dessas previsões é que não há escapatória. Toda e qualquer serventia deve ter um Encarregado. A segunda é que o CNJ exigirá esse dever de maneira proporcional à capacidade de cada cartório.

Funções do encarregado de dados

A LGPD define o encarregado de dados como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (art. 5º, VIII, LGPD). As funções do encarregado de dados são detalhadas no art. 41:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. (...)
>
> § 2º As atividades do encarregado consistem em:
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Como é fácil perceber pela leitura da lei, a maior qualidade do encarregado de dados não é conhecer a fundo questões técnicas, mas ser um

bom comunicador, pois três das quatro atribuições previstas na lei dizem respeito a essa aptidão.

Isso significa que o encarregado de dados não deve apenas encaminhar as soluções técnicas para as demandas apresentadas, mas também prestar esclarecimentos ao demandante, seja ele titular de dados pessoais ou autoridade pública (integrante da ANPD ou corregedor).

Nesse sentido, o encarregado precisa ter uma boa capacidade de adaptar sua linguagem perante os diferentes públicos com os quais precisa se comunicar. Internamente, deve atuar orientando os colaboradores e o próprio

agente delegado, não apenas em relação a questões práticas, mas em termos conceituais.

Depois do agente delegado, o encarregado é o **principal responsável pela conscientização** da equipe no que diz respeito à LGPD. Sua missão é criar uma verdadeira cultura de privacidade na serventia, para que haja respeito aos direitos dos titulares em todas as situações e, além disso, sejam evitadas sanções e condenações cíveis ao delegatário.

Deveres e responsabilidades

A indicação do encarregado de dados não afasta os deveres do agente delegado, enquanto controlador de dados. Embora inciso IV do art. 10 se refira apenas ao dever de atendimento aos titulares de dados, é lícito interpretar essa disposição em caráter mais amplo.

Afinal, o tudo o que fizer deverá estar em plena conformidade com as orientações do delegatário, a quem compete definir as finalidades do tratamento. Isso é especialmente verdadeiro no caso de encarregados internos, conforme se depreende do art. 22 da Lei 8.935/1994.

Do ponto de vista da responsabilidade civil e administrativa, o controlador responde perante os titulares de dados ou corregedores, por eventuais ilícitos ou danos. No caso dos cartórios, segundo o atual entendimento do STF (Recurso Extraordinário nº 842.846), o Estado responderá direta e objetivamente, ao passo que o agente delegado responderá em ação de regresso, por culpa e dolo.

Já o encarregado responde se tiver atuado com culpa e dolo. Se ele for interno, vale o art. 22 da Lei 8.935/1994, que é lei mais específica. E mesmo que seja externo – pessoa física ou jurídica – entende-se que a LGPD indica um sistema de responsabilidade subjetivo[9].

[9] STINGHEN, João R.; SANTOS, Rodrigo Bley. Cartórios e proteção de dados: responsabilidade civil. **Jota**, 24 mai. 2020. Disponível em: https://bit.ly/3ihGhd7. Acesso em jan. 2021.

CAPÍTULO VI - 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 gere risco a direitos e liberdades fundamentais, 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; e
>
> III – franquear, a título de transparência, aos afetados a possibilidade de se manifestarem a respeito do conteúdo.
>
> IV – elaborar o documento previamente à adoção de novos procedimentos ou tecnologias.
>
> § 1º Para o cumprimento das providências a que trata o caput do artigo, poderão ser fornecidos, pelas entidades representativas de classe, modelos, formulários e programas de informática adaptados para cada especialidade de serventia para elaboração de Relatório de Impacto.
>
> § 2º Serventias Classe I e II poderão adotar modelo simplificado de Relatório de Impacto conforme orientações do CPD/CN/CNJ para a simplificação do documento. Na ausência de metodologia simplificada, adotar-se-á o Relatório completo.
>
> § 3º Serventias Classe III adotarão o modelo completo de Relatório de Impacto, conforme instruções metodológicas do CPD/CN/CNJ.

Comentários

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é necessário quando há processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais (art. 5º, XVII da LGPD).

Nele estão descritos os riscos de violações aos dados ou aos direitos dos titulares de dados, bem como medidas técnicas ou administrativas para mitigar tais riscos.

A eficácia do RIPD depende da assertividade em identificar medidas pertinentes e suficientes para mitigar os riscos identificados, sem desconsiderar o contexto do cartório e sua realidade financeira.

Para tanto, é recomendável que o cartório tenha mapeado processos, produzindo a partir disso seu Inventário de Dados Pessoais (IDP), e conte com o apoio de profissionais de diferentes áreas (ao menos, jurídica e de tecnologia).

Em quais casos elaborar o RPID

O Provimento prevê apenas duas situações em que é necessário o RIPD: "previamente a contrato ou convênio" e "previamente à adoção de novos procedimentos ou tecnologias".

Tais orientações são exemplificativas. Pode-se listar várias outras situações em que tal relatório se mostra necessário, a partir de diferentes critérios.

O primeiro é a **NATUREZA DOS DADOS** tratados. Nesse sentido, o RIPD é recomendável quando houver tratamento de:

- dados sensíveis, com exceção de dados biométricos para gestão de controle de acesso e horários para jornada laboral;
- conjunto de dados cuja combinação possa proporcionar riscos ao titular
- dados pessoais relacionados a condenações criminais;
- dados financeiros, incluindo *status* social que posso acarretar riscos à segurança pessoal ou a integridade física/psíquica do titular;
- dados de crianças e adolescentes;
- dados referentes à geolocalização.

Ainda, é recomendável a realização do RIPD quando o **TIPO DE TRATAMENTO** envolver:

- grande volume de dados pessoais;
- uso de tecnologias inovadoras para processar, controlar, interagir, avaliar dados pessoais titular, inclusive direcionando decisões;
- monitoramento contínuo dos titulares de dados;
- decisões automatizadas, análises preditivas que produzam efeitos

jurídicos ao titular ou afetem sua segurança pessoal ou a integridade física/psíquica;

- tratamento dos dados impeça os titulares dos dados de exercer um direito ou de utilizar um serviço.

Por fim, a realização do RIPD é obrigatória em situações para as quais haja **DETERMINAÇÃO DAS AUTORIDADES** competentes:

- exigência da ANPD, após análise de comunicação de violação de dados pessoais, ou nas hipóteses de tratamento com base no legítimo interesse (Art. 10, § 3º, LGPD);
- exigência do Poder Judiciário, seja no exercício de sua função fiscalizadora, seja no exercício de sua competência jurisdicional.

Pode-se elaborar um RIPD para todas as operações de tratamento ou pode haver um RIPD para cada atividade. Deve-se avaliar a necessidade de um ou mais relatórios de acordo com critérios como a natureza dos dados tratados, o volume desses dados e número de processos de tratamento.

A escolha dos processos que demandam a confecção do RIPD depende de uma análise interna de cada serventia. A tabela abaixo correlaciona critérios gerais com situações típicas da atividade notarial e registral:

Critério geral	Comentários
Adoção de novas tecnologias ou novos processos de trabalho	Ex: novo sistema do cartório; solicitação/acompanhamento de pedidos pelo site;
Alterações nas leis e regulamentos com reflexo em proteção de dados	Ex: novas formas de processamento dos dados (Prov. 48/2017); extensão de competências dos cartórios (Prov 67/2018 CNJ)
Acumulação de funções	(novo acervo, com maior volume de dados, que podem estar desorganizados)
Tratamento que envolva alto risco para os dados pessoais, as liberdades civis e os direitos fundamentais dos titulares	Lembrando que a proteção de dados, em si mesma, é um direito fundamental[10]

[10] Constituição Federal: "Art. 5º (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

Tratamento de dados sensíveis, ou de grupos vulneráveis	A LGPD fala em crianças e adolescentes, mas também se incluem nessa categoria idosos e pessoas com deficiência, sobretudo cognitiva/mental.
Tratamento de dados que possa resultar em algum tipo de dano	Por exemplo, o tratamento de dados bancários, cujo vazamento pode gerar danos financeiros (Prov. 127/2022 do CNJ)
Tratamento de dados pessoais realizados para fins de atividades de investigação e repressão de infrações penais (art. 4º, III, "d", LGPD)	O cumprimento das obrigações constantes no Provimento nº 88/2019 do CNJ enquadra-se nessa hipótese.
Infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos.	Ver artigos 31 e 32 da LGPD[11]. Cartórios são equiparados a órgãos públicos (art. 23, § 4º, LGPD).
A qualquer momento sob determinação da ANPD	Nada impede que as corregedorias peçam o relatório também

Por fim, é preciso estar atendo às publicações da ANPD e das corregedorias, que poderão elaborar listas com hipóteses em que é obrigatória a elaboração do RIPD[12].

Conteúdo mínimo do RIPD

Segundo modelo disponibilizado pelo Governo Digital[13], o RIPD pode ser realizado com a seguinte estrutura:

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO
2 – NECESSIDADE DE ELABORAR O RELATÓRIO
3 – DESCRIÇÃO DO TRATAMENTO
    3.1 – NATUREZA DO TRATAMENTO

[11] Art. 31. Quando houver **infração a esta Lei** em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação. /Art. 32. A **autoridade nacional poderá solicitar** a agentes do Poder Público a publicação de **relatórios de impacto** à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.
[12] LGPD: "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial".
[13] **GOVERNO DIGITAL**. Segurança e Proteção de dados. Guias e modelos. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd

A tabela abaixo orienta de maneira mais clara o item 3 dessa estrutura, com definições e exemplos de aplicação às Serventias Extrajudiciais:

Item	Modelo Governo	Exemplo
Natureza do tratamento	representa o modo de tratamento de dados pretendido ou já executado pela serventia	Qualificação dos documentos (físicos/digitais); Cadastro no sistema; Consultas a bancos de dados diversos (centrais, entes públicos); fluxo de dados internos
Escopo do tratamento	Abrangência do tratamento de dados	Tipo de dados, volume de dados, volume de atividades de tratamento, área geográfica, etc.
Contexto do tratamento	Fatores internos e externos que podem afetar as expectativas do titular dos dados. Equilíbrio expectativa x tratamento.	Natureza do relacionamento da organização com os indivíduos (colaborador, usuário, terceiros, beneficiário final – Prov. 88); grupos vulneráveis
Finalidade do tratamento	Razão pela qual se deseja tratar os dados pessoais (resultado pretendido, benefícios esperados, base legal)	Obrigação legal; política pública (normas ou convênios); outros do art. 7º e 11 da LGPD; atentar-se aos artigos 14 e 23 também

Segundo o Provimento, são requisitos para o RIPD:

- a adoção de metodologia que resulte na indicação de medidas, salvaguardas e mecanismos de mitigação de risco: o relatório não deve ser feito com base numa análise exclusivamente subjetiva, mas pautada por padrão de boas práticas reconhecidos no mercado.
- o franqueamento aos afetados da possibilidade de se manifestarem a respeito do conteúdo do RIPD: as partes afetadas podem ser os titulares

de dados ou outros agentes de tratamento, como fornecedores, centrais de serviços, entidades de classe e órgãos públicos em geral.

A metodologia orientará a avaliação dos riscos de uma forma abrangente mantendo uma avaliação a partir de diretrizes de reconhecimento mundial, como as normas ABNT ISO/IEC 31000 que trata de riscos corporativos e a norma ABNT ISO/IEC 27005 que trata de riscos tecnológicos, dentre outras. A própria exigência de metodologia decorre da recomendação trazida pela norma ABNT ISO/IEC 29134[14].

É bom lembrar que, segundo o Provimento, poderão ser fornecidos, pelas entidades representativas de classe, **modelos, formulários e programas de informática** para elaboração de Relatório de Impacto.

Por fim, o Provimento dispõe que as serventias Classe I e II poderão adotar modelo simplificado de Relatório de Impacto conforme orientações da Corregedoria Nacional. Ainda assim, na ausência de metodologia simplificada, deverão adotar o modelo de Relatório completo.

Já as serventias Classe III devem adotar o Relatório completo.

[14] "Art. 38. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados".

CAPÍTULO VII - 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);

c) plano de resposta a incidentes (art. 48 da LGPD).

II – avaliação dos sistemas e bancos de dados em que houver tratamento de dados pessoais e/ou tratamento de dados sensíveis, submetendo tais resultados à apreciação do encarregado pelo tratamento de dados pessoais da serventia, para as devidas deliberações;

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.

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.

Art. 14. A inutilização e eliminação de documentos em conformidade com a Tabela de Temporalidade de Documentos prevista no Provimento nº 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.

Comentários

Uma política formal tem um papel fundamental em direcionar os recursos adequados para as necessidades de Segurança da Informação.

Ela permite controlar mais efetivamente tudo o que acontece no acesso à rede e demais sistemas e plataformas da serventia. Seu principal objetivo é minimizar riscos decorrentes de ameaças externas (malwares e cybercriminosos) e internas (funcionários com má intenção ou despreparo).

O Provimento exige que a Política de Segurança da Informação indique: a) medidas de segurança técnicas; b) mecanismos de segurança desde a concepção de novos produtos ou serviços (*security by design*); e c) plano de resposta a incidentes.

a) medidas de segurança técnicas e organizacionais

As medidas básicas para qualquer serventia adotar constam no Provimento 74/2018 do CNJ:

- *plano de continuidade* para eventuais incidentes de segurança, que atenda às normas de interoperabilidade, legibilidade e recuperação de informações (art. 2º, parágrafo único) e possibilite a transmissão facilitada do acervo, em caso de sucessão (art. 7º).
- *padrões mínimos de segurança* e integridade para armazenamento de dados, com *backups em nuvem e backups físicos* de periodicidade máxima de 24 horas e hospedagem em local distinto da instalação da serventia (art. 3º).
- sistema *escalas de permissões* seccionados por função, associados a perfis individuais, cujo acesso deve ocorrer dupla *autenticação*: por usuário e senha e por certificação digital ou biometria (art. 4º).
- *trilhas de auditoria* que permitam rastrear e identificar acessos ou modificações, as quais devem ser preservadas no backup (art. 5º).

Além delas, o Provimento 74 prevê recursos tecnológicos mínimos para todos os cartórios (com algumas distinções conforme o faturamento[15]). A tabela abaixo elenca todos os recursos exigidos e explica sua importância:

Recurso exigido pelo Provimento 74	Importância prática para o cartório
Energia estável, rede elétrica devidamente aterrada	Manter a infraestrutura adequada garante a proteção dos ativos da organização de intempéries, bem como de danos elétricos que possam vir da rede elétrica.
Link de comunicação de dados mínimo de 2 megabits	A escolha de um link de dados que possa suportar os trabalhos sem lentidão ou perda de dados transmitidos é de suma importância
Endereço eletrônico (e-mail) da unidade para correspondência e acesso ao sistema	Criar endereços de e-mail comercial de forma que possa criar grupos de recebimento por meio deles ajudará o controle das informações e manutenção do endereço, que se fosse usado endereços pessoais em cada troca eles deveriam também ser trocados o que poderia acarretar perda de informações.
Local técnico (CPD) isolado dos demais ambientes preferencialmente por estrutura física de alvenaria ou, na sua impossibilidade, por divisórias. Em ambos os casos, com possibilidade de controle de acesso (porta com chave) restrito aos funcionários da área técnica.	A proteção do local em que se encontra todos os equipamentos que prove a infraestrutura de atendimento ao ambiente, deverá ser mantido fechado, para que não haja roubo de dados ou até incidentes físicos devido a descuido ou desconhecimento.
Local técnico com refrigeração compatível com a quantidade de equipamentos e metragem	Permite a manutenção dos equipamentos em seu melhor desempenho, evitando superaquecimento e garantindo sua longevidade
Unidade de alimentação ininterrupta (nobreak) compatível com os servidores instalados, com autonomia de pelo menos 30 minutos	Os nobreaks mantêm o funcionamento de equipamentos diante de interrupções inesperadas de energia, o que permite desligá-los de maneira apropriada. Isso evita a corrupção dos dados lógicos e evita danos aos sistemas e aos equipamentos.
Dispositivo de armazenamento (storage), físico ou virtual	O backup é essencial para manter as atividades caso haja incidentes de segurança, e deve ser armazenado em local distinto da serventia. O intervalo para a atualização do banco de dados não pode ser superior a 24 horas (a programação automática garante isso).
Serviço de cópias de segurança na internet (backup em nuvem) do Banco de Dados	

[15] Serventias com arrecadação, por semestre: (Classe 1) de até 100 reais mil; (Classe 2) entre R$ 100 e 500 mil reais; (Classe 3); superior a 500 mil reais.

