LEI GERAL DE PROTEÇÃO DE DADOS – LGPD E OS SERVIÇOS NOTARIAIS E DE REGISTROS

MARCELO Guimarães RODRIGUES

Desembargador do
Tribunal de Justiça do Estado de Minas Gerais

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD E OS SERVIÇOS NOTARIAIS E DE REGISTROS

CNB/MG

Belo Horizonte

2021

Revisão: Cida Ribeiro

Projeto gráfico e diagramação: Walter Santos

Capa: João Corsino

COLÉGIO NOTARIAL DO BRASIL - SEÇÃO MINAS GERAIS

Av. Afonso Pena, 4.374, 3º andar - Bairro Cruzeiro - Belo Horizonte

Entrada pela rua lateral - Américo Diamantino, 91 - 3º andar

Contatos:

contato@cnbmg.org.br

(31) 3284-7500

R696l Rodrigues, Marcelo Guimarães

Lei Geral de Proteção de Dados – LGPD e os Serviços Notariais e de Registros. / Marcelo Guimarães Rodrigues. – Belo Horizonte : Colégio Notarial do Brasil - MG, 2021.

243 p.
ISBN 978-65-992759-0-6

1. Direito notarial e registral. 2. Lei Geral de Proteção de Dados. 3. Registros Públicos. I. Título.

CDU: 347.961(815.1)

À minha mãe, Amarilis Leite Guimarães, violinista e professora virtuosa. Mãe e mulher destemida.

SUMÁRIO

Apresentação

Eduardo Calais 9

1 Introdução 13

2 Enquadramento Constitucional 17

3 Do acesso à informação (art. 5º, inc. XXXIII, CR e Lei federal 12.527/2011) 29

4 O contexto da Lei 13.709/2018 (LGPD) 35

4.1 O que mudou com a redação dada pela Lei 13.853, de 8 de julho de 2019 42

4.2 Sobre a estrutura e inspiração da LGPD brasileira 45

4.3 Direito comparado 47

4.4 Importância, estrutura e alcance da LGPD 53

4.5 Sobre os dados pessoais e os dados sensíveis 60

4.6 Sobre a transferência internacional de dados e acórdão do Tribunal de Justiça (Grande Seção) da União Europeia 62

4.7 Do consentimento 74

4.8 Assimetrias entre a LGPD, a Lei do Cadastro Positivo e o Marco Civil da Internet 78

4.9 Correção, anonimização, pseudonimização, bloqueio ou eliminação de dados pessoais 80

4.10 Do controlador, operador, encarregado e titular 85

4.11 Da segurança e do sigilo de dados 89

4.12 Dados de conteúdo *versus* dados de tráfego: interpretação à luz dos princípios constitucionais 95

4.13 Efeitos da LGPD nas relações do trabalho 106

a) Na fase pré-contratual de recrutamento e seleção 106

b) Na fase contratual 107

c) Na fase pós-contratual 108

d) Na etapa ou procedimento de terceirização 108

4.14 Das sanções 109

4.15 Do legítimo interesse do controlador ... 112

4.16 Sobre a *blockchain* e *compliance* na LGPD ... 116

5 Impactos da LGPD nos serviços notariais e de registros ... 121

5.1 Da publicidade notarial e registral ... 129

5.2 Informação *versus* publicidade e direito à privacidade na legislação concernente aos registros públicos ... 134

5.3 Princípio da conservação ... 139

5.4 A publicidade e o legítimo interesse ... 142

5.5 Algumas situações concretas no âmbito das atribuições dos Tabeliães e Oficiais Registradores ... 152

5.6 Da adoção de medidas preventivas ... 157

REFERÊNCIAS ... 167

ANEXO A – Lei 13.709, de 14 de agosto de 2018 (com a redação dada pela Lei 13.853, de 8 de julho de 2019) – Lei Geral de Proteção de Dados Pessoais (LGPD) ... 175

ANEXO B – Decreto nº 10.474, de 26 de agosto de 2020 ... 219

Anexo I – Estrutura Regimental da Autoridade Nacional de Proteção de Dados ... 221

ÍNDICE ALFABÉTICO REMISSIVO ... 239

Apresentação

Há mais de uma década, o matemático britânico Clive Humby cunhou a famosa frase "Data is the new oil", o que, em tradução livre, seria o mesmo que dizer que os dados são o novo petróleo. Todavia, ao contrário da natureza finita do combustível fóssil, os dados seguem crescendo em ritmo avassalador, notadamente em uma sociedade cada mais vez mais digital.

Os dados, contudo, diferentemente do petróleo, não têm um valor imanente, isto é, não possuem um atributo valorativo quando analisados isoladamente – como acontece, por exemplo, com um barril de petróleo – e, para que ganhem significância, deverão ser tratados por alguém que consiga extrair informações relevantes e conclusões aproveitáveis. Diante disso, ganham especial relevância as regras atinentes à forma como esses dados poderão ser tratados, com o objetivo de resguardar um dos bens mais importantes do ser humano: o direito à privacidade e à intimidade. Como conciliar os interesses daqueles que detêm e gerem um sem-número de informações com tais direitos?

Nesse contexto, inspirada na GDPR (*General Data Protection Regulation*), foi editada em 14 de agosto de 2018 a Lei federal 13.709, conhecida como Lei Geral de Proteção de Dados, com o objetivo de regular o tema da proteção dos dados individuais e coletivos no Brasil.

Na qualidade de agentes públicos responsáveis pela guarda de dados dos cidadãos desde o seu nascimento até o final da vida, os notários e registradores atuam gerindo milhões de informações da população brasileira e têm acesso a dados relevantes que merecem tratamento adequado.

Embora os atos notariais e registrais sejam públicos, os dados neles constantes são privados. Essa dicotomia, que até então era pouco explorada, com o advento da LGPD, ganha especial relevância e deverá ser propulsora de uma mudança paradigmática na forma de trabalho dos notários e registradores brasileiros.

Nessa conjuntura, a presente obra ilumina o caminho dos notários e registradores brasileiros que se veem diante de um tema tão relevante, mas ao mesmo tempo desconhecido. Ao fazer uma análise completa e profunda da LGPD com o foco específico na atividade notarial e registral, a presente obra nasce como instrumento essencial para que a nossa classe coloque-se mais uma vez na vanguarda, adequando-se e cumprindo todas as novas exigências normativas, cujos objetivos vão ao encontro daqueles buscados pelos cartórios, qual seja, a proteção do cidadão.

Destaca-se que não apenas para aqueles que militam no Di-reito Notarial e Registral, mas para todos os estudiosos do direito, a presente obra vai surpreender com sua capacidade didática e pedagógica em desbravar um tema novo e tão relevante.

Para aqueles que já tiveram o prazer de estudar o *Tratado de Registros Públicos e Direito Notarial*, bem como o *Código de Normas dos Serviços Notariais e de Registro do Estado de Minas Gerais Comentado*, entre outros artigos e produções acadêmicas do autor, certamente, já sabem o que esperar de mais este trabalho. A dosagem certa de densidade teórica e dogmática, aliada à capacidade de síntese e sistematização por meio de um texto fluído de fácil intelecção fazem do Desembargador Marcelo Rodrigues um dos maiores autores jurídicos do Brasil.

Certamente, estamos diante de um trabalho que influenciará a forma como os notários e registradores enfrentarão o tema da proteção de dados. Temos aqui preciosas lições de um magistrado e doutrinador que, com vasta experiência prática e décadas de estudos, vem construindo sólida e relevante doutrina jurídica no campo do Direito Notarial e Registral brasileiro. Tenho certeza de que esta obra acompanhará todos os notários e registradores espalhados por todo o território nacional, servindo como aliada ao fiel cumprimento do dever que nossa classe tem de proteger as pessoas, seus dados, seu patrimônio e, assim, prover cidadania e justiça.

Eduardo Calais

Tabelião do 1º Cartório de Notas de Igarapé-MG, Presidente do CNB-MG, Vice- Presidente da Serjus/Anoreg-MG, Di-retor do Conselho Federal do CNB. Mestre em Processo Civil pela UFMG e Mestre em Direito Público pela FUMEC.

1

Introdução

Em 14 de agosto de 2018 foi editada e publicada a Lei federal 13.709, já com a redação da Lei federal 13.853, que lhe seguiu em 08/07/19, introduzindo no ordenamento jurídico nacional prin-cípios fundamentais, normas gerais, especiais, finais e também algumas transitórias, a respeito da proteção, tratamento, registro, armazenamento, uso, difusão e compartilhamento – em seus mais variados aspectos – de dados pessoais individuais e coletivos, bem jurídico mais do que relevante, sobretudo reconhecidos como geo-estratégicos a países, governos e corporações, e que, até então, não obstante, vagavam no universo das transações comerciais, pessoais e estatais sem a devida segurança, condicionamento e controle por meio de tutela específica, eficiente e adequada à relevância, complexidade e repercussões nas esferas pública e privada que os cercam.

Vivemos em quadra, conforme já referido, da era da infor-mação, impulsionada pelo notável desenvolvimento e rapidez na disseminação da tecnologia e da ciência, como nunca antes fora na história da humanidade.

Os relacionamentos e interações jurídicos, profissionais, co-merciais, oficiais, sociais e pessoais assumiram novas roupagens e dinâmicas, se tornaram massivos, instantâneos, invasivos, intensivos, impessoais, globalizados e frenéticos até. Em igual medida, exalam também certa fluidez e horizontalidade, tudo conformando o que se denominou de período da pós-modernidade[1].

---

[1] A partir da década de 1970, ocorre uma reestruturação mundial do capitalismo, com a inten-sificação do comércio global, formação de blocos regionais, processo de flexibilização das fronteiras nacionais, centralização do sistema financeiro, bem como uma reorganização do mun-do do trabalho e do processo produtivo, notadamente através da substituição da era indus-trial das máquinas pesadas pelos sistemas de informação e pela revolução tecnológica contínua.
Na política, surge uma reconfiguração do papel do Estado, qual seja, um abandono do Estado do bem-estar social, como fortemente interventor e promotor da cidadania e dos direitos sociais, em favor de um Estado mínimo centrado de forma predominante em garantir a ordem.
As novas tecnologias permitem obter o máximo de flexibilidade no que respeita a processos de produção, desenhos e produtos, bem como a ocupação da força de trabalho, em confronto direto com a rigidez do fordismo.
Ela se apoia na flexibilidade dos processos de trabalho, novos mercados de trabalho, dos produtos e padrões. Caracteriza-se pelo surgimento de setores de produção inteiramente novos, novas maneiras de fornecimento de serviços financeiros, novos mercados e, sobretudo, taxas altamente intensificadas de inovação comercial, tecnológica e organizacional.

A respeito, Bauman[2] elege, dentre as várias definições para a época atual, a expressão *modernidade líquida* para destacar a fluidez da realidade em contraposição à solidez do período anterior.

Conforme discorro no *Tratado de registros públicos e direito notarial*:[3]

> Essa fluidez não é apenas *econômica* – que transfere em questões de segundo grandes volumes de capital de um canto do mundo a outro, ou de uma empresa que se instala em um país e dele migra tão rápido quanto entrou – ou *política* – mudanças contínuas de legislação, leis de patentes, fim dos direitos adquiridos dos trabalhadores, crise dos partidos tradicionais de esquerda e de direita etc. –, ela também se reproduz nas demais áreas da vida humana, como as *relações pessoais* – amor e amizade cada vez mais fluidos e passageiros, identidade pessoal fluida –, o *lazer* – intensificação do turismo, das migrações –, as *artes* e o *conhecimento acadêmico*, cada vez mais ávido por novidades, em especial nas áreas tecnológicas.

Nesse cenário desafiador, recolher, armazenar, tratar, usufruir e compartilhar dados pessoais assume feição estratégica a justificar a atuação e controle preventivos do Estado, de modo a exprimir, mediante um conjunto de princípios e normas cogentes, os valores expressos na Constituição da República, nomeadamente no que concerne ao objetivo maior de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da persona-lidade da pessoa natural" (art. 1º, *caput*).

A nova lei passa a integrar importante e, a esta altura, robusto microssistema, a exemplo da Lei 9.507/1997, da Lei 12.414/2011 (com a redação fornecida pela Lei Complementar 166/2019), da Lei 12.527/2011, da Lei 12.965/2014, assim como os respectivos decretos regulamentadores,[4] bem como o Provimento 88, de 1º/10/19, da Corregedoria Nacional de Justiça, municiando o ordenamento ju-rídico com normas, princípios e instrumentos especiais, alguns tidos mesmo como inovadores, dado resultar 'de interesse nacional' e de observância obrigatória 'pela União, Estados, Distrito Federal e Municípios' (§1º, art. 1º), além das pessoas jurídicas de direito público e privado. E, como tal, não escapa à órbita de atuação das serventias do

---

[2] BAUMAN, Zygmunt. *Modernidade líquida*. Rio de Janeiro: Zahar, 2001.

[3] RODRIGUES, Marcelo. *Tratado de registros públicos e direito notarial*. 2. ed. São Paulo: Atlas, 2016, p. 502.

[4] **Lei 9.507/97** (Lei do Habeas Data), regula o direito de acesso a informações e disciplina o rito processual do *habeas data*; **Código Civil** (art. 11 a 21, Capítulo II, Título I, Livro I, Parte Geral: Dos Direitos da Personalidade das Pessoas Naturais); **Lei 12.414/11** (Lei do Cadastro Positivo), convertida da MP 518/10, disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, e foi regulamentada pelo Decreto 9.936, de 24/07/19; **Lei 12.527/11** (Lei do Acesso à Informação), regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei 8.112, de 11 de dezembro de 1990; revoga a Lei 11.111, de 5 de maio de 2005, e dispositivos da Lei 8.159, de 8 de janeiro de 1991; e dá outras providências e foi regulamentada pelo Decreto 9.690, de 23/01/19, com a redação do Decreto 9.716, de 26/02/19; **Lei 12.965/14** (Marco Civil da Internet), estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, regulamentada pelo Decreto 8.771, de 11/05/16. Em complemento, deve ser acrescido ainda o **Provimento 88, de 1º/10/19, da Corregedoria Nacional de Justiça**, a respeito dos procedimentos e os controles a serem adotados pelos notários e registradores visando à prevenção dos crimes de lavagem de dinheiro, previstos na Lei 9.613, de 3 de março de 1998, e do financiamento do terrorismo, previsto na Lei 13.260, de 16 de março de 2016, e que dá outras providências.

extrajudicial e dos profissionais do Direito que nelas atuam, Tabeliães, Oficiais Registradores e seus prepostos, nos moldes delineados na Lei federal 8.935/1994 (Lei dos Cartórios), ainda que por equiparação (§3º, art. 23).

Como, então, se preparar e precaver, no âmbito das atribuições legais e normativas em que inseridos os serviços notariais e de registros, face às novas responsabilidades e exigências, em área de atuação administrativa voltada, desde sua gênese, a irradiar publi-cidade a respeito dos mais importantes e valiosos atos da vida civil?

Neste ligeiro estudo, naturalmente desprovido da pretensão de esgotar o tema, procuramos alinhavar alguns subsídios que auxiliem na compreensão da matéria e a respeito dos novos desafios a serem superados.
(...)

4.4 Importância, estrutura e alcance da LGPD

O pano de fundo da LGPD resulta da regulação do direito à autodeterminação informativa na era digital premida por uma sociedade centrada na informação. Em jogo, os interesses das garantias individuais da privacidade, honra e vida privada, além da livre circulação da informação numa economia digital baseada, entre outros fatores, no processamento e compartilhamento massivo de dados.

A premissa maior é a de que o cidadão deve ter controle sobre os seus dados pessoais. Para tanto, são alinhadas algumas regras intocáveis:

a) conhecimento;
b) consentimento;
c) oposição; e
d) cancelamento.

Nas sociedades democráticas, o direito à privacidade é um princípio fundador da cidadania e da liberdade de pensamento e de expressão e constitui um instrumento fundamental na limitação do poder dos Estados e das organizações sobre os indivíduos e da construção de relações de confiança. O grande desafio está em garantir o controle sobre a privacidade dos dados nessa sociedade (supostamente) de informação. O crescimento da internet, das redes sociais e de modelos de negócios digitais cria uma equação de difícil resolução: de um lado, os indivíduos atraídos (voluntariamente, seja inconscientemente) a compartilhar com terceiros, com frequência, nem tão próximos, dados de suas vidas pessoais, alguns tangencian-do aspectos íntimos de suas existências e cotidianos, geralmente sem avaliar com lucidez os possíveis efeitos colaterais. De outro, as organizações que capturam cada vez mais informações sobre seus clientes, em certa medida com o objetivo de fornecer mais e melhores serviços e produtos, ou ainda como modo de rentabilizar a informação.

