Patricia Peck Pinheiro

PROTEÇÃO DE DADOS PESSOAIS

COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)

De acordo com:

- Lei n. 13.853/2019 – Altera diversos dispositivos da LGPD



2ª edição

saraiva jur

Nenhuma parte desta publicação poderá ser reproduzida por qualquer meio ou forma sem a prévia autorização da Editora Saraiva.

A violação dos direitos autorais é crime estabelecido na Lei n. 9.610/98 e punido pelo artigo 184 do Código Penal.

ISBN 9788553613403

Pinheiro, Patricia Peck

Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD) / Patricia Peck Pinheiro – 2. ed. – São Paulo : Saraiva Educação, 2020.

152 p.

Bibliografia

1. Direito à privacidade – Legislação – Brasil 2. Direitos fundamentais 3. Proteção de dados I. Título.

20-0246

CDD 340

Índices para catálogo sistemático:

Direitos fundamentais : Proteção : Brasil 342.7(81)

Direção executiva *Flávia Alves Bravin*

Direção editorial *Renata Pascual Müller*

Gerência editorial *Roberto Navarro*

Gerência de produção e planejamento *Ana Paula Santos Matos*

Gerência de projetos e serviços editoriais *Fernando Penteado*

Planejamento *Clarissa Boraschi Maria (coord.)*

Novos projetos *Melissa Rodriguez Arnal da Silva Leite*

Edição *Daniel Pavani Naveira* | *Estevão Bula Gonçalves*

Produção editorial *Luciana Cordeiro Shirakawa*

Arte e digital *Mônica Landi (coord.)* | *Amanda Mota Loyola* | *Camilla Felix Cianelli Chaves* | *Claudirene de Moura Santos Silva* | *Deborah Mattos* | *Fernanda Matajs* | *Guilherme H. M. Salvador* | *Tiago Dela Rosa* | *Verônica Pivisan Reis*

Planejamento *Clarissa Boraschi Maria (coord.)*

Projetos e serviços editoriais *Kelli Priscila Pinto* | *Marília Cordeiro* | *Mônica Gonçalves Dias*

Diagramação (Livro Físico) *Mônica Landi*

Revisão *Estela Janiski Zumbano* | *Ivani Aparecida Martins Cazarim* | *Ivone Rufino Calabria*

Capa *Deborah Mattos*

Livro digital (E-pub)

Produção do e-pub *Guilherme Henrique Martins Salvador*

Data de fechamento da edição: 11-2-2020

Dúvidas?

Acesse sac.sets@somoseducacao.com.br

SUMÁRIO

SOBRE A AUTORA

INTRODUÇÃO

1. PANORAMA INTERNACIONAL DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

2. COMO A LEI N. 13.709/2018 ESTÁ DIVIDIDA?

3. ATUALIZAÇÕES DA LEI N. 13.709/2018

4. CONCEITOS E TERMINOLOGIAS

5. APLICAÇÃO MATERIAL E TERRITORIAL

6. PRINCÍPIOS APLICADOS AO TRATAMENTO DE DADOS PESSOAIS

7. PENALIDADES

8. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
   ANPD – NATUREZA, ESTRUTURA E FUNCIONAMENTO

9. ANÁLISE COMPARATIVA COM O REGULAMENTO EUROPEU (GDPR)

10. COMO FICAR EM CONFORMIDADE COM A NOVA LEI – CHECK-LIST

11. COMENTÁRIOS À LGPD
   LEI N. 13.709, DE 14 DE AGOSTO DE 2018
      Capítulo I DISPOSIÇÕES PRELIMINARES
         Art. 1°
         Art. 2°
         Art. 3°
         Art. 4°
         Art. 5°
         Art. 6°
      Capítulo II DO TRATAMENTO DE DADOS PESSOAIS
         Seção I Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7°
Art. 8°
Art. 9°
Art. 10.
Seção II Do Tratamento de Dados Pessoais Sensíveis
Art. 11.
Art. 12.
Art. 13.
Seção III Do Tratamento de Dados Pessoais de Crianças e de Adolescentes
Art. 14.
Seção IV Do Término do Tratamento de Dados
Art. 15.
Art. 16.
Capítulo III DOS DIREITOS DO TITULAR
Art. 17.
Art. 18.
Art. 19.
Art. 20.
Art. 21.
Art. 22.
Capítulo IV DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO
Seção I Das Regras
Art. 23.
Art. 24.
Art. 25.
Art. 26.
Art. 27.
Art. 28.
Art. 29.
Art. 30.
Seção II Da Responsabilidade

Art. 31.
Art. 32.
Capítulo V DA TRANSFERÊNCIA INTERNACIONAL DE DADOS
Art. 33.
Art. 34.
Art. 35.
Art. 36.
Capítulo VI DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS
Seção I Do Controlador e do Operador
Art. 37.
Art. 38.
Art. 39.
Art. 40.
Seção II Do Encarregado pelo Tratamento de Dados Pessoais
Art. 41.
Seção III Da Responsabilidade e do Ressarcimento de Danos
Art. 42.
Art. 43.
Art. 44.
Art. 45.
Capítulo VII DA SEGURANÇA E DAS BOAS PRÁTICAS
Seção I Da Segurança e do Sigilo de Dados
Art. 46.
Art. 47.
Art. 48.
Art. 49.
Seção II Das Boas Práticas e da Governança
Art. 50.
Art. 51.
Capítulo VIII DA FISCALIZAÇÃO
Seção I Das Sanções Administrativas

Art. 52.
Art. 53.
Art. 54.
Capítulo IX DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE
Seção I Da Autoridade Nacional de Proteção de Dados (ANPD)
Art. 55.
Art. 55-A.
Art. 55-B.
Art. 55-C.
Art. 55-D.
Art. 55-E.
Art. 55-F.
Art. 55-G.
Art. 55-H.
Art. 55-I.
Art. 55-J.
Art. 56.
Art. 57.
Seção II Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
Art. 58.
Art. 59.
Capítulo X DISPOSIÇÕES FINAIS E TRANSITÓRIAS
Art. 60.
Art. 61.
Art. 62.
Art. 63.
Art. 64.
Art. 65.
REFERÊNCIAS

Agradeço a Larissa Lotufo por seu apoio permanente nos projetos de pesquisa relacionados à inovação tecnológica e novas regulamentações.

SOBRE A AUTORA

- Programadora desde os 13 anos autodidata em Basic, Cobol, C++, HTML.
- Advogada especialista em Direito Digital formada pela Universidade de São Paulo.
- Doutora pela Universidade de São Paulo (Departamento de Direito Internacional).
- Pesquisadora convidada do Max Planck Institute de Munique e Hamburgo (Alemanha).
- Pesquisadora convidada da Universidade de Columbia – NYC (EUA).
- Professora convidada pela Universidade de Coimbra (Portugal).
- Professora convidada pela Universidade Central do Chile.
- Professora convidada especialista em Cibersegurança pela Escola de Inteligência do Exército Brasileiro.
- Professora convidada da Banca Examinadora de Doutorado do Instituto de Tecnologia da Aeronáutica (ITA).
- Árbitra do Conselho Arbitral do Estado de São Paulo (CAESP).
- Vice-Presidente Jurídica da Associação Brasileira dos Profissionais e Empresas de Segurança da Informação.
- Recebeu o prêmio Compliance digital do LEC em 2017.
- Reconhecida como a advogada mais admirada em Propriedade Intelectual no Brasil por 12 anos consecutivos (2008 a 2019).
- Condecorada com quatro medalhas militares.
- Recebeu duas vezes o prêmio Security Leaders.
- 25 livros publicados sobre Direito Digital.
- Sócia e Head de Direito Digital do escritório Pires & Gonçalves Advogados (www.pgadvogados.com.br).
- Sócia-fundadora da empresa de treinamentos Peck Sleiman Edu (www.pecksleiman.com.br).
- Presidente do Instituto iStart de Ética Digital (www.istart.org.br).

INTRODUÇÃO

A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

A Lei de Proteção de Dados Pessoais, que ficou também conhecida pela sigla LGPD, foi promulgada pelo presidente Michel Temer no dia 14 de agosto de 2018 e foi originária do PLC n. 53/2018. É uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humanos.

