

## **Aula 00**

*TJ-MG (Oficial Judiciário) Lei de proteção  
de dados pessoais*

Autor:

**Paulo H M Sousa**

16 de Fevereiro de 2023

# Índice

1) Lei Geral de Proteção de Ddaos Pessoais - Parte I .....	3
--	---



# LEI DE PROTEÇÃO DE DADOS

## 1. DISPOSIÇÕES GERAIS



Do que trata a LGPD? Ela **dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado**. E por que é necessário tratar dos dados das pessoas? De acordo com o art. 1º, o **objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**.

O parágrafo único ainda prevê que as normas gerais contidas na lei são de interesse nacional e, por isso, devem ser observadas pela União, Estados, Distrito Federal e Municípios.

A norma disciplina da proteção de dados pessoais e tem certos fundamentos a lhe sustentar. Conforme o art. 2º, **a proteção de dados pessoais tem como fundamentos:**

- Respeito à privacidade
- Autodeterminação informativa
- Liberdade de expressão, de informação, de comunicação e de opinião
- Inviolabilidade da intimidade, da honra e da imagem
- Desenvolvimento econômico e tecnológico e inovação
- Livre iniciativa, livre concorrência e defesa do consumidor
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais

Qual o âmbito de aplicação da proteção dos dados pessoais? Enuncia o art. 3º que **a lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:**



I. A operação de tratamento seja realizada no território nacional

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

III. Os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Consideram-se coletados no território nacional os dados cujo titular nele se encontre no momento da coleta

Atente para o inc. I. Se a operação de tratamento de dados for realizada no território nacional, deve ser aplicado o inc. IV do art. 4º, visto no quadro abaixo, exige o §2º do art. 3º. Se, de um lado, a lei prevê as hipóteses nas quais ela se aplica, inversamente, prevê o art. 4º que a **lei NÃO se aplica ao tratamento de dados pessoais:**



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

II. Realizado para fins exclusivamente

- a) jornalístico e artísticos
- b) acadêmicos

III. Realizado para fins exclusivos de

- a) segurança pública
- b) defesa nacional
- c) segurança do Estado
- d) atividades de investigação e repressão de infrações penais

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

No caso de dados pessoais utilizados para fins acadêmicos, aplicam-se as regras dos arts. 7º e 11. O art. 7º versa sobre o tratamento de dados pessoais e o art. 11 sobre o tratamento de dados pessoais sensíveis.

Ou seja, **apesar de a LGPD não se aplicar aos dados com fins acadêmicos, no geral, ela se aplica especificamente quanto a esses dois aspectos.** Isso porque, é sabido, é comum o uso extensivo de dados pessoais em pesquisas acadêmicas.

No caso de tratamento de dados para fins de segurança *lato sensu*, versados no inc. III (segurança pública, defesa nacional, segurança do Estado e atividade de investigação e repressão), há alguns cuidados a tomar. Primeiro, **esse tipo de dados é regido por legislação específica**, que deve prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos da lei (§1º). Até o momento, porém, a lei ainda não foi editada.

Segundo, determina o §2º do art. 4º que **fica vedado o tratamento desses dados por pessoa jurídica de direito privado. Poderão as pessoas jurídicas de direito privado fazê-lo, desde que sob tutela de pessoa jurídica de direito público**, que serão objeto de informe específico à autoridade nacional. Ainda assim, as pessoas jurídicas de direito privado não poderão, em nenhum caso, obter a totalidade dos dados pessoais de banco de dados a esse respeito, salvo por aquela que possua capital integralmente constituído pelo poder público (§4º).



Terceiro, a autoridade nacional deve emitir opiniões técnicas ou recomendações referentes às exceções previstas no tratamento de dados para fins de segurança *lato sensu*. Deve, ainda, solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais (§3º).



Na sequência, o art. 5º da LGPD traz uma série de conceitos para a aplicação da lei. Isso é algo bastante comum em leis mais “técnicas”, que extrapolam os limites jurídicos, geralmente no setor de tecnologia, engenharia ou saúde. Assim, **esses são conceitos que VOCÊ DEVE DECORAR:**

**Dado pessoal (*stricto sensu*):** informação relacionada a pessoa natural identificada ou identificável.

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

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

**Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

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

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

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

**Encarregado:** pessoa indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

**Agentes de tratamento:** o controlador e o operador.

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

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

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



**Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

**Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

**Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

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

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

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

**Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Chamo sua atenção para dois detalhes, que têm mais probabilidade de aparecerem numa prova, dado o potencial de pegadinhas. Primeiro, distingue-se dado pessoal de dado pessoal sensível, sem que se conceitue precisamente o que é dado pessoal. Por isso, tudo o que não é dado pessoal sensível é dado pessoal *stricto sensu*. Por exemplo, endereço ou CPF.