O fato é que as organizações se capacitam para saber cada vez mais sobre os padrões de comportamento, a condição geográfica, social, econômico-financeira,

religiosa, política etc. de seus clientes ou mesmo de potenciais clientes, por vezes, antes deles próprios.

Essa tensão entre o direito à privacidade e a importância que os dados pessoais assumiram no âmbito das organizações experimenta crescimento contínuo e, ao que tudo indica, irrefreável, especialmente a partir do desenvolvimento e oferta de uma gama cada vez mais diversificada de produtos gerados pela inovação tecnológica, a exemplo dos telefones inteligentes, os dispositivos *wearable*[5] ou a *Internet of Things*.[6]

A partir da necessidade de endereçar esses desafios a um ambiente regulatório que exprima e assegure os valores consagrados em nossa Constituição, foi editada a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018).

A LGPD assenta-se nos princípios fundantes da proteção integral da liberdade, privacidade e segurança; consentimento expresso, acesso às informações para correções e imediato atendimento, caso o titular dos dados pessoais (ou representante legal) manifeste a vontade de excluir seus dados, entre outros aspectos.

Compreende os direitos de acesso a todos os dados pessoais, de forma a ensejar, por simples requerimento, retificação, atualização, eliminação, bloqueio, portabilidade (= encaminhamento das infor-mações pessoais do requerente a outras empresas), listagem das entidades públicas e privadas com as quais houve compartilhamento de dados, entre outros, além de eventual reparação de danos morais e materiais na Justiça.

A lei não protegerá somente os dados pessoais digitais, mas igualmente aqueles oriundos de coletas feitas em papel, como fichas de cadastro e cupons promocionais. Dados coletados por intermédio de imagens e sons também ficam englobados na proteção legal.

O art. 17 da LGPD destaca como principal e fundamental direito público subjetivo do indivíduo, quanto ao tema, a incondicional e irre-nunciável titularidade dos dados sobre a pessoa natural respec-tiva.[7] E o exercício desse direito pode se dar a qualquer mo-mento – imprescritível que é – e por meio de simples requisição (art. 18), por si ou por representante, diretamente ao agente de trata-mento: con-trolador (a exemplo de notário ou registrador), seja operador (prestador terceirizado), inclusive quando "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o in-teresse público que justificaram sua disponibilização" (art. 7º,

---

[5] *Wearable* é a palavra que resume o conceito das chamadas 'tecnologias vestíveis', que consistem em dispositivos tecnológicos que podem ser utilizados pelos usuários como peças do vestuário. O vocábulo inglês *wearable* significa 'vestível' ou 'usável', na tradução literal para a língua portuguesa.

[6] A expressão 'Internet das Coisas' se refere a uma revolução tecnológica que tem como objetivo conectar os itens usados do dia a dia à rede mundial de computadores. Cada vez mais surgem eletrodomésticos, meios de transporte e até mesmo tênis, roupas e maçanetas conectadas à Internet e a outros dispositivos, como computadores e *smartphones*.

[7] A PEC 17/2019, em tramitação, pretende alçar este direito ao *status* de garantia fundamental, a exem-plo de outros países.

§3º). Na eventualidade de compartilhamento de dados, cabe aos agentes de tratamento dar ciência com quem compartilhou a respeito da requisição, de modo que toda a cadeia envolvida no compartilhamento confirme a salvaguarda dos direitos do titular.

Especificamente a respeito dos serviços notariais e de registros, a requisição poderá também ser feita ao juiz corregedor e (ou) à Corregedoria-Geral de Justiça, além da própria Autoridade Nacional (art. 18, §1º).

Sem prejuízo, como todo direito, também possui limitações. A requisição, em tese, poderá vir a ser denegada, ainda que não ignorada, desde que com a devida fundamentação. A limitação de tratamento, em caso de bloqueio, será temporal ou quantitativa. Suprimida a não conformidade, apto se torna o tratamento. Em relação à hipótese de eliminação dos dados tratados (art. 18, inc. IV e VI), ao menos no âmbito dos serviços notariais e de registros, é medida que conflita com seu dever precípuo de conservação (cf. arts. 6º, inc. II, e 46, Lei 8.935/1994), como se verá de forma mais abran-gente em item próprio à frente.

A LGPD aplica-se a qualquer operação de tratamento realizada no território nacional, ou mesmo fora do território nacional (produz efeitos no território nacional e fora dele), independentemente de onde os agentes de tratamento estão sediados ou os dados estão localizados, desde que:

a) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território brasileiro;
b) a atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território brasileiro;
c) os dados pessoais objeto do tratamento tenham sido cole-tados no território brasileiro.

Todavia, a LGPD *não se aplica* ao tratamento de dados pessoais (art. 4º), nas seguintes situações:

a) realizado por pessoa natural para fins exclusivamente parti-culares e não econômicos;
b) concernente a pessoas jurídicas;
c) a respeito de pessoas mortas;
d) realizado para fins exclusivamente jornalísticos, artísticos, acadêmicos;
e) realizado para fins exclusivos de segurança pública, de defe-sa nacional, de segurança do estado;
f) em atividades de investigação e repressão de infrações penais;
g) provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja reali-zada qualquer operação de tratamento.

A normativa em foco igualmente não revoga ou impede a aplicação de normas setoriais que também regulamentam dados pessoais, que devem continuar a ser observadas.

A LGPD tem por objetivos precípuos dar efetividade aos seguin-tes conceitos (art. 2º):

a) privacidade;
b) transparência;
c) desenvolvimento;
d) padronização;
e) proteção do mercado;
f) concorrência.

Por *privacidade* entende-se dar concretude ao direito constitu-cional à privacidade e à proteção de dados pessoais dos cidadãos, por meio de práticas transparentes e seguras, em garantia aos direitos e liberdades fundamentais.

Transparência evoca a disposição de regras claras e objetivas quanto ao tratamento de dados pessoais por empresas, órgãos e entidades, públicas e privadas.

O *desenvolvimento* econômico e tecnológico deve ser fomentado.

A *padronização* implica em estabelecer regras únicas e harmô-nicas sobre o tratamento de dados pessoais, independentemente do setor envolvido, facilitando as relações comerciais e reduzindo custos decorrentes de incompatibilidades sistêmicas de tratamentos feitos por diferentes agentes.

A *proteção do mercado* tem por escopo fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.

A *concorrência* deve ser estimulada por meio da portabilidade facilitada.

A seu turno, descortina-se a LGPD sob o balizamento da boa-fé objetiva, permeada ainda pelos seguintes princípios (art. 6º):

a) finalidade;
b) adequação;
c) necessidade;
d) livre acesso;
e) qualidade dos dados;
f) transparência;
g) segurança;
h) prevenção;
i) não discriminação; e
j) responsabilização e prestação de contas.

Em que:

Tem por ordem a *finalidade* a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com tais valores.

Compreende-se por *adequação* a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

A *necessidade* impõe limitação do tratamento ao mínimo ne-cessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O *livre acesso* tem por escopo garantir, aos titulares, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Atem-se a *qualidade dos dados* à garantia, aos titulares, de exa-tidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Pela *transparência* permite-se garantir, aos titulares, informa-ções claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

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

A *prevenção* é assegurada pela adoção de medidas eficazes para precaver a ocorrência de danos em virtude do tratamento de dados pessoais.

Pelo princípio da *não discriminação* impede-se a realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Já a *responsabilização e prestação de contas* validam a 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.

Denomina-se 'tratamento' qualquer operação feita a partir da coleta, recepção, armazenamento, compartilhamento ou transmissão de dados pessoais, vale dizer, todo e qualquer procedimento que permita às empresas, órgãos e entidades públicas e particulares adquirir, a qualquer título, pacotes de dados com informações rele-vantes aos seus respectivos fins e objetivos, sejam esses de índole per-ma-nentes ou transitórias (art. 5º, inc. X).

4.5 Sobre os dados pessoais e os dados sensíveis

As informações pessoais protegidas pela lei são necessaria-mente determinadas ou determináveis. Isto é, quaisquer dados que per-mitam a identificação de pessoa natural, que os facilitem ou que os tornem possíveis.

Por 'dados pessoais' entende-se (art. 5º, inc. I):

a) nome civil;
b) endereço do domicílio ou residência física;
c) endereço eletrônico (*e-mail*);
d) número(s) de documento de identificação e (ou) de cartão de crédito;
e) dados de localização de um *smartphone* ou *tablet*;

f) endereço de *Internet Protocol* (IP)
g) testemunhos de conexão (*cookies*);
h) identificador de publicidade do telefone;
i) dados bancários; e (ou)
j) informações, fichas, prontuários médicos em meios físicos ou eletrônicos etc.

Nesse cenário, podem não vir a ser considerados 'dados pes-soais', nos termos e limites da referida normativa:

a) dados obtidos por um estabelecimento de saúde que per-mitam identificar um paciente ou seu responsável de modo inequívoco;
b) número de registro e (ou) endereço eletrônico de pessoa jurí-dica individual ou coletiva;
c) dados anônimos.

O 'tratamento' de dados pessoais será permitido nas seguintes hipóteses (art. 7º):

a) a partir do consentimento expresso do usuário;
b) quando necessário ao planejamento de política pública;
c) nas situações que tenham por objetivo assegurar a vida e a inte-gridade de uma ou mais pessoas naturais, em conjunto;
d) na execução de contratos ou nas questões relacionadas ao tema;
e) na proteção ao crédito, hipótese em que serão observadas as normas especiais dispostas na legislação consumerista;
f) em questões relacionadas à saúde;
g) em processos judiciais e administrativos;
h) na imposição de obrigação legal para a realização do trata-mento;
i) em proveito de estudos por órgãos de pesquisa, hipótese em que o acesso será franqueado apenas aos dados, vedada a identificação de seus titulares.

A classe denominada 'dados sensíveis' visa conferir proteção especial a dados singulares, tais como raça, etnia, gênero, convicção religiosa, opinião política, filiação a sindicato, organização de caráter religioso, filosófico ou político, referentes ainda à saúde, à orientação ou à vida sexual, genético ou biomédico, entre outros, de modo a precaver todo e qualquer tipo de ações discriminatórias. Esses dados são submetidos a restrições de publicidade e, naturalmente, não podem ser livremente divulgados (art. 11).

Na perspectiva da LGPD, os dados pessoais sensíveis, cujo acesso somente é admitido em situações previamente definidas e no atendimento de finalidades específicas, por si só contêm carga informacional potencialmente apta a fomentar políticas e ações discriminatórias pelo setor público ou pelo setor privado.

Além disso, a LGPD não permite o tratamento de dados pes-soais sensíveis para atender ao interesse legítimo do controlador ou de terceiros, ou proteção do crédito. Por outro lado, permanece a possibilidade de tratar os dados pessoais sensíveis quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados, para o exercício regular de direitos em

processo judicial, administrativo ou arbitral ou necessário para a execução de contrato.

É invariavelmente vedada a exigência de dados pessoais que não decorra de propósitos legítimos do controlador e que não seja estritamente necessária ao cumprimento das obrigações estabelecidas em relação ao titular e (ou) decorrentes de lei, ainda assim mediante informação expressa e com destaque ao titular (art. 9º, §3º).

Outra vertente de dados pessoais submetida à regulamentação especial está compreendida nas seguintes situações:

a) para cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, inc. II, "a");
b) no exercício regular de direitos, inclusive em âmbito admi-nistrativo, judicial ou arbitral (art. 11, inc. II, "d") ou
c) para garantia de proteção à fraude e à segurança do titular (art. 11, inc. II, "g").

4.6 Sobre a transferência internacional de dados e acórdão do Tribunal de Justiça (Grande Seção) da União Europeia

A normativa brasileira prevê, sinteticamente, que transferência internacional de dados poderá ser feita, apenas (art. 33):

a) para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;
b) quando for necessária para a proteção da vida ou da inco-lumidade física do titular ou de terceiro; ou
c) quando o titular tiver fornecido o seu consentimento espe-cífico e em destaque para a transferência.

Como se vê, muito pouco foi disposto sobre a disciplina da questão. No contexto da globalização e avanço da tecnologia impul-sionando o comércio, trocas e serviços internacionais, o tema, decerto, carecerá de detalhamento específico na regulamentação da LGPD.

A título de ilustração, faz-se remissão a excertos de acórdão de julgamento proferido pelo Tribunal de Justiça (em sua composição plena) da União Europeia, a partir de reclamação oferecida por cidadão austríaco e usuário da rede social Facebook, cujo *data center* mundial, como se sabe, é situado em território norte-americano (Califórnia), ao abrigo, portanto, das leis norte-americanas. Contextualizando, os dados pessoais foram recolhidos em território da União Europeia, porém transferidos, armazenados, tratados – possivelmente de modo incompatível com as finalidades da transferência – e franqueados – nesta última hipótese, eventualmente, para acessos pelas autoridades estadunidenses (país terceiro) –, como de resto pode suceder, de ordinário, com todos os usuários mundiais das redes sociais e aplicativos de mensagens instalados em territórios norte-americano, russo e chinês.

Pôs-se em cotejo no julgamento a proteção do direito funda-mental do respeito da vida privada diante do primado dos requisitos de segurança nacional, interesse público ou cumprimento da lei, plasmado sobre os 'princípios de porto seguro' da legislação esta-dunidense. A questão foi analisada sob o prisma da adequação ou não da legislação do país estrangeiro (EUA) aos níveis de proteção dos dados pessoais exigidos na diretriz europeia (RGPD) e até que ponto as limitações à proteção dos dados pessoais, no caso concreto, estavam ou não contidas na 'estrita medida do necessário'.

(...)

4.7 Do consentimento

A LGPD estabelece regras específicas para a obtenção do con-sentimento, sob pena de nulidade, caso se trate de uma autorização genérica ou se baseado em informações com conteúdo enganoso ou abusivo. A cláusula a respeito, física, seja virtual (caixa de verificação), deve estar destacada das demais, desprovida de subterfúgios ou expediente enganoso, em linguagem clara e objetiva.

Resulta, assim, da imperiosa adoção de cuidados a respeito da base legal para tratamento de dados que poderá ser utilizada no caso concreto. Quando o tratamento de dados pessoais for baseado no consentimento, o controlador deve manter documentação com-probatória da sua obtenção em conformidade com a legislação. Quando o tratamento de dados pessoais for baseado no interesse legítimo, o controlador deve adotar medidas para garantir a trans-parência de tal tratamento, que poderá sempre ser revisto pela autoridade nacional de proteção de dados à luz do caso concreto. Será necessário manter registro e fundamentação coerente e adequada sobre as operações de tratamento de dados pessoais, especialmente quando baseado no interesse legítimo.

Como visto, o consentimento na LGPD é condição indissociável para a viabilidade das operações de tratamento dos dados de uma pessoa. Atesta a higidez acerca de uma 'manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica' (art. 5º, inc. XII).

Nesse descortino, os usuários devem ter a sua disposição, de forma expressa, clara, com linguagem acessível, todas as informações acerca do tratamento a que os dados serão submetidos, a exemplo da finalidade para a qual estão sendo coletados; o meio de captura; o período de tempo em que ficarão armazenados; a identificação do controlador com o respectivo contato; se serão compartilhados com terceiros; quais as responsabilidades dos agentes que realizarão o tratamento; entre outras.

No que concerne aos dados pessoais de crianças e adoles-centes, o tratamento exigirá o consentimento específico e em destaque de pelo menos um dos pais ou do responsável legal (art. 14, §1º). É atri-buição do controlador, com base nas tecnologias disponíveis, empreender todos os esforços razoáveis para confirmar que o

consentimento de fato tenha sido dado por um dos pais ou pelo responsável legal (art. 14, §5º).

A única hipótese em que a LGPD permite a coleta de dados pessoais sem o consentimento de pais ou responsável legal se dá em caso da coleta necessária para realizar contato com os pais ou responsável legal (art. 14, §3º). Nesse caso, os dados pessoais coletados sem o consentimento somente poderão ser utilizados uma única vez e não poderão ser armazenados sob nenhum fundamento ou circunstância, dado que sua única finalidade é e será a realização do referido contato.

Antes de mais, deve-se verificar se o consentimento do titular é o fundamento de legitimidade adequado quando está em causa uma relação contratual com um cliente, uma vez que o tratamento de dados necessário à execução de um contrato não precisa do consentimento do cliente.

Se o que estiver em causa for um tratamento de dados pessoais adicionais em relação ao contrato, então, se o consentimento que obteve anteriormente foi dado de forma implícita, é preciso pedir um novo consentimento ao titular dos dados nas condições exigíveis pela LGPD.

O consentimento, uma vez solicitado, tem de ser *explícito*, isto é, a pessoa tem de manifestar a sua vontade em autorizar, de forma livre e consciente. Tem também de prestar as informações que vêm referidas no artigo 9º, inc. I a VI, da LGPD, pressuposto da autodeterminação informativa (art. 2º, inc. II) e adequadas ao caso concreto, não se esquecendo de informar o titular dos dados de que pode revogar o consentimento a todo o momento e indicando o meio como pode fazê-lo.

O consentimento tem ainda de ser *específico*. Deve ser diferen-ciado, por exemplo, quando da utilização de dados para fins distintos ou quando da comunicação de dados a terceiros, e acompanhado sempre da informação necessária relativa a cada situação.

Também não é possível, lado outro, fazer depender a execução de um contrato do consentimento do titular dos dados ainda que, para tanto, a circunstância deva ser previamente informada (art. 9º, §3º).

O consentimento deve ser fornecido por escrito ou por outro meio que demonstre a efetiva manifestação de vontade do titular, em cláusula destacada dos demais termos contratuais (art. 8º, §1º). Fórmulas prontas e frequentemente observadas, tais como 'clique aqui para finalizar o seu cadastro' e, na sequência, 'clicando aqui você concorda com os termos de uso e política de privacidade', poderão ser questionadas com boa probabilidade de nulidade. Será imperioso que o usuário ou cliente forneça o seu consentimento, *i.e.*, marcando uma caixa de diálogo específica (caixa de verificação), com linguagem clara, de fácil compreensão e objetiva.

Se e quando ocorrer tratamento diverso daquele informado ou alteradas as finalidades iniciais, será imperioso que o controlador obtenha novo consentimento do titular (art. 8º, §6º).

E, sim, é claro que o titular poderá, a qualquer tempo, revogar o consentimento (art. 8º, §5º), ficando o tratamento dos dados pelo controlador limitado às hipóteses em que o consentimento é dispensado, respeitados os demais requisitos legais. É direito do titular dos dados a retirada ou revogação do consentimento, bem como, se houver mudança na finalidade dos dados coletados origi-nalmente, efetuar novo consentimento, a qualquer tempo. Consoante anteriormente assinalado, o titular tem o direito de corrigir ou alterar seus dados a todo momento.

E as opções à disposição do usuário ou cliente devem ser facilitadas e disponibilizadas gratuitamente. Além de ter o direito a informações claras acerca do tratamento de dados, *o titular tem o direito a obter gratuitamente as seguintes providências, mediante requisição expressa ao controlador*:

a) confirmação da existência de tratamento e acesso aos dados pessoais;
b) correção de dados incompletos, inexatos ou desatua-li-za-dos;
c) anonimização, bloqueio ou eliminação de dados desneces-sários, excessivos ou tratados em desconformidade com a legislação;
d) portabilidade dos dados a outro fornecedor de serviço ou produto;
e) eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas as hipóteses de guarda para cumpri-mento de obrigação legal ou regulatória;
f) informação a respeito do uso compartilhado de dados pessoais;
g) informação sobre a possibilidade de não fornecer consen-timento e sobre as consequências da negativa;
h) possibilidade de revogação do consentimento, por procedi-mento gratuito e facilitado.

4.8 Assimetrias entre a LGPD, a Lei do Cadastro Positivo e o Marco Civil da Internet

Note-se que o prévio consentimento exigido pela LGPD segue outra vertente em relação às disposições da Lei do Cadastro Positivo (12.414/2011), tal como se vê em vigor, que regulamenta o banco de dados dos bons pagadores, em complemento à legislação consu-merista que, a seu turno, cuida, em certa medida, de balizar também os direitos dos maus pagadores. Aqui, no âmbito da LGPD, dados, relatórios de crédito e algoritmos de risco apenas serão tratados com o prévio consentimento de consumidores (*opt in* – cf. art. 7º, inc. I).[8]

[8] O termo *opt in* refere-se à expressão da vontade de um usuário de internet ou *mobile*, a partir do que é afastada a presunção de aceite pelo silêncio. Corresponde ao conjunto de regras segundo as quais as mensagens de marketing ou de caráter comercial só são enviadas para aqueles que expressem, prévia e explicitamente, o seu consentimento. Dessa forma, uma mesma mensagem é enviada para todos os indivíduos que concordaram ou que manifestaram interesse em receber informações sobre um produto ou serviço de uma empresa ou organização. O usuário manifesta sua concordância através do preenchimento de uma caixa de verificação (*check box*). Ao fazê-lo, indica ao gestor da base de dados daquela empresa ou organização que gostaria de ser informado acerca das novidades, informações e campanhas promovidas. As regras definidas

Por sua vez, na Lei do Cadastro Positivo, a lógica partiu de prin-cípio inverso, segundo o qual os dados dos clientes relativos ao crédito sejam tratados automática e compulsoriamente pelas instituições financeiras e que o titular possa apenas requisitar pos-teriormente a revisão ou até a eliminação de seus dados (*opt out* – cf. art. 5º, incisos I, III, VI e seu §7º). [9]

Mas, na medida em que o Marco Civil da Internet (Lei 12.965, de 23/04/14) exige o consentimento para toda e qualquer situação de tratamento de dados pessoais, a LGPD estabelece algumas exceções, a principiar pelos dados pessoais tornados 'manifestamente públicos' pelo titular (art. 7º, §4º) Para além, ainda em caráter excepcional, o consentimento poderá vir a ser dispensado em outras doze (12) hipóteses que se alongam nas letras "a" a "g", inc. II, art. 11, conjuga-das com as situações estampadas nos incisos I a IV, §1º, art. 26, com-binado com o disposto no art. 27, inc. II, todos da Lei 13.709/2018.

Também em relação ao crédito, a LGPD examina a questão de maneira específica, com destaque para a possibilidade de tratamento de dados para proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, inc. X). Os dados *pessoais* em geral estão disponíveis para tratamento por diferentes interessados, enquanto os dados *de crédito* apenas são acessíveis por instituições financeiras.

4.9 Correção, anonimização, pseudonimização, bloqueio ou eliminação de dados pessoais

O titular dos dados poderá requerer a correção de dados que considere incompletos, inexatos ou desatualizados, bem como soli-citar a anonimização, bloqueio ou eliminação de dados pessoais considerados como desnecessários, excessivos ou tratados em descon-formidade com a LGPD.

Como dito, para fins da LGPD, 'anonimização' é um procedi-mento por meio do qual um dado perde a possibilidade de identificar um titular, ao passo que se entende por 'bloqueio' a suspensão tem-porária de qualquer operação de tratamento

---

pelo *opt in* estabelecem o envio de mensagens, pela internet ou *mobile*, apenas para aqueles que expressamente o tenham solicitado.

[9] A expressão *opt out* refere-se às regras do envio, geralmente associadas ao meio do correio eletrônico (*e-mail*), de mensagens informativas vinculadas a campanhas de marketing, sem que os destinatários particulares as tenham solicitado. Pressupõe a visita (física ou virtual), solicitação de informação ou aquisição de um produto, bem ou serviço, a partir do que se dá a inclusão numa lista de correio, independentemente do consentimento do destinatário (procedimento automático). Na sequência, o destinatário começa a receber na sua caixa de correio eletrônico mensagens da empresa e das suas congêneres com as quais partilha igual lista de correio. A correspondência enviada ao destinatário inclui um mecanismo para a interrupção e o cancelamento do envio desse tipo de correio eletrônico (*opt out of*), que pode ser ativada por um *hyperlink* incluído no corpo da mensagem, ao solicitar o envio de uma resposta para um endereço de correio electrónico, ou por qualquer outro meio. Enquanto os destinatários não efetivarem esse procedimento, continuarão a receber as mensagens, desde o princípio ou presunção de que deram sua permissão para esta ação. Dessa forma, recolhem-se numerosos endereços eletrônicos e a base de dados de contatos da organização vai aumentando exponencialmente. Em muitos casos o destinatário só atua tardiamente e quando cancela essa subscrição os seus dados já constam de outras listas semelhantes, pelo que continuarão a receber mensagens de conteúdo similar.

de dados pessoais. Em caso de dados tratados com fundamento no consentimento, o titular dos dados poderá solicitar a eliminação de quaisquer dados coletados, ressalvadas as hipóteses de armazenamento permitidas pela LGPD, o que inclui a guarda de dado especialmente para cumpri-mento de obrigação legal pelo controlador ou para uso exclusivo do controlador. Nesta última eventualidade, os dados deverão ser anonimizados.

Caso a empresa, órgão ou entidade tenha realizado uso com-partilhado de dados para os quais fora requisitado pelo titular correção, anonimização, bloqueio ou eliminação, cabe informar de maneira imediata tal providência aos demais agentes de tratamento de modo que repitam o procedimento.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão 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 e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. O tratamento dos dados de saúde deverá ser efetuado por pessoa sujeita a dever de sigilo e, em determinados casos, por profissional obrigado a sigilo ou sujeito a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação. Os dados pessoais tratados nesse contexto deverão ser eliminados ou anonimizados, logo que se esgotem as finalidades para as quais foram tratados.

Digno de nota, o setor de saúde está desobrigado a obter o consentimento em todas as situações de tratamento de dados (hipó-teses de exceções nomeadamente dos arts. 7º, 10 e 11). Em caráter excepcional, a dispensa se dá nos casos de proteção à vida ou tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; obrigação legal ou regulatória; para execução de contratos com o titular dos dados; em processos judiciais ou administrativos; quando há legítimo interesse do controlador; ou, ainda, no caso de estudo por órgãos de pesquisa.

Para além disso, a lei revela que é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxilia-res de diagnose e terapia, em benefício dos interesses dos titulares de dados.

No caso de pesquisas, o uso de dados é também limitado. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclu-sivamente dentro do órgão e estritamente para a finalidade de reali-zação de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regula-mento específico e que

incluam, sempre que possível, a anonimização ou pseudo-nimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Para fins de atendimento dessa regra, 'pseudonimização' é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Na prática, o legislador não se contenta com pouco. Exige evidências, justificativas e muita documentação. Especialmente na saúde, caberá ao princípio da transparência desempenhar papel nuclear, em conexão também com a legislação consumerista.

Ao capturar os consentimentos nos termos da saúde (como o de internação, o de análise laboratorial e outros) ou ainda nas regras sobre a Política de Privacidade e Proteção de Dados Pessoais publicadas em sítios eletrônicos e nos aplicativos da saúde, incidirá desde logo a necessidade de cumprir as exigências da LGPD (arts. 8º e 9º), no sentido de que o consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular; deve constar de cláusula destacada das demais cláusulas contratuais; a informação sobre o tratamento de dados pessoais deve ocorrer de forma clara, adequada e ostensiva, e trazer informações sobre a finalidade específica do tratamento, forma e duração, identificação e contatos do controlador, informações sobre compartilhamento de dados pessoais e menção expressa dos direitos assegurados (art. 18).

A LGPD instituiu também o direito de portabilidade, pelo qual o titular dos dados poderá, mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto. Ou mesmo a revisão de decisão automatizada: O titu-lar dos dados poderá requisitar a revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado, inclusive decisões destinadas à formação de perfis.

O titular dos dados ainda poderá solicitar a disponibilização de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para formação da decisão automatizada. E caso não possa cumprir de imediato a providência requerida pelo titular dos dados, o controlador deverá enviar ao titular uma justificativa com as razões que impediram o cumprimento imediato do direito exercido ou uma comunicação para indicar que não é o agente de tratamento dos dados e, caso tenha conhecimento, apontar quem é o agente de fato.

Na tutela do direito à informação ao titular dos dados é asse-gurado acesso facilitado a informações relacionadas ao trata-mento de dados pessoais, incluindo, mas não se limitando a informações (invariavelmente prestadas de forma clara e adequada) acerca da:

a) finalidade específica do tratamento;
b) forma e duração do tratamento;
c) identificação e contato do controlador;
d) uso compartilhado de dados e a respectiva finalidade;

e) responsabilidade dos agentes de tratamento;
f) imposição do tratamento de dados pessoais como condição para o fornecimento de produto ou de serviço ou para o exercício de direito, caso aplicável;
g) e dos demais direitos do titular, nos termos da LGPD.

Todavia, ao conceituar dados 'anonimizados', a par do que, aparentemente, não os equiparou a dados pessoais e 'pseudoni-mização', também não os enquadrou no rol de possíveis exceções, mas, sim, apenas como informações que, no primeiro caso, por não poderem mais ser associadas direta ou indiretamente a uma pessoa e, no segundo, por se referir às relações adicionais dessas conexões, permitiu que sejam manejadas com mais liberdade desde que preservada a privacidade de seus titulares, tornando mais seguras as operações de tratamento definidas em seu artigo 3º.

A circunstância de os repositórios operarem com dados ano-nimizados, ou com aqueles que passaram por processos de pseudo-nimização não compreende, por si só, garantia na aplicação da LGPD. Atualmente, o volume, o dinamismo, a complexidade e a velocidade de *Big Datas,* em crescimento exponencial, permitem antever que alguma ferramenta analítica mais sofisticada e de alto desempenho possa captar e interpretar qualquer tipo de dado, criando correlações a partir das quais é possível identificar pessoas com uma precisão cada vez mais eficiente, resultando em possível brecha legal.

Desde que a base da garantia da anonimização e da pseudo-nimização é, grosso modo, a ausência de identificadores dos titulares da informação, existem dados que, mesmo não apontando para alguém em particular, poderão fazê-lo desde que empregadas téc-nicas de conjunto e dados complementares.

Vale dizer, as bases de dados anonimizados ou que passaram por um processo de pseudonimização não são imunes a consultas com cruzamento de informações e identificação de padrões, ou que adotam engenharias sociais distintas e informações externas.

Neste ponto, discorre Ruiz:[10]

> *A LGPD, no artigo 5º, inciso I, diz, expressamente, que dado pessoal é informação relacionada a pessoa natural identificada ou identificável. Dessa forma, são dados que, por vezes, não são diretamente associados a um indivíduo, mas, analisados em conjunto com outros dados disponíveis, possuem altas chances de (re)identificação de um indivíduo, esse indivíduo é identificável e, portanto, esses dados devem ser considerados como dados pessoais.*
>
> *Dizer que os dados pseudonimizados devem ser considerados dados pessoais e, portanto, devem ter o respaldo da LGPD é defender a proteção dos dados pessoais dentro do próprio texto da lei.*

[10] RUIZ, Isadora Maria Roseiro. O dado pseudonimizado é um dado protegido pela Lei Geral de Proteção de Dados? Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/332299/o-dado-pseudonimizado-e-um-dado-protegido-pela-lei-geral-de-protecao-de-dados?U=223C0B13_CFC&utm_source=informativo&utm_medium=1264&utm_campaign=1264 Acesso em: 24 ago. 2020.

De qualquer forma, os dados obtidos antes da entrada em vigor da lei, mas empregados para tratamento após sua vigência, em princípio, estarão também sujeitos às disposições da normativa, a partir do término da *vacatio legis*.

4.10 Do controlador, operador, encarregado e titular

Titular compreende a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, inc. V).

A figura do *controlador* refere-se à pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, inc. VI).

Operador é a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, inc. VII).

Controlador e *operador* são ambos agentes de tratamento de dados pessoais, devendo manter registro das operações de tratamento que realizarem, especialmente quando baseadas em legítimo interesse (art. 37).

O operador deve realizar o tratamento de dados de acordo com as instruções fornecidas pelo controlador (art. 39). O controlador e o operador de processamento de dados, em conjunto, dão corpo à denominação legal dos agentes de tratamento. A LGPD não veda a terceirização da atividade de operador de dados, mas estabelece que nos casos de agentes públicos, determinada classe de dados só pode ser processada por ente privado sob tutela do ente público (art. 4º, §2º).

São de observância obrigatória pelo controlador as deter-mi-nações da ANPD sobre os padrões de interoperabilidade dos dados (formatos que possam ser lidos e utilizados em diversas plataformas), livre acesso aos dados e segurança e o tempo de guarda dos registros (art. 40).

Também incide ao controlador o ônus da prova de que o con-sentimento do titular foi obtido nos termos da lei, bem como comu-nicar ao titular mudança de finalidade no tratamento de dados. A identificação de quem é o controlador de dados deve ser clara e disponível ao titular, com ampla divulgação. O controlador é igualmente responsável pelo cumprimento dos direitos do titular, listados nos arts. 18 a 22 da normativa.

Cabe ao controlador tomar as decisões acerca do tratamento de dados pessoais, bem como zelar por sua conservação e atender aos requisitos e exigências formulados pelas autoridades.

Nesse sentido, a LGPD *impõe* ao controlador as seguintes responsabilidades:

a) provar que o consentimento foi obtido em conformidade com a lei;
b) confirmar a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular, em formato simplificado, imediatamente, ou 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, fornecida no prazo de até 15 (quinze) dias;

c) manter registro das operações de tratamento de dados pessoais que realize, podendo a autoridade nacional deter-minar que seja elaborado relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações.

Caso a autoridade faça a requisição, cabe ao controlador inserir no relatório, ao menos, as seguintes informações:

a) descrição dos tipos de dados coletados;
b) metodologia utilizada para a coleta de dados;
c) metodologia utilizada para garantir a segurança das infor-mações;
d) sua análise no tocante às medidas, salvaguardas e meca-nismos de mitigação de riscos adotados.

O controlador também é responsável por indicar quem é o 'encarregado pelo tratamento dos dados pessoais (ETD)', divulgando publicamente, de forma clara e objetiva, preferencialmente no seu sítio eletrônico, a identidade da pessoa e suas informações de contato. Conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados, é facultado à Autoridade Nacional regular as hipóteses de dispensa da necessidade de sua indicação (art. 41, §3º).

Nas hipóteses em que o consentimento for exigido, o controlador deverá informar o titular caso haja alguma alteração na finalidade para a coleta de dados. Nesse momento, o titular poderá optar por renovar o consentimento ou revogá-lo. Caso não haja consentimento do titular, o controlador somente poderá fundamentar o tratamento de dados pessoais atestando que há finalidade legítima para tanto.

Com relação a essa exigência, somente dados pessoais estri-tamente necessários para a finalidade pretendida poderão ser trata-dos e devem ser adotadas medidas que garantam sua transparência.
O controlador que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para tanto, exceto em caso de o titular dos dados tê-los tornado manifestamente públicos.

Cumpre destacar que o ônus de provar a adequação às deter-minações da LGPD é do controlador, quando verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa, a critério do juiz (art. 8º, §2º). E a inversão do ônus de prova se dá agora sem qualquer condicionante, a respeito da obtenção do consentimento (art. 42, §2º).

Cabe ao controlador indicar o ETD (art. 41), observados os seguintes aspectos:

a) ser pessoa natural que atue como canal de comunicação en-tre o controlador e a autoridade competente e os titulares;
b) a identidade e as informações de contato do encarregado devem ser públicas, claras e objetivas, de preferência no sítio eletrônico do controlador (art. 41, §1º).

Em linhas gerais, as atividades do ETD consistem em (art. 41, §2º):

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) receber comunicações da autoridade nacional e adotar pro-vidências;
c) orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares emitidas pela autoridade nacional de proteção de dados.

Dado que "A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados" (art. 41, §3º), *muitas outras questões de relevo deverão ser esclarecidas na regulamentação da normativa, tais como*:

a) Será obrigatória a designação de ETD pelas entidades ou órgãos públicos?
b) Estarão obrigadas as empresas, na qualidade de responsáveis pelos tratamentos, seja de subcontratantes, a designar um ETD se tratarem dados sensíveis ou dados relativos a con-denações penais e infrações, em larga escala ou se reali-zarem tratamentos em larga escala relativos ao controle regular e sistemático dos titulares dos dados?
c) É ao responsável pelo tratamento e ao subcontratante que compete avaliar, em cada situação, se os tratamentos de dados realizados pela sua organização exigem a designação de um ETD?
d) É preciso fazer algum registro do ETD, publicar seus contatos, dar conhecimento aos titulares de dados e comunicar à ANPD?
e) Será permitido duas ou mais empresas partilharem o mesmo encarregado de proteção de dados, dentro ou fora do mesmo grupo empresarial?
f) Será possível usar o mesmo formulário de notificação para comunicar à ANPD a designação de um ETD dentro do mesmo grupo?
g) Os ETD precisam de alguma certificação para desempenhar as suas funções?
h) Será permitido usar os dados biométricos já recolhidos no contexto laboral para outra finalidade (a exemplo do controle de acesso às máquinas de venda automática)?
i) Será autorizado o uso da biometria para controlar o acesso dos clientes às instalações da empresa, órgãos e entidades?
j) Será exigida uma avaliação de impacto sobre a proteção de dados para tratar dados biométricos?
k) Precisará de autorização da ANPD para colocar um sistema biométrico?
l) O que deverá ser feito se pretender alterar o funcionamento do sistema biométrico já existente?
m) Como será feita a notificação de violações de dados pessoais à ANPD? Etc.

4.11 Da segurança e do sigilo de dados

Em relação aos temas 'segurança e sigilo de dados', cumpre destacar que os agentes de tratamento devem adotar medidas de segurança (desde a concepção até a execução do produto ou serviço) aptas a proteger os dados pessoais de acessos não autorizados e de eventos acidentais ou ilícitos de destruição, perda, alteração, comu-nicação ou difusão ou qualquer outra ocorrência decorrente de tratamento inadequado ou ilícito (art. 46).

Padrões técnicos mínimos poderão ser definidos pela autoridade competente, e sistemas de tratamento de dados pessoais devem ser estruturados para atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais da LGPD e demais normas da autoridade competente (art. 49).

Imputa-se aos agentes de tratamento, individualmente ou por meio de associações, formular regras de boas práticas e de governança que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas, mecanismos de supervisão e mitigação de riscos e outras medidas relacionadas ao tratamento (art. 50).

Cumpridas as finalidades para as quais foram coletados, uma vez constatado que deixaram de ser necessários, sucedendo hipótese de revogação do consentimento ou ainda por determinação das autoridades competentes, os dados devem ser eliminados (art. 15), ou seja, excluídos dos bancos de dados do controlador e do operador (art. 5º, inc. XVI).

A inobservância do princípio da segurança (art. 6º, inc. VII) pode, em caso de dano ao titular, gerar responsabilidade civil e criminal solidária entre controlador e operador e o dever de reparar os danos (art. 42), a par das sanções administrativas.

Fica autorizada a conservação de dados para cumprimento de obrigação legal ou regulatória (art. 16, inc. I) ou para uso exclu-sivo do controlador, vedado o acesso por terceiros e desde que ano-ni-mizados[11] (art. 16, inc. IV).

O dado anonimizado é o dado anônimo, característica e requi-sito de informação pessoal que escapa das condicionantes da LGPD. Ou melhor, a anonimização seria, ela própria, a primeira condi-cionante para o tratamento desprovido de consentimento. No contexto da LGPD são estipulados alguns critérios, todos objetivos, para a com-preensão se o dado poderá, ou não, permitir a identificação de uma pessoa. São eles: (*i*) custo; (*ii)* tempo; (*iii*) tecnologia.

A definição do que é anonimizado ou não será dinâmica, no-meadamente porque as tecnologias estão em constante evolução. Trata-se de um conceito aberto. No diálogo com a Lei de Acesso a Informação, a que remete já no art. 1º da LGPD, nota-se que a normativa faz uso do emprego de políticas de dados abertos com relativa frequência. Gestores públicos podem, de modo legítimo, abrir dados, todavia sem a possibilidade de identificação de seus titulares, a despeito de que, ao

[11] 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 (art. 5º, inc. III, LGPD).

abri-los, surge o risco de cruzamento desses dados com outros, a partir do que o anonimato do titular poderá ser rompido. Evitar, a todo custo, esse risco é essencial.

A autoridade competente poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais referente a suas operações de tratamento de dados (art. 38). O relatório conterá, 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.

De todo modo, o controlador deve comunicar à autoridade com-petente e ao titular, em prazo razoável a ser definido pela primeira, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48).

Importa ainda anotar que o RGPD (*GDPR*) assumiu o pionei-rismo mundial ao introduzir dois novos conceitos denominados por *Privacy by Design*[12] *e Privacy by Default*, no objetivo de orientar algumas estruturas utilizadas por empresas e organizações no intuito de se adequarem às diretrizes das leis de proteção de dados.

Por *Privacy by Design* entende-se que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma empresa ou organização devem ter a privacidade em primeiro lugar. O conceito de privacidade deve estar totalmente impregnado no projeto e, neste descortino, não se aplica às iniciativas em que a privacidade é avaliada somente em sua fase derradeira. Parte do princípio de que as empresas e organizações que se orientem pela *Privacy by Design* concebam seus projetos internos, desenvolvimentos de *software*, departamento de TI e planejamento estratégico alinhados com a ideia de privacidade, e não como algo à parte. Na

---

[12] O conceito de *Privacy by Design* (PbD) resultou originalmente de uma formulação proposta pela Dra. Ann Cavoukian, diretora executiva do Instituto de Privacidade e *Big Data* da Universidade de Ryerson, em Ontário, capital da província de Toronto, Canadá. Remotamente, no final do século XIX, mais precisamente em 1890, o advogado Samuel D. Warren e o ex-juiz associado da Suprema Corte norte-americana Louis D. Brandeis publicaram o artigo 'The Right to Privacy' (cf. WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890), considerado um dos maiores estudos relacionados à defesa da privacidade. É nessa obra que se aponta a inter-relação entre o '*right to be let alone'* e o direito à privacidade (cf. ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos. *Revista Brasileira de Direito Civil – RBDCivil*, Rio de Janeiro, v. 3, p. 9-28, jan./mar. 2015), no sentido de que, à época, o indivíduo deveria possuir o direito de ter sua intimidade e vida privada protegidas de invasões pelos jornais. Nesse contexto, já havia um embate entre privacidade e publicidade, temas que, por si sós, demandam abordagem própria. Muitos estudos e novas tecnologias marcaram a história a partir de então, até que na década de 1990 uma série de acontecimentos começa a moldar conceitos e definições profundamente ligados à atualidade. Como se sabe, é na década de 1990 que se tem o lançamento da *World Wide Web* pelo cientista da computação britânico Tim Berners-Lee, em outubro de 1990, que possibilitava (e possibilita) criar e editar páginas navegáveis com base em três tecnologias fundamentais: a linguagem HTML, o endereço URL e o protocolo HTTP (cf. ARAYA, Elizabeth Roxana Mass; VIDOTTI, Silvana Aparecida Borsetti Gregório. *Criação, proteção e uso legal de informação em ambientes da World Wide Web [online].* São Paulo: Editora da UNESP; São Paulo: Cultura Acadêmica, 2010. 144 p. Ver também: World Wide Web Foundation. History of the Web. Disponível em: https://webfoundation.org/about/vision/history-of-the-web/. Acesso em: 25 ago. 2020. Quase 30 anos depois, já não se faz muita coisa fora dos ambientes virtuais e dos sítios eletrônicos que armazenam e coletam dados pessoais de variadas formas. Com esse avanço de forma acelerada, o campo da legislação e das normas começou a apresentar algumas respostas. Jan Holvast (2009, p. 30) destaca o *Children's Online Privacy Protection Act* (COPPA), de 1998, o *Fair Health Information Practice* (1997), e as emendas ao *Fair Credit Reporting Act* de 1997, todos nos Estados Unidos, como maneiras de se assegurar a proteção dos dados de cidadãos. O Parlamento do Reino Unido, por sua vez, adotou em 1998 o *Data Protection Act*. Ainda na mesma década, que o Parlamento Europeu e o Conselho adotaram a Diretiva 95/46/CE, relacionada à proteção das pessoas no que toca ao tratamento de dados pessoais e à livre circulação desses dados, normativa que antecede o RGPD (*GDPR*), de 2016.

prática, isso significa que a organização deve garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida. Também deve assegurar a segurança das informações de ponta a ponta. O escândalo envolvendo o Facebook e a Cambridge Analytica sucedeu porque não houve a proteção de dados em uma das etapas do processo.

Por sua vez, o conceito de *Privacy by Default* (privacidade por padrão) implica que um produto ou serviço, ao ser lançado, dis-ponibilizado ou demandado, contenha as configurações de priva-cidade no modo mais restrito possível já como padrão, nessa medida, cabendo ao usuário a decisão de liberar acesso à coleta de mais in-for-mações apenas caso julgue necessário. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço. Dado que mais informações do que o necessário para fornecer o serviço sejam divulgadas, a ação resultará na violação do conceito.

Tem-se em ordem que o conceito de *Privacy by Design* é proativo e não reativo. Antecipa os problemas e diminui o risco de vazamen-tos de dados. Os projetos são pensados para que o usuário tenha o con-trole para alterar as configurações-padrão e optar por fornecer ou não seus dados, e ainda assim conseguir utilizar o produto ou serviço. Sempre que possível, as transações que envolvam dados pessoais devem ser feitas com dados não identificáveis, ou seja, que não permitam saber quem é o titular daquela informação.

Na prática, em um sítio que utiliza testemunhos de conexão (*cookies*), referida *funcionalidade* só poderá ser habilitada se e quando o usuário ativar tal modo de coleta de dados. Do contrário, não haverá a coleta de informações pessoais do usuário ou mero visitante da página eletrônica. A LGPD exige que todas as empresas e organizações que façam o uso dos *cookies* os deixem, por princípio-padrão, desativados, cabendo ao usuário a tomada de decisão a respeito de quais dados deseja compartilhar.

Nesse viés, a LGPD proporciona uma evolução significativa na filosofia de interação com o público em geral, com ganho substancial em transparência e credibilidade. Os conceitos de *Privacy by Design* e *by Default* serão aplicados em organizações públicas e privadas, multinacionais e nacionais, *startups* e todas as que processam de al-guma forma os dados pessoais de seus clientes, utentes, colaboradores e fornecedores.

A propósito, já no âmbito do RGPD aflora sua conotação disrup-tiva ao acolher os paradigmas de conformidade e de *accountability*[13] *(cf. art. 24º),*[14] *que nomeadamente*

---

[13] *Accountability* é uma expressão da língua inglesa que, traduzida para o português, pode expressar a responsabilidade com ética e remete à obrigação, à transparência, de membros de um órgão administrativo ou representativo, de prestar contas a instâncias controladoras ou a seus representados.

[14] RGPD: "*Artigo 24.º*.
Responsabilidade do responsável pelo tratamento
1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para

deságuam nos conceitos de Privacy by Design e *Privacy by Default,* ambos destacados em seu art. 25º.[15]

Nas palavras da Conservadora de Registro Predial em Portugal, Profa. Madalena Teixeira: "Visa-se aqui o cumprimento do 'princípio de responsabilidade' que aforava na Diretiva 95/46/CE, mas que não lograra tornar efetivo nos termos pretendidos, suscitando-se a observância das regras atinentes à proteção de dados pessoais desde a raiz, isto é, desde o momento da concepção ou definição dos meios de tratamento, até ao momento da concretização das operações de projetadas, e exigindo-se, para o efeito, a adoção das medidas técnicas e organizativas necessárias ao cumprimento efetivo dos prin-cípios da proteção de dados, designadamente dos princípios da fina-lidade e da minimização dos dados".[16]

Ponha-se em ordem que os negócios, serviços e produtos devem, agora e por diante, levar em conta, desde a sua concepção, a necessidade indeclinável de proteção dos dados pessoais e o direito à privacidade no âmbito conceitual do *Privacy by Design*.

---

assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.
2 Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.
3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.º ou de procedimentos de certificação aprovados conforme referido no artigo 42.º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento".

[15] RGPD: "*Artigo 25.º*
Proteção de dados desde a conceção e por defeito
1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do trata-mento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas ade-quadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabele-cidas nos n.ºs 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.º".

[16] Em: A Lei Geral de Proteção de Dados em Debate e os Registros Públicos. *Boletim IRIB em Revista Especial*, n. 361, p. 36, jul. 2020.