O prazo inicial estabelecido para adaptação às novas regras foi de dezoito meses[1], tanto para a iniciativa pública como para a privada, considerando qualquer porte e segmento de mercado e a necessidade de atender às exigências de forma eficiente e sustentável, atingindo um nível de proteção de dados inclusive em âmbito internacional quando há tratamento do dado fora do Brasil. Findo esse prazo, poderão, então, ser aplicadas as penalidades previstas, consideradas elevadas, seguindo a mesma tendência das demais regulamentações sobre a mesma matéria em outros países, inspirada, especialmente, pelo Regulamento Europeu de Proteção de Dados Pessoais, também conhecido como GDPR.

O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.

1.

PANORAMA INTERNACIONAL DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.

A base desse pacto é a liberdade, mas o fiel da balança é a transparência. Sendo assim, as leis sobre proteção de dados pessoais têm uma característica muito peculiar de redação principiológica e de amarração com indicadores mais assertivos, de ordem técnica, que permitam auferir de forma auditável se o compromisso está sendo cumprido, por meio da análise de trilhas de auditoria e da implementação de uma série de itens de controle para uma melhor governança dos dados pessoais.

A liderança do debate sobre o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão "free data flow". O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades.

Este, por sua vez, ocasionou um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as

da América Latina, não poderia se dar.

Segundo o preâmbulo (2) e (13) do GDPR, o regulamento tem como objetivo: a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros.

Destaque-se que a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes.

Foi nisso que a nova legislação inovou, ou seja, padronizou, ou melhor, normalizou, quase como uma norma ISO, o que seriam os atributos qualitativos da proteção dos dados pessoais sem a presença dos quais haveria penalidades.

Os efeitos do GDPR são principalmente econômicos, sociais e políticos. Trata-se de apenas uma das muitas regulamentações que vão surgir nessa linha, em que se busca trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras.

2.

COMO A LEI N. 13.709/2018 ESTÁ DIVIDIDA?

A Lei n. 13.709/2018 está dividida em 10 Capítulos, com 65 artigos. Comparativamente, ela é menor que a sua referência europeia (GDPR), que possui 11 Capítulos, com 99 artigos.

- Capítulo I – Disposições Preliminares (arts. 1º ao 6º).
- Capítulo II – Do Tratamento de Dados Pessoais (arts. 7º ao 16): possui Seção I (Dos Requisitos para o Tratamento dos Dados), Seção II (Do Tratamento de Dados Pessoais Sensíveis), Seção III (Do Tratamento de Dados Pessoais de Crianças e Adolescentes) e Seção IV (Do Término do Tratamento de Dados).
- Capítulo III – Dos Direitos do Titular (arts. 17 ao 22).
- Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público (arts. 23 ao 32): possui Seção I (Das Regras) e Seção II (Da Responsabilidade).
- Capítulo V – Da Transferência Internacional de Dados (arts. 33 ao 36).
- Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais (arts. 37 ao 45): possui Seção I (Do Controlador e do Operador), Seção II (Do Encarregado pelo Tratamento de Dados Pessoais) e Seção III (Da Responsabilidade e do Ressarcimento de Danos).
- Capítulo VII – Da Segurança e das Boas Práticas (arts. 46 ao 51): possui Seção I (Da Segurança e do Sigilo de Dados) e Seção II (Das Boas Práticas e da Governança).
- Capítulo VIII – Da Fiscalização (arts. 52 ao 54): possui Seção I (Das Sanções Administrativas).
- Capítulo IX – Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55 ao 59): possui Seção I (Da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Seção II (Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade) – veto presidencial.
- Capítulo X – Disposições Finais e Transitórias (arts. 60 ao 65).

Portanto, a versão nacional é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir

espaço para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê "prazo razoável".

Além disso, houve, inicialmente, o veto presidencial no tocante à criação da Autoridade Nacional de Proteção de Dados Pessoais e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. O que depois foi alterado pela MP n. 869/2018 e pela Lei n. 13.853/2019.

Na época, foi muito discutido, pois o veto à criação da ANPD geraria uma lacuna inicial estruturante no projeto de implementação da nova regulamentação no país, além de não permitir que o Brasil recebesse o reconhecimento por parte da União Europeia de legislação de mesmo nível do GDPR, pois um dos requisitos é a existência de uma autoridade nacional de fiscalização independente, o que poderia não apenas dificultar a aplicação e fiscalização das medidas propostas, mas também criar um entrave nas relações comerciais para o Brasil.

Por certo, há a possibilidade de a fiscalização ocorrer por intermédio dos agentes legitimados para tanto, como o Ministério Público; no entanto, isso pode gerar alguns entraves, visto que a matéria é nova e de ordem técnica elevada, e a centralização do diálogo com um único órgão central fiscalizador facilitaria sobremaneira os avanços na implementação das novas exigências, visto que o órgão foi pensado para garantir o cumprimento e o melhor proveito da regulamentação, por meio de normas complementares, pareceres técnicos e procedimentos de inspeção, devendo concentrar ali uma equipe treinada para tanto.

Ainda que seja por uma boa causa, a implementação da conformidade à LGPD trará um impacto grande nas instituições, podendo contribuir para o aumento do "custo Brasil", especialmente nos setores de Startups, pequenas empresas e no setor público, com especial atenção aos que tratam muitos dados pessoais sensíveis, como os de saúde.

Mas é importante ter em mente que não basta ter a lei de proteção de dados pessoais, é preciso educar, capacitar. Por isso a importância do papel orientantivo da Autoridade (ANPD) e a relevância de sua atuação proativa junto à sociedade e às instituições, para encontrar medidas viáveis de implementação da nova regulamentação, que gerem menor impacto possível nos setores produtivos e que sejam adaptados e aderentes aos usos e costumes.

3.

ATUALIZAÇÕES DA LEI N. 13.709/2018

Apesar de ser uma legislação bem recente, podemos afirmar que a LGPD já passou por algumas atualizações relevantes, iniciadas desde a Medida Provisória n. 869, de dezembro de 2018, que foi motivada essencialmente com a intenção de criar a Autoridade Nacional de Proteção de Dados (ANPD), uma importante figura para a garantia da eficácia e aplicação prática das normas trazidas com a regulação de proteção de dados no Brasil e para se alcançar o mesmo nível de adequação do Regulamento GDPR, e também com a finalidade de ampliação do prazo para sua entrada em vigor.

Desde a publicação da MP n. 869, em dezembro de 2018, até sua aprovação em maio de 2019, aconteceu muita discussão em torno das alterações propostas, principalmente porque no texto da LGPD previa-se uma Autoridade Nacional (ANPD) diferente do que a MP n. 869 efetivamente entregou. Com a transformação da MP n. 869 em lei, por meio da Lei n. 13.853, de 8 de julho de 2019, observou-se que a LGPD foi reativada em alguns trechos que a MP n. 869 pretendia suprimir, algumas modificações propostas pela MP foram mantidas e outros aspectos foram alterados por um novo texto inaugurado pela Lei n. 13.853.

Polêmicas à parte, a ANPD foi criada e trouxe mais segurança e estabilidade para a futura aplicação da Lei Geral de Proteção de Dados. Da mesma forma, trouxe algumas modificações à LGPD, como se pode observar na tabela abaixo (note-se que a tabela está atualizada com as modificações recebidas com a MP n. 869, a Lei n. 13.853/19 e também o Veto n. 24, de outubro de 2019):

PRINCIPAIS ATUALIZAÇÕES DA Lei n. 13.709/2018 (LGPD)	
ARTIGOS DA LGPD ALTERADOS PELA LEI N. 13.853/2019	**COMENTÁRIOS**
Art. 1º, § 1º	Acrescentou-se que as normas gerais contidas no regulamento são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. Dessa forma, a MP trouxe a obrigatoriedade de observância da Lei por todos os entes federativos.

