A PROTEÇÃO DE DADOS

JOSÉ FRANKLIN DE SOUSA
Pós-graduado pela PUC-SP em Direito Processual Civil e Direito do Consumidor

O autor é advogado em São Paulo e Fortaleza. Graduado e pós-graduado pela PUC-SP. Especialista em Direito Processual Civil e Direito do Consumidor. Publicou as seguintes obras, todas pela Editora J. H. Mizuno: Elementos da Ação Cautelar, Responsabilidade Civil e Intervenção de Terceiros e Coisa Julgada.

A PROTEÇÃO DE DADOS

A PROTEÇÃO DE DADOS

1.Introdução.

A LGPD regulamenta o tratamento de dados e informações pessoais, inclusive em meios digitais, por entes públicos e privados. A lei é inspirada na regulamentação já utilizada na Europa, com uma diferença importante: no Brasil as empresas públicas também estão sujeitas à lei. Empresas que não se adequarem às exigências poderão pagar multa de até R$ 50 milhões, entre outras sanções.

Na Idade Antiga (4000 a. C. a 476 d. C.), com fins militares estratégicos, o imperador romano Júlio César (101. a. C. a 44 a. C.) criou a *Cifra de Cesar* para a transmissão de mensagens a seus comandados, substituindo cada letra do alfabeto pela correspondente a três casas a frente na ordem alfabética, de modo que somente o pessoal devidamente treinado poderia captar a mensagem transmitida.

Na Idade Moderna (1453-1789), a rainha da Escócia Maria Stuart (1542-1587), mesmo presa, se comunicava com rebeldes católicos por meio de linguagem criptografada, sendo necessária a intervenção do criptoanalista Thomas Phelippes para quebrar a cifragem. [1] Criptoanalista é aquele que faz

a criptoanálise, conjunto de métodos que tem por objetivo descodificar ou decifrar criptogramas.

A demonstração de preocupação com a vida íntima do indivíduo teve como marco histórico a publicação de um artigo na *Harvard Law Review*, em 15 de dezembro 1890, elaborado pelo advogado Samuel Warren e pelo juiz Louis Brandeis, intitulado '*The right to privacy*'.

Os autores americanos de Boston reclamavam a identificação legal da proteção de um '*right to be let alone*', para proteger as dimensões da personalidade que os mesmos entendiam estarem sendo violadas pela imprensa local da época. [2]

A Constituição da República Portuguesa de 1976 foi a primeira da Europa a dedicar um dispositivo à matéria de proteção de dados pessoais (em seu art. 35º), dispondo sobre normas gerais de tratamento de dados pessoais no âmbito da informática e aqueles constantes de ficheiros manuais. No sentido da CRP/1976, foi a Constituição espanhola (de 27 de dezembro de 1978, em seu art. 18º, nº 1), a Constituição finlandesa (art. 8º) e a Constituição grega de 1975, modificada em 2001 (art. 9º). [3]

No Direito Comunitário europeu, foi de enorme importância a Diretiva 95/46/CE do Parlamento do Conselho, de 24 de outubro de 1995, que regulou a proteção de pessoas singulares no que tange ao tratamento de dados pessoais e à sua livre circulação.

Na época, os países europeus trataram de promover a transposição da referida Diretiva para as suas respectivas ordens jurídicas internas, como, por exemplo, na Itália, pela Lei 675/96, de 11 de dezembro e no Reino Unido, pelo *Data Protection Act of 1998,* de julho.

Mas alguns países já tinham suas legislações sobre proteção de dados, como era o caso da Alemanha (*Bundesdatenschutzgesetz* de 21 de janeiro de 1977 e posteriores alterações), da Espanha (Ley Orgánica de 29 de outubro de 1992) e da França (*Loi Informatique et Libertés* Lei 17, de 6 de janeiro de 1978), que posteriormente promoveram a transposição da Diretiva UE 46/1995 para os seus respectivos ordenamentos.

Atualmente, vige o modelo europeu instituído pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre

circulação desses dados, que revogou a Diretiva 95/46/CE. É o chamado Regulamento Geral sobre a Proteção de Dados – RGPD.