Servidor com sistema de alta disponibilidade que permita a retomada do atendimento à população em até 15 minutos após eventual pane do servidor principal Impressoras e scanners (multifuncionais)	Um servidor (físico ou virtual) de alta disponibilidade é mais um recurso que viabiliza a continuidade dos serviços diante de falhas ou incidentes.
Switch para a conexão de equipamentos internos Roteador para controlar conexões internas e externas	Uma boa infraestrutura de rede mantém a qualidade na comunicação e protege as informações que trafegam nas redes, algo essencial num momento em que vem crescendo o número de roubos e sequestros de dados
Softwares licenciados para uso comercial	O uso de softwares não licenciados (piratas) gera grave risco à integridade do acervo, porque geralmente os crackers incutem vulnerabilidades nos programas violados. Portanto, é necessário realizar um inventário de softwares com objetivo de identificar aqueles que não são licenciados para substituí-los ou mesmo cessar sua utilização, caso não seja realmente necessários.
Software antivírus e antissequestro	Um antivírus com credibilidade de mercado ajuda a proteção da rede, cotidianamente exposta a ameaças, que podem vir da internet ou de outros dispositivos, como pen drives. É preciso configurar para que faça varreduras periódicas e sempre que um arquivo for acessado pela primeira vez.
Firewall	Conjunto de instruções definidas que analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas, protegendo a rede de ameaças. O firewall pode ser um hardware ou um software.
Proxy	Utilizado normalmente como ponte entre origem e destino de uma requisição. Os servidores proxy ajudam a evitar acessos inesperados a destinos indesejados pela serventia.
Banco de Dados	É conjunto estruturado de dados, em suporte eletrônico ou físico. É importante que tenha uma boa performance e espaço para armazenamento. A plataforma de banco de dados deverá possuir recurso de trilha de auditoria ativada.

b) mecanismos de segurança desde a concepção de novos produtos ou serviços (security by design)

Ao utilizar a expressão “security by design”, o Provimento remete à conhecida metodologia *privacy by design* (PbD), desenvolvida por Ann

Cavoukian e adotada por inúmeras legislações mundo afora, inclusive pela LGPD (art. 46, § 2º).

O PbD se baseia em 7 princípios: (1) ação proativa, não reativa, ou seja, ato preventivo, e não corretivo; (2) privacidade como a configuração padrão; (3) privacidade incorporada ao design; (4) funcionalidade completa, devendo ocorrer uma soma positiva, e não soma zero; (5) segurança de ponta a ponta, para garantir a proteção total do ciclo de vida do tratamento de dados; (6) visibilidade e transparência; e (7) respeito pela privacidade do usuário, colocando os seus interesses no centro.

Aplicado à segurança, tal metodologia é o *security by design*: a preocupação com segurança permeia todos os procedimentos. Veja os exemplos abaixo:

- Se vou contratar um novo fornecedor de sistema operacional, faço uma análise de riscos e exijo desse fornecedor a demonstração de que seu software é seguro.
- Se uma atualização legislativa criar uma nova atribuição para o cartório, pensarei em como desempenhá-la com segurança.
- Se eu aderir a um convênio prevendo uso compartilhado de dados com órgãos públicos, tomo precauções antes de começar as transferências de dados.

c) plano de resposta a incidentes

No tratamento dos dados sempre há vulnerabilidades que, se exploradas, poderão gerar incidentes. Eles geralmente se relacionam aos seguintes fatores:

- **Sistemas:** falhas técnicas ou de processos de TI
- **Pessoas:** conduta errônea do profissional responsável pelo uso e manutenção dos ativos

- **Invasões:** atores externos que promovem ataques mal intencionados com o objetivo de roubar dados ou simplesmente destruí-los

O incidente de segurança é um evento que impacta negativamente um dos três atributos da informação[16]. Para entender, veja a tabela:

Atributo	Definição	Exemplos de incidente
Confidencialidade	Acesso restrito a pessoas autorizadas	Envio de dados a pessoa errada; Fofoca; Roubo de dados; Acessos não autorizados a documentos e sistemas
Integridade	Informação correta e atualizada	Alteração indevida de dados no sistema
Disponibilidade	Acesso à informação quando necessário	Extravio de documentos; Sequestro de Dados; Sistema operacional indisponível

Quando for constatado que o incidente apresentar *"risco ou dano relevante aos titulares"* (art. 48, LGPD), ele deve ser comunicado à ANPD e aos corregedores (Juiz Corregedor Permanente e Corregedoria Geral da Justiça).

Nas situações em que **não possuir risco relevante** – como por exemplo, o envio de um e-mail contendo poucos dados para pessoa errada – o cartório ainda assim deverá manter um registro do incidente, que pode ser cobrado em futuras fiscalizações.

Segundo a LGPD, a comunicação deve ser realizada preferencialmente de maneira imediata, ou em **prazo razoável**, indicando os motivos da demora (art. 48, § 1º). Segundo o Provimento, o prazo máximo é de 48 horas úteis.

Ao receber a comunicação, as autoridades verificarão a gravidade do incidente, podendo determinar medidas para reverter ou mitigar seus efeitos.

[16] BAARS, Hans; HITZBERGEN, Jule; HITZBERGEN, Kees; SMULDERS, André. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. Brasport, 2018. Ebook.

Em certos casos, é possível que também exijam a divulgação do fato em meios de comunicação (art. 48, § 2º, LGPD), a fim de alertar os titulares de dados afetados, o que possibilitará que adotem medidas protetivas por sua conta.

Avaliação de sistemas e análises de segurança

Além da Política de Segurança – e da implementação das medidas técnicas e administrativas do Provimento 74 – o Provimento prevê que as serventias possuam meios de avaliar sistemas e comunicações.

Não basta possuir mecanismos de segurança, é preciso garantir sua efetividade prática e melhoria contínua, a partir das seguintes atividades:

1. Avaliação periódica das configurações do ambiente tecnológico;
2. Testes nos sistemas operacionais e novas tecnologias de softwares;
3. Monitoramento do ambiente crítico;
4. Treinamento dos profissionais responsáveis pelas tecnologias, serviços para garantir o uso máximo da capacidade e performance.

Se adotadas de maneira consistente, essas medidas permitem uma gestão de riscos eficaz, que evitará muitos incidentes ou mitigará o impacto daqueles que forem inevitáveis.

Por fim, o Provimento se refere a “realização de treinamentos” como uma das medidas de segurança. Esse tema, porém, será abordado quando comentarmos o **Capítulo VIII** do Provimento, que trata apenas do Treinamento.

Gestão de documentos

As informações utilizadas pela serventia são geralmentearmazenadas em suporte digital, a maioria acondicionada em sistemas operacionais fornecidos por empresas especializadas.

A preponderância do digital é uma consequência do progresso tecnológico. Diante disso, o art. 15 do Provimento orienta que a digitalização do acervo seja realizada sempre que possível, em consonância com o dever de manter os dados em “formato interoperável” (art. 25, LGPD).

Ainda assim, o armazenamento de arquivos físicos é bastante recorrente para conservar documentos de colaboradores e atos jurídicos contemplados em livros e documentos oficiais.

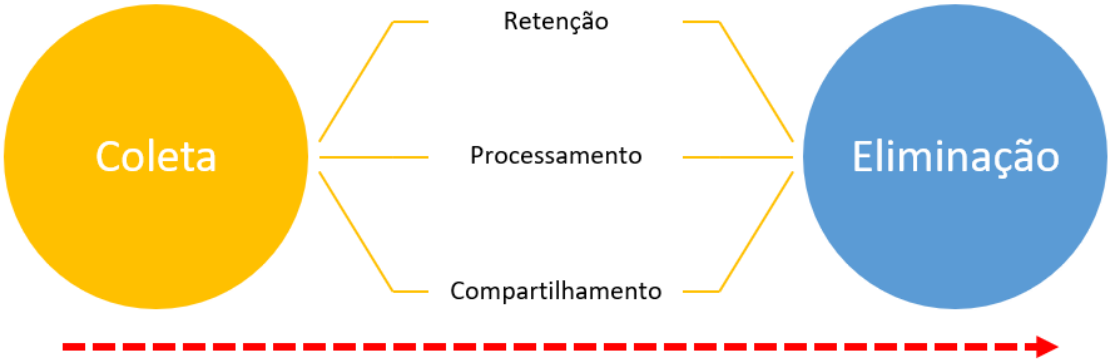
A gestão dos documentos exige um controle auditável para restringir a retirada de documentos pelos funcionários, tampouco mecanismo que permita a rastreabilidade do documento em caso de extravio.

Para tanto, recomenda-se o controle de entrada e saída de informação de maneira documental. O **registro de entrada/saída** de documentos deve ser efetuado de imediato, contendo as seguintes informações: (i) data de saída ou recebimento; (ii) nome do receptor; (iii) descrição do documento. A título de exemplo, esse mecanismo é similar ao utilizado em bibliotecas. Além disso, como medida adicional, pode-se instalar câmeras de segurança em todas as salas em que sejam armazenados arquivos físicos.

Também é recomendável o **controle de impressões**. O ideal seria um controle com uso de senha, a fim de permitir a rastreabilidade do fluxo de informações em caráter físico. Caso as impressoras não possuam a funcionalidade de controle por senhas, recomenda-se afixar ao lado de cada equipamento um cartaz de conscientização sobre o uso adequado das impressoras, conforme as regras de segurança do cartório.