Art. 4º, § 4º	Na primeira versão da LGPD, a proibição do tratamento integral de informações classificadas dentro dos requisitos do art. 4º, III, era total e expressa em relação a uma pessoa de direito privado. Com o art. 4º, § 4º, da Lei n. 13.853/2019, tal proibição ganha uma exceção: se a pessoa de direito privado possuir capital integralmente constituído pelo Poder Público, poderá sim realizar o tratamento de dados elencados no art. 4º, III, da LGPD.
Art. 5º, VIII Art. 5º, XVIII e XIX	Em seu texto original, a LGPD previa em seu art. 5º, VIII, a obrigatoriedade de o encarregado de dados ser pessoa física, com as atualizações essa obrigação deu lugar à possibilidade de se indicar uma pessoa física ou jurídica, podendo, portanto, o encarregado ser também pessoa jurídica, ou mesmo um terceirizado, tornando a lei mais adequada à tendência global e
Art. 5º, VIII Art. 5º, XVIII e XIX	abrindo possibilidades para empresas oferecerem esse tipo de serviço. Em relação a esse aspecto, a lei não é clara sobre a possibilidade ou não do fornecimento do serviço de encarregado de maneira automatizada, abrindo a possibilidade para que as empresas fornecedoras desse tipo de serviço desenvolvam "softwares encarregados (DPO-Bot)" para lidar com a demanda. As atualizações na lei também adicionaram a necessidade de tanto o Controlador quanto o Operador indicarem um Encarregado e não somente o Controlador, como previa o texto legal anterior. Essa alteração torna o processo de comunicação entre Controladores/Operadores e Autoridade e/ou titular mais ágil e direto. Ainda no art. 5º, em seu inciso XIX, a LGPD considerava que a Autoridade Nacional seria um órgão da administração pública indireta, o que poderia restringir a sua atuação. Com a Lei n. 13.853/2019, a palavra indireta foi suprimida, garantindo assim que a Autoridade Nacional seja um órgão que pertence à administração pública e, por isso, possua competência em todo o território nacional e tenha autonomia somente decisória e técnica, já que não mais se configura como uma autarquia ou agência e sim um órgão vinculado ao Poder Executivo. Mas devemos ficar atentos, pois ainda no art. 55-A, § 1º, a redação continua dizendo que a ANPD é da administração pública federal indireta (talvez um mero equívoco ainda ter ficado o termo indireto aqui).
Art. 7º, VIII Art. 7º, § 1º Art. 7º, § 2º Art. 7º, § 7º	Outra alteração importante aconteceu em relação aos dados pessoais de saúde. Isso porque o art. 7º da LGPD determina em seu § 7º algumas especificações para o tratamento posterior dos dados pessoais de saúde, cujo acesso é público ou é tornado público, manifestamente, pelo titular de dados.
Art. 7º, VIII Art. 7º, § 1º Art. 7º, § 2º Art. 7º, § 7º	No art. 7º, VIII, garante-se exclusividade do tratamento de dados pessoais de saúde aos profissionais de saúde, serviços de saúde e autoridade sanitária, delimitando as bases legais para o tratamento desses dados. A Lei n. 13.853 ainda revogou o art. 7º, § 1º e § 2º, permitindo que o ente de tratamento que realiza tratamento de dados pessoais de saúde não informe ao titular dos dados quando seus dados forem tratados em hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador, incluindo, nesse aspecto, o Poder Público. Isso garante que os dados sensíveis de saúde necessários à execução de políticas públicas possam continuar a serem utilizados pelos órgãos governamentais sem a necessidade de informar ao titular de dados. E garantiu a possibilidade de acrescentar novas finalidades ao tratamento de dados pessoais de saúde, cujos dados são de acesso público ou tornados públicos pelo titular, de acordo com as necessidades do tratamento, com a adição do art. 7º, § 7º.

Art. 11, f **Art. 11, § 4º** **Art. 11, § 5º**	A Lei n. 13.853 também alterou o tratamento de dados sensíveis de saúde por meio do art. 11, f, § 4º e seus incisos e § 5º. Tais modificações trouxeram a possibilidade de compartilhamento de dados pessoais sensíveis, relativos à saúde, entre controladores, para a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde. Essa possibilidade é válida até mesmo nas situações em que os entes buscam a obtenção de vantagem econômica, sob a ressalva de que seja em benefício dos interesses dos titulares de dados. Ao mesmo tempo, o art. 11, § 5º, exclui a possibilidade de tratamento de dados sensíveis de saúde para a realização de análise e seleção de riscos ou contratação e exclusão de beneficiários
Art. 18, V **Art. 18, § 6º**	No que diz respeito à regulação da portabilidade dos dados pessoais, o art. 18 apresenta alterações no inciso V e no § 6º e prevê que a Autoridade Nacional ficará responsável por regulamentar a portabilidade dos dados em tratamento, observando os segredos comercial e industrial. O art. 18, § 6º, acrescenta ainda a possibilidade de o controlador não comunicar os demais agentes de tratamento que tenham realizado uso compartilhado de dados se esta comunicação for comprovadamente impossível ou implique esforço desproporcional. Todavia, o parágrafo peca ao não especificar ou quantificar o grau de esforço que pode ser considerado desproporcional.
Art. 20, caput **Art. 20, § 1º e § 2º**	Outra situação que foi alterada pela Lei n. 13.853 concerne ao direito do titular de pedir revisão de decisão tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluindo decisões destinadas a definir perfil pessoal, profissional, de consumo e de crédito. Cabe ao controlador fornecer as informações claras e adequadas sobre os critérios, sendo observados os segredos comercial e industrial.
Art. 23, III e IV	A Lei n. 13.853 manteve o escopo do inciso III com a exigência de que seja indicado um Encarregado de Dados (DPO) quando houver tratamento de dados pessoais nos termos do art. 39, mas vetou o inciso IV que havia sido incluído pela MP n. 869 e que visava acrescentar mais uma especificação para o tratamento de dados realizado pelos entes públicos com o objetivo de proteger e preservar os dados pessoais dos requerentes da Lei de Acesso à Informação, vedando o compartilhamento na esfera do poder público e com pessoas jurídicas de direito privado.
Art. 26, IV e V	A Lei n. 13.853 legitimou a possibilidade da transferência de dados pessoais do Poder Público para entidades privadas nas situações em que há a previsão legal, na existência de contratos, convênios, congêneres ou para a prevenção de fraudes e irregularidades, segurança ou ainda para garantir a integridade do titular dos dados. Essa alteração é interessante para os entes privados como um aliado na prevenção ao crime, tendo em vista que todo Controlador deverá ter um encarregado de proteção de dados constituído e com essa abertura poderá – por meio de contratos – garantir a prevenção a fraudes com ajuda do Poder Público, inclusive para transferência de dados do titular, independentemente do consentimento desse sujeito de direito.
Art. 27, parágrafo único	Apesar de a Lei n. 13.853 garantir aberturas e maior flexibilidade nas possibilidades de compartilhamento de dados entre os entes públicos e privados, a norma não deixou de se preocupar com a transparência de tais relações. Por isso mesmo, acrescentou um parágrafo único ao art. 27 da LGPD pontuando a necessidade de realizar a comunicação à ANPD quando houver o compartilhamento de dados pessoais entre Pessoa Jurídica de Direito Público e Pessoa Jurídica de Direito Privado.