No Brasil, a Constituição da República de 1988 declarou como direito fundamental do cidadão a inviolabilidade de dados e a autodeterminação informativa (art. 5º, incisos X, XI, XII e LXXII). A LGPD brasileira foi fortemente inspirada no RGPD europeu, sendo o último resultado de anos de experiência legislativa europeia quanto à proteção de dados pessoais. [4]

Os velozes avanços tecnológicos somados ao cada vez mais potencializado processo de globalização despertaram nos europeus a necessidade de se criar um instrumento de harmonização e uniformização sobre a proteção de dados na União Europeia, conforme apontam os considerandos do RGPD europeu (especialmente os de número 6 a 9).

O artigo 1º, n. 1, do Regulamento (UE) 2016/679 dispõe que referida norma estabelece regras relativas à proteção das pessoas singulares quanto ao tratamento de seus dados pessoais.

O RGPD estabelece princípios e condições ao tratamento de dados, procedimentos de segurança para com os dados, prevê indenizações em caso de danos materiais e imateriais quando do tratamento de dados e prevê tantas outras questões. O documento possui 173 considerandos e 99 artigos.

Pautando-se na Lei portuguesa n. 67/98, de 26 de outubro, a jurista portuguesa Catarina Sarmento e Castro [5] ensina, sobre dado pessoal e seu respectivo titular: ‘qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (‘titular dos dados’); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural e local’.

Transpôs para a ordem jurídica portuguesa a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados. Tal norma encontra-se revogada pela

Lei nº 58/2019, de 8 de agosto, lei de execução do RGPD europeu.

A definição acima é quase idêntica àquela antes prevista no artigo 2º, “a” da velha Diretiva UE 46/95. Referida Diretiva proporcionava considerável espaço para variação jurídica por cada um dos países membros do bloco europeu, o que não ocorre com o atual RGPD 2016/679, que tem eficácia imediata, sem a necessidade de transposição dos seus países membros, sendo muito mais prescritivo e padronizador. [6]

Assim, por exemplo, a Ley Orgánica 15/1999, de 13 de dezembro (transposição da Diretiva UE 46/95 para o ordenamento espanhol), dispunha em seu art. 3º que se consideram dados de caráter pessoal ‘*cualquier información concerniente a personas físicas identificadas o identificables’.* [7]

A Lei italiana 675/96 definia, em seu art. 1º, n. 1, “c”, como dado pessoal, ‘*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale’.* [8]

A lei italiana (hoje revogada na ordem interna do país), o titular dos dados pessoais poderia ser pessoa física, pessoa jurídica, ente ou associação a quem se referem os dados pessoais. O atual RGPD não abrange o tratamento de dados pessoais relativos a pessoas coletivas (jurídicas), conforme expressamente previsto no considerando n. 14.

No capítulo que trata de provisões interpretativas básicas, o *Data Protection Act of 1998*, define que 'dados pessoais significa dados relativos a um indivíduo vivo que pode ser identificado'. [9] '*Personal data means data which relate to a living individual who can be identified*'.

No âmbito do ordenamento português, dados sensíveis se referem a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, vida sexual, incluindo os dados genéticos. [10]

Em sentido muito parecido foi o *Data Protection Act of 1998,* do Reino Unido e a Lei italiana n. 675/96, conforme salienta Monducci, [11] '*L'art. 22 della legge 675/96 tutela i veri e propri dati sensibili, ovvero i dati 'idonei a rivelare': (a) l'origine razziale ed etnica; (b) le convinzioni religiose, filosofiche o di altro genere e le opinioni politiche; (c) l'adesione a partiti,*

sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale; (d) lo stato di salute; (e) la vita sessuale'.

Com base na Diretiva 95/46/CE, 'qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição',

José Augusto Delgado [12] ensina que os direitos de privacidade (termo aqui empregado de forma genérica e ampla, englobando o direito à intimidade), que são expressamente amparados pela Constituição Federal e pela atual LGPD, são direitos humanos de terceira geração, e que estes são direitos fundamentais. A República Federativa do Brasil rege-se nas suas relações internacionais pela prevalência dos direitos humanos, conforme expressamente previsto no art. 4º, inciso II da CF/88.

A Carta Magna de 1988 declara como direitos fundamentais do cidadão a inviolabilidade de sua

privacidade, de seus dados e, inspirada pela Constituição Portuguesa de 1976, consagra a autodeterminação informativa, tudo conforme art. 5º, incisos X, XI, XII e LXXII. [13]

O conceito de intimidade é geralmente empregado para designar a esfera secreta da vida do indivíduo, que busca evitar o conhecimento dos demais, como, por exemplo, suas relações sexuais.

Já o conceito de privacidade engloba informações restritas da vida do indivíduo, como sua relação com familiares e amigos, o que o renomado autor chama de vida interior, que envolve atividades que geralmente não são tornadas públicas, não devendo ser objeto de divulgações por terceiros. [14]

Quanto ao domicílio do indivíduo, trata-se do local onde o mesmo reside, ou seja, sua casa, conforme preleciona Manoel Gonçalves Ferreira Filho. [15] Assim, ‘a Constituição está reconhecendo que o homem tem direito fundamental a um lugar em que, só ou com sua família, gozará de uma esfera jurídica privada e íntima, que terá que ser respeitada como sagrada manifestação da pessoa humana’. [16]

A Constituição prevê também a inviolabilidade do sigilo das comunicações pessoais, que deve ser

entendida como uma proibição de abertura de cartas e outros meios de correspondência escrita ou a interrupção do seu curso, bem como da interceptação de telefonemas, garantindo-se o sigilo de dados pessoais, a fim de proteger a intimidade do indivíduo. [17]

Dados pessoais, no âmbito da CF/88, são quaisquer informações relativas ao indivíduo. Neste sentido, a 'inviolabilidade do sigilo de dados (art. 5º, XII) complementa a previsão ao direito à intimidade e vida privada (art. 5º, X)'. [18]

Os incisos X e XI do art. 5º da Carta Magna tratam da inviolabilidade da intimidade, da vida privada e da casa do indivíduo, enquanto o inciso XII salvaguarda a confidencialidade dos dados. Em suma, além de tratarem da segurança do domicílio e das comunicações pessoais, os três incisos tratam também da proteção de informações pessoais, de modo que devem ser interpretados sistematicamente, pois o que se pretende resguardar, além da segurança, é a esfera particular do indivíduo contra a curiosidade pública e a ingerência de estranhos. [19]

Os incisos X e XI do art. 5º da Carta Magna tratam da inviolabilidade da intimidade, da vida privada e da casa do indivíduo, enquanto o inciso XII

salvaguarda a confidencialidade dos dados. Além de tratarem da segurança do domicílio e das comunicações pessoais, os três incisos tratam também da proteção de informações pessoais, de modo que devem ser interpretados sistematicamente, pois o que se pretende resguardar, além da segurança, é a esfera particular do indivíduo contra a curiosidade pública e a ingerência de estranhos. [20]

Ainda, conforme preleciona Catarina Sarmento e Castro, [21] ‘o direito à autodeterminação informativa nasce, assim, para garantir um direito à intimidade privada no que aos tratamentos de dados pessoais diz respeito’.

Conforme assevera Alexandre de Moraes [22] sobre as citadas disposições constitucionais, ‘a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de

informes dados ou recebidos em razão de segredo profissional’.

Em razão da crescente utilização dos meios informáticos para a prática de ilícitos, foi editada também a Lei n. 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos. Tal lei foi apelidada de ‘Lei Carolina Dieckmann’, face o vazamento de fotos íntimas que estavam armazenadas em um dispositivo eletrônico da referida atriz. [23]

Conforme a exposição de motivos da Lei n. 13.709/18 (LGPD), um dos fatores que mais motivou a edição da referida norma foi o avanço da tecnologia da informação e a exacerbada quantidade de dados pessoais expostos na Internet. [24]

Para a lei brasileira, o titular dos dados pessoais protegidos é sempre uma pessoa singular, enquanto aqueles que tratam tais dados (chamados pela lei de controlador e operador) podem ser pessoa natural ou jurídica, abrangendo, neste último caso, o Estado.

Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados

pessoais. Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, incisos VI e VII da LGPD).

De acordo com o art. 5º, inciso I da LGPD, dado pessoal é informação relacionada à pessoa natural identificada ou identificável. Dados pessoais do titular relativos à sua origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual etc. são considerados dados pessoais sensíveis (art. 5º, inciso II), cujo tratamento recebe forte restrição (art. 11)

A Lei nº 13.709/2018 Lei traz regras para disciplinar a forma como os dados pessoais dos indivíduos podem ser armazenados por empresas ou mesmo por outras pessoas físicas. O objetivo da Lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Os serviços atualmente oferecidos, especialmente por meio de empresas que trabalham com novas tecnologias, têm como uma de suas características a constante coleta de dados pessoais do usuário.

Assim, por exemplo, a partir do momento em que uma pessoa faz uma conta e acessa o

Facebook, o Instagram ou qualquer outra rede social, a empresa passa a coletar dados pessoais relacionados com aquele usuário. Tais informações vão sendo inseridas em um banco de dados cada dia mais completo a respeito da pessoa.

Nesse banco de dados há informações sobre seu nome, e-mail, cidade, profissão, círculo de amizades e, principalmente, seus gostos e interesses. Isso acontece, como já dito, com praticamente todos os serviços baseados nas novas tecnologias. É o caso do Google, do WhatsApp, do Uber, do Airbnb, do Waze etc. Em toda interação por meio da internet, há coleta de dados.

Tais dados são muito valiosos economicamente porque eles definem tendências de consumo, políticas, religiosas, comportamentais etc. podendo servir para que empresas e políticos direcionem suas estratégias de acordo com essas informações.

Sempre houve suspeita de que esses dados poderiam ser utilizados de forma indevida. Essa suspeita ganhou contornos mais reais quando se descobriu que houve um vazamento de dados de 87 milhões de usuários do Facebook para a empresa de marketing político Cambridge Analytica, que atuou

na campanha eleitoral de Donald Trump. No Brasil, foram vazados os dados de 443 mil pessoas.

Diante desse cenário, entendeu-se necessário regulamentar essa atividade a fim de evitar abusos que gerem violação aos direitos fundamentais dos indivíduos, dentre eles, a privacidade e a intimidade. Essa é uma preocupação internacional, devendo-se destacar que, em 25/05/2018, entrou em vigor o 'Regulamento Geral de Proteção de Dados', conhecido como GPDR, sua sigla em inglês. A GPDR é uma legislação editada pela União Europeia que estabelece regras sobre como as empresas e os órgãos públicos devem lidar com os dados pessoais.

A Lei nº 13.709/2018 utiliza, em diversos momentos, a expressão 'tratamento de dados pessoais'. Tratamento de dados pessoais é toda 'operação' realizada com dados pessoais. Ex: uma empresa de pesquisas coleta dados pessoais em uma pesquisa realizada em um supermercado com os clientes que estavam ali. Em seguida, essa empresa vende esses dados para uma empresa de *marketing*.

A empresa de marketing contrata uma outra empresa para analisar, filtrar e classificar esses

dados. Com esses resultados, a empresa de marketing vende tais informações para uma indústria alimentícia. Nesse exemplo, todas as empresas fizeram o tratamento de dados pessoais. Tratamento de dados pessoais, portanto, é toda e qualquer operação realizada com dados pessoais. Isso inclui toda e qualquer conduta realizada com dados pessoais.

Exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão e extração. Em suma, tratamento de dados pessoais significa praticar alguma atividade que envolva dados pessoais. O grande objetivo da Lei nº 13.709/2018, portanto, é esse: estabelecer regras sobre como as empresas e o poder público tratam os dados pessoais, ou seja, como coletam, como armazenam, como vendem etc., fixando limites para que isso ocorra. Dado pessoal é a informação relacionada a uma pessoa natural. Exemplo: seu nome, RG, CPF, profissão, estado civil, grau de escolaridade etc.

A disciplina da proteção de dados pessoais tem como fundamentos:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Essa Lei se aplica a qualquer operação de tratamento de dados pessoais:

> a) realizada por pessoa natural ou por pessoa jurídica de direito público ou privado;
> b) independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> b.1) os dados pessoais tenham sido coletados no Brasil ou qualquer outra operação de tratamento seja realizada em nosso país. Ex: a pesquisa no supermercado;
> b.2) a atividade de tratamento tenha sido feita fora do Brasil, mas ela tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional. Ex: cadastro no Facebook ou em outros sites estrangeiros, mas que utilizem esses dados para vender produtos aqui no Brasil.

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

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) jornalísticos e artísticos; ou b) acadêmicos (em caso de fins acadêmicos não se aplica a lei toda, mas apenas os arts. 7º e 11); III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

O tratamento de dados pessoais nestes casos (inciso III) será regido por legislação específica, que deverá prever como será feito esse tratamento dos dados pessoais, devendo isso ser realizado de forma proporcional e estritamente necessária ao atendimento do interesse público. Deverão ser assegurados o devido processo legal, os princípios gerais de proteção e os direitos do titular.

Em regra, é vedado o tratamento desses dados do inciso III por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa

jurídica de direito público. Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III poderá ser tratada por pessoa de direito privado.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

> I - finalidade: o tratamento dos dados pessoais deverá ser realizado com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - 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;
> V - 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;
> VI - 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;
> VII - 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;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - 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.

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular. A primeira e mais importante premissa é a seguinte: alguém só pode coletar ou tratar de qualquer outra forma dados pessoais seus, se você permitir. Assim, as empresas não podem coletar dados pessoais sem o consentimento dos titulares.

É a manifestação livre, informada e inequívoca pela qual o titular concorda com o

tratamento de seus dados pessoais para uma finalidade determinada. Quando a Lei fala em ‘titular’, significa a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento. Eu sou titular dos dados pessoais que se referem a mim.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Caso o consentimento seja fornecido por escrito, isso deverá ser feito por meio de cláusula destacada das demais cláusulas contratuais. Se houver dúvida se foi ou não concedido o consentimento, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a Lei.

É vedado o tratamento de dados pessoais mediante vício de consentimento. Ex: o titular foi induzido em erro para fornecer seus dados pessoais. O consentimento 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.

O consentimento deverá referir-se a finalidades determinadas. As autorizações genéricas

para o tratamento de dados pessoais serão nulas. Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Ex: titular autorizou o tratamento de seus dados pessoais para aprimorar um software que ele utiliza; o consentimento foi para isso; no entanto, agora a empresa do software quer utilizar esses dados para vender anúncios personalizados. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular.

O procedimento para a revogação do consentimento deve ser gratuito e facilitado. Enquanto não houver requerimento de eliminação, os tratamentos realizados sob amparo do consentimento anteriormente manifestado são válidos. Ex: João concedeu consentimento em abril de 2020. Em junho de 2021, ele revogou o consentimento. Os dados que foram tratados nesse período de 1 ano e 1 mês são válidos, salvo se João requerer a eliminação.

A Lei diz que o ‘controlador’ que obteve o consentimento do titular, se necessitar comunicar ou compartilhar dados pessoais com outros controladores, deverá obter consentimento específico do titular para esse fim. Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios desta Lei. A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na Lei nº 13.709/2018, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Vale ressaltar que, mesmo nesse caso, o titular deverá ser informado que será feito o

tratamento de seus dados (coleta, armazenamento, classificação etc.).

Dado anonimizado é o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Em outras palavras, anonimizar os dados pessoais significam, como o próprio nome sugere, fazer com que o titular dos dados se torne anônimo, isto é, fazer com que não se possa identificar que aquela informação está ligada àquela pessoa específica.

A Lei define ‘órgão de pesquisa’ como sendo o 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. Exemplo de órgão de pesquisa: o IBGE.

O órgão de pesquisa até pode ser uma pessoa jurídica de direito privado, mas não poderá ter fins lucrativos. Logo, o ‘órgão de pesquisa’ de que trata a lei não pode ser aquelas empresas comerciais que

fazem pesquisas pagas para vender esses dados para outras empresas.

O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca. Trata-se do ‘princípio do livre acesso’.

O titular deverá ter direito às seguintes informações:

> 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; e VII - direitos do titular.

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

> I - apoio e promoção de atividades do controlador; e II - 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.

Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. Dado pessoal sensível é o 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.

O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

> I - quando o titular ou seu responsável legal consentir. Desde que esse consentimento seja dado 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;