Ciclo de Vida dos dados e Descarte

O movimento feito pelos dados pessoais dentro do cartório é o Fluxo de Dados, ao passo que o itinerário percorrido é o seu Ciclo de Vida. Esse itinerário tem 5 etapas:



A **COLETA** é a entrada dos dados na serventia. Ela pode ocorrer por via física ou digital, através de diversos canais de recepção: preenchimento de formulários e cadastros (no site ou no balcão de atendimento); qualificação de documentos; comunicações entre cartórios; consultas a bancos de dados estatais, de centrais ou de entidades de classe; recrutamento de pessoal; troca de e-mails e mensagens; dentre outros.

Uma vez inserida nos bancos de dados do cartório, a informação passará por uma (ou mais de uma) das três fases seguintes dizem respeito às principais formas de destinar os dados coletados:

	Conceito	Exemplos nos cartórios
Processamento	Classificação, utilização, reprodução, avaliação, modificação ou controle da informação	O processamento de dados ocorre em quase todas as atividades praticadas no cartório, sejam elas atividades-fim (lavrar, protestar, registrar, etc.) ou atividades meio (contratar, gerenciar, pagar, etc).
Retenção	Armazenamento, físico ou digital.	Os cartórios têm como uma de suas principais funções o armazenamento seguro do seu acervo. Além disso, precisam reter documentação de colaboradores.
Compartilhamento	Transmissão, distribuição, comunicação ou difusão	Ocorre por meio da emissão de certidões, bem como de todas as formas de transferência de dados (corregedorias, outras serventias, entidades de classe, centrais de serviços, instituições bancárias, corregedorias e entes estatais diversos).

O Ciclo de Vida se encerra com a **ELIMINAÇÃO**. Ela deverá ocorrer quando: **(1)** foi alcançada a finalidade do tratamento; **(2)** o período previsto de tratamento terminou; **(3)** houve justa solicitação do titular de dados; **(4)** houve determinação pelo Judiciário ou pela ANPD.

No caso dos cartórios, o Provimento nº 50/2015 do CNJ determina o período previsto de tratamento dos dados inscritos nos documentos oficiais da serventia. Ainda assim, é preciso organizar uma **Tabela de Temporalidade** para orientar o descarte de informações não contempladas nesse provimento, como os dados de colaboradores, por exemplo.

Segundo o art. 2º do Provimento 50, “documentos que venham a ser descartados devem ser previamente desfigurados de modo que as informações não possam ser recuperadas, especialmente as indicações de identidade pessoal e assinaturas”.

Para descarte de papel, é recomendável utilizar máquinas fragmentadoras; para descarte de mídias eletrônicas, recomenda-se a destruição ou a a sanitização de *hardware*.

Note-se que, segundo o Provimento, a eliminação de documentos não afasta a responsabilidade pelo tratamento dos dados que “remanescerem em índices, classificadores, indicadores, banco de dados, arquivos de segurança ou qualquer outro modo de conservação adotado pelo cartório”.

Isso reforça a importância de possuir um Inventário de Dados Pessoais (IDP) completo e vem executado, que permita o rastreamento de todos os dados e oriente sua eliminação completa.

CAPÍTULO VIII - 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 associação de classe para capacitação de seus prepostos

Comentários

A simples atualização legislativa não gera, por si só, a mudança comportamental esperada das pessoas. A eficácia social da LGPD depende de um constante esforço de adaptação e de uma mudança de consciência da população. Ciente disso, o CNJ destinou um capítulo à parte do Provimento 134 apenas para tratar dos treinamentos.

Note-se que o Provimento prevê dois objetivos para os treinamentos: a implementação da **cultura de privacidade e proteção de dados** e a **capacitação** sobre os novos controles, processos e procedimentos.

Não se trata de pleonasmo, pois essa distinção é relevante na prática. O treinamento da equipe envolve duas facetas a racional (intelecto) e a axiológica (valores). Se é preciso conhecer os aspectos técnicos da LGPD, também é fundamental internalizar o valor dela para a organização.

Do ponto de vista prático, aspecto racional se alcança pela **capacitação**: **ensinar** aspetos técnicos sobre o que deve ser feito (controles, processos e procedimentos). Por sua vez, o aspecto axiológico se conquista pela **conscientização**: **educar** sobre importância de respeitar os direitos dos titulares de dados, a fim de criar uma cultura de proteção de dados.

Engajamento de toda a equipe

Qualquer um pode contribuir ou obstaculizar a proteção de dados. O cartório pode ter um excelente sistema de segurança e mesmo assim ser envolvido em vazamentos de dados porque algum funcionário cometeu um erro pequeno que veio a comprometer todo o acervo.

Treinar a equipe não é simplesmente inscrevê-la em cursos e eventos. O engajamento verdadeiramente eficaz é a adesão autêntica, profunda e duradoura. Ela depende do envolvimento coletivo num propósito em comum, em que todos se sintam responsáveis e aptos a prestar contas.

E isso só é possível se o responsável pela serventia se envolver pessoalmente nessas ações educativas, estando presente nas palestras, participando ativamente, fomentando o debate e sempre ressaltando, da sua própria boca, a importância do tema. Esse apoio é fundamental para o sucesso do projeto, sendo uma tarefa indelegável.

Também é preciso respeitar as diferenças individuais, tais como limitações culturais e de níveis hierárquicos, exigindo mais daqueles que podem compreender mais. Com essas adaptações, o plano de conscientização acaba sendo muito mais eficaz.

Enfim, sem a adesão e o engajamento da equipe – através de uma mudança cultural – dificilmente terá sucesso qualquer projeto de implementação. Portanto, o investimento em ações educacionais faz parte da estratégia de adequação à LGPD bem sucedida de qualquer atividade, sob pena de todo os investimentos restantes se tornarem infrutíferos.

Certificados e comprovantes

O dever de manter os comprovantes da participação em atividades formativas efetiva o princípio da responsabilização e prestação de contas, previsto no art. 6º, X da LGPD.

Interessante destacar que o Provimento 134 orienta que a documentação comprobatória indique o “conteúdo das orientações transmitidas”. É algo que não existe em todos os certificados, mas que à luz da nova regra é interessante começar a cobrar dos fornecedores de serviços educacionais.

Treinamentos periódicos e de integração

Engana-se aquele que entender é o suficiente tomar apenas medidas pontuais e datadas. A esperada adesão de todos às políticas de tratamento de dados pessoais só ocorre por meio das ações educacionais constantes e diversificadas.

Portanto, transcorrida a etapa de conscientização ou sensibilização inicial, é preciso constante rememoração por meio de treinamentos regulares para atualizar e reciclar o conhecimento e o envolvimento da equipe.

Além disso, é preciso garantir que novos colaboradores tenham acesso às capacitações, mediante treinamentos chamados “de integração”.

Programa de conscientização

A organização e o planejamento sempre fazem a diferença e por isso o Provimento 134 determina que seja feito um “programa de conscientização”. Esse programa contribui para que as atividades não sejam abandonadas em meio ao peso das tarefas cotidianas.

Nessa tarefa, o delegatário deve contar com seu encarregado de dados, em cujas atribuições está a orientação da equipe a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (art. 41, III, LGPD).

O conteúdo desse programa não é algo fixo, mas deve ser devidamente direcionado ao público que o recebe, variando conforme três aspectos principais:

- **natureza dos dados tratados**: a orientação para os integrantes da equipe em cuja função existe maior tratamento de dados sensíveis deve possuir maior carga horária de treinamento.
- **tipo de tratamento realizado:** difere o treinamento conforme a complexidade do tratamento realizado. Por exemplo, pessoas que efetuam processamento dos dados para a realização de assentos notariais/registrais executam atividades mais complexas do que aqueles que apenas coletam dados no balcão de atendimento.
- **nível hierárquico**: o treinamento deve ser direcionado conforme o poder de decisão da pessoa na organização. Em ordem crescente: estagiários; auxiliares do cartório; escreventes; substitutos.

Estabelecido os critérios básicos, o delegatário pode se valer de diferentes instrumentos para concretizar as orientações:

1. **Acesso facilitado**: é fundamental providenciar o acesso facilitado os documentos próprios da implementação, como políticas e manuais de conduta. Não se trata apenas de divulgar no site, pois facilitar quer dizer deixar em formato amigável e próximo do cotidiano. Isso pode ser feito de inúmeras maneiras, com criatividade. Recomenda-se, por exemplo: deixar versões impressas em papel colorido em locais de maior visibilidade entre os funcionários; enviar e-mails semanais contendo trechos da política (para ser lida parte a parte); utilizar a criatividade, por

meio de “apps, games, cartilhas, guias, panfletos, avisos, jornais internos”[17];

2. **Linguagem acessível**: os documentos da adequação, como políticas e manuais, devem ter sido redigidos em linguagem acessível e facilitada, para fácil compreensão de todos. Fazer isso sem perder a necessária qualidade técnica é um grande desafio, daí a vantagem da contratação de consultorias especializadas para esse serviço;
3. **Formação**: ninguém nasce sabendo. Não adianta mandar as pessoas lerem a lei seca da LGPD e dos regulamentos pertinentes. E mesmo a leitura de publicações técnicas (como este livro, por exemplo) não garante a sua compreensão. É preciso algum tipo de orientação mais humanizada sobre os conceitos envolvidos, uma tutoria que adapte a formação às necessidades de cada público. Por isso, é preciso investir em bons treinamentos para a equipe;
4. **Reuniões abertas**: a efetividade de programas de compliance depende de um engajamento real e profundo. Promover reuniões periódicas com a equipe sobre temas relevantes para o cartório, ouvindo o que todos têm a dizer, é uma forma muito eficiente para conquistar uma adesão real e profunda. Nesses encontros, as pessoas precisam ser ouvidas, para retirar suas dúvidas e fazer sugestões, e tudo o que disserem deve ser levado em consideração com respeito.
5. **Divulgação interna**: o *ser humano é aquele que esquece*, como diriam os antigos. Para manter uma cultura de privacidade, é preciso constantemente rememorar as pessoas, o que pode ser feito de maneira discreta, mas constate: envio de e-mails semanais; afixação de cartazes nas paredes ou nas mesas de trabalho; conversas individuais; criação de uma “semana de privacidade”, na qual todos são incentivados a prestarem mais atenção no tema; etc.

[17] VIEIRA, Elba L. C. A proteção de dados desde a concepção (*by design*) e por padrão (*by defaut*) in MALDONADO, Viviane Nóbrega (coord). **Lei Geral de Proteção de Dados Pessoais**: manual de implementação. São Paulo: Thompson Reuters, 2019. p. 239.

6. **Observatório de novidades**: a ideia é fornecer um repositório de informações de privacidade e proteção de dados sempre atualizado para a equipe. Para tanto, é recomendável designar um colaborador para ser responsável por monitorar as publicações sobre o tema e trazê-las à equipe, sobretudo as produzidas pelo Poder Judiciário, pela ANPD e pelas associações de notários e registradores. Esse colaborador pode ser o encarregado de proteção de dados, no caso da LGPD.

CAPÍTULO IX - 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

I – fluxo para atendimento aos direitos dos titulares de dados pessoais, requisições e/ou reclamações apresentadas, desde o seu ingresso até o fornecimento da resposta.

Art. 18. Deverão ser divulgadas em local de fácil visualização e consulta pelo público informações básicas a respeito dos procedimentos de tratamento de dados, especialmente:

I – quais dados são coletados e para quais finalidades;

II – os direitos dos titulares dos dados;

III – o canal de atendimento disponibilizado aos titulares de dados para que exerçam seus direitos; e

IV – 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.

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.

Comentários

Levando em consideração que o objetivo da LGPD é tutelar os direitos dos titulares de dados, com vistas ao desenvolvimento de sua personalidade, as medidas contempladas neste capítulo do Provimento estão entre as mais importantes.

Canal de Atendimento

O canal de atendimento nada mais é que um mecanismo visível para que os titulares de dados possam enviar solicitações sobre a LGPD.

Em termos práticos, é um formulário para envio de e-mails com algumas opções pré-definidas disposto no site da serventia (ou em suas dependências físicas). No exemplo abaixo, veja-se os campos mínimos recomendados:

Canal de atendimento
Nome completo:
E-mail:
Assunto:
Mensagem:

Caso a serventia deseje aprimorar ainda mais a comunicação, pode colocar opções no campo “Assunto”, indicando por exemplo a qual direito do art. 18 da LGPD a solicitação do titular está se referindo.

A forma de disponibilização do canal de atendimento, física ou digital, é de livre escolha de cada serventia. A única exigência é que ele esteja disponível de maneira visível para todos os interessados; para tanto, recomenda-se que sempre seja afixado na serventia um cartaz de divulgação com os dados do encarregado e o meio de acesso ao canal de atendimento.

Se o Canal de Atendimento for eletrônico, é preciso tomar o cuidado de direcionar os e-mails à pessoa correta.

Fluxo para atendimento aos direitos dos titulares

Quando as normas se referem a fluxos, procedimentos e políticas, querem com isso dizer que é preciso de algo **escrito**.

Sem prejuízo de maiores detalhamentos, entende-se pertinentes os seguintes passos para o fluxo:

(i) localização do cadastro do solicitante (se houver);
(ii) verificação da identidade do solicitante;
(iii) análise jurídica do pedido;
(iv) adoção das medidas cabíveis;
(v) comunicação a terceiros que tenham ingerência sobre os dados;
(vi) registro do atendimento.

Desses itens, destaca-se a **verificação da identidade do titular**, que é muito importante para evitar o repasse de informações a terceiros desautorizados. A verificação pode se dar de diferentes maneiras, tais como solicitação de envio de documentos por e-mail, confirmação de dados por ligação ou mesmo do recebimento de SMS/WhatsApp.

Por fim, é importante ressaltar que sempre se deve registrar os atendimentos das solicitações, mesmo que a resposta seja negativa. Isso é muito importante para que a serventia possua provas de que está cumprindo a LGPD e atende os direitos dos titulares.

Aviso de Privacidade de Proteção de Dados

Também chamado de “política de privacidade”, o aviso de privacidade e proteção de dados é documento informativo pelo qual o cartório informa aos interessados como efetua o tratamento de dados pessoais, qual a legitimidade desse tratamento e como os direitos dos titulares estão sendo respeitados.

Esse aviso torna público, a todos os interessados, os principais aspectos da atividade de tratamento realizada por determinado agente. Logo, sua principal função é o direito de informação do titular de dados, que decorre **princípio da transparência**, previsto no art. 6º, V da LGPD.

A partir do que consta no Provimento 134, na LGPD e em padrões de boas práticas, tem-se que uma aviso de privacidade deve conter no mínimo:

(1) Conceitos fundamentais. Como a política de privacidade é um documento informativo, é interessante fazer constar nelas algumas definições básicas necessárias para que os leitores compreendam do que ela trata sem precisar consultar outras fontes. É interessante constar, por exemplo, o conceito de dados pessoais, de titular de dados, de agentes de tratamento, etc.

(2) Orientações sobre direitos dos titulares. É conveniente indicar algumas orientações básicas sobre como os titulares podem exercer seus direitos. Para tanto, recomenda-se que conste os contatos do Encarregado, da Autoridade Nacional de Proteção de dados (ANPD) e das corregedorias, com orientações sobre como fazer requerimentos.

(3) Relação de dados tratados e a finalidade do tratamento. Envolve a informação dos dados pessoais que a serventia trata e qual a finalidade do tratamento (motivo). Disso se antevê que o mapeamento de dados prévio é necessário para que a política de privacidade seja realizada de maneira adequada.

(4) Legitimação do tratamento (bases legais). Todo o tratamento de dados deve ser subsumido a alguma das hipóteses de tratamento previstas nos artigos 7º e 11 da LGPD (para dados pessoais comuns e sensíveis, respectivamente). Por isso, é preciso informar ao titular a legitimação de cada tipo de tratamento realizado.

Caso seja utilizada a base legal de consentimento, a LGPD descarta a importância de informar ao titular sobre a possibilidade de não conceder consentimento, bem como de revogá-lo a qualquer tempo (conforme art. 18, VIII e IX da LGPD.

(5) Relação de agentes de tratamento com os quais os dados são compartilhados. É importante que haja informações claras o uso compartilhado de dados. Tanto assim é, que prevê essa informação como um direito específico, contemplado no art. 18, VII da LGPD.

Nesse sentido, é preciso se atentar a política de privacidade deve ser específica, pois cada cartório é livre para escolher seus fornecedores e prestadores de serviço. Não faz sentido algum “copiar” a política de privacidade integralmente sem contemplar a realidade do compartilhamento de dados no cartório em específico.

Direitos dos Titulares de Dados

O art. 18 da LGPD elenca o rol de direitos dos titulares. Embora esse rol não seja exaustivo, é um excelente parâmetro. Abaixo, mencionam-se as hipóteses legais de maneira resumida, para facilitar a compreensão:

Direito	Explicação
Confirmação de tratamento	O titular tem direito de saber o agente de tratamento utiliza seus dados de alguma forma. Trata-se de uma resposta “sim” ou “não”, dada de forma imediata.
Acesso aos dados	O acesso pode ser concedido de duas formas: (i) em formato simplificado, com prazo imediato (art. 19, I, LGPD); ou (ii) por meio de declaração completa, com prazo de 15 dias (art. 19, II, LGPD).
Correção de dados	Os titulares têm direito de que seus dados sejam completos, exatos e atualizados. Caso contrário, podem pedir as devidas correções.
Eliminação de dados	Quando verificar que há algum tratamento de dados realizado em desconformidade com a LGPD, o titular tem direito de exigir a eliminação dos dados.
Revogação do consentimento	Como ato de vontade livre, informado e inequívoco, o consentimento pode ser revogado a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado (art. 8º, § 5º, LGPD).
Portabilidade dos dados	A portabilidade é o direito de requisitar de um fornecedor de serviços ou produtos a transferência de seus dados a outro fornecedor do mesmo setor.
Informação	O princípio da transparência concede aos titulares de dados um dever geral de informação. O conteúdo básico das informações a que tem direito é previsto nos artigos 9º e 18 da LGPD.