	A maneira pela qual tal comunicação deverá ser realizada será objeto de regulamentação posterior pela Autoridade Nacional de Proteção de Dados.
Art. 29	A relevância da ANPD na fiscalização das relações entre os entes públicos e privados foi assegurada por meio do art. 29, no qual a Lei n. 13.853 adicionou a possibilidade de solicitação de informações pela Autoridade Nacional aos órgãos e entidades governamentais.
Art. 41, § 4º	A MP n. 869 fez algumas alterações em relação à figura do Encarregado de Dados, pontuando no art. 41, § 4º, os requisitos mínimos necessários para o encarregado poder desempenhar a sua função. Dentre tais requisitos, destacava-se a necessidade de o encarregado deter conhecimentos jurídicos-regulatórios e ser apto a prestar serviços especializados em proteção de dados. No entanto, a Lei n. 13.853/2019 vetou tal inciso, não havendo mais exigências na lei de um perfil específico para o encarregado (DPO). Apesar disso, ficou mantido que a Autoridade (ANPD) poderá estabelecer normas complementares sobre a definição e atribuições do Encarregado, inclusive sobre hipóteses de dispensa de sua indicação conforme natureza e porte da entidade e volume de tratamento de dados (semelhante ao que existe no GDPR, mas lá já previsto no próprio regulamento, aqui a depender da ANPD).
Art. 52, X, XI e XII e § 3º e § 6º	A questão das penalidades foi um dos pontos que ficou indo e vindo na lei, com mudanças ocorridas com a MP n. 869, depois com a Lei n. 13.853 e depois por meio do Veto n. 24/2019 recebido pelo Congresso Nacional. Ao final, os vetos foram rejeitados e prevaleceu a previsão da suspensão parcial do funcionamento do banco de dados, a suspensão do exercício da atividade de tratamento de dados pessoais e a proibição parcial ou total do exercício das atividades relacionadas a tratamento de dados pessoais, todavia só podem ser aplicadas após já ter sido imposta uma das sanções previstas nos incisos I, III, IV, V e VI do caput do art. 52. E se o controlador estiver submetido a outro órgão (ex: Bacen, Anatel), este deve ser ouvido antes. No § 5º, o art. 52 pontua a destinação da arrecadação das multas aplicadas pela ANPD que irão para o Fundo de Defesa de Direitos Difusos e reforça o sistema de gradação das sanções.
Art. 52, X, XI e XII e § 3º e § 6º	O artigo ainda se preocupa em destacar que no caso de controladores submetidos a outros órgãos ou entidades com competências sancionatórias a ANPD poderá agir em conjunto, mas os conflitos envolvendo proteção de dados são de competência exclusiva da ANPD.
Art. 52, § 7º	Há um ponto muito relevante trazido pela atualização da lei que traz a possibilidade de conciliação direta entre controlador e titular nos casos de vazamentos individuais ou os acessos não autorizados de que trata o art. 46.
Art. 55-A	No art. 55-A a lei versa sobre a natureza jurídica da ANPD. A Lei n. 13.853 criou a ANPD como um ente vinculado à Presidência da República, no entanto o § 1º aduz que essa sua natureza jurídica é transitória e poderá ser transformada em autarquia após 2 anos, mediante proposta do Poder Executivo.
Art. 55-C	A composição da Autoridade é prevista no art. 55-C da Lei n. 13.853. O artigo pontua que a ANPD será composta por 6 elementos: i) Conselho Diretor; ii) Conselho Nacional de Proteção de Dados; iii) Corregedoria; iv) Ouvidoria; v) Órgão de Assessoramento Jurídico Próprio; vi) Unidades Administrativas e Unidades Especializadas que garantam a aplicação da lei.

Art. 55-J	No que diz respeito às competências da ANPD elencadas no art. 55-J, é possível destacar: - zelar pela proteção dos dados pessoais, nos termos da legislação; - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; - 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;
Art. 55-J	- apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; - 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; - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; - 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 a esta Lei; - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n. 10.741, de 1º de outubro de 2003 (Estatuto do Idoso). É relevante pontuar que o art. 55-K deixa claro que compete exclusivamente à ANPD a aplicação das sanções previstas na LGPD, e que suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.
Art. 65, II	Outra novidade importante trazida com a Lei n. 13.853 foi a alteração do início da vigência da LGPD. O texto original previa que a LGPD passaria a vigorar a partir de 18 meses após a publicação da Lei n. 13.709, no entanto, com a alteração, esse prazo se estendeu para 24 meses a partir da data de publicação da LGPD. Dessa forma, a LGPD entra em vigor em agosto de 2020 e não mais em fevereiro de 2020.

4.

CONCEITOS E TERMINOLOGIAS

Alguns conceitos e terminologias trazidos pela lei são fundamentais e devem ser objeto de harmonização em documentos, com especial atenção às políticas, às normas, aos procedimentos e aos contratos.

- **Titular**

  Pessoa a quem se referem os dados pessoais que são objeto de algum tratamento.

- **Tratamento dos dados**

  Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Dados pessoais**

  Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

- **Dados pessoais sensíveis**

  São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- **Dados anonimizados**

São os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.

- **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. Não é o único motivo que autoriza o tratamento de dados, mas apenas uma das hipóteses.

- **Agentes de tratamento**

O controlador que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal.

- **Encarregado**

Pessoa natural, indicada pelo controlado, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

- **Transferência internacional de dados**

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

5.

APLICAÇÃO MATERIAL E TERRITORIAL

Em primeiro lugar, a lei se aplica a todos aqueles que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, que realizam qualquer operação de tratamento de dados pessoais, independentemente do meio, que possa envolver pelo menos um dos seguintes elementos:

(i) ocorrer em território nacional;

(ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

(iii) em que os dados tenham sido coletados no território nacional.

Sendo assim, a LGPD não está relacionada à cidadania ou à nacionalidade dos dados pessoais, tampouco à residência do indivíduo titular.

Por outro lado, a lei não se aplica quando o tratamento dos dados é realizado por uma pessoa física, para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos e artísticos e para tratamentos realizados para fins de segurança pública e defesa nacional, conforme o art. 4º, I, II, III e IV.

Como visto, a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Desse modo, o dado pessoal tratado por uma empresa de serviço de cloud computing que armazene o dado fora do país terá que cumprir as exigências da LGPD.

6.

PRINCÍPIOS APLICADOS AO TRATAMENTO DE DADOS PESSOAIS

A regulamentação de proteção de dados pessoais é uma legislação principiológica, como já foi dito. Sendo assim, tanto na origem europeia como na versão nacional traz um rol de princípios que precisam ser atendidos. A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido.

Essa metodologia foi uma forma mais objetiva encontrada pelo regulador de se tratar uma regra que, apesar de se referir a direitos fundamentais, como a proteção da privacidade, necessita de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais.

Portanto, a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

Quando analisado o GDPR, que entrou em vigor em 25 de maio de 2018, verifica-se que o seu artigo 5º traz os princípios que devem ser seguidos no tratamento de dados pessoais, e que são expressos, depois, nas notificações da Autoridade Fiscalizadora, quando há algum tipo de denúncia ou autuação; são eles:

(i) licitude;

(ii) lealdade;

(iii) transparência;

(iv) limitação da finalidade;

(v) minimização dos dados;

(vi) exatidão;

(vii) limitação da conservação;

(viii) integridade e confidencialidade (que são os mesmos da segurança da informação);

(ix) responsabilidade.

Pela LGPD, as atividades de tratamento legítimo, específico e explícito de dados pessoais informado previamente ao titular devem estar orientadas pelos seguintes princípios: da finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas.

Sendo assim, no tratamento de dados pessoais deve-se observar a boa-fé e os seguintes princípios, em destaque:

(i) finalidade do tratamento;

(ii) compatibilidade do tratamento com as finalidades informadas ao titular;

(iii) limitação do tratamento ao mínimo necessário para a realização de suas finalidades;

(iv) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma do tratamento;

(v) garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) transparência aos titulares;

(vii) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais;

(viii) prestação de contas, pelo agente, da adoção de medidas capazes de comprovar a proteção de dados pessoais.

Além disso, há alguns pontos de atenção fundamentais que devem ser observados para a aplicação dos princípios da LGPD no tratamento dos dados pessoais.

A linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas. No entanto, pode haver situações de exceção em que o tratamento de dados pessoais ocorre sem necessidade de consentimento expresso, com finalidade específica declarada pelo titular, quais sejam:

- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- quando necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- para a proteção da vida do titular ou de terceiro;
- quando necessário para atender aos interesses legítimos do controlador ou de

terceiro;

- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Um dos grandes impactos da LGPD está relacionado à necessidade de se garantir os direitos dos titulares, alguns deles novos para o ordenamento jurídico e para as empresas públicas e privadas, tais como o direito à portabilidade dos dados pessoais. Sendo assim, em resumo, passaram a ser direitos dos titulares e que as instituições devem estar preparadas para atender dentro de um prazo razoável, pela lei brasileira:

(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 o disposto na Lei;

(v) portabilidade dos dados a outro fornecedor de serviço ou produto;

(vi) eliminação dos dados pessoais tratados com o consentimento do titular;

(vii) informação sobre a possibilidade de não fornecer consentimento e consequências da negativa;

(viii) revogação do consentimento.

7.

PENALIDADES

No tocante às penalidades previstas pela LGPD, frise-se que algumas sanções sofreram veto presidencial e ficaram menores do que as previstas pelo GDPR, tendo em vista a necessidade de adaptação para a realidade e o contexto do cenário econômico e social brasileiros.

Foram previstas as seguintes penalidades, sendo que o critério de aplicação deverá observar alguns requisitos, especialmente o da proporcionalidade:

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 – 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; (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei n. 13.853, de 2019)

Sendo assim, um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade.

A Lei prevê que 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.

Além disso, as sanções previstas pelos incisos X, XI e XII só podem ser aplicadas 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.

Entre os itens que podem ser considerados na minimização de uma punição pela Autoridade fiscalizadora responsável, conforme previsto pelo próprio art. 52, § 1º, estão:

- a gravidade da infração;
- a boa-fé do infrator;
- a vantagem auferida;
- a condição econômica do infrator;
- a reincidência;
- o grau de dano causado;
- a cooperação do infrator;
- a demonstração de adoção de mecanismos e procedimentos para mitigar os danos;
- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas;
- a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Portanto, a governança corporativa precisará focar nos princípios que foram previstos pela LGPD para que o negócio seja sustentável.

8.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Pode-se afirmar que a ANPD foi criada para trazer mais segurança e estabilidade para a aplicação da Lei Geral de Proteção de Dados. No caso específico do Brasil há uma previsão bem ampla de artigos da Lei que dependem de futura regulamentação por parte da Autoridade, logo caberá a ela executar as adequações necessárias para que a legislação tenha uma aderência maior com a realidade social e econômica. O que já traz consigo uma grande responsabilidade de quem vier a assumir a ANPD, especialmente no primeiro mandato, que será muito mais estruturante de todo o framework legal da proteção de dados pessoais no país.

A ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional mas principalmente internacional para que o Brasil saiba se posicionar no mercado digital global.

A etapa após a entrada em vigor da lei é a mais importante, pois devem ser estabelecidas políticas públicas de adequação, e a aplicação de Códigos de Conduta e Certificações será primordial. Esse é um tema inclusive mais bem tratado no GDPR, com uma grande riqueza de detalhes nos artigos 40 ao 43, enquanto na LGPD nos limitamos a poucas linhas do artigo 50.

Nesse sentido, o que se pode esperar da atuação da ANPD no Brasil pode ser espelhado na experiência de outros países. Segundo dados do IAPP[2], existem cerca de 150 Data Protection Authorities (DPAs), que é o nosso equivalente da ANPD, e há dois perfis muito distintos em termos de abordagem de atuação: 1) Orientativo/Fiscalizatório e 2) Punitivo/Arrecadatório.

Algumas Autoridades têm se apresentado mais disponíveis para responder consultas públicas, atuar junto às entidades representativas dos setores para homologar Códigos de Conduta específicos, bem como aplicar multas com valor educativo, em que a penalidade máxima só é aplicada nos casos excepcionais de vazamento de dados com evidências de negligência do controlador.

Por outro lado, há outro perfil de Autoridade muito mais "caça às bruxas" que visa à aplicação de multas como foco principal.

Uma forma de acompanhar como tem sido a aplicação das penalidades pelas Autoridades dos outros países é acessar o site https://www.enforcementtracker.com/.

Em suma, o que se observou no trabalho das Autoridades de Proteção de Dados pelo mundo desde o advento do GDPR foi uma mudança de comportamento por parte das empresas em alguns passos centrais e iniciais:

- **Verificação dos bancos de informações internos**: os tratamentos de dados pessoais estão minimizados? As finalidades estão informadas? Os titulares de dados estão cientes e de acordo com o tratamento?
- **Apagamento dos dados pessoais que estejam sendo tratados em desacordo com o previsto em lei**, incluindo os dados que as empresas não deveriam ter coletado – sem o consentimento ou a ciência dos titulares. Sendo que a consecução de tal etapa foi – e está sendo – garantida por meio das notificações e sanções às empresas que seguem em desacordo;
- **Identificação dos bancos de dados em tratamento** para garantir a transparência das informações, sendo que as empresas passaram a ter que listar: que tipos de dados pessoais possuem em tratamento? Por que estão tratando os dados? Os dados são compartilhados com outra empresa/entidade? Por que há necessidade do compartilhamento? Há transferência internacional dos dados em tratamento? De maneira que todas as informações pudessem ser acessíveis às autoridades e garantissem a segurança das informações;
- **Atendimento ao titular na resolução de conflitos ou questionamentos envolvendo o tratamento de seus dados pessoais.**

De maneira geral, conforme o apontado pelo website Information Comissioner's Office (ICO)[3] – Autoridade de Proteção de Dados da Inglaterra –, o trabalho das autoridades de dados basicamente constitui-se em 4 pilares: i) garantia do enforcement da regulação de proteção de dados; ii) fiscalização, auditoria e aconselhamento às empresas acerca da rotina envolvendo tratamento de dados; iii) compartilhamento de dados e informações acerca de melhores práticas em proteção de dados; e iv) monitoração dos tratamentos.

Esse trabalho realizado pelas autoridades europeias busca garantir a aplicação da lei e disseminar uma cultura de proteção aos dados pessoais e respeito à privacidade.

Nesse sentido, é importante compreender a previsão legal de como vai funcionar a ANPD e verificar como será a aplicação de tais rotinas no contexto brasileiro.

ANPD – NATUREZA, ESTRUTURA E FUNCIONAMENTO

No que diz respeito à regulamentação da Autoridade Nacional de Proteção de Dados (ANPD) em si, o Capítulo IX reserva os arts. 55-A a 55-K para a matéria.

Inicialmente, é importante ressaltar que a ANPD será responsável pela orientação geral no que tange à adequação e aplicação da Lei Geral de Proteção de Dados brasileira, determinando as diretrizes do tratamento de dados no Brasil, além de poder alterar a Lei n. 13.709/2018 (LGPD). A ANPD também será responsável pela fiscalização dos tratamentos e aplicação das sanções e multas previstas pela LGPD.

No art. 55- A, a Lei versa sobre a natureza jurídica da ANPD, que foi criada como um ente vinculado à Presidência da República, no entanto o § 1º aduz que essa sua natureza jurídica é transitória e poderá ser transformada em autarquia após 2 anos, mediante proposta do Poder Executivo.

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

§ 1º 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.

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias (BRASIL, 2019).

De maneira comparada, observa-se que a Autoridade de Proteção de Dados da Inglaterra segue uma natureza jurídica possivelmente similar, tendo em vista que o ICO é um órgão público que reporta diretamente ao Parlamento inglês e não possui um departamento especial. Outros países, como França, Portugal e Irlanda, optaram por modelos independentes, do tipo agência reguladora.

A previsão de alteração do status da ANDP é positiva, tendo em vista que isso poderá garantir mais autonomia ao órgão, embora também seja possível observar em outros países exemplos positivos que adotam esses moldes de dependência ao Poder Público central.

A composição da Autoridade é prevista no art. 55-C da MP n. 869 e prevê que a ANPD será composta por 6 elementos, conforme se verifica abaixo:

Conselho Diretor ➲ composto por 5 integrantes que deverão ser indicados pela Presidência da República e terão mandatos de 4 anos, sendo esse o órgão máximo

de direção da Autoridade (art. 55-D | MP n. 869/18);

Conselho Nacional de Proteção de Dados ➲ composto por 23 representantes, sendo 6 do Poder Executivo, 1 do Senado Federal, 1 da Câmara dos Deputados, 1 da Câmara Nacional de Justiça, 1 do Conselho Nacional do Ministério Público, 1 do Comitê Gestor da Internet no Brasil, 4 de entidades da sociedade civil com atuação na proteção de dados, 4 de instituições (científicas, tecnológicas e de inovação, 4 de entidades representativas do setor empresarial relacionado à proteção de dados (art. 58-A | MP n. 869/2018). Todos esses representantes não receberão remuneração e terão mandatos de 2 anos;

Corregedoria;

Ouvidoria;

Órgão de Assessoramento Jurídico Próprio;

Unidades Administrativas e **Unidades Especializadas** que garantam a aplicação da lei (BRASIL, 2019).

No que diz respeito às competências da ANPD – art. 55-J –, é possível destacar:

- zelar pela proteção dos dados pessoais, nos termos da legislação;
- elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- 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;
- apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- 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;

- realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
- 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 a esta Lei;
- garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n. 10.741, de 1º de outubro de 2003 (Estatuto do Idoso).

É relevante pontuar que o art. 55-K deixa claro que compete exclusivamente à ANPD a aplicação das sanções previstas na LGPD, e que suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Por fim, a ANDP será incumbida de tornar a LGPD mais clara, acessível e palatável, tanto para os titulares de dados quanto para os agentes de tratamento, garantindo maior segurança jurídica às transações que envolvem o tratamento das informações pessoais, já que essas são uma das competências da Autoridade, conforme o art. 55-J da Lei Geral de Proteção de Dados.

De maneiral geral, pode-se afirmar que a constituição da ANPD é essencial para que o enforcement da Lei de Proteção de Dados seja possível, ou seja, é esse regulamento que torna a aplicação da lei possível. Isso ocorre porque um regulamento com previsão de sanções sem órgão fiscalizador não tem efetividade nem garantia de funcionamento.

9.

ANÁLISE COMPARATIVA COM O REGULAMENTO EUROPEU (GDPR)

O tema da proteção dos dados pessoais teria sido mais bem recepcionado em sede de um tratado internacional, visto que a natureza atual dos fluxos de dados nos negócios é transfronteiriça.

Na União Europeia, conseguiu-se alcançar o objetivo de consolidar em um único regulamento geral a regra de 28 Estados--Membros, conquistado com o GDPR; a mesma sorte não houve nas demais regiões do planeta. Há hoje leis nacionais sobre a matéria nos demais países que fizeram com que as instituições, dependendo do tipo de operação do seu negócio, tivessem que construir uma matriz de análise comparativa (direito comparado) para analisar qual a regra aplicável em determinado caso concreto que envolva dados de um determinado titular.

Apenas a título ilustrativo, uma instituição brasileira que capture dados no Brasil, em território nacional, mas que tenha um aplicativo que permita que o cliente seja de qualquer cidadania, nacionalidade, residência, e, portanto, o usuário do serviço, titular dos dados, pode ser um europeu, que mantém sua vida em um país da União Europeia, mas está temporariamente a trabalho no Brasil, utiliza cartão de crédito internacional, acaba por atrair, em termos de aplicação de leis e jurisdição para a sua operação, tanto a regulamentação nacional (LGPD) como também a regulamentação europeia (GDPR). Se essa instituição brasileira utilizar recursos na nuvem e fizer a guarda internacional dos dados pessoais em outro país, poderá atrair ainda outras regulamentações (como o Cloud Act, dos EUA).

Considerando a comparação entre a LGPD e o GDPR, ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais, buscando em si a defesa dos direitos fundamentais das pessoas naturais.

ITEM DE CONFORMIDADE	REGIME BRASILEIRO (LGPD)	REGIME EUROPEU (GDPR)
Definição e distinção do que são dados pessoais e dados sensíveis.	Define que dado pessoal é qualquer informação que identifique	Adota os mesmos princípios e conceitos para realizar a distinção e delimitação dos

Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico	ou torne identificável a pessoa natural; já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer da pessoa natural.	direitos relativos aos dados pessoais e dados sensíveis, e ainda pontua considerações acerca dos dados genéticos, biométricos e os relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitação do tratamento do dado conforme finalidade	A coleta e o tratamento de dados só poderão ser realizados se o usuário (dono dos dados ou responsável legal no caso de menores legais) der consentimento. Todo agente deve apontar finalidade certa, garantida e justificável ao tratamento do dado. Além disso, deve garantir que ele será utilizado somente para tal finalidade.	Prevê a necessidade de uso do dado conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. São definidos dois agentes de tratamento: o responsável – cuja competência é decidir sobre o tratamento dos dados – e o operador – a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados. Ambos os agentes são juridicamente responsáveis pela segurança e privacidade dos dados.	Há a mesma distinção entre titularidade e agentes, mas os agentes são divididos em controlador e processador de dados. O controlador é quem realiza as decisões acerca do tratamento de dados; o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.
Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes	Além dos agentes, aponta-se a necessidade da indicação de um encarregado – pessoa natural – pela comunicação de qualquer informação ou fato relevante em relação ao tratamento dos dados. Ele deve atuar como um canal entre os agentes, titulares e órgãos competentes e deve ser indicado pela organização responsável pelo tratamento (Agente de Proteção de Dados).	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações	Do consentimento ao fornecimento de dados ao término do tratamento dos dados, as informações acerca do processo devem ser claras, acessíveis e adequadas à linguagem e compreensão do usuário, de forma que o seu consentimento possa ser revogado a qualquer momento. O consentimento do usuário deve ser realizado por escrito ou de qualquer outro modo que demonstre a sua livre manifestação da vontade.	Os titulares também têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.
	Da mesma forma que as organizações são responsáveis no	Também aponta que as empresas devem criar

Aplicação de medidas de segurança e dever de reportar	caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações. Ainda assim, no caso de qualquer incidente é obrigação da organização notificar as autoridades imediatamente.	medidas – como pseudoanonimização e encriptação de dados – para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal	O titular do dado pode alterar ou excluir seu dado pessoal a qualquer momento, exceto nas hipóteses previstas na lei, como fins fiscais, por exemplo. Da mesma forma, assim que o tratamento de dados chegar ao	Os titulares dos dados também podem alterar ou excluir seus dados.
Possibilidade de alteração e exclusão do dado pessoal	final – seja porque cumpriu sua finalidade, seja porque o usuário revogou seu consentimento –, as informações devem ser eliminadas.	
Aplicação de sanções no caso do descumprimento das regras	As punições variam entre advertências, aplicação de multas, suspensão e até mesmo proibição das atividades relacionadas ao tratamento de dados. Essas punições variam de forma gradativa de acordo com cada caso, conforme a gravidade do dano, a condição econômica do infrator, a reincidência, a boa-fé do infrator etc., e devem ser investigadas por meio de um processo administrativo que assegura o contraditório, a ampla defesa e o direito de recurso. As multas podem ser simples ou diárias, com valor relativo a 2% do faturamento da organização privada, limitadas a um total de R$ 50 milhões por infração.	Também prevê a aplicação de sanções gradativas e multas administrativas, que podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa.
Criação de um órgão competente para fiscalizar e zelar pela proteção de dados pessoais e da privacidade	Criada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).	Possui um Órgão de Controle e Fiscalização de Proteção de Dados Pessoais por Estado (28) e aplica o princípio do Balcão único.

10.

COMO FICAR EM CONFORMIDADE COM A NOVA LEI – CHECK-LIST

Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de compliance digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.

A LGPD traz um grande impacto social e econômico. O usuário brasileiro titular de dados pessoais precisará saber o que é proteção de dados pessoais, assim como haverá necessidade de se disponibilizar recursos financeiros para que o sistema da pequena empresa e de startups possam se adequar.

A lei prevê e exige que existam encarregados da proteção dos dados pessoais nas organizações. O controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas, seja por aplicação de recursos de anonimização, controle de acesso, procedimentos, políticas de gestão e treinamentos para equipes. Fica a questão de quem deve ser esta pessoa e como fazer o treinamento e a seleção desse profissional na organização, seja ele interno ou terceirizado.

A vacatio legis é de 24 meses, conforme atualização dada pela Lei n. 13.853/2019, o que é considerado ainda assim um prazo curto. Agora todo e qualquer projeto já precisa ser iniciado com as premissas do privacy by design, e os projetos em andamento devem ser adaptados para atender aos mesmos princípios, ou seja, estar preparados para atender à nova realidade regulatória brasileira e internacional.

Para iniciar a implementação dos requisitos de conformidade à LGPD, o primeiro passo é a realização de um levantamento. Ou seja, deve-se fazer uma análise de diagnóstico para identificar como a instituição está no tocante aos indicadores de conformidade e o que falta para atender aos controles exigidos. Para tanto, a primeira atividade é fazer o inventário dos dados pessoais (quais são e onde estão). Depois, deve-se montar a matriz de tratamento dos dados pessoais (quais os tipos de tratamento e para que finalidades). Em seguida, como está sendo feito o controle de gestão de consentimentos. Com esse

panorama, é desenvolvido o mapa de risco e elaborado o plano de ação, que permite fazer a cotação dos investimentos necessários às conformidades, implementadas, em geral, em quatro níveis: no nível técnico (ferramentas), documental (atualizar normas, políticas, contratos), procedimental (adequar a governança e a gestão dos dados pessoais) e cultural (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes).

A complexidade da implementação desse tipo de regulamentação se dá pelo fato de que os negócios estão globalizados, e o fluxo de dados está internacionalizado ainda mais com os recursos digitais e a internet. Logo, há necessidade de se aplicar uma abordagem de direito comparado e de direito internacional.

Dependendo do ramo do negócio, da empresa e da maturidade da governança dos dados pessoais, é fundamental criar um programa de compliance digital, com risk assessment, planos de respostas a incidentes, treinamentos e comunicação, due diligence de terceiros em um contexto multissetorial dentro do negócio e com visão holística para a legislação nacional e internacional.

Logo, em resumo, o passo a passo consiste:

a) na revisão e atualização da política de privacidade para estar em conformidade com as novas regulamentações de proteção de dados pessoais;

b) na atualização das cláusulas de contratos (seja com titular de dados pessoais consumidor final ou funcionário);

c) na atualização das cláusulas de contratos com os parceiros e fornecedores que realizam algum tipo de tratamento de dados, principalmente fornecedores de soluções de gestão de informação, nuvem, monitoração, mensageria, e-mail marketing, credit score, big data, mídias sociais (coleta, produção, recepção, classificação, acesso, utilização, transmissão, armazenagem, processamento, eliminação, enriquecimento);

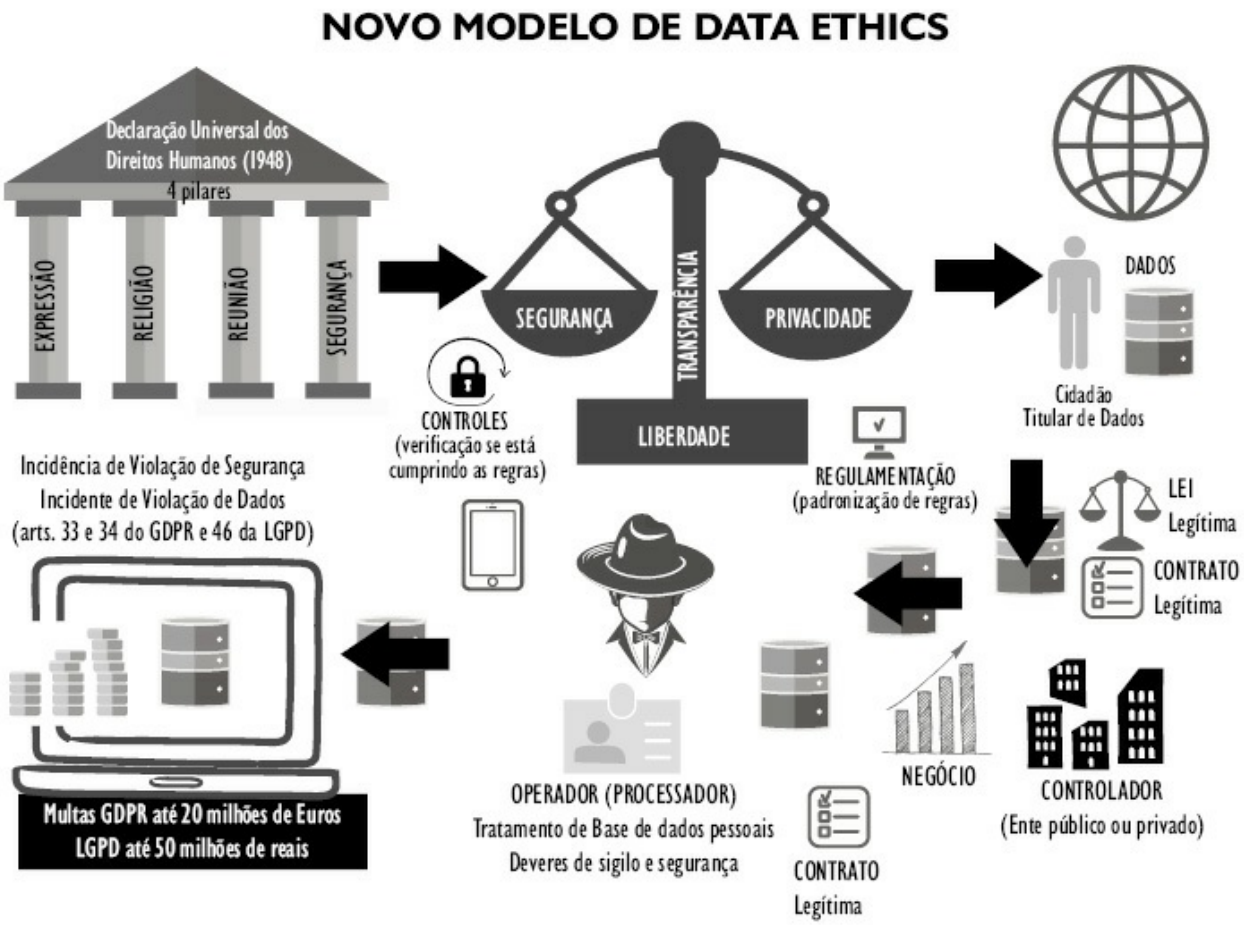
d) no mapeamento do fluxo de dados para definição da nova governança junto a TI dos controles de consentimento (ciclo de vida do dado – coleta, uso, compartilhamento, enriquecimento, armazenamento nacional ou internacional, com ou sem uso de nuvem, eliminação, portabilidade);

e) no modelo de resposta para o Notice Letter do Órgão de Controle de Dados (sobre nível de conformidade da empresa e controles auditáveis) para prevenção a aplicação de multas e fiscalizações;

f) no modelo de check-list de compliance para uso da área de compras para novos

fornecedores e parceiros, que precisarão estar em conformidade com as novas regulamentações de proteção de dados pessoais;

g) no modelo para gestão e guarda de trilha de auditoria para gestão dos logs de consentimento.



Lista de documentos que precisam ser atualizados:

- Mapa de fluxo de dados pessoais (Personal Data Flow Map).
- Tabela de temporalidade de guarda de logs de consentimento.
- Política de gestão de dados pessoais (que deve ser assinada inclusive inter companies – entre empresas do mesmo grupo econômico, entre matriz e filiais).
- Política para tratamento de dados pessoais para terceirizados (providers que realizam tratamento de dados pessoais – vários procedimentos trazidos no GDPR e na LGPD sobre fluxo, padrão de criptografia, guarda de logs etc.).
- Termo de uso e Política de privacidade (atualizar batendo tratamento x finalidade de uso x justificativa jurídica x matriz de consentimentos, novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação e outros).
- Contratos (atualizar com cláusulas que preveem GDPR e LGPD).

- NDA (atualizar com cláusulas que preveem GDPR e LGPD).
- Check-list Compliance (atualizar com cláusulas que preveem GDPR e LGPD).
- Código de Conduta (atualizar com cláusulas que preveem respeito à proteção de dados pessoais).
- Política de Segurança da Informação (atualizar com cláusulas que preveem GDPR e LGPD).

11.

COMENTÁRIOS À LGPD

LEI N. 13.709, DE 14 DE AGOSTO DE 2018

Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte lei:

Capítulo I
DISPOSIÇÕES PRELIMINARES

Art. 1º 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.

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

A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade. Pode-se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e a expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder.

Pensando nisso, a atuação das empresas no contexto digital trouxe consigo a necessidade de criação de mecanismos de regulação e proteção dos dados pessoais daqueles que utilizam serviços, compras ou realizam qualquer tipo de transação on-line que envolve o fornecimento de informações pessoais. Toda situação ou ação realizada no ambiente virtual faz parte da realidade de qualquer pessoa, portanto os direitos

garantidos no "mundo offline" devem ser assegurados também no espaço virtual. Em virtude disso, é importante apontar que a lei brasileira não protege somente os dados pessoais nos meios digitais.

Assim como o GDPR – lei europeia que trata do assunto –, a LGPD advém da evolução e expansão dos direitos humanos e resulta da atualização/adaptação de documentos internacionais de proteção aos direitos humanos. No caso da Europa, é interessante destacar a Diretiva da União Europeia n. 95/46/CE, que por muito tempo foi referência em relação ao tratamento de dados não só na Europa, mas até em países de outros continentes, como Brasil, México, Argentina etc. Com a aprovação do GDPR, a Diretiva n. 95/46/CE foi revogada.

O GDPR ainda pontua em seu artigo (1) que toma por base o artigo 8º, n. 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16º, n. 1, do Tratado sobre o Funcionamento da União Europeia. Embora a lei brasileira não faça menção a documentos específicos que originam o seu texto, é importante relembrar alguns tratados dos quais o país é signatário e que pontuam a questão dos dados pessoais: a Convenção de Berna de 1886 já tratava da base de dados em seu texto, embora ainda de forma um pouco indefinida e incipiente; o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS – aprovado no Brasil em 1994), em seu artigo 10 (2), pontua que as compilações de dados devem receber o mesmo tratamento da criação intelectual, mas não se aprofunda em relação à proteção pessoal dos dados compilados.

Em relação às normas internas, o Brasil já previa algum tipo de proteção aos dados pessoais por meio dos seguintes dispositivos:

(i) Código de Defesa do Consumidor – art. 43[4];

(ii) Decreto n. 7.962/2013 (Comércio Eletrônico) – art. 4º, VII[5];

(iii) Marco Civil da Internet – arts. 7º, I, III, VII, VIII, IX, X, XI, e 11[6], §§ 1º e 2º.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I – o respeito à privacidade;

II – a autodeterminação informativa;

III – a liberdade de expressão, de informação, de comunicação e de opinião;

IV – a inviolabilidade da intimidade, da honra e da imagem;

V – o desenvolvimento econômico e tecnológico e a inovação;

VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e

VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A proteção aos direitos fundamentais é bastante evidente no art. 2º da LGPD, que pode ser relacionado ao texto constitucional brasileiro no que concerne ao conteúdo, haja vista que a Constituição Federal Brasileira é pautada na proteção aos direitos fundamentais. Entre os artigos constitucionais destacáveis, pode-se citar: art. 3º, I e II; art. 4º, II; art. 5º, X e XII; art. 7º, XXVII; e art. 219[7].

Da mesma maneira, o GDPR aponta que o seu documento é pautado nos direitos fundamentais e visa proteger e garantir a privacidade, liberdade, segurança, justiça das pessoas, assim como promover o progresso econômico e social, além de garantir a segurança jurídica dos países: preâmbulo (1), (2), (13)[8]; art. 1º (2)[9].

Art. 3º 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, 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.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

O art. 3º da LGPD objetiva delimitar a abrangência do tratamento de dados no que concerne à sua territorialidade, destacando que se considera a lei aplicável aos dados coletados dentro do território nacional ou cujo objeto de transação – oferta de bens e serviços – tenha ocorrido dentro do território nacional; a mesma lógica vale para os titulares dos dados coletados, assim como foi previsto pelo Marco Civil da Internet, em seu art. 11, §§ 1º e 2º[10].

O GDPR pontua a questão da territorialidade no art. 3º, destacando que o regulamento se aplica ao tratamento de dados pessoais efetuados por controlador ou processador situados dentro do território da União, independentemente se o tratamento em si foi realizado dentro ou fora da União. O mesmo é válido para o tratamento realizado em relação às atividades mercadológicas – compra, venda de bens ou serviços – dos consumidores titulares da União. Portanto, ainda que o controle transacional não seja da União, o mero fato de os participantes da ação serem originários da União permite que o regulamento seja aplicado.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II – realizado para fins exclusivamente:

a) jornalísticos e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III – realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

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 nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá 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 nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

A delimitação da aplicabilidade da lei em relação aos tipos de dados que são considerados regulados pela LGPD demonstra que o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado. Da mesma forma, o uso doméstico com fins não econômicos não recebe a aplicação da lei, tendo em vista que um dos focos de ação do dispositivo é regular as atividades cujo objetivo seja a oferta ou o fornecimento de bens ou serviços.

Essa restrição do campo de alcance contribui para reduzir os impactos econômicos e sociais, visto que há elevados custos na implementação das exigências trazidas pela legislação de proteção de dados pessoais. Além disso, há sempre necessidade de equilibrar a proteção da privacidade (como um direito individual) e a proteção da segurança pública (como um direito coletivo), especialmente diante da obrigação de fortalecer o combate ao crime organizado, à fraude digital e ao terrorismo.

O GDPR, por sua vez, também limita a sua atuação, não abrangendo os dados pessoais relativos às pessoas jurídicas, as informações anônimas ou anonimizadas que garantam que o titular não possa ser identificado ou identificável e os dados pessoais de pessoas falecidas, conforme o preâmbulo (14), (26) e (27). É importante pontuar que a questão da anonimização dos dados ainda levanta muitos questionamentos, haja vista que os métodos de anonimização são considerados corruptíveis e passíveis de falhas[11].

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

I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

III – 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;

IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX – agentes de tratamento: o controlador e o operador;

X – 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;

XI – 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;

XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII – bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI – 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;

XVII – 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;

XVIII – 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; e

XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A especificação dos termos utilizados no contexto dos dados pessoais é particularmente importante e visa resolver os problemas de conceituação e até mesmo categorização que as informações coletadas sofriam. A partir da LGPD, passa a ficar claro e apontável o que é ou não dado pessoal, assim como todos os processos, as técnicas ou os procedimentos relativos ao tratamento de dados.

O GDPR reserva o art. 4º para pontuar as definições dos principais termos utilizados no documento. É notável como a lei brasileira se espelhou no modelo adotado pelo documento europeu. Apesar de alguns termos e expressões se diferenciarem, os papéis e as funções de cada sujeito ou processo são equivalentes tanto no documento brasileiro quanto no europeu. É exemplo disso a questão do controlador/processador do GDPR, que no LGPD ganharam o nome de controlador/operador, cujas ações, funções e responsabilidades são equivalentes, só se modificando a nomenclatura adotada. Importante destacar que no caso do Brasil o encarregado de dados (DPO) ficou com um termo bem abrangente de pessoa (podendo, então, ser tanto pessoa física como jurídica), e há ainda o entendimento de que, como seria uma função de comunicação, ela poderia ser assumida por um comitê (grupo de pessoas representando setores, áreas, sob uma liderança), adequando-se conforme o modelo de governança de cada instituição.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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

IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

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

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

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

VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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

A garantia da proteção dos direitos dos titulares dos dados pessoais é pautada na indicação de princípios relativos ao tratamento de dados pessoais, cuja ação deve respeitar os limites dos direitos fundamentais.

Da mesma maneira, o GDPR aponta a previsão de princípios norteadores do tratamento de dados pessoais no artigo 5º.

Capítulo II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

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, observadas as disposições do Capítulo IV desta Lei;

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, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (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; ou

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

§ 1º (Revogado.)

§ 2º (Revogado.)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º 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.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá 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 nesta Lei.

Outro ponto da LGPD que demonstra a influência do GDPR na criação do documento brasileiro diz respeito aos requisitos aplicados ao tratamento de dados pessoais. A LGPD destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares.

O artigo 5º do GDPR também comenta quais os princípios e limites que o tratamento de dados pessoais deve seguir, de maneira que a licitude, a lealdade, a transparência, a finalidade, o limite, a proporcionalidade, a exatidão, a integridade e a confidencialidade são algumas das principais características que o tratamento de dados deve seguir. Os artigos 12, 13 e 14 do regulamento europeu pontuam de maneira mais explícