Aula 00 - Prof Paulo Sousa

TRT-MG 3ª Região - Legislação

Autor:
Equipe Direito Administrativo, Equipe Legislação Específica Estratégia Concursos, Herbert Almeida, Paulo H M Sousa, Ricardo Torques

14 de Abril de 2023

Índice

1) Lei Geral de Proteçaõ de Ddaos Pessoais - Parte I 3

2) Lei Geral de Proteçaõ de Dados Pessoais - Parte II 18

3) Lei de Proteção de Dados Pessoais - Questões comentadas - Multibancas 39

4) Lei de Proteção de Dados Pessoais - Lista de Questões 59

LEI DE PROTEÇÃO DE DADOS

1. DISPOSIÇÕES GERAIS

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

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

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

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

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

I. A operação de tratamento seja realizada no território nacional
II. A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional
III. Os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Consideram-se coletados no território nacional os dados cujo titular nele se encontre no momento da coleta

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

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

II. Realizado para fins exclusivamente

- a) jornalístico e artísticos
- b) acadêmicos

III. Realizado para fins exclusivos de

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Agentes de tratamento: o controlador e o operador.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. TRATAMENTO DOS DADOS PESSOAIS

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

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

2.1. Requisitos para tratamento dos dados pessoais

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

I. Mediante o fornecimento de consentimento pelo titular;

II. Para o cumprimento de obrigação legal ou regulatória pelo controlador

III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral (neste caso, nos termos da Lei 9.307/1996, a Lei de Arbitragem);

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

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

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

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

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

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

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

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

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

O consentimento deve ser específico, ou seja, deve referir-se a finalidades determinadas.
Assim, nulas são as autorizações genéricas para o tratamento de dados pessoais, não deixa margem de dúvida o §4º.

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

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

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

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

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

I. Finalidade específica do tratamento;

II. Forma e duração do tratamento, observados os segredos comercial e industrial;

III. Identificação do controlador;

IV. Informações de contato do controlador;

V. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI. Responsabilidades dos agentes que realizarão o tratamento;

VII. Direitos do titular (com menção explícita aos direitos previstos no art. 18);

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

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

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

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

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

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

2.2. Tratamento de dados pessoais sensíveis

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

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

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

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

A) Cumprimento de obrigação legal ou regulatória pelo controlador;

B) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

C) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

D) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (neste caso, nos termos da Lei 9.307/1996, a Lei de Arbitragem);

E) Proteção da vida ou da incolumidade física do titular ou de terceiro;

F) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

G) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3. Tratamento de dados pessoais de crianças e adolescentes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4. Término do tratamento de dados

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

I. Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II. Fim do período de tratamento;

III. Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;

IV. Determinação da autoridade nacional, quando houver violação ao disposto na lei.

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

I. Cumprimento de obrigação legal ou regulatória pelo controlador;

II. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei;

IV. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados;

3. DIREITOS DO TITULAR

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

I. Confirmação da existência de tratamento
II. Acesso aos dados
III. Correção de dados incompletos, inexatos ou desatualizados
IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei
V. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial
VI. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na lei
VII. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados
VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
IX. Revogação do consentimento, nos termos da lei

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LEI DE PROTEÇÃO DE DADOS

4. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

4.1. Regras

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas na Lei 12.527/2011 (Lei de Acesso à Informação – LAI), deve ser **realizado para o atendimento de sua finalidade pública, na persecução do interesse público,** determina o art. 23. Esse tratamento tem de ter por objetivo executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> I. Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> III. Seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD.

A autoridade nacional pode dispor sobre as formas de publicidade das operações de tratamento (§1º). No entanto, as disposições da LGPD não dispensam essas pessoas jurídicas de instituir as autoridades previstas na LAI (§2º). Aém disso, prevê o art. 7º, §2º, que a forma de disponibilização das informações previstas no § 1º e no inc. I do *caput* do art. 23 pode ser especificada pela autoridade nacional.

Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público devem observar o disposto em legislação específica, em especial as disposições constantes da Lei 9.507/1997 (Lei do *Habeas Data*), da Lei 9.784/1999 (Lei Geral do Processo Administrativo) e da Lei 12.527/2011 (Lei de Acesso à Informação).

Os serviços notariais e de registro exercidos em caráter privado, por delegação, têm o mesmo tratamento dispensado às pessoas jurídicas de direito público (§4º). Isso significa que esses serviços devem fornecer acesso aos dados por meio eletrônico para a Administração Pública (§5º).

Já as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência (sujeitas ao disposto no art. 173 da CF/1988) **têm o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares,** esclarece art. 24.

Excepcionalmente, porém, determina o parágrafo único, que **se as empresas públicas e as sociedades de economia mista estiverem operacionalizando políticas públicas, e no âmbito da execução delas, passam a ter o mesmo tratamento dispensado às pessoas jurídicas de direito público.**

Os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (art. 25). O estabelecimento de um pretenso *e-Gov*, inclusive, depende dessa interoperabilidade.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas. Ademais, devem ser respeitados os princípios de proteção de dados pessoais elencados no art. 6º, aduz o art. 26.

Porém, **o Poder Público não pode transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso**, restringe o §1º. Só poderá fazê-lo em determinadas hipóteses e desde que os contratos e convênios para tanto sejam comunicados à autoridade nacional:

- Primeiro, em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI (inc. I);
- Segundo, nos casos em que os dados forem acessíveis publicamente (inc. III);
- Terceiro, quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (inc. IV);
- Quarto, na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (inc. V.)

A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado deve ser informado à autoridade nacional, obriga o art. 27. O parágrafo único prevê que essas informações são objeto de regulamentação específica. Em regra, de toda sorte, depende-se de consentimento do titular.

No entanto, **dispensa-se o consentimento do titular nas hipóteses de dispensa legal de consentimento** (inc. I). Também é dispensável o consentimento nos casos **de uso compartilhado de dados** (inc. II). E, por fim (inc. III), dispensa-se-a quando houver **(a) execução descentralizada de atividade pública, (b) acessibilidade pública dos dados, (c) previsão legal ou respaldo em instrumento contratual, (d) objetivo exclusivo vinculado à segurança** (hipóteses do art. 26, §1º).

De acordo com o art. 29, a autoridade nacional pode solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado. Pode, também, emitir parecer técnico complementar para garantir o cumprimento da Lei. Por fim, **compete à autoridade nacional estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais** (art. 30).

4.2. Responsabilidade

Em que pese o estabelecimento de um rol de deveres bem extenso e da criação de uma esfera de proteção absurdamente grande para os dados pessoais, a LGPD é curiosamente lacônica quando da responsabilização. Apenas dois artigos tratam do assunto. Ambos, porém, pouco dizem a respeito.

Segundo o art. 31, quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação. Além disso, a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público. (art. 32).

5. TRANSFERÊNCIA INTERNACIONAL DE DADOS

Quando se permite a transferência internacional de dados pessoais? Segundo o art. 33, apenas nos casos em que:

I. Países ou organismos internacionais proporcionem grau de proteção de dados pessoais adequado ao previsto da LGPD;

II. O controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei, na forma de:

- cláusulas contratuais específicas para determinada transferência
- cláusulas-padrão contratuais
- normas corporativas globais
- selos, certificados e códigos de conduta regularmente emitidos;

III. A transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV. A transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V. A autoridade nacional autorizar a transferência;

VI. A transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII. A transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos da lei;

VIII. O titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;

IX. Necessário para atender a hipótese de:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- necessidade para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral.

No caso do inc. II, **a definição do conteúdo de cláusulas**-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta **será realizada pela autoridade nacional,** estatui o art. 35. Para isso, **devem ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios da lei** (§1º).

Nessa análise, podem ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário (§2º). O §3º ainda prevê que a autoridade nacional pode designar organismos de certificação para a realização dessa análise. Esses organismos permanecerão sob fiscalização da autoridade nacional, nos termos definidos em regulamento.

Os atos realizados por organismo de certificação podem ser revistos pela autoridade nacional. Em caso de desconformidade com a LGPD, devem ser submetidos a revisão ou anulados (§4º). As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular devem ser também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, arremata o §5º.

Por fim, determina o art. 36 que as alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular devem ser comunicadas à autoridade nacional.

Atente para o caso de transferência internacional de dados pessoais a países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto da LGPD, previsto no inc. I. Nesse caso, as pessoas jurídicas de direito público referidas na LAI, no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, **podem requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional,** esclarece o parágrafo único.

Já o art. 34 estabelece que **o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela autoridade nacional. A autoridade nacional deve levar em consideração:**

> I. As normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
>
> II. A natureza dos dados;
>
> III. A observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;
>
> IV. A adoção de medidas de segurança previstas em regulamento;
>
> V. A existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais;
>
> VI. Outras circunstâncias específicas relativas à transferência .

6. AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Ultrapassadas as questões que envolvem a transmissão de dados pessoais, a LGPD passa a versar dos agentes de tratamento de dados pessoais. Como controlador e operador têm características comuns, são tratados em conjunto; em separado, trata-se do encarregado.

Você lembra a semelhança e distinção entre eles? **Apenas controlador e operador são considerados agentes de tratamento, mas não o encarregado. Além disso, o controlador e o operador podem ser pessoas jurídicas, mas o encarregado sempre será pessoa natural.**

Por fim, há as questões que envolvem a responsabilidade do controlador, do operador e do encarregado.

6.1. Controlador e operador

Estabelece o art. 37 que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseadas no legítimo interesse. A autoridade nacional pode determinar ao **controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis.**

O relatório se refere a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (art. 38). O parágrafo único prevê que esse relatório deve conter, no mínimo, (i) a descrição dos tipos de dados coletados, (ii) a metodologia utilizada para a coleta e para a garantia da segurança das informações e (iii) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Além disso, **o operador deve realizar o tratamento segundo as instruções fornecidas pelo controlador, que é responsável pela verificção da observância das próprias instruções e das normas sobre a matéria** (art. 39). A autoridade nacional pode dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência (art. 40).

Esses dispoisitivos minudenciam bem os papeis no tratamento de dados. O controlador é a quem competem as decisões referentes ao tratamento de dados pessoais, ao passo que o operador é quem realiza o tratamento dos dados pessoais em nome do controlador. **Por isso, em que pese o operador trate dos dados *in loco*, responsável é o controlador pelos seus atos, na posição de decisor.**

6.2. Encarregado

Exige o art. 41 que o controlador indique encarregado pelo tratamento de dados pessoais. **As identidades e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador** (§1º).

Mas em que consistem as atividades do encarregado? De acordo com o §2º, **as atividades do encarregado consistem em:**

I. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências

II. Receber comunicações da autoridade nacional e adotar providências

III. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

IV. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares

Para além das normas previstas, **a autoridade nacional pode 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** (§3º). Aqui, regulamento deve dispensar a necessidade de indicação do encarregado, especialmente nas sociedades empresariais de menor porte, já que provavelmente será o próprio empresário ou alguns poucos funcionários a controlar, operar e se encarregar do tratamento dos dados.

6.3. Responsabilidade e ressarcimento de danos

Se a responsabilidade pelo tratamento de dados pessoais pelo Poder Público era praticamente inexistente, os agentes privados têm responsabilização minudenciada em lei. O art. 42 traz disposição que lembra muito o art. 186 do CC/2002, que conceitua o ato ilícito.

Segundo ele, **o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano** patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, **é obrigado a repará-lo. Trata-se, portanto, de responsabilidade civil objetiva, que dispensa prova de culpa.**

A fim de assegurar a efetiva indenização ao titular dos dados, estabelece o §1º, inc. I, que **o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.** Nessa hipótese, o operador equipara-se ao controlador.

Segundo o §1º, inc. II, se estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, **os controladores respondem solidariamente.** Evidentemente, **aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis,** na medida de sua participação no evento danoso (§4º). Ou seja, a responsabilidade do controlador e do operador é solidária, mas há direito de regresso de uns contra os outros.

Talqualmente ocorre no CDC, o §2º permite, no processo civil, que **o juiz inverta o ônus da prova a favor do titular dos dados** quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. Além disso, **as ações de reparação por danos coletivos que tenham por objeto a responsabilização civil podem ser exercidas coletivamente em juízo,** observado o disposto na legislação pertinente (§3º).

Pode haver exclusão da responsabilidade civil dos agentes – controlador e operador, mas não o encarregado – de tratamento de dados? Sim. **Os agentes de tratamento (controlador e operador) só não serão responsabilizados quando provarem que:**

I. Não realizaram o tratamento de dados pessoais que lhes é atribuído;

II. Embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;

II. O dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

No entanto, atente porque o art. 43 **prevê um rol taxativo (*numerus clausus*) de excludentes de responsabilidade. Ou seja, excludentes tradicionais de responsabilização não podem ser arguidas em desfavor do titular dos dados pessoais.**

Já o art. 44 estabelece que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes. O que são "circunstâncias relevantes"? De acordo com a norma, **consideram-se circunstâncias relevantes, dentre outras (rol exemplificativo ou *numerus apertus*):**

I. O modo pelo qual é realizado;

II. O resultado e os riscos que razoavelmente dele se esperam;

III. As técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado;

As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente, rege o art. 45. Assim, o CDC continua aplicável nas situações de dano ao consumidor.

7. SEGURANÇA E BOAS PRÁTICAS

7.1. Segurança e sigilo de dados

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a **proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito,** exige o art. 46. Essa é uma responsabilidade incomensurável, especialmente para pequenas sociedades empresariais.

Novamente, reafirmo o que disse antes. Se o custo de manutenção de dados for demasiado alto, o empresário terá de abrir mão de controlar dados, sob pena de responsabilização.

A autoridade nacional pode dispor sobre padrões técnicos mínimos para tornar aplicável o disposto nesse dispositivo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia (§1º). Isso tem impacto, especialmente no caso de dados pessoais sensíveis.

As medidas tratadas acima devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (§2º). Ademais, o parágrafo único do art. 44 prevê que **responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46, der causa ao dano.**

Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na lei em relação aos dados pessoais, mesmo após o seu término, determina o art. 47. Trata-se de norma assemelhada às presentes no CDC, ensejando responsabilização de todos os que intervenham na segurança da "relação de dados".

O art. 48 ordena que o controlador comunique à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Como se fará essa comunicação? **A comunicação deve ser feita em prazo razoável, conforme definido pela autoridade nacional, e deve mencionar, no mínimo (§1º):**

I. A descrição da natureza dos dados pessoais afetados;

II. As informações sobre os titulares envolvidos;

III. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. Os riscos relacionados ao incidente;

V. Os motivos da demora, no caso de a comunicação não ter sido imediata;

VI. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A autoridade nacional, então, **verifica a gravidade do incidente e pode, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências.** Quais são essas providências?

O §2º do art. 48 menciona dois exemplos, ou seja, trata-se de rol exemplificativo (*numerus apertus*): **(i) ampla divulgação do fato em meios de comunicação; e (ii) medidas para reverter ou mitigar os efeitos do incidente.**

No juízo de gravidade do incidente deve ser avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (§3º). Pretende-se, assim, mitigar os danos causados pelo vazamento de dados pessoais.

Por fim, prevê o art. 49 que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos em lei e às demais normas regulamentares. Assim, necessário analisar essas boas práticas de governança.

7.2. Boas práticas e governança

Prenuncia o art. 50 que **os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, podem formular regras de boas práticas e de governança.** Essas regras vão estabelecer as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador devem levar em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular (§1º).

Estabelece o art. 6º, no inc. VII, o princípio da 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"), e, no inc. VIII, o princípio da prevenção ("adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"). **Na aplicação desses princípios, o controlador pode:**

- **I. Implementar programa de governança em privacidade que, no mínimo:**

  A) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

  B) Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

  C) Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

D) Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

E) Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

F) Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

G) Conte com planos de resposta a incidentes e remediação;

H) Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

- **II. Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento da lei**

Esclarece o §2º do art. 50 que **essas práticas devem observar a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados.** Isso porque, evidentemente, a forma de tratar dados pessoais será radicalmente diferente em se tratando da *Apple* e a maçã do amor do carrinho do Seu José, ali da esquina.

A *Apple* tem uma estrutra, uma escala e um volume de operações significativamente maior. Além disso, trata de dados muito mais sensíveis. Ela tem dados bancários, de hábitos digitais e de propriedade intelectual, por vezes. Seu José tem apenas o número de telefone das pessoas que participam do grupo de *Whatsapp* dele, informando o ponto da cidade no qual ele estará no dia.

Essas regras de boas práticas e de governança devem ser publicadas e atualizadas periodicamente e podem ser reconhecidas e divulgadas pela autoridade nacional (§3º). Por fim, determina o art. 51 que a autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

8. Autoridade Nacional de Proteção de Dados

Depois de ser vetada, na redação original da LGPD, a Autoridade Nacional de Proteção de Dados – ANPD foi recriada, de maneira bastante curiosa, pela Lei 13.853/2019. O art. 55-A estabelece que **a ANPD é órgão da administração pública federal,** integrante da Presidência da República.

Sua natureza jurídica é transitória e pode ser ela transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República, estabelece o §1º. Deve ser feita uma avaliação quanto à transformação da ANPD em em até 2 anos da data da entrada em vigor de sua estrutura regimental.

A ANPD tem assegurada autonomia técnica e decisória (art. 55-B), **sendo ela composta pelos seguintes órgãos** (art. 55-C, incisos):

I – Conselho Diretor, órgão máximo de direção

II – Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

III – Corregedoria

IV – Ouvidoria

V – Órgão de assessoramento jurídico próprio

VI – unidades administrativas e unidades especializadas necessárias à aplicação das disposições da LGPD

O Conselho Diretor da ANPD será composto de 5 diretores, incluído o Diretor-Presidente (art. 55-D), **cujo mandado é de 4 anos** (§3º). No entanto, os mandatos dos primeiros membros nomeados serão de dois, três, quatro, cinco ou seis anos, conforme estabelecido no ato de nomeação (§4º). Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor (§5º).

Os membros são escolhidos pelo Presidente e por ele nomeados, após aprovação pelo Senado Federal, na forma da CF/1988 (art. 52, inc. III, alínea f). Devem ser brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados (§§1º e 2º).

Prevê o art. 55-E que **os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.** Cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que deve ser conduzido por comissão especial constituída por servidores públicos federais estáveis (§1º). Preventivamente, pode o Presidente da República determinar o afastamento do membro, mas somente quando assim recomendado pela comissão especial.

Os membros do Conselho Diretor, após o exercício do cargo, se submetem aos conflitos de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal, previstos no art. 6º da Lei 12.813/2013. Em suma, a previsão do art. 55-F pretende evitar o uso de informação privilegiada no exerício do cargo ou, na quarentena (6 meses depois da saída da função), contratar ou ser contratado por pessoa física ou jurídica relacionada à a´rea de atuação. A infração ao dispositivo, inclusive, caracteriza ato de improbidade administrativa.

O Conselho Diretor pode indicar ocupantes de cargos em comissão e funções de confiança da ANPD. Porém, compete ao Diretor-Presidente nomear ou designar tais pessoas, evidencia o art. 55-I

Quais são as competência da ANPD? Não são poucas, e o examinador pode ser tentado a tratar de competências que não são da ANPD ou, ao inverso, dizer que esta ou aquela competência não é da ANPD. Segundo o art. 55-J, **são as vinte e quatro competências da ANPD:**

I - zelar pela proteção dos dados pessoais, nos termos da legislação

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade – PNPDP

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação. Essas reclamações podem ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada, permite o §6º

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei

XII - elaborar relatórios de gestão anuais acerca de suas atividades

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o

tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento

XV - arrecadar e aplicar suas receitas e publicar, em relatório de gestão, o detalhamento de suas receitas e despesas

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de sua fiscalização, e com a devida observância da PNPDP, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o Poder Público

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com as regras da LINDB

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à LGPD

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos da LGPD e do Estatuto do Idoso

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a lei

Ou seja, a ANPD tem importantíssimos papeis, daí a gritaria geral quando foi ela vetada na refação original da lei. Com a Lei 13.853/2019, a ANPD pode assumir um papel relevante, semelhante a órgãos europeus de controle de dados.

Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção. Com isso, ficam assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da CF/1988 e da própria LGPD, determina o §1º do art. 55-J. Por sua vez, na esteira da LINDB, o §2º estabelece que **os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.**

A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma da lei (§3º). Ela deve manter fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD (§4º).

Tendo em vista a sensibilidade e relevância dos dados na *sociedade algorítmica*, a autoridade deve, no exercício de sas competências, zelar pela preservação do segredo empresarial e do sigilo das informações (§5º).

Quem pode aplicar sanções no caso de violação de dados? Segundo o art. 55-K, **a aplicação das sanções previstas na LGPD compete exclusivamente à ANPD. A norma ainda esclarece que suas competências prevalecem, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.**

Para isso, o parágrafo único prevê que a ANPD deve articular sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais. Ela funciona como órgão central de da LGPD e do estabelecimento de normas e diretrizes para a sua implementação.

Finalmente, o art. 55-L estabelece que constituem receitas da ANPD:

> I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos
>
> II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados
>
> III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade
>
> IV - os valores apurados em aplicações no mercado financeiro das receitas previstas no art. 55-L
>
> VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais
>
> VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública

9. DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Ao fim e ao cabo, como esperado, a LGPD traz algumas, disposições finais e transitórias. A mais importante delas é a última, dramaticamente. Primeiro, os direitos e princípios expressos na lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte (art. 64).

Em se tratando de empresa estrangeira, ela será notificada e intimada de todos os atos processuais previstos na LGPD, independentemente de procuração ou de disposição contratual ou estatutária, **na pessoa do agente ou representante ou pessoa responsável** por sua filial, agência, sucursal, estabelecimento ou escritório instalado **no Brasil.** A regra do art. 61 visa a evitar questionamentos a respeito das comunicações processuais.

Como a lei exige mudanças relativamente complexas, necessário dar tempo aos agentes de tratamento de dados. São duas as regras. Primeiro, a autoridade nacional deve estabelecer normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da lei, consideradas a complexidade das operações de tratamento e a natureza dos dados, determina o art. 63.

Por fim, o art. 65 trata da vigência da Lei 13.709, de 14 de agosto 2018. **Publicada em 15/08/2018, a LGPD entra em vigor após decorridos 24 meses de sua publicação oficial.** Levando-se em conta as regras da LINDB, da LC 95/1998 e do CC/2002 a respeito da contagem de prazos de vigência legal, **a Lei Geral de Proteção de Dados Pessoais – LGPD entra em vigor apenas em 15/08/2020.**

De maneira excepcional, porém, o art. 65, inc. I, estabelece que entram em vigor os arts. 55-A a 55-L (que tratam da ANPD) e os arts. 58-A e 58-B (que tratam do CNPDPP) em 28/12/2018. A norma é curiosa, já que a ANPD, que fora vetada pelo ex-presidente Michel Temer, foi por ele recriada, por MP, e passou a ter vigência imediata, ainda antes de se tornar lei (a MP 869/2018 foi converida na Lei 13.853/2019), no apagar das velas do cargo. Ademais, a Lei 14.010/2020 (que dipõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado - RJET- no período da pandemia do coronavírus) protraiu a vigência dos arts. 52, 53 e 54, que tratam das sanções administrativas, para 01/08/2021.

LEGISLAÇÃO PERTINENTE

O Capítulo VIII da LGPD trata, no âmbito da fiscalização da norma, das **sanções administrativas aplicáveis:**

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> VII - (VETADO);
>
> VIII - (VETADO);
>
> IX - (VETADO).

X - (VETADO);

XI - (VETADO);

XII - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando

não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

Já a Seção II do Capítulo IX da LGPD trata do **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPDP**. O Conselho foi incluído na norma pela Lei 13.853/2019, que alterou significativamente a lei:

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos:

I - 5 (cinco) do Poder Executivo federal;

II - 1 (um) do Senado Federal;

III - 1 (um) da Câmara dos Deputados;

IV - 1 (um) do Conselho Nacional de Justiça;

V - 1 (um) do Conselho Nacional do Ministério Público;

VI - 1 (um) do Comitê Gestor da Internet no Brasil;

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação;

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo;

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e

XI - 2 (dois) de entidades representativas do setor laboral.

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação.

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública.

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes:

I - serão indicados na forma de regulamento;

II - não poderão ser membros do Comitê Gestor da Internet no Brasil;

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução.

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada.

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III - sugerir ações a serem realizadas pela ANPD;

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Veja as principais e introdutórias regras do **Marco Civil da internet**:

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
>
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.
>
> Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

A Lei 13.787/2018 dispõe sobre **a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.** Veja que, logo de cara, no art. 1º, a norma determina a aplicação da LGPD:

> Art. 1º A digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela Lei nº 13.709, de 14 de agosto de 2018.
>
> Art. 2º O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital.
>
> § 1º Os métodos de digitalização devem reproduzir todas as informações contidas nos documentos originais.
>
> § 2º No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito.
>
> § 3º O processo de digitalização deve obedecer a requisitos dispostos em regulamento.
>
> Art. 3º Os documentos originais poderão ser destruídos após a sua digitalização, observados os requisitos constantes do art. 2º desta Lei, e após análise obrigatória de comissão permanente de revisão de prontuários e avaliação de documentos, especificamente criada para essa finalidade.
>
> § 1º A comissão a que se refere o caput deste artigo constatará a integridade dos documentos digitais e avalizará a eliminação dos documentos que os originaram.
>
> § 2º Os documentos de valor histórico, assim identificados pela comissão a que se refere o caput deste artigo, serão preservados de acordo com o disposto na legislação arquivística.
>
> Art. 4º Os meios de armazenamento de documentos digitais deverão protegê-los do acesso, do uso, da alteração, da reprodução e da destruição não autorizados.
>
> Parágrafo único. Os documentos oriundos da digitalização de prontuários de pacientes serão controlados por meio de sistema especializado de gerenciamento eletrônico de documentos, cujas características e requisitos serão especificados em regulamento.
>
> Art. 5º O documento digitalizado em conformidade com as normas estabelecidas nesta Lei e nos respectivos regulamentos terá o mesmo valor probatório do documento original para todos os fins de direito.

§ 1º Para fins do disposto no caput deste artigo é mandatório que a guarda, o armazenamento e o manuseio dos documentos digitalizados também estejam em conformidade com as normas estabelecidas nesta Lei e nos respectivos regulamentos.

§ 2º Poderão ser implementados sistemas de certificação para a verificação da conformidade normativa dos processos referida no caput deste artigo.

Art. 6º Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados.

§ 1º Prazos diferenciados para a guarda de prontuário de paciente, em papel ou digitalizado, poderão ser fixados em regulamento, de acordo com o potencial de uso em estudos e pesquisas nas áreas das ciências da saúde, humanas e sociais, bem como para fins legais e probatórios.

§ 2º Alternativamente à eliminação, o prontuário poderá ser devolvido ao paciente.

§ 3º O processo de eliminação deverá resguardar a intimidade do paciente e o sigilo e a confidencialidade das informações.

§ 4º A destinação final de todos os prontuários e a sua eliminação serão registradas na forma de regulamento.

§ 5º As disposições deste artigo aplicam-se a todos os prontuários de paciente, independentemente de sua forma de armazenamento, inclusive aos microfilmados e aos arquivados eletronicamente em meio óptico, bem como aos constituídos por documentos gerados e mantidos originalmente de forma eletrônica.

JORNADAS DE DIREITO CIVIL

Na contemporânea sociedade da informação, a proteção de dados é extremamente importante e, infelizmente, ainda pouco difundida. O Enunciado 404 reconhece que **a tutela da privacidade da pessoa humana compreende o controle dos próprios dados. Por isso, é necessário o expresso consentimento da pessoa para tratamento de informações** que versem especialmente sobre o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas:

Enunciado 404
A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas.

RESUMO

Ainda não é possível saber, com algum grau de precisão, o que será cobrado sobre essa Lei. Por isso, me parece mais válido você dar uma passada geral nela do que focar neste ou naquele ponto.

QUESTÕES COMENTADAS

1. (CEBRASPE – PC/RJ – Delegado – 2022) Com relação ao tratamento de dados pessoais de que trata a Lei nº 13.709/2018, Lei Geral de Proteção de Dados, assinale a opção correta.

a) O tratamento de dados pessoais não poderá ser condição para o fornecimento de produto ou de serviço ou exercício de um direito.

b) O consentimento do tratamento de dados pelo titular deverá ter uma finalidade determinada, e as autorizações poderão ser genéricas quando formalizadas por meio de contrato.

c) O tratamento de dados pessoais poderá ser realizado mediante o fornecimento de consentimento a manifestação pelo titular de forma verbal, desde que demonstre a manifestação de livre vontade e na presença três testemunhas maiores e capazes.

d) O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por ambos os pais.

e) O consentimento do tratamento de dados poderá ser revogado mediante manifestação expressa do titular, ratificados os tratamentos já realizados sob amparo de consentimento anteriormente manifestado enquanto não houver requerimento de eliminação de dados pessoais tratados.

Comentários:

A **alternativa A** está errada, pois é possível que os dados pessoais sejam condição para o fornecimento de produto ou de serviço ou exercício de um direito, porém desde que o titular seja informa. Eis o que dia o §3º do art. 9º, da LGPD: "Art. 9º. § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei".

A **alternativa B** está errada, pois as autorizações não podem ser genéricas, ao contrário, elas devem ser específicas, caso contrário, serão nulas, conforme dita o §4º do art. 8º, da LGPD: "Art. 8º. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas".

A **alternativa C** está errada, pois o fornecimento do consentimento poderá ser escrito ou por meio que demonstre a manifestação de vontade do titular, não havendo a necessidade da presença de testemunhas, conforme é possível depreender pelo expresso no art. 8º, da LGPD: "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular".

A **alternativa D** está errada, pois o consentimento poderá ser dado por apenas um dos pais, conforme dita o §1º do art. 14, da LGPD: "Art.14. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal".

A **alternativa E** está certa, conforme o §5º do art. 8º, da LGPD: "§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei".

2. (FGV/ DPE-RJ - 2021) Vinícius é dirigente sindical dos servidores da concessionária de água e esgoto Água Limpa do Estado X. A concessionária Água Limpa oferece aos seus servidores telefones celulares e linha telefônica com a LigueJá para o desempenho de suas funções. Ao adquirir cada linha telefônica, Água Limpa celebra contrato de adesão com a LigueJá e, em paralelo, o servidor preenche formulário de informações pessoais para empresas de cobranças e recuperação de créditos. Vinicius notando tal fato, notifica a LigueJá e a Água Limpa pedindo esclarecimentos sobre a cessão das informações. A LigueJá responde afirmando que, no contrato de adesão assinado com Água Limpa e no formulário assinado por Vinicius, constava autorização de uso geral e irrestrito dos dados por LigueJá, e que essa disposição, por si só, autorizava a cessão dos dados pessoais.

Nesse contexto, é correto afirmar que:

a) a aposição da cláusula que autorizou o uso dos dados para quaisquer finalidades, por LigueJá, é legítimo exercício de autonomia privada e, portanto, em respeito ao princípio da força vinculante dos contratos, tem-se por regular a cessão dos dados pessoas por LigueJá;

b) por trata-se de uso pela administração pública, o uso dos dados pessoais poderá dar-se na forma supracitada, considerando a prevalência do interesse público sobre os demais interesses em jogo;

c) a responsabilidade civil do tratador de dados pessoais dá-se por meio de culpa presumida, de modo que o uso e cessão dos dados pessoais poderão ser feitos na forma supracitada, apurando-se a responsabilidade civil posteriormente;

d) tendo sido Vinicius informado do uso de seus dados pessoais na forma apresentada, inexiste ato ilícito praticado por LigueJá, constituindo sua conduta exercícios regular de direito;

e) a informação de Vinicius constitui dado pessoal sensível, por dizer respeito à filiação a sindicato e, portanto, seu tratamento dependeria de consentimento expresso do titular, requerendo-se a indicação da finalidade do uso.

Comentários

A **alternativa A** está incorreta, pois, o de acordo com a LGPD, os dados somente podem ser tratados com o consentimento expresso do titular ou responsável legal, além de serem apresentadas as justificativas acerca da finalidade da cessão.

A **alternativa B** está incorreta, uma vez que contraria o art. 7º, inc. III, da LGPD: " O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei"

A **alternativa C** está incorreta, pois independentemente da maneira como se dá a culpa na caracterização da responsabilidade civil, o tratamento dos dados somente é possível com o devido

consentimento do titular ou de seu responsável legal, além de serem apresentadas as justificativas acerca da finalidade da cessão.

A **alternativa D** está incorreta, pois para que a cessão fosse possível, deveria haver o consentimento expresso de Vinícius, além da justificativa acerca da finalidade, logo, a cessão é ilícita.

A **alternativa E** está correta, de acordo com a dicção do art. 11, inc. I, da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

3. (CESGRANRIO - Banco do Brasil – Escriturário – 2021) Ao realizar a matrícula do seu curso, o estudante preencheu uma ficha cadastral com os seguintes dados: nome, endereço, telefone, religião, estado civil, raça, nome dos pais, número de filhos e sindicato ao qual era filiado. Segundo a Lei Geral de Proteção de Dados (LGPD), consideram-se sensíveis os seguintes dados solicitados:

(A) religião, raça e filiação a sindicato

(B) religião, estado civil e filiação a sindicato

(C) religião, estado civil e raça

(D) número de filhos, raça e religião

(E) número de filhos, raça e estado civil

Comentários:

A **alternativa A** está correta, pois, de acordo com o art. 5º, inc. II, da LGPD, constam no rol dos dados sensíveis a religião, raça e filiação à sindicato: "Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre **origem racial ou étnica**, **convicção religiosa**, opinião política, **filiação a sindicato** ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

A **alternativa B** está incorreta, pois o estado civil não consta no rol de dados sensíveis, conforme analisado acima.

A **alternativa C** está incorreta, pela mesma razão que a alternativa B.

A **alternativa D** está incorreta, uma vez que o número de filhos não se trata de dado sensível, nos termos da LGPD.

A **alternativa E** está incorreta, pois tanto o número de filhos quanto o estado civil, não se tratam de dados sensíveis.

4. (CESGRANRIO - Banco do Brasil – Escriturário – 2021) Um cliente comparece ao banco em que possui conta salário para comprovação de vida, seguindo norma legal sobre o tema. Aproveitando sua presença na instituição financeira, resolve agendar reunião com o gerente de relacionamento, que, com toda presteza, combina recebê-lo em meia hora. Após as conversas

iniciais, ele questiona o gerente sobre os melhores investimentos disponíveis. Algumas opções são apresentadas, e o interesse final é dirigido a dois novos produtos. O gerente, então, comunica ao cliente a necessidade de atualização de sua ficha cadastral, pois surgiu nova legislação sobre proteção de dados. Diante da aquiescência, o gerente apresenta formulário padronizado para o correntista autorizar, expressamente, o compartilhamento dos seus dados com integrantes do grupo econômico do banco (corretoras, entre outras). Nos termos da Lei nº 13.709, de 14 de agosto de 2018, essa autorização

(A) seria desnecessária, por ser decorrente do contrato originário.

(B) está correta, se considerado o claro consentimento do correntista.

(C) seria exigível para quebra de sigilo bancário por ordem judicial.

(D) deve ser ponderada com as necessidades negociais do banco.

(E) decorre da novidade dos produtos apresentados, não se aplicando a produtos já constantes da carteira do banco.

Comentários:

A **alternativa A** está incorreta, pois a autorização é necessária independentemente de contrato anterior, conforme se depreende do expresso pelo art. 11, inc. I, da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

A **alternativa B** está correta, pois a autorização se restringe ao compartilhamento referentes às finalidades específicas quais sejam as necessidades negociais do banco e dependem do claro consentimento do correntista, conforme determina o art. 11, inc. I da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

A **alternativa C** está incorreta, pois mediante ordem judicial é dispensável a autorização, conforme art. 11, inc. II, alínea a, da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: cumprimento de obrigação legal ou regulatória pelo controlador".

A **alternativa D** está incorreta, conforme analisado no art. 11, inc. I, da LGPD, a autorização não deve apenas ser ponderada de acordo com as necessidades negociais do banco, pois antes deve haver o claro consentimento do titular dos dados, que se restringem às suas necessidades negociais.

A **alternativa E** está incorreta, pois a proteção aos dados alcança qualquer dado pessoal, independentemente da época em que foi fornecido, conforme §1º, do art. 11, da LGPD: "§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica".

5. **(FGV/ DPE-RJ - 2021)Vinícius é dirigente sindical dos servidores da concessionária de água e esgoto Água Limpa do Estado X. A concessionária Água Limpa oferece aos seus servidores telefones celulares e linha telefônica com a LigueJá para o desempenho de suas**

funções. Ao adquirir cada linha telefônica, Água Limpa celebra contrato de adesão com a LigueJá e, em paralelo, o servidor preenche formulário de informações pessoais para empresas de cobranças e recuperação de créditos. Vinicius notando tal fato, notifica a LigueJá e a Água Limpa pedindo esclarecimentos sobre a cessão das informações. A LigueJá responde afirmando que, no contrato de adesão assinado com Água Limpa e no formulário assinado por Vinicius, constava autorização de uso geral e irrestrito dos dados por LigueJá, e que essa disposição, por si só, autorizava a cessão dos dados pessoais.

Nesse contexto, é correto afirmar que:

a) a aposição da cláusula que autorizou o uso dos dados para quaisquer finalidades, por LigueJá, é legítimo exercício de autonomia privada e, portanto, em respeito ao princípio da força vinculante dos contratos, tem-se por regular a cessão dos dados pessoas por LigueJá;

b) por trata-se de uso pela administração pública, o uso dos dados pessoais poderá dar-se na forma supracitada, considerando a prevalência do interesse público sobre os demais interesses em jogo;

c) a responsabilidade civil do tratador de dados pessoais dá-se por meio de culpa presumida, de modo que o uso e cessão dos dados pessoais poderão ser feitos na forma supracitada, apurando-se a responsabilidade civil posteriormente;

d) tendo sido Vinicius informado do uso de seus dados pessoais na forma apresentada, inexiste ato ilícito praticado por LigueJá, constituindo sua conduta exercícios regular de direito;

e) a informação de Vinicius constitui dado pessoal sensível, por dizer respeito à filiação a sindicato e, portanto, seu tratamento dependeria de consentimento expresso do titular, requerendo-se a indicação da finalidade do uso.

Comentários

A **alternativa A** está incorreta, pois, o de acordo com a LGPD, os dados somente podem ser tratados com o consentimento expresso do titular ou responsável legal, além de serem apresentadas as justificativas acerca da finalidade da cessão.

A **alternativa B** está incorreta, uma vez que contraria o art. 7º, inc. III, da LGPD: " O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei”

A **alternativa C** está incorreta, pois independentemente da maneira como se dá a culpa na caracterização da responsabilidade civil, o tratamento dos dados somente é possível com o devido consentimento do titular ou de seu responsável legal, além de serem apresentadas as justificativas acerca da finalidade da cessão.

A **alternativa D** está incorreta, pois para que a cessão fosse possível, deveria haver o consentimento expresso de Vinícius, além da justificativa acerca da finalidade, logo, a cessão é ilícita.

A **alternativa E** está correta, de acordo com a dicção do art. 11, inc. I, da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

6. **(Quadrix / CRBM - 2021) À luz da Lei n.° 6.839/1980, da Lei n.° 12.037/2009, da Lei n.° 13.709/2018 e do Decreto n.° 9.094/2017, julgue o item.**

A Lei Geral de Proteção de Dados Pessoais destina-se à proteção dos direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da personalidade da pessoa natural.

Comentários:

A **afirmativa** está correta, conforme expressa o art. 1º da Lei 13.709/2018: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

7. **(Quadrix / CRBM -2021) À luz da Lei n.° 6.839/1980, da Lei n.° 12.037/2009, da Lei n.° 13.709/2018 e do Decreto n.° 9.094/2017, julgue o item.**

O princípio da adequação, que deverá ser observado nas atividades de tratamento de dados pessoais, previsto na Lei Geral de Proteção de Dados Pessoais, refere-se à compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Comentários:

A **afirmativa** está correta, conforme inc. II, do art. 6º, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

8. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

O respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem são fundamentos observados no diploma legal, os quais disciplinam a proteção de dados pessoais.

Comentários:

A **afirmativa** está correta, conforme dispõe o art. 2º, incs. I, IV: "A disciplina da proteção de dados pessoais tem como fundamentos: o respeito à privacidade; a inviolabilidade da intimidade, da honra e da imagem".

9. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento por seu titular, mesmo que este os tenha tornado manifestamente públicos.

Comentários:

A **afirmativa** está incorreta, pois, o §4º, do art. 7º, da LGPD abre uma exceção ao que diz respeito à dispensa de consentimento do titular dos dados: "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

10. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, com a estrita finalidade de realização de estudos e pesquisas, desde que observada a ética e as normas de tratamento de dados pertinentes.

Comentários:
A **afirmativa** está correta, vez que está em conformidade com o expresso pelo art. 13 da LGPD: "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".

11. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, com o objetivo exclusivo de prevenção de fraudes.

Comentários:
A **afirmativa** está incorreta, uma vez que contraria o expresso pelo inc. V, do §1º, do art. 26, da LGPD: "É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades".

12. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

A transferência internacional de dados pessoais só é admitida na legislação pátria quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Comentários:
A **afirmativa** está incorreta, conforme dicção do art. 33, pois há mais razões pelas quais é permitida a transferência internacional de dados pessoas: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro".

13. (IESES / MSGás - Tecnologia da Informação -2021) Sobre a Lei Geral de Proteção de Dados (Lei n. 13.709 de 14 de agosto de 2018), verifique as assertivas e assinale a INCORRETA.

a) As normas gerais contidas nesta Lei são de interesse internacional e nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

b) Para os fins desta Lei, considera-se banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) Para os fins desta Lei, considera-se dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

d) Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Comentários:
ATENÇÃO, a questão pede pela alternativa INCORRETA.

A **alternativa A** está incorreta, conforme transcrição do parágrafo único, do art. 1º da LGPD: "As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios".

A **alternativa B** está correta, conforme o art. 5º, inc. IV, da LGPD: "Para os fins desta Lei, considera-se: banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico".

A **alternativa C** está correta, pois converge com o expresso pelo art. 5º, inc. I, da LGPD: "Para os fins desta Lei, considera-se: dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

A **alternativa D** está correta, conforme o *caput* do art. 1º, da LGPD: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

14. (CESPE/TJ/PA - 2020) A Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) prevê a realização do tratamento de dados pessoais, mediante o consentimento do titular dos dados, para o cumprimento de obrigação legal ou regulatória e para a realização de

estudos ou execução de contratos a pedido do titular. As hipóteses em questão são exemplos de

a) princípios das atividades de tratamento de dados pessoais.

b) requisitos para o tratamento de dados pessoais sensíveis.

c) tratamento de dados pessoais de crianças e adolescentes.

d) direitos do titular dos dados.

e) requisitos para o tratamento de dados pessoais.

Comentários
A **alternativa A** está incorreta, uma vez que os princípios ali descritos não fazem parte do rol de princípios expressos no art. 6º e incs. da LGPD, os quais cita-se finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

A **alternativa B** está incorreta, porque o enunciado não trata sobre os requisitos para o tratamento de dados pessoais sensíveis que são observados na seção II da LGPD, a qual conta com os arts. 11 a 13.

A **alternativa C** está incorreta, pois, em se tratando dos dados da criança e do adolescente, estes estão descritos na seção III da LGPD, pelo art. 14 e §§. A leitura de tais dispositivos permite inferir que o enunciado não se trata do tratamento de dados pessoais de crianças e adolescentes.

A **alternativa D** está incorreta, já que o enunciado não diz respeito aos direitos do titular dos dados presente no Capítulo III da LGPD, que compreende os arts. 17 a 22.

A **alternativa E** está correta, eis que o enunciado diz respeito aos requisitos para o tratamento de dados pessoas, conforme é possível depreender da dicção do art. 7º, incs. I, II e IV: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: mediante o fornecimento de consentimento pelo titular; para o cumprimento de obrigação legal ou regulatória pelo controlador; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais".

15. (CESP /TJ-PA - 2020) De acordo com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), as atividades de tratamento de dados pessoais devem observar a boa-fé e o princípio

a) de dado pessoal, segundo o qual a informação é relacionada à pessoa natural identificada ou identificável.

b) de banco de dados, como um conjunto estruturado de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) da anonimização, com a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

d) da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

e) da eliminação, que é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Comentários

A **alternativa D** está correta, uma vez que é a única assertiva que traz um dos princípios que devem ser observados no tratamento dos dados pessoas. É o que se conclui a partir da dicção do inc. VIII, do art. 6º, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

16. (INSTITUTO AOCP /MJ-SP - 2020) Considerando o que dispõe a Lei n° 13.709/2018, de Proteção de Dados, 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, dentre outras características, de

a) sigilo quanto a informações de contato do controlador.

b) informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

c) não divulgação das responsabilidades dos agentes que realizarão o tratamento.

d) não identificação do controlador.

e) sigilo quanto à finalidade específica do tratamento.

Comentários:

A **alternativa A** está incorreta, pois as informações sobre o contato do controlador deve ser de livre acesso, conforme dispõe o art. 9º, inc. IV, da LGPD: "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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: informações de contato do controlador".

A **alternativa B** está correta, uma vez que está de acordo com o inc. V, art. 9º, da LGPD: "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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: informações acerca do uso compartilhado de dados pelo controlador e a finalidade".

A **alternativa C** está incorreta, uma vez que também contraria a disposição da LGPD, como se percebe pela dicção do inc. IV, do art. 9º: "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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: responsabilidades dos agentes que realizarão o tratamento".

A **alternativa D** está incorreta, porque contraria o expresso pelo art. 9º, inc. III, da LGPD: "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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: identificação do controlador".

A **alternativa E** está incorreta, já que é contrária ao que dispõe o art. 9º, inc. I, da LGDP: 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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: finalidade específica do tratamento".

17. (INSTITUTO AOCP/MJ-SP -2020) Para fins da Lei n° 13.709/2018, de Proteção de Dados, considera-se

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

b) operador a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

c) dado pessoal sensível 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.

d) controlador a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

e) anonimização o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Comentários:

A **alternativa A** está incorreta, conforme disposição do in. III do art. 5º da LGPD: "Para os fins desta Lei, considera-se: 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".

A **alternativa B** está incorreta, de acordo com o inc. VII, do art. 5º, da LGPD: "Para os fins desta Lei, considera-se: operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

A **alternativa C** está correta, pois está em conformidade com o art. 5º, inc. II, da LGPD: "Para os fins desta Lei, considera-se: dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

A **alternativa D** está incorreta, de acordo com o art. 5º, inc. VI, da LGPD: "Para os fins desta Lei, considera-se: controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

A **alternativa E** está incorreta, pois, está em desconformidade com o expresso pelo art. 5º, inc. XI: "Para os fins desta Lei, considera-se: anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

18. (INSTITUTO AOCP/MJ-SP -2020) Considerando o que dispõe a Lei n° 13.709/2018, de Proteção de Dados, assinale a alternativa correta.

a) O término do tratamento de dados pessoais ocorrerá, dentre outras hipóteses, quando se verificar que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

b) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a confirmação da existência de tratamento.

c) A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, prevista na Lei n° 13.709/2018, inclui dados que já tenham sido anonimizados pelo controlador.

d) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

e) Ao titular dos dados pessoais não é dado o direito de peticionar em relação aos seus dados, perante a autoridade nacional, contra o controlador.

Comentários:

A **alternativa A** está correta, uma vez que vai de encontro com o que dita o art. 15, inc. I, da LGPD: "O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada".

A **alternativa B** está incorreta, de acordo com o art. 18, inc. I, da LGPD: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: confirmação da existência de tratamento".

A **alternativa C** está incorreta, conforme se depreende da dicção do art. 18, §7º, da LGPD: "A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador".

A **alternativa D** está incorreta, vez que está em desconformidade com o expresso pelo art. 18, inc. VIII, da LGPD: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa".

A **alternativa E** está incorreta, pois, contraria o §1º, do art. 18, da LGPD: "O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional".

19. (INSTITUTO AOCP/MJ-SP - 2020) Considerando o que dispõe a Lei nº 13.709/2018, que trata da Proteção de Dados, quanto aos princípios e sua conceituação legal, que, juntamente com o princípio da boa-fé, deverão ser observados nas atividades de tratamento de dados pessoais, analise as assertivas e assinale a alternativa que aponta as corretas.

I. Livre acesso: 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.

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

III. Adequação: 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.

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

a) Apenas II e IV.

b) Apenas I e III.

c) Apenas I e II.

d) Apenas II e III.

e) I, II, III e IV.

Comentários:

O **item I** está incorreta, pois, contaria a real definição do princípio da qualidade dos danos prevista no inc. V, do art. 6º, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: 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".

O **item II** está correto. A afirmativa está de acordo com o expresso pelo inc. II, do art. 6º, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: qualidade dos dados: prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

O **item III** está incorreto, pois a afirmativa está em desacordo com o inc. X, do art. 6º, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: 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 **item IV** está correto, de acordo com o expresso pelo art. 6º, inc. IX, da LGPD: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos".

20. (INSTITUTO AOCP/MJ-SP -2020) Segundo a Lei nº 13.709/2018, de Proteção de Dados, a transferência internacional de dados pessoais é permitida nas seguintes situações, EXCETO

a) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei específica.

b) quando a autoridade nacional autorizar a transferência.

c) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro.

d) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

e) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internos.

Comentários:

Atenção! A questão busca a alternativa INCORRETA!

A **alternativa A** está correta, vez que está em conformidade com o art. 33, inc. I, da LGPD: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei".

A **alternativa B** está correta, conforme disposto no art. 33, inc. V, da LGPD: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: quando a autoridade nacional autorizar a transferência".

A **alternativa C** está correta, de acordo com os ditames do art. 33, inc. IV: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro".

A **alternativa D** está correta, conforme disposição do art. 33, inc. VIII: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades".

A **alternativa E** está incorreta, vez que contraria a disposição do inc. III, do art. 33, da LGPD: "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional".

21. (INSTITUTO AOCP/MJ-SP - 2020) Nos termos da Lei Brasileira que trata da Proteção de Dados, Lei nº 13.709/2018, a respeito da Autoridade Nacional de Proteção de Dados (ANPD), assinale a alternativa correta.

a) A natureza jurídica da ANPD é permanente, podendo ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

b) Ato do Ministro da Ciência, Tecnologia, Inovações e Comunicações disporá sobre a estrutura regimental da ANPD.

c) Não é da competência da ANDP apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação.

d) Os valores apurados na venda ou no aluguel de bens móveis e imóveis de sua propriedade não constituem receitas da ANDP.

e) Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal.

Comentários:

A **alternativa A** está incorreta, pois, a natureza jurídica é transitória, nos termos do art. 55-A, §1º da LGPD: "A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República".

A **alternativa B** está incorreta, nos termos do art. 55-G da LGPD: "Ato do Presidente da República disporá sobre a estrutura regimental da ANPD".

A **alternativa C** está incorreta, pois, a competência de que se refere a assertiva é de competência da ANPD, conforme expresso no art. 55-J, inc. V, da LGPD: "Compete à ANPD: apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação".

A **alternativa D** está incorreta, conforme o inc. III, do art. 55-L, da LGPD: "Constituem receitas da ANPD: os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade".

A **alternativa E** está correta, nos termos do expresso pelo art. 55-H da LGPD: "Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal".

22. (CESPE / CEBRASPE - Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

Entre os fundamentos que disciplinam a proteção de dados pessoais no Brasil, estão o respeito à privacidade, a autodeterminação informativa e a liberdade de expressão, de informação, de comunicação e de opinião.

Comentários:

A **afirmação** está correta, como é possível depreender a partir do expresso pelo art. 2º, incs. I, II e III, da LGPD: "A disciplina da proteção de dados pessoais tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião".

23. (CESPE / CEBRASPE-Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

A referida lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins econômicos.

Comentários:

A **afirmação** está incorreta, pois está em dissonância com o que prega o art. 4º, inc. I, da LGPD: "Esta Lei não se aplica ao tratamento de dados pessoais: realizado por pessoa natural para fins exclusivamente particulares e não econômicos".

24. (CESPE / CEBRASPE -Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

Os dados pessoais serão eliminados após o término de seu tratamento, sendo autorizada a sua conservação para a finalidade de estudo por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização desses dados.

Comentários:

A **afirmativa** está correta, conforme é possível depreender a partir da dicção do art. 16, inc. II, da LGPD: "Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: "estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais".

25. (CESPE / CEBRASPE - Ministério da Economia -2020) Com base no Decreto n.° 10.332/2020, julgue os itens subsequentes.

Uma das iniciativas da implementação da Lei Geral de Proteção de Dados é o estabelecimento de uma plataforma de gestão da privacidade de dados dos cidadãos.

Comentários:
A **afirmativa** está correta, como é possível depreender a partir do item 10.2 anexado no Decreto nº 10.332/2020: Iniciativa 10.2. Estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

26. (VUNESP/ Ministério da Economia -2020) A Lei Geral de Proteção de Dados considera como dados pessoais sensíveis os dados sobre

a) contas bancárias.

b) viagens realizadas.

c) formação acadêmica.

d) origem racial ou étnica.

e) numeração de documentos.

Comentários:

A **alternativa D** está correta, pois, traz o expresso pelo art. 5º, inc. II, da LGPD: "Para os fins desta Lei, considera-se: dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Consequentemente, estão incorretas as **alternativas A, B, C e E.**

27. **(CESPE / CEBRASPE - Ministério da Economia - 2020) Julgue o item subsequente, com relação ao Decreto n.º 10.332/2020, que institui a estratégia de Governo Digital, no âmbito dos órgãos e das entidades da administração pública federal.**

Entre os objetivos a serem atingidos por meio da Estratégia de Governo Digital, estão implementar a Lei Geral de Proteção de Dados Pessoais, no âmbito do governo federal; garantir a segurança das plataformas de governo digital; e disponibilizar a identificação digital ao cidadão.

Comentários:
A **afirmativa** está correta, conforme expresso no Anexo I do Decreto 9.319/2018: "Os objetivos a serem alcançados, por meio da Estratégia de Governo Digital incluem: implementar a Lei Geral de Proteção de Dados, no âmbito do Governo federal, e garantir a segurança das plataformas de governo digital; disponibilizar a identificação digital ao cidadão".

28. **(EDUCA / Prefeitura de Cabedelo - PB -2020) Inúmeros escândalos de vazamento de dados aconteceram nos últimos anos, e muitos desses vazamentos envolveram empresas famosas como o Facebook e o Uber. No Uber, foram vazados dados pessoais de 57 milhões de clientes e motoristas, e no Facebook, 87, milhões de usuários do Facebook tiveram seus dados violados. Dada a recorrência de acontecimentos desta natureza, o mundo sentiu a necessidade de implementar leis que protejam a privacidade dos usuários de serviços. No Brasil, foi criada a lei 13.709/18, também conhecida como Lei Geral da Proteção de Dados Pessoais (ou LGPD), que estabelece que dado pessoal é toda informação relacionada à pessoa natural "identificada" ou "identificável", e determina condições específicas para o tratamento desses dados. Sobre a LGPD, assinale a alternativa INCORRETA:**

a) A LGPD foi criada em agosto de 2018, mas somente entrou em vigor em 2020.

b) A LGPD foi inspirada em uma lei europeia, a GDPR.

c) A LGPD regulamentará qualquer atividade que envolva utilização de dados pessoais, seja a atividade relacionada a meios digitais ou não.

d) A LGPD rege que o consentimento de acesso aos dados por uma empresa pode ser revogado a qualquer momento mediante manifestação expressa do titular dos dados.

e) A LGPD aplica-se a qualquer operação de tratamento realizada apenas no Brasil.

Comentários:

A **alternativa A** está correta, a LGPD foi criada em 2018, porém, teve vacatio de dois anos, entrando em vigor somente em 2020, conforme determinação do art. 65, inc. II: "Esta Lei entra em vigor: 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos".

A **alternativa B** está correta, de fato, uma das inspirações para a criação da LGPD foi a GDPR criada pela União Europeia.

A **alternativa C** está correta, conforme art. 1º da LGPD: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

A **alternativa D** está correta, conforme previsão do art. 8º, §5º, da LGPD: "O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei".

A **alternativa E** está incorreta, pois a LGPD aplica-se independentemente do país de sede do ente detentor dos dados, conforme é possível depreender da dicção do art. 3º da LGPD: "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados".

29. **(IDIB / Câmara Municipal de Condado -2020) Com o uso cada vez mais ampliado da tecnologia para as mais diversas atividades em todo o mundo, como para estudar, se locomover, trabalhar, efetuar compras e usar serviços públicos, por exemplo, o volume de dados dos usuários da Internet cresceu exponencialmente e ensejou a criação de uma lei no Brasil que visa proteger informações pessoais sensíveis do uso e do compartilhamento indevidos. Assinale a alternativa que indica corretamente como ficou conhecida essa lei, em vigência desde setembro de 2020.**

a) Lei da Segurança da Informação

b) Lei do Direito ao Sigilo Pessoal

c) Lei Geral de Proteção dos Dados

d) Lei da Segurança na Internet

Comentários:

A **alternativa C** está correta. A Lei de que trata o enunciado é a Lei Geral de Proteção de Dados (13.709/2018), promulgada em agosto de 2018, mas com vacatio de 2 anos. Sendo assim, entrou em vigor em setembro de 2020, e suas disposições, de acordo com o art. 1º, dispõem: "sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

30. **(IADES / CRN - 3ªREGIÃO – 2019) A Lei n° 13.709/2018 (Lei Geral de Proteção de Dados) incide quanto ao cadastro de usuários e clientes, alterando a maneira como as organizações devem tratar dados pessoais, com vistas a proteger os direitos fundamentais de liberdade e de privacidade e a respeitar o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania. Considerando o disposto na referida lei, assinale a alternativa correta.**

a) Essa lei aplica-se exclusivamente a dados coletados por meio digital.

b) Para os fins dessa lei, considera-se dado pessoal qualquer informação relacionada a pessoa física ou jurídica identificada ou identificável.

c) O tratamento de dados pessoais, bem como o compartilhamento desses dados, somente é permitido mediante consentimento do titular, salvo casos de exceção previstos na lei.

d) Dados pessoais de crianças podem ser coletados sem consentimento prévio e armazenados para fins de contato com os pais ou o responsável legal.

e) O consentimento do tratamento dos dados deve ser fornecido pelo titular antecipadamente à coleta dos dados e presume concordância com o compartilhamento dos respectivos dados pessoais com entidades parceiras por tempo indeterminado.

Comentários

A **alternativa A** está incorreta, pois, de acordo com o art. 1º da LGPD: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

A **alternativa B** está incorreta, conforme inc. I, do art. 5º da LGPD: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

A **alternativa C** está correta, vez que está em consonância com o expresso pelo art. 7º *caput* e §4º, da LGPD: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

A **alternativa D** está incorreta, vez que contraria o §3º, do art. 14 da LGPD, proíbe o armazenamento dos dados do menor: "Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo".

A **alternativa E** está incorreta, o consentimento não gera tal presunção, conforme se depreende da dicção do inc. XII, do art. 7º, da LGPD: "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

31. (IADES / BRB – 2019) Considere que, em um órgão público, foi detectada a necessidade da atribuição de responsáveis para manterem registro das operações de tratamento de dados pessoais. De acordo com a Lei nº 13.709/2018, quem devem ser esses responsáveis?

a) Os agentes de tratamento de dados e o conselho diretor.

b) O controlador e o operador.

c) O presidente da República e o controlador.

d) A autoridade nacional e o operador.

e) O governante e a autoridade nacional.

Comentários

A **alternativa B** está correta, uma vez que se encontra em consonância com o art. 37 da LGDP: "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

Consequentemente, estão incorretas as **alternativas A, C, D e E**.

32. (COMPERVE / UFRN -2019) O Regulamento Geral de Proteção de Dados ou GDPR (General Data Protection Regulation) recentemente adotado pela União Europeia (UE) é um rigoroso conjunto de regras sobre privacidade, válido para a UE, baseado em três pilares: governança de dados, gestão de dados e transparência de dados. No Brasil, existe a Lei Geral de Proteção de Dados (Lei nº 13.709) ou LGPD, sancionada em 14 de agosto de 2018 e que entrará em vigor a partir de agosto de 2020. O principal objetivo da LGPD é garantir transparência no uso dos dados das pessoas físicas em quaisquer meios. Esta lei altera a Lei nº 12.965, de 23 de abril de 2014, popularmente chamada de Marco Civil da Internet. Considerando que a empresa Security10, criada e sediada apenas no Brasil, comercializa soluções de TI no mercado nacional e recentemente fechou contrato com uma empresa em Londres para a comercialização de seus produtos na UE, ela deve

a) apenas se ajustar ao LGPD e Marco Civil, por se tratar de uma empresa brasileira e, portanto, sujeita às leis do Brasil.

b) se ajustar não somente à LGPD e Marco Civil, mas também ao GDPR, sob o risco de ser penalizada na UE.

c) apenas se ajustar ao GDPR, pois esta é mais abrangente e se sobrepõe à LGPD e ao Marco Civil

d) se preocupar com privacidade dos dados apenas em 2020, quando a LGPD entrará em vigor.

Comentários:
A **alternativa B** está correta, conforme se depreende dos itens do art. 3 da GDPR: "O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público".

LISTA DE QUESTÕES

1. (CEBRASPE – PC/RJ – Delegado – 2022) Com relação ao tratamento de dados pessoais de que trata a Lei nº 13.709/2018, Lei Geral de Proteção de Dados, assinale a opção correta.

a) O tratamento de dados pessoais não poderá ser condição para o fornecimento de produto ou de serviço ou exercício de um direito.

b) O consentimento do tratamento de dados pelo titular deverá ter uma finalidade determinada, e as autorizações poderão ser genéricas quando formalizadas por meio de contrato.

c) O tratamento de dados pessoais poderá ser realizado mediante o fornecimento de consentimento a manifestação pelo titular de forma verbal, desde que demonstre a manifestação de livre vontade e na presença três testemunhas maiores e capazes.

d) O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por ambos os pais.

e) O consentimento do tratamento de dados poderá ser revogado mediante manifestação expressa do titular, ratificados os tratamentos já realizados sob amparo de consentimento anteriormente manifestado enquanto não houver requerimento de eliminação de dados pessoais tratados.

2. (FGV/ DPE-RJ - 2021) Vinícius é dirigente sindical dos servidores da concessionária de água e esgoto Água Limpa do Estado X. A concessionária Água Limpa oferece aos seus servidores telefones celulares e linha telefônica com a LigueJá para o desempenho de suas funções. Ao adquirir cada linha telefônica, Água Limpa celebra contrato de adesão com a LigueJá e, em paralelo, o servidor preenche formulário de informações pessoais para empresas de cobranças e recuperação de créditos. Vinicius notando tal fato, notifica a LigueJá e a Água Limpa pedindo esclarecimentos sobre a cessão das informações. A LigueJá responde afirmando que, no contrato de adesão assinado com Água Limpa e no formulário assinado por Vinicius, constava autorização de uso geral e irrestrito dos dados por LigueJá, e que essa disposição, por si só, autorizava a cessão dos dados pessoais.

Nesse contexto, é correto afirmar que:

a) a aposição da cláusula que autorizou o uso dos dados para quaisquer finalidades, por LigueJá, é legítimo exercício de autonomia privada e, portanto, em respeito ao princípio da força vinculante dos contratos, tem-se por regular a cessão dos dados pessoas por LigueJá;

b) por trata-se de uso pela administração pública, o uso dos dados pessoais poderá dar-se na forma supracitada, considerando a prevalência do interesse público sobre os demais interesses em jogo;

c) a responsabilidade civil do tratador de dados pessoais dá-se por meio de culpa presumida, de modo que o uso e cessão dos dados pessoais poderão ser feitos na forma supracitada, apurando-se a responsabilidade civil posteriormente;

d) tendo sido Vinicius informado do uso de seus dados pessoais na forma apresentada, inexiste ato ilícito praticado por LigueJá, constituindo sua conduta exercícios regular de direito;

e) a informação de Vinicius constitui dado pessoal sensível, por dizer respeito à filiação a sindicato e, portanto, seu tratamento dependeria de consentimento expresso do titular, requerendo-se a indicação da finalidade do uso.

3. (CESGRANRIO - Banco do Brasil – Escriturário – 2021) Ao realizar a matrícula do seu curso, o estudante preencheu uma ficha cadastral com os seguintes dados: nome, endereço, telefone, religião, estado civil, raça, nome dos pais, número de filhos e sindicato ao qual era filiado. Segundo a Lei Geral de Proteção de Dados (LGPD), consideram-se sensíveis os seguintes dados solicitados:

(A) religião, raça e filiação a sindicato

(B) religião, estado civil e filiação a sindicato

(C) religião, estado civil e raça

(D) número de filhos, raça e religião

(E) número de filhos, raça e estado civil

4. (CESGRANRIO - Banco do Brasil – Escriturário – 2021) Um cliente comparece ao banco em que possui conta salário para comprovação de vida, seguindo norma legal sobre o tema. Aproveitando sua presença na instituição financeira, resolve agendar reunião com o gerente de relacionamento, que, com toda presteza, combina recebê-lo em meia hora. Após as conversas iniciais, ele questiona o gerente sobre os melhores investimentos disponíveis. Algumas opções são apresentadas, e o interesse final é dirigido a dois novos produtos. O gerente, então, comunica ao cliente a necessidade de atualização de sua ficha cadastral, pois surgiu nova legislação sobre proteção de dados. Diante da aquiescência, o gerente apresenta formulário padronizado para o correntista autorizar, expressamente, o compartilhamento dos seus dados com integrantes do grupo econômico do banco (corretoras, entre outras). Nos termos da Lei nº 13.709, de 14 de agosto de 2018, essa autorização

(A) seria desnecessária, por ser decorrente do contrato originário.

(B) está correta, se considerado o claro consentimento do correntista.

(C) seria exigível para quebra de sigilo bancário por ordem judicial.

(D) deve ser ponderada com as necessidades negociais do banco.

(E) decorre da novidade dos produtos apresentados, não se aplicando a produtos já constantes da carteira do banco.

5. (FGV/ DPE-RJ - 2021)Vinícius é dirigente sindical dos servidores da concessionária de água e esgoto Água Limpa do Estado X. A concessionária Água Limpa oferece aos seus servidores telefones celulares e linha telefônica com a LigueJá para o desempenho de suas funções. Ao adquirir cada linha telefônica, Água Limpa celebra contrato de adesão com a LigueJá e, em paralelo, o servidor preenche formulário de informações pessoais para empresas de cobranças

e recuperação de créditos. Vinicius notando tal fato, notifica a LigueJá e a Água Limpa pedindo esclarecimentos sobre a cessão das informações. A LigueJá responde afirmando que, no contrato de adesão assinado com Água Limpa e no formulário assinado por Vinicius, constava autorização de uso geral e irrestrito dos dados por LigueJá, e que essa disposição, por si só, autorizava a cessão dos dados pessoais.

Nesse contexto, é correto afirmar que:

a) a aposição da cláusula que autorizou o uso dos dados para quaisquer finalidades, por LigueJá, é legítimo exercício de autonomia privada e, portanto, em respeito ao princípio da força vinculante dos contratos, tem-se por regular a cessão dos dados pessoas por LigueJá;

b) por trata-se de uso pela administração pública, o uso dos dados pessoais poderá dar-se na forma supracitada, considerando a prevalência do interesse público sobre os demais interesses em jogo;

c) a responsabilidade civil do tratador de dados pessoais dá-se por meio de culpa presumida, de modo que o uso e cessão dos dados pessoais poderão ser feitos na forma supracitada, apurando-se a responsabilidade civil posteriormente;

d) tendo sido Vinicius informado do uso de seus dados pessoais na forma apresentada, inexiste ato ilícito praticado por LigueJá, constituindo sua conduta exercícios regular de direito;

e) a informação de Vinicius constitui dado pessoal sensível, por dizer respeito à filiação a sindicato e, portanto, seu tratamento dependeria de consentimento expresso do titular, requerendo-se a indicação da finalidade do uso.

6. **(Quadrix / CRBM - 2021) À luz da Lei n.° 6.839/1980, da Lei n.° 12.037/2009, da Lei n.° 13.709/2018 e do Decreto n.° 9.094/2017, julgue o item.**

A Lei Geral de Proteção de Dados Pessoais destina-se à proteção dos direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da personalidade da pessoa natural.

7. **(Quadrix / CRBM -2021) À luz da Lei n.° 6.839/1980, da Lei n.° 12.037/2009, da Lei n.° 13.709/2018 e do Decreto n.° 9.094/2017, julgue o item.**

O princípio da adequação, que deverá ser observado nas atividades de tratamento de dados pessoais, previsto na Lei Geral de Proteção de Dados Pessoais, refere-se à compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

8. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

O respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem são fundamentos observados no diploma legal, os quais disciplinam a proteção de dados pessoais.

9. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da**

personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.

O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento por seu titular, mesmo que este os tenha tornado manifestamente públicos.

10. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, com a estrita finalidade de realização de estudos e pesquisas, desde que observada a ética e as normas de tratamento de dados pertinentes.

11. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, com o objetivo exclusivo de prevenção de fraudes.

12. **(Quadrix / CRECI - 14ªREGIÃO -2021) A Lei Geral de Proteção de dados dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com relação às disposições legais contidas no referido ato normativo, julgue o item.**

A transferência internacional de dados pessoais só é admitida na legislação pátria quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros.

13. **(IESES / MSGás - Tecnologia da Informação -2021) Sobre a Lei Geral de Proteção de Dados (Lei n. 13.709 de 14 de agosto de 2018), verifique as assertivas e assinale a INCORRETA.**

a) As normas gerais contidas nesta Lei são de interesse internacional e nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

b) Para os fins desta Lei, considera-se banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) Para os fins desta Lei, considera-se dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

d) Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

14. (CESPE/TJ/PA - 2020) A Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) prevê a realização do tratamento de dados pessoais, mediante o consentimento do titular dos dados, para o cumprimento de obrigação legal ou regulatória e para a realização de estudos ou execução de contratos a pedido do titular. As hipóteses em questão são exemplos de

a) princípios das atividades de tratamento de dados pessoais.

b) requisitos para o tratamento de dados pessoais sensíveis.

c) tratamento de dados pessoais de crianças e adolescentes.

d) direitos do titular dos dados.

e) requisitos para o tratamento de dados pessoais.

15. (CESP /TJ-PA - 2020) De acordo com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), as atividades de tratamento de dados pessoais devem observar a boa-fé e o princípio

a) de dado pessoal, segundo o qual a informação é relacionada à pessoa natural identificada ou identificável.

b) de banco de dados, como um conjunto estruturado de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) da anonimização, com a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

d) da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

e) da eliminação, que é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

16. (INSTITUTO AOCP /MJ-SP - 2020) Considerando o que dispõe a Lei n° 13.709/2018, de Proteção de Dados, 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, dentre outras características, de

a) sigilo quanto a informações de contato do controlador.

b) informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

c) não divulgação das responsabilidades dos agentes que realizarão o tratamento.

d) não identificação do controlador.

e) sigilo quanto à finalidade específica do tratamento.

17. (INSTITUTO AOCP/MJ-SP -2020) Para fins da Lei n° 13.709/2018, de Proteção de Dados, considera-se

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

b) operador a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

c) dado pessoal sensível 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.

d) controlador a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

e) anonimização o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

18. (INSTITUTO AOCP/MJ-SP -2020) Considerando o que dispõe a Lei n° 13.709/2018, de Proteção de Dados, assinale a alternativa correta.

a) O término do tratamento de dados pessoais ocorrerá, dentre outras hipóteses, quando se verificar que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

b) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a confirmação da existência de tratamento.

c) A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, prevista na Lei n° 13.709/2018, inclui dados que já tenham sido anonimizados pelo controlador.

d) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

e) Ao titular dos dados pessoais não é dado o direito de peticionar em relação aos seus dados, perante a autoridade nacional, contra o controlador.

19. (INSTITUTO AOCP/MJ-SP - 2020) Considerando o que dispõe a Lei nº 13.709/2018, que trata da Proteção de Dados, quanto aos princípios e sua conceituação legal, que, juntamente com o princípio da boa-fé, deverão ser observados nas atividades de tratamento de dados pessoais, analise as assertivas e assinale a alternativa que aponta as corretas.

I. Livre acesso: 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.

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

III. Adequação: 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.

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

a) Apenas II e IV.

b) Apenas I e III.

c) Apenas I e II.

d) Apenas II e III.

e) I, II, III e IV.

20. (INSTITUTO AOCP/MJ-SP -2020) Segundo a Lei nº 13.709/2018, de Proteção de Dados, a transferência internacional de dados pessoais é permitida nas seguintes situações, EXCETO

a) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei específica.

b) quando a autoridade nacional autorizar a transferência.

c) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro.

d) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

e) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internos.

21. (INSTITUTO AOCP/MJ-SP - 2020) Nos termos da Lei Brasileira que trata da Proteção de Dados, Lei nº 13.709/2018, a respeito da Autoridade Nacional de Proteção de Dados (ANPD), assinale a alternativa correta.

a) A natureza jurídica da ANPD é permanente, podendo ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

b) Ato do Ministro da Ciência, Tecnologia, Inovações e Comunicações disporá sobre a estrutura regimental da ANPD.

c) Não é da competência da ANDP apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação.

d) Os valores apurados na venda ou no aluguel de bens móveis e imóveis de sua propriedade não constituem receitas da ANDP.

e) Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal.

22. (CESPE / CEBRASPE - Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

Entre os fundamentos que disciplinam a proteção de dados pessoais no Brasil, estão o respeito à privacidade, a autodeterminação informativa e a liberdade de expressão, de informação, de comunicação e de opinião.

23. (CESPE / CEBRASPE-Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

A referida lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins econômicos.

24. (CESPE / CEBRASPE -Ministério da Economia - 2020) Acerca da Lei Geral de Proteção de Dados Pessoais (LGPD) e suas alterações, julgue o item que se segue.

Os dados pessoais serão eliminados após o término de seu tratamento, sendo autorizada a sua conservação para a finalidade de estudo por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização desses dados.

25. (CESPE / CEBRASPE - Ministério da Economia -2020) Com base no Decreto n.° 10.332/2020, julgue os itens subsequentes.

Uma das iniciativas da implementação da Lei Geral de Proteção de Dados é o estabelecimento de uma plataforma de gestão da privacidade de dados dos cidadãos.

26. (VUNESP/ Ministério da Economia -2020) A Lei Geral de Proteção de Dados considera como dados pessoais sensíveis os dados sobre

a) contas bancárias.

b) viagens realizadas.

c) formação acadêmica.

d) origem racial ou étnica.

e) numeração de documentos.

27. (CESPE / CEBRASPE - Ministério da Economia - 2020) Julgue o item subsequente, com relação ao Decreto n.º 10.332/2020, que institui a estratégia de Governo Digital, no âmbito dos órgãos e das entidades da administração pública federal.

Entre os objetivos a serem atingidos por meio da Estratégia de Governo Digital, estão implementar a Lei Geral de Proteção de Dados Pessoais, no âmbito do governo federal; garantir a segurança das plataformas de governo digital; e disponibilizar a identificação digital ao cidadão.

28. (EDUCA / Prefeitura de Cabedelo - PB -2020) Inúmeros escândalos de vazamento de dados aconteceram nos últimos anos, e muitos desses vazamentos envolveram empresas famosas como o Facebook e o Uber. No Uber, foram vazados dados pessoais de 57 milhões

de clientes e motoristas, e no Facebook, 87, milhões de usuários do Facebook tiveram seus dados violados. Dada a recorrência de acontecimentos desta natureza, o mundo sentiu a necessidade de implementar leis que protejam a privacidade dos usuários de serviços. No Brasil, foi criada a lei 13.709/18, também conhecida como Lei Geral da Proteção de Dados Pessoais (ou LGPD), que estabelece que dado pessoal é toda informação relacionada à pessoa natural "identificada" ou "identificável", e determina condições específicas para o tratamento desses dados. Sobre a LGPD, assinale a alternativa INCORRETA:

a) A LGPD foi criada em agosto de 2018, mas somente entrou em vigor em 2020.

b) A LGPD foi inspirada em uma lei europeia, a GDPR.

c) A LGPD regulamentará qualquer atividade que envolva utilização de dados pessoais, seja a atividade relacionada a meios digitais ou não.

d) A LGPD rege que o consentimento de acesso aos dados por uma empresa pode ser revogado a qualquer momento mediante manifestação expressa do titular dos dados.

e) A LGPD aplica-se a qualquer operação de tratamento realizada apenas no Brasil.

29. **(IDIB / Câmara Municipal de Condado -2020) Com o uso cada vez mais ampliado da tecnologia para as mais diversas atividades em todo o mundo, como para estudar, se locomover, trabalhar, efetuar compras e usar serviços públicos, por exemplo, o volume de dados dos usuários da Internet cresceu exponencialmente e ensejou a criação de uma lei no Brasil que visa proteger informações pessoais sensíveis do uso e do compartilhamento indevidos. Assinale a alternativa que indica corretamente como ficou conhecida essa lei, em vigência desde setembro de 2020.**

a) Lei da Segurança da Informação

b) Lei do Direito ao Sigilo Pessoal

c) Lei Geral de Proteção dos Dados

d) Lei da Segurança na Internet

30. **(IADES / CRN - 3ªREGIÃO – 2019) A Lei n° 13.709/2018 (Lei Geral de Proteção de Dados) incide quanto ao cadastro de usuários e clientes, alterando a maneira como as organizações devem tratar dados pessoais, com vistas a proteger os direitos fundamentais de liberdade e de privacidade e a respeitar o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania. Considerando o disposto na referida lei, assinale a alternativa correta.**

a) Essa lei aplica-se exclusivamente a dados coletados por meio digital.

b) Para os fins dessa lei, considera-se dado pessoal qualquer informação relacionada a pessoa física ou jurídica identificada ou identificável.

c) O tratamento de dados pessoais, bem como o compartilhamento desses dados, somente é permitido mediante consentimento do titular, salvo casos de exceção previstos na lei.

d) Dados pessoais de crianças podem ser coletados sem consentimento prévio e armazenados para fins de contato com os pais ou o responsável legal.

e) O consentimento do tratamento dos dados deve ser fornecido pelo titular antecipadamente à coleta dos dados e presume concordância com o compartilhamento dos respectivos dados pessoais com entidades parceiras por tempo indeterminado.

31. (IADES / BRB – 2019) Considere que, em um órgão público, foi detectada a necessidade da atribuição de responsáveis para manterem registro das operações de tratamento de dados pessoais. De acordo com a Lei nº 13.709/2018, quem devem ser esses responsáveis?

a) Os agentes de tratamento de dados e o conselho diretor.

b) O controlador e o operador.

c) O presidente da República e o controlador.

d) A autoridade nacional e o operador.

e) O governante e a autoridade nacional.

32. (COMPERVE / UFRN -2019) O Regulamento Geral de Proteção de Dados ou GDPR (General Data Protection Regulation) recentemente adotado pela União Europeia (UE) é um rigoroso conjunto de regras sobre privacidade, válido para a UE, baseado em três pilares: governança de dados, gestão de dados e transparência de dados. No Brasil, existe a Lei Geral de Proteção de Dados (Lei nº 13.709) ou LGPD, sancionada em 14 de agosto de 2018 e que entrará em vigor a partir de agosto de 2020. O principal objetivo da LGPD é garantir transparência no uso dos dados das pessoas físicas em quaisquer meios. Esta lei altera a Lei nº 12.965, de 23 de abril de 2014, popularmente chamada de Marco Civil da Internet. Considerando que a empresa Security10, criada e sediada apenas no Brasil, comercializa soluções de TI no mercado nacional e recentemente fechou contrato com uma empresa em Londres para a comercialização de seus produtos na UE, ela deve

a) apenas se ajustar ao LGPD e Marco Civil, por se tratar de uma empresa brasileira e, portanto, sujeita às leis do Brasil.

b) se ajustar não somente à LGPD e Marco Civil, mas também ao GDPR, sob o risco de ser penalizada na UE.

c) apenas se ajustar ao GDPR, pois esta é mais abrangente e se sobrepõe à LGPD e ao Marco Civil

d) se preocupar com privacidade dos dados apenas em 2020, quando a LGPD entrará em vigor.

GABARITO

1.	PC/RJ	E	
2.	DPE-RJ		E
3.	CESGRANRIO - Escriturário	A	
4.	CESGRANRIO - Escriturário	D	
5.	DPE-RJ		E
6.	CRBM	C	
7.	CRBM	C	
8.	CRECI - 14ªREGIÃO	C	
9.	CRECI - 14ªREGIÃO	E	
10.	CRECI - 14ªREGIÃO	C	
11.	CRECI - 14ªREGIÃO	E	
12.	CRECI - 14ªREGIÃO	E	
13.	MSGás	A	
14.	TJ/PA	E	
15.	TJ/PA	D	
16.	MJ-SP	B	
17.	MJ-SP	C	
18.	MJ-SP	A	
19.	MJ-SP	A	
20.	MJ-SP	E	
21.	MJ-SP	E	
22.	Ministério da Economia	C	
23.	Ministério da Economia	E	
24.	Ministério da Economia	C	
25.	Ministério da Economia	C	
26.	Ministério da Economia	D	
27.	Ministério da Economia	C	
28.	Prefeitura de Cabedelo - PB	E	
29.	Câmara Municipal de Condado	C	
30.	CRN - 3ªREGIÃO	C	
31.	BRB	B	
32.	UFRN	B	

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

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

1.

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

2.

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

3.

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

4.

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

5.

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

6.

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

7.

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

8.

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

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