A tabela acima fornece um panorama sobre os direitos dos titulares, mas a operacionalização nos cartórios depende de adaptações.

Abaixo, comentam-se alguns dos direitos que mais comumente são exercidos em face de serventias extrajudiciais.

Informações

O direito à informação é um reflexo do princípio da transparência, que garante aos titulares de dados "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" (art. 6º, VI da LGPD). De maneira mais concreta, o dever de informação abarca os elementos contidos no art. 9º da LGPD, bem como do art. 18 do Provimento 134.

Como dito, o Aviso de Privacidade é o principal documento para cumprir o dever de transparência. Todavia, o dever de informação não se encerra num único documento, devendo ser considerado em todas as comunicações com os titulares, inclusive as realizadas mediante atendimento presencial ou telefônico.

Retificação e eliminação

É evidente que atos notariais e registrais inscritos nos livros da serventia merecem retificação, quando contiverem informação equivocada. Todavia, a natureza pública destes documentos exige procedimentos específicos para que isso ocorra. Diante disso, os pedidos de retificação de informações nos atos oficiais dos cartórios – mesmo que tais informações sejam pessoais – devem seguir tais procedimentos.

Note-se, porém, uma ressalva: o item acima diz respeito a "dado pessoal constante em registro e em ato notarial". Não abarca, portanto, outros cadastros e bancos de dados, como as informações sobre os colaboradores do cartório, por exemplo.

Nada impede que as informações que não constam em atos registrais ou notariais propriamente ditos sofram retificação de maneira simplificada e gratuita.

Acesso

A maior parte das disposições do Provimento 134 sobre direitos dos titulares de dados aborda o direito de acesso. Isso faz bastante sentido, já que não haveria sentido na função notarial e registral de conservar informações se não houvesse a possibilidade de consulta.

Com efeito, os titulares de dados têm direito de acesso a seus dados pessoais por meio gratuito (sem cobrança de emolumentos) e facilitado (sem

burocracias desnecessárias). Contudo, tal direito não se confunde com a emissão de certidões. Estas são documentos com fé pública, ao contrário de qualquer documento impresso fornecido a título de direito de acesso.

A tabela resume bem essa diferença entre o pedido com base no direito de acesso e a requisição de certidões:

	Direito de acesso	Certidões
Fundamento	LGPD (art. 18, II) e Provimento 134 do CNJ (art. 20)	Lei nº 8.935/1994 (artigos 10, IV, 11, VII 13, III), Lei 6.015/1973 (artigo 16, I).
Objetivo	Informar ao titular detalhes referentes ao tratamento de seus dados pessoais.	Fazer prova com mesmo valor que o documento original, com fé pública e presunção de veracidade (Lei 6.015/1973, artigo 194).
Abrangência	Dados pessoais constantes nos sistemas administrativos da serventia.	Dados próprios do acervo registral.
Custo	Sempre gratuito.	Exige pagamento de emolumentos, salvo em hipóteses de gratuidade específicas. (Lei 6.015/1973, artigo 14).
Formato	Tem acesso facilitado, verbal ou escrito.	É um documento escrito, fornecido em meio digital ou em papel, com os requisitos legais e regulamentares.
Destinatário	Apenas ao titular de dados, que deve estar identificado (ou seu mandatário).	Qualquer pessoa que faça o requerimento. (Lei 6.015/1973, artigos 16, I e 17, caput).

CAPÍTULO X - DAS CERTIDÕES E COMPARTILHAMENTO DE 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.

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.

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 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.

Art. 26. Os registradores e notários poderão remeter os dados com a finalidade da formação de índices e indicadores estatísticos a suas entidades associativas, desde que estes sejam anonimizados ou pseudonimizados, nos termos da Lei Geral de Proteção de Dados.

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.

Comentários

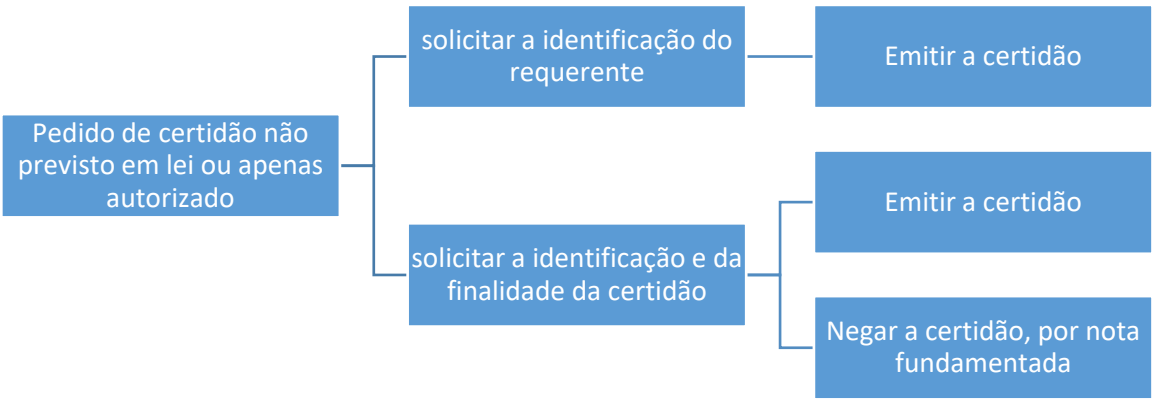
A Constituição Federal (art. 5º, XXXIV, "b") e a Lei de Registros Públicos (art. 17) preveem o direito dos cidadãos de pedir certidões, bem como o dever das serventias de emiti-las.

Após a vigência da LGPD, é preciso que essa atividade de tratamento de dados seja adequada. Não se trata de uma oposição limitante, mas de um contrapeso que harmoniza o interesse público (publicidade notarial e registral) e os direitos fundamentais do cidadão (proteção de dados e privacidade).

Para tanto, o Provimento 134 estabeleceu no art. 21 critérios gerais para emissão de certidões, trazendo regras mais específicas nos capítulos destinados ao regramento de cada especialidade.

O primeiro critério geral é a **previsão legal expressa** para o pedido de certidão, de forma que o interessado precisa da certidão para garantir direitos. Nesses casos, a emissão da certidão deve ocorrer normalmente.

Se o pedido for apenas autorizado em lei – ou se não possuir nenhuma previsão legal –, deve-se fazer a análise o tipo de requerimento, segundo as regras específicas de cada especialidade. A partir disso, deve-se tomar alguma das medidas abaixo:



Nas hipóteses em que solicitar a finalidade da certidão, o delegatário deve qualificá-la. O objetivo é entender se a emissão da certidão é compatível com o sistema de proteção de dados brasileiro, de modo a não ofender os direitos dos titulares de dados pessoais.

Nessa avaliação, o delegatário deve aplicar um juízo de ponderação, apurando a adequação, a necessidade e a proporcionalidade do conteúdo da certidão e da finalidade apontada.

Evidentemente, não é apenas com base num juízo subjetivo que as certidões podem ser negadas. Para isso, existem regras diferentes para cada especialidade, conforme as regras previstas nos próximos capítulos do Provimento, a serem comentados mais adiante.

Nas hipóteses de o requerimento de certidão por via telemática, o solicitante será identificado por meio reconhecido pela entidade responsável pela tramitação do serviço eletrônico (isto é, central ou operador nacional).

Uso compartilhado de dados

A primeira questão importante sobre o compartilhamento de dados com as centrais é que ele está legitimado de antemão pelo início do texto do art. 23 (“O compartilhamento de dados com centrais de serviços eletrônicos compartilhados é compatível com a proteção de dados pessoais”).

Embora haja respeitável posicionamento em sentido contrário[18], uma vez em vigor o Provimento 134, entende-se superada a questão do ponto de vista prático. Ainda assim, a crítica trouxe importante consideração sobre a necessidade os riscos dessa centralização.

[18] DONEDA, Danilo; BACHUR, João P.; FUJIMOTO, Mônica. As centrais de cartórios e os riscos à proteção de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/as-centrais-de-cartorios-e-os-riscos-a-protecao-de-dados-pessoais-01062021. Acesso em 26 set. 2022.

O parágrafo único do art. 23 serve como contrapeso a tais riscos, ao prever a “descentralização das bases de dados” pela limitação do repasse de informações às centrais além do que seja estritamente necessário, “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”.

Com igual propósito, o art. 24 disciplina o compartilhamento de dados com órgãos públicos, também bastante frequente no cotidiano das serventias. O critério para a legalidade desse compartilhamento é a existência de previsão escrita que legitime tal compartilhamento: lei, ato normativo do órgão solicitante, convênio ou outro instrumento formal. Destaque-se que tal instrumento deve possuir “objeto compatível com as atribuições e competências legais da atividade notarial e registral”.

Em respeito ao princípio da necessidade (art. 6º, III, LGPD), as informações compartilhadas devem ser específicas, adequadas, necessárias e proporcionais ao atendimento das finalidades presentes na política pública perseguida pelo órgão. O objetivo dessas restrições é evitar a transferência de bancos de dados, a não ser quando isso seja estritamente necessário.

Caso entenda haver desproporcionalidade na solicitação de compartilhamento de dados pelo órgão público, o delegatário deverá “consultar a Corregedoria Nacional de Justiça, no prazo de 24 horas, oferecendo suas razões”.

Esse mecanismo de consulta é extremamente benéfico para garantir a efetividade prática das restrições de compartilhamento estabelecidas no Provimento, pois evita que o delegatário precise “assumir” a responsabilidade por negar dados a órgãos públicos, contornando uma série de inconvenientes.

O art. 25 orienta a adoção de medida técnica de segurança da informação para salvaguardar o uso compartilhado de dados. Alternativamente, cabe ao delegatário promover a criptografia ou a pseudonimização dos dados compartilhados, desde que isso seja viável (“sempre que possível”). Além de

viável, a medida deve ser compatível com a finalidade perseguida e tipo de tratamento de dados realizado.

A criptografia é uma técnica pela certo conjunto de dados é convertido de um formato legível para um ilegível. A reversão da criptografia é feita por meio de uma chave criptográfica de acesso restrito.

Definida no § 4º do art. 13 da LGPD, a pseudonimização é retirar a associação do dado pessoal com seu titular. Após a aplicação da técnica de pseudonimização, o dado pessoal não é passível de associação direta com uma pessoa, a não ser pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Por fim, a art. 26 prevê a possibilidade de os registradores e notários compartilharem dados com suas entidades associativas para a formação de "índices e indicadores estatísticos", desde que estes sejam anonimizados ou pseudonimizados.

A anonimização é a aplicação de técnica que retira a característica de dado pessoal de determinada informação, de maneira irreversível. A irreversibilidade do processo de anonimização não precisa ser absoluta, mas deve ser segura considerando os "meios técnicos razoáveis e disponíveis na ocasião" (art. 5º, III, LGPD).

CAPÍTULOS SOBRE CADA ESPECIALIDADE

CAPÍTULO XI - DO TABELIONATO DE NOTAS

Art. 28. A emissão e o fornecimento de certidão de ficha de firma e dos documentos depositados por ocasião de sua abertura somente poderão ser realizados a pedido do titular referido nos documentos, seus representantes legais e mandatários com poderes especiais ou mediante decisão judicial.

Art. 29. O fornecimento de certidões para os solicitantes legitimados pode ocorrer por meio de cópia reprográfica.

Art. 30. O pedido de lavratura de ata notarial, realizado por um dos pais, ou pelo responsável legal, envolvendo dados pessoais de sujeito menor de 12 (doze) anos de idade será considerado como consentimento específico e em destaque para o tratamento dos dados da criança.

Art. 31. Nos atos protocolares e nas escrituras públicas, não haverá necessidade de inserção da condição de pessoa exposta politicamente.

Art. 32. A certidão de testamento somente poderá ser fornecida ao próprio testador ou mediante ordem judicial.

Parágrafo único. Após o falecimento, a certidão de testamento poderá ser fornecida ao solicitante que apresentar a certidão de óbito.

Art. 33. No ato notarial, serão inseridos na qualificação dos sujeitos: o nome completo de todas as partes; o documento de identificação, ou, na sua falta, a filiação; o número de CPF; a nacionalidade; o estado civil; a existência de união estável; a profissão e o domicílio, sendo dispensada a inserção de endereço eletrônico e número de telefone.

CAPÍTULO XII - DO REGISTRO DE TÍTULOS E DOCUMENTOS E CIVIL DE PESSOAS JURÍDICAS

Art. 34. As notificações que contenham dados pessoais tratados devem ser feitas preferencialmente pelo Registro de Títulos e Documentos da circunscrição do destinatário. Quando assim não ocorrer, a notificação deverá ser enviada juntamente com folha adicional informativa com os dados tratados do notificado.

CAPÍTULO XIII - DO REGISTRO CIVIL DE PESSOAS NATURAIS

Art. 35. É livre o acesso às informações constantes nos livros de Registro Civil das Pessoas Naturais, por meio de certidões de breve relato, com as informações regulamentadas pelo Provimento n. 63/2017, da Corregedoria Nacional de Justiça, independentemente de requerimento ou de identificação do requerente.

Art. 36. As certidões de registro civil em geral, inclusive as de inteiro teor, requeridas pelos próprios interessados, seus representantes legais, mandatários com poderes especiais, serão expedidas independentemente de autorização do Juiz Corregedor Permanente.

§ 1º Nas hipóteses em que a emissão da certidão for requerida por terceiros e a certidão contiver dados sensíveis, somente será feita a expedição mediante a autorização do juízo competente.

§ 2º Após o falecimento do titular do dado sensível, as certidões de que trata o caput deste artigo poderão ser fornecidas aos parentes em linha reta, independentemente de autorização judicial.

Art. 37. Nas certidões de breve relato deverão constar somente as informações previstas no Provimento CN n. 63/2017, sendo que qualquer outra informação solicitada pela parte constante do registro ou anotações e averbações posteriores somente poderá ser fornecida por meio de certidão por quesitos ou por inteiro teor, de acordo com as disposições previstas neste Provimento.

Parágrafo único. Sempre deverão constar do campo destinado às observações a existência de adoção simples realizada por meio escritura pública; as alterações de nome indígena; a declaração do registrado como indígena; a etnia ou a inclusão de etnia; e a alteração de nome em razão da cultura ou do costume indígena.

Art. 38. As solicitações de certidões por quesitos, ou informações solicitadas independentemente da expedição de certidões, receberão o mesmo tratamento destinado às certidões solicitadas em inteiro teor quando os dados solicitados forem restritos, sensíveis ou sigilosos.

§ 1º São considerados elementos sensíveis os elencados no inciso II do art. 5º da Lei n. 13.709/2018, ou outros, desde que previstos em legislação específica.

§ 2º São considerados elementos restritos os previstos nos artigos 45 e 95 da Lei n. 6.015/1973, no artigo 6º e seus parágrafos, da Lei n. 8.560/1992, e no artigo 5º do Provimento n. 73/ 2018, da Corregedoria Nacional de Justiça, ou outros, desde que previstos em legislação específica.

§ 3º São considerados elementos sigilosos os previstos no parágrafo 7º do artigo 57 da Lei n. 6.015/1973, ou outros, desde que previstos em legislação específica.

Art. 39. A emissão de certidão em inteiro teor sempre depende de requerimento escrito com firma reconhecida do requerente ou com assinatura digital nos padrões ICP-Brasil, no padrão do sistema gov.br ou com assinatura confrontada com o documento de identidade original.

§ 1º O reconhecimento de firma será dispensado quando o requerimento for firmado na presença do Oficial ou de preposto.

§ 2º Os requerimentos poderão ser recepcionados por e-mail ou por meio da Central de Informações do Registro Civil – CRC, desde que assinados digitalmente, nos padrões da ICP-Brasil, cuja autenticidade e integridade serão conferidas no verificador de conformidade do ITI – Instituto Nacional de Tecnologia da Informação, por meio do sistema de assinatura gov.br ou com assinatura confrontada com o documento de identidade original.

§ 3º O requerimento de certidão em inteiro teor deverá conter a identificação do requerente, o motivo em virtude do qual se requer a certidão sob a forma de inteiro teor e o grau de parentesco com o registrado, caso exista, bem como o fato de ser este falecido ou não.

§ 4º A certidão com referência à circunstância de ser legítima a filiação poderá ser fornecida, inclusive a terceiros, independentemente de autorização judicial.

Art. 40. Não é necessário requerimento ou autorização judicial para emissão de certidão de óbito em nenhuma de suas modalidades.

Art. 41. As restrições relativas aos dados sensíveis elencados pelo inciso II do art. 5º da Lei n. 13.709/2018 não se aplicam ao caso de pessoa falecida.

Art. 42. A emissão e o fornecimento de certidão sobre procedimentos preparatórios ou documentos apresentados para a realização de atos no Registro Civil das Pessoas Naturais somente poderão ser realizados a pedido do próprio interessado ou do titular do documento, seus representantes legais e mandatários com poderes especiais ou mediante autorização judicial ou, ainda, quando o documento solicitado for público com publicidade geral e irrestrita.

Parágrafo único. Após o falecimento do titular, a certidão de que trata o caput deste artigo poderá ser fornecida ao solicitante que apresentar a certidão de óbito.

Art. 43. É facultado a qualquer interessado, independentemente de justificação ou de requerimento, realizar buscas nos índices dos Registros Civis das Pessoas Naturais, respeitados os emolumentos estabelecidos pelas legislações estaduais.

Parágrafo único. A realização de buscas baseadas em outras fontes, além dos índices de registros dos livros do cartório, somente será autorizada mediante requerimento escrito fundamentado, sujeito à análise de finalidade pelo Oficial do Registro Civil das Pessoas Naturais, de cuja decisão, em caso de indeferimento, caberá revisão pelo juiz competente.

Art. 44. O edital de proclamas conterá tão somente o nome, o estado civil, a filiação, a cidade e circunscrição do domicílio dos noivos.

Parágrafo único. Quando os nubentes residirem em circunscrições diferentes, constará do edital o endereço dos nubentes para a comprovação deste fato, nos termos do art. 67, § 4º, da Lei n. 6.015/1973.

CAPÍTULO XIV - 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.

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.

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.

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.

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.

CAPÍTULO XV - DO PROTESTO DE TÍTULOS E OUTROS DOCUMENTOS DE DÍVIDA

Art. 51. Das certidões individuais de protesto deverão constar, sempre que disponíveis, os dados enumerados no art. 17, parágrafo único, do Provimento 87, da Corregedoria Nacional de Justiça, excetuados endereço completo, endereço eletrônico e telefone do devedor.

Art. 52. As certidões em forma de relação sobre inadimplementos por pessoas naturais serão elaboradas pelo nome e CPF dos devedores, devidamente identificados, devendo abranger protestos por falta de pagamento, de aceite ou de devolução, vedada exclusão ou omissão, espécie do título ou documento de dívida, data do vencimento da dívida, data do protesto da dívida e valor protestado.

Art. 53. Nas informações complementares requeridas em lote ou em grande volume poderão constar CPF dos devedores, espécie do título ou documento de dívida, número do título ou documento de dívida, data da emissão e data do vencimento da dívida, valor protestado, protocolo e data do protocolo, livro e folha do registro de protesto, data do protesto, nome e endereço do cartório.

Art. 54. O fornecimento de cópias ou certidões de documentos arquivados na serventia se limita ao documento protestado propriamente dito, nos termos do art. 22 da Lei n. 9.492/1997, enquanto perdurar o protesto, e dentro do prazo máximo de 10 (dez) anos, nos termos do art. 30 Lei n. 9.492/1997, não devendo ser fornecidas cópias dos demais documentos, salvo para as partes ou com autorização judicial.

Parágrafo único. Tratando-se de documento de identificação pessoal, a cópia arquivada somente deve ser fornecida ao próprio titular.

Art. 55. O tabelião de protesto poderá devolver ou eliminar documentos apresentados para protesto ou para cancelamento que forem considerados desnecessários à prática do ato almejado, após adequada qualificação.

§ 1º O documento cujo original não precise ser guardado por imposição legal deve ser eliminado de maneira segura quando for digitalizado, evitando-se a duplicidade (art. 35, § 2º, Lei n. 9.492/1997).

§ 2º Fica o tabelião de protesto autorizado a eliminar o documento após o término do prazo da tabela de temporalidade prevista no Provimento 50, da Corregedoria Nacional de Justiça, ou superada a necessidade de sua guarda por outras circunstâncias, tais como prescrição civil, tributária e penal.

Art. 56. Antes da expedição do edital para intimação do devedor, o tabelião poderá buscar outros endereços em sua base de dados, endereços em que outros tabeliães realizaram a intimação, desde que na mesma base da sua competência

territorial, ou endereços eletrônicos, a serem compartilhados por meio da CENPROT, bem como endereços constantes de bases de natureza jurídica pública e de acesso livre e disponível ao tabelião.

Parágrafo único. A CENPROT deverá compartilhar entre os tabeliães os endereços em que foi possível a realização da intimação de devedores, acompanhado do CNPJ ou CPF do intimado, bem como da data de efetivação.

Art. 57. A declaração eletrônica de anuência para fins de cancelamento de protesto, recebida na forma prevista no art. 17, inciso V, do Provimento 87, da Corregedoria Nacional de Justiça, poderá ser comunicada ao interessado por meio dos Correios, empresas especializadas, portador do próprio tabelião ou correspondência eletrônica, via internet ou qualquer outro aplicativo de mensagem, ficando autorizado o encaminhamento de boleto bancário, outro meio de pagamento ou instruções para pagamento dos emolumentos e despesas relativos ao cancelamento do protesto.

Comentários

As disposições a respeito de cada especialidade são regras bastante precisas, cujo cumprimento não depende de intepretações abertas.

Esse tipo de interpretação ocorrerá quando for necessário analisar se a finalidade de determinado pedido de certidão está de acordo com sistema de proteção de dados. Mas para esse tipo de análise já bastam os comentários feitos para o art. 21 do Provimento, em capítulo anterior.

CAPÍTULO XVI - DAS DISPOSIÇÕES FINAIS

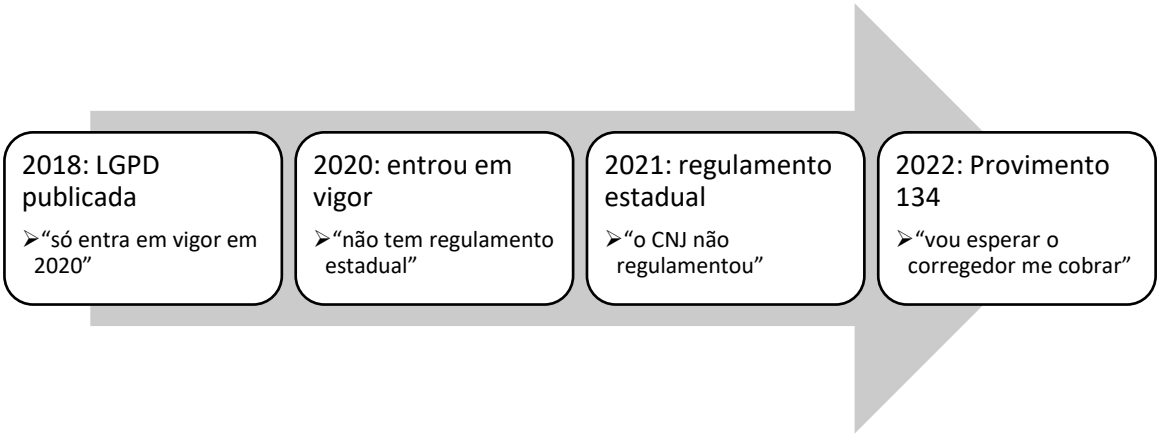
> Art. 58. As Corregedorias Gerais da Justiça dos Estados e do Distrito Federal fiscalizarão a efetiva observância das normas previstas neste Provimento pelas unidades do serviço extrajudicial, expedindo as normas complementares que se fizerem necessárias, bem como promoverão, no prazo estabelecido no 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.

Comentários

Ao longo dos primeiros anos de vigência da LGPD, a maior parte das Corregedoras-gerais da Justiça publicaram provimentos sobre o tema. Em vários casos, esse provimentos são diferentes do que ficou consolidado no Provimento 134. Diante disso, a previsão do art. 58 é importante para evitar conflitos de normas que poderiam causar insegurança jurídica.

Como a LGPD já está vigente há mais de 2 anos, espera-se que a adequação já tenha sido feita há muito tempo. Nesse sentido, o prazo de 180 dias do art. 59 diz respeito apenas às adaptações às novidades trazidas pelo Provimento 134.

Porém, não é difícil constatar que muitas serventias encarrem esse novo prazo como a exigência final de adequação à LGPD como um todo. Pois sempre existe uma “desculpa”, como as que constam na linha do tempo abaixo:



Mas nossa ideia aqui não é criticar ninguém pelo que já passou. Temos sempre ter uma visão de futuro. “Ok, não me adequei, mas agora eu vou dar a devida atenção à LGPD no meu cartório“. Esse é o espírito!

O que realmente não recomendamos é achar uma nova desculpa para procrastinar um dever que já existe há anos. Como você pode constatar ao longo desses comentários, a LGPD é uma coisa séria e demanda muito trabalho para ser cumprida.

Não brinque com a segurança do seu acervo, não crie situações em que você pode ser facilmente punido pela corregedoria e condenado em ações cíveis e trabalhistas.

Mas não encare o dever de adequação como um fardo pesado, como uma exigência “sem sentido” que o CNJ está impondo porque é um órgão “chato”. Encare como uma oportunidade de proteger mais seu acervo e criar um ambiente onde as pessoas sejam mais respeitadas, auxiliando ainda mais na sua missão de garantir segurança jurídica!

E nessa missão, conte com a equipe do ICNR. Estaremos muito felizes em te atender!

Clique aqui para falar com o ICNR!