Segundo, veja que **apenas controlador e operador são considerados agentes de tratamento, mas não o encarregado. Além disso, o controlador e o operador podem ser pessoas jurídicas, mas o encarregado sempre será pessoa natural.**

No tratamento de dados pessoais deve-se observar o princípio da boa-fé. Além desse princípio geral do Direito Privado, **quais outros princípios específicos devem ser observados?** O art. 6º os minudencia:

**Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

**Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

**Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

**Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

**Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

**Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

**Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

**Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

**Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

**Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

## 2. TRATAMENTO DOS DADOS PESSOAIS

Ao versar sobre o tratamento de dados pessoais, a lei **distingue os dados pessoais** (informação relacionada a pessoa natural identificada ou identificável) **dos dados pessoais sensíveis** (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural). Mas não só.

**Distingue-se ainda o tratamento dos dados pessoais *lato sensu*, que englobam os dados pessoais *stricto sensu* e dados pessoais sensíveis, dos dados pessoais de crianças e adolescentes.**

### 2.1. Requisitos para tratamento dos dados pessoais

Quando é possível tratar de dados pessoais? Na dicção do art. 7º, **o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:**

- I. Mediante o fornecimento de consentimento pelo titular;
- II. Para o cumprimento de obrigação legal ou regulatória pelo controlador



- III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (neste caso, nos termos da Lei 9.307/1996, a Lei de Arbitragem);
- VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

**Em regra, o tratamento de dados pessoais exige fornecimento de consentimento específico do titular (art. 7º, inc. I), mas em outras hipóteses não se exige o consentimento (art. 7º, incs. II a X). No entanto, é dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo próprio titular, resguardados os direitos do titular e os princípios previstos na lei (§4º).**

Mesmo quando o controlador obteve o consentimento da pessoa, se necessitar comunicar ou compartilhar dados pessoais com outros controladores **deve obter consentimento específico do titular para esse fim**, exige o §5º. Evidentemente, isso não se exige quando se trata de dispensa do consentimento.

Assim, por exemplo, se uma farmácia obteve minha autorização para tratamento de meus dados pessoais, exige-se que ela obtenha autorização específica para compartilhar essas informações com terceiros. No entanto, se a informação é exigida por entidade de proteção de crédito, não é necessário minha anuência, pelo que a farmácia pode fornecer meus dados a essa pessoa jurídica diretamente.

De qualquer forma, a eventual dispensa da exigência do consentimento – seja pela publicação dos dados pelo titular, seja pela dispensa legal – não desobriga os agentes de tratamento das demais obrigações previstas em lei. Isso vale, especialmente, para a observância dos princípios gerais e para a garantia dos direitos do titular, detalha o §6º.

Não à toa, o §3º determina que **o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização**. Por isso, pode-se dar publicidade a respeito dos rendimentos de um servidor público, mas não é adequado que se detalhe que um certo desconto em sua folha foi feito para indenizar alguém, por exemplo.





Além disso, o tratamento posterior dos dados pessoais a que se referem os §§3º e 4º pode ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na lei (§7º).

E como se dará o consentimento do titular? De acordo com o art. 8º, **o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular**. Assim, a lei exige forma escrita para o consentimento, mas não afasta a validade de consentimento dado verbalmente, desde que, por exemplo, ele tenha sido gravado em vídeo.

Isso é bastante salutar, especialmente numa sociedade de massas na qual ficar guardando montanhas de papel é injustificável, física e economicamente. Além disso, num contato telefônico, por exemplo, isso seria praticamente impossível. De qualquer sorte, **cabe ao controlador que detém os dados o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na lei (§2º)**.



**O consentimento deve ser específico**, ou seja, deve referir-se a finalidades determinadas.

Assim, nulas são as autorizações genéricas para o tratamento de dados pessoais, não deixa margem de dúvida o §4º.

Veda-se, conseqüentemente, o tratamento de dados pessoais mediante vício de consentimento (art. 8º, §3º). Reiterando essa noção, o art. 9º, §1º, estabelece que na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

E é possível que esse consentimento esteja contido dentro do próprio contrato celebrado pelo titular dos dados? Sim, caso o consentimento seja fornecido por escrito, isso é possível, desde que conste de cláusula destacada das demais cláusulas contratuais (art. 8º, §1º).

De outra banda, **o consentimento pode ser revogado a qualquer momento** mediante manifestação expressa do titular. O §5º esclarece que **a revogação se faz por procedimento gratuito e facilitado**. Ficam desde já ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

E se for alterada a finalidade específica do tratamento, a forma e duração do tratamento, a identificação do controlador ou o uso compartilhado de dados, o que ocorre? Obriga o §6º que, nesses casos, o controlador informe ao titular, com destaque de forma específica do teor das alterações. Pode o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

De modo a facilitar o controle do titular sobre seus dados, ele **deve ter acesso facilitado às informações sobre o tratamento de seus dados**. Isso deve ser disponibilizado de forma clara, adequada e ostensiva acerca de, entre outras, características previstas em regulamentação para o atendimento do princípio do livre acesso (art. 9º):

- I. Finalidade específica do tratamento;
- II. Forma e duração do tratamento, observados os segredos comercial e industrial;



- III. Identificação do controlador;
- IV. Informações de contato do controlador;
- V. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI. Responsabilidades dos agentes que realizarão o tratamento;
- VII. Direitos do titular (com menção explícita aos direitos previstos no art. 18);

**Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato.** Deve ser também informado sobre os meios pelos quais poderá exercer seus direitos de titular elencados no art. 18 da Lei, estatui o §3º.

E quando o controlador pode obter e tratar dados pessoais? Essa é uma das questões mais importantes da LGPD, já que, atualmente, a maioria dos dados pessoais colhidos não parece ter necessidade. Você já não foi abordado por algum atendente exigindo uma longa lista de informações ao tentar comprar um chiclete ou uma aspirina?

Pois é. Por isso, o controlador somente pode fundamentar o tratamento de dados pessoais para finalidades legítimas. Mas, o que é uma finalidade legítima? O art. 10 traz **um rol exemplificativo (numerus apertus) de situações concretas que permitem legitimamente fundamentar o tratamento de dados pessoais:**

- Apoio e promoção de atividades do controlador;
- Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais;

Veja que a primeira situação traz uma margem de discricionariedade expressiva. Mas não é bem assim. **Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (§1º).**

O controlador ainda deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse (§2º). Além disso, a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (§3º).

## 2.2. Tratamento de dados pessoais sensíveis

O tratamento de dados pessoais sensíveis tem regulamentação específica, em razão, bem, da “sensibilidade” dos dados. Mas, **o que é mesmo “dado sensível”?** Dados pessoais sensíveis são aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.



Pois bem. Não pode haver tratamento de dados pessoais sensíveis com a mesma liberdade que há em relação aos demais dados pessoais *stricto sensu*. De acordo com o art. 11, **o tratamento de dados pessoais sensíveis somente pode ocorrer nas seguintes hipóteses:**

I. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II. Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- A) Cumprimento de obrigação legal ou regulatória pelo controlador;
- B) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- C) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- D) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (neste caso, nos termos da Lei 9.307/1996, a Lei de Arbitragem);
- E) Proteção da vida ou da incolumidade física do titular ou de terceiro;
- F) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- G) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Prevê o §1º que **essa regra se aplica a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular**. A ressalva fica por conta do disposto em legislação específica.

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica pode ser objeto de vedação ou de regulamentação por parte da autoridade nacional (§3º). Antes disso, porém, deve ouvir os órgãos setoriais do Poder Público, no âmbito de suas competências.

Além disso, **veda-se a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica. As exceções ficam por conta da portabilidade de dados consentida pelo titular e das transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo (§4º, incs. I e II)**. Isso ocorre, por exemplo, na migração de um plano de saúde a outro.



Igualmente vedado às operadoras de planos de saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (§5º). Trata-se de norma evidente, para evitar a discriminação de potenciais contratantes.

Especificamente nos casos de cumprimento de obrigação legal ou regulatória pelo controlador e de tratamento compartilhado de dados necessários à execução de políticas públicas (alíneas “a” e “b” supramencionadas), é dispensado o consentimento do titular. No entanto, exige-se (§2º) publicidade à referida dispensa de consentimento, nos termos do inc. I do art. 23 da lei.

ESCLARECENDO!



E se os dados, mesmo que sensíveis, forem anonimizados? O art. 12 prevê que **os dados anonimizados não serão considerados dados pessoais para os fins legais**. Ou seja, podem ser utilizados mais livremente.

No entanto, **se o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido, não são eles considerados anonimizados (caput), e continuam a ser tratados como dados pessoais**. Podem ser igualmente considerados como dados pessoais os dados utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (§2º).

A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (§1º). A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais – CNPDP (§3º).

O art. 13 permite que, **na realização de estudos em saúde pública, os órgãos de pesquisa tenham acesso a bases de dados pessoais. Esses dados devem ser tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas** e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico.

A segurança deve incluir, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese pode revelar dados pessoais (§1º).

Veja que a LGPD distingue a anonimização da pseudonimização. A anonimização é o ato de tornar um dado anônimo, de modo que não se saiba quem é o titular. Já o §4º **define a pseudonimização como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro**.

CURIOSIDADE



E quem é responsável por isso? Prevê o §2º que **o órgão de pesquisa é o responsável pela segurança da informação; não permitida, em circunstância alguma, a transferência dos dados a terceiro**.

Por fim, o acesso aos dados supramencionados será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências, arremata o §3º.



### 2.3. Tratamento de dados pessoais de crianças e adolescentes

Em se tratando de tratamento de dados pessoais de crianças e de adolescentes, a LGPD tem norma específica, tendo em vista a sensibilidade aguçada envolvida. O art. 14 determina que **o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse**, nos termos da LGPD e do ECA.

**Para que seja feito o tratamento de dados pessoais de crianças, deve-se obter o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (§1º).** Nesse caso, os controladores devem manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos previstos no art. 18, prevê o §2º.

**Podem ser coletados dados pessoais de crianças sem o consentimento antes mencionado? Sim, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento. Igualmente, podem ser coletados tais dados para proteção da criança.** De qualquer forma, em nenhum caso poderão ser repassados a terceiro sem o consentimento específico supramencionado (§3º).

Agora, desçamos à Terra novamente. Muito comum que crianças e adolescentes tenham acesso praticamente irrestrito a recursos de tecnologia em casa. Computadores, celulares, *tablets* e toda a parafernália tecnológica que nos rodeia está a apenas um dedo de distância.

Como o controlador do aplicativo *Candy Crush* saberá que eu assisti meu filho na inserção de dados pessoais? Como o aplicativo *Saúde* do *iPhone* sabe que eu consenti no tratamento de dados obtidos simplesmente porque a pessoa carrega o celular no bolso?

Primeiro, **os controladores não deverão condicionar a participação dos titulares em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (§4º).** Não só isso, estabelece o §5º que **o controlador deve realizar todos os esforços razoáveis para verificar que o consentimento exigido foi dado pelo responsável pela criança**, consideradas as tecnologias disponíveis.



Ora, atualmente é razoável a um aplicativo altamente rentável, como o *Candy Crush*, que ele seja obrigado a exigir autenticação biométrica ou facial dos responsáveis legais pela criança? Evidente que sim. Boa parte dos novos celulares vêm com recurso biométrico e todos eles, já há muitos anos, contam com câmera. Isso é tecnologicamente viável.

O *Candy Crush* certamente alegará, com grande dose de razão, que isso traz custos extras. E traz. Mas a equação é simples. Se o aplicativo não quer ter de obter esse consentimento, basta não tratar dados pessoais, ou seja, deixar as pessoas acessá-lo sem armazenar informações.

Mas não é potencialmente a informação que ele armazena uma fonte de recursos no “mercado das informações” digitais? Precisamente. Veja que muitos desses aplicativos têm, há muito tempo, um bônus, que é o de utilizar as informações das pessoas gratuitamente. Não podem, portanto, reclamar de um ônus, qual seja o de tratar essas informações de maneira adequada, clara e pública.

Por fim, as informações sobre o tratamento de dados referidas deverão ser fornecidas de maneira simples, clara e acessível. Isso deve levar em consideração as características físico-motoras, perceptivas,



sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (§ 6º).



**Há um detalhe no art. 14 da LGPD. Ao passo que o *caput* trata de “crianças e adolescentes”, o §1º fala apenas em “crianças”. Erro do legislador ou intencional?**

Não sei. E nem você. O fato é que se aparecesse na minha prova “o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal”, eu marcaria INCORRETO. Falo isso porque a literalidade do §1º diz “crianças”.

Isso porque o art. 2º da Lei 8.069/1990, o ECA, estabelece que se considera criança a pessoa até 12 anos de idade incompletos, e adolescente aquela entre 12 e 18 anos de idade. Crianças e adolescentes compreendem faixas etárias distintas.

Pela literalidade da LGPD, portanto, não é necessário obter o consentimento dos responsáveis legais daqueles que tenham mais de 12 anos, mas o é caso o absolutamente incapaz tenha menos de 16 anos. Se eu fosse um examinador melindroso, confundiria você ainda mais: absolutamente e relativamente incapaz.

Isso porque toda criança é absolutamente incapaz (porque tem menos de 12 anos), mas há adolescentes que são absolutamente incapazes (entre 12 e 16 anos) e adolescentes que são relativamente incapazes (entre 16 e 18 anos). Sacou que dá pra jogar com esses conceitos e fazer pegadinhas bobas, mas fáceis de cair, se você não estiver 100% ligado?

## 2.4. Término do tratamento de dados

Os dados podem ser tratados eternamente? Não. De acordo com o art. 15, **o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:**

- I. Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- II. Fim do período de tratamento;
- III. Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;
- IV. Determinação da autoridade nacional, quando houver violação ao disposto na lei.



Alcançado o término do tratamento de dados, o que fazer com eles? Estabelece o art. 16 que **os dados pessoais devem ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades. Autoriza-se, porém, sua conservação para:**

- I. Cumprimento de obrigação legal ou regulatória pelo controlador;



- II. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei;
- IV. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados;

### 3. DIREITOS DO TITULAR



De maneira sóbria, a LGPD estabelece que a **titularidade dos dados pessoais é da própria pessoa natural**. Isso é assegurado pelo art. 17, que ainda menciona os direitos fundamentais de liberdade, de intimidade e de privacidade. Por isso, rege o art. 18 que **o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:**

I. Confirmação da existência de tratamento

II. Acesso aos dados

III. Correção de dados incompletos, inexatos ou desatualizados

IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei

V. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial

VI. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na lei

VII. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa

IX. Revogação do consentimento, nos termos da lei

No caso específico do inc. V, a portabilidade dos dados pessoais não inclui dados que já tenham sido anonimizados pelo controlador. A previsão do §7º é lógica, já que, nesse caso, o controlador já não sabe mais precisamente a quem pertencem os dados anonimizados.

O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional (§1º) e também perante os organismos de defesa do consumidor (§8º).



Ele igualmente **pode se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento legal (§2º).**

Para exercer esses direitos, o titular ou o representante legalmente constituído deve fazer requerimento expresso ao agente de tratamento (§3º). **O requerimento tem de ser gratuito ao titular (§5º).** Em caso de impossibilidade de adoção imediata da providência, o controlador enviará ao titular resposta em que poderá (§4º):



I. Comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente;

II. Indicar as razões de fato ou de direito que impedem a adoção imediata da providência;

O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento (§6º). Exceção se verifica nos casos em que tal comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Como se fará a confirmação de existência ou o acesso a dados pessoais, depois da requisição do titular? Depende de como ela será feita, minudencia o art. 19 em seus dois incisos.

**Se for em formato simplificado, imediatamente. Agora, se for por meio de declaração clara e completa,** que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, **a informação deve ser fornecida no prazo de até 15 dias, contados da data do requerimento do titular.** A autoridade nacional pode dispor de forma diferenciada acerca dos prazos previstos acima para os setores específicos (§4º).

Os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso (§1º). **O fornecimento dessas informações pode se dar, a critério do titular tanto por meio eletrônico, seguro e idôneo para esse fim, quanto sob forma impressa (§2, incisos).**

Quando o tratamento tiver origem em contrato ou no consentimento do titular, ele pode solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional (§3º). A cópia tem de ser emitida em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

O art. 20 da LGPD ainda prevê ao titular dos dados o **direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais** que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Houve sutil mudança do dispositivo com a Lei 13.709/2019, que deixou de exigir que a revisão fosse feita por “pessoa física”.

O controlador deve fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada (§1º). **Se não forem dadas essas informações, sob a justificativa de segredo comercial e industrial, a autoridade nacional pode realizar auditoria** para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (§2º).





**A justificativa pode ser plausível, ou não.** Por exemplo, o *Google* não se tornou o maior motor de buscas na *internet* à toa. Nem o *Facebook* se tornou a maior rede social do mundo por puro acaso.

Ambos os aplicativos se tornaram os maiores de sua espécie precisamente por se utilizarem de algoritmos complexos que lhes trouxeram vantagens em relação aos concorrentes. Não podem ser tornados públicos esses critérios e procedimentos sem que haja uma perda econômica grave a ambos.

ESCLARECENDO!



**Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo,** esclarece o art. 21. Essa é uma questão complexa, já que dificilmente uma sociedade empresarial de concessão de crédito não levará em conta o histórico do consumidor que já ajuizou dezoito ações revisionais de contrato bancário, ou um empregador simplesmente ignorará que o candidato a emprego já reclamou quatorze vezes contra empregadores prévios. A lei, porém, proíbe tais práticas.

Por fim, o art. 22 determina que a defesa dos interesses e dos direitos dos titulares de dados pode ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. No caso, aplicáveis as normas do CDC, do CPC/2015, da Lei da Ação Civil Pública etc.

# ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



**1** Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



**2** Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



**3** Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



**4** Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



**5** Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



**6** Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



**7** Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



**8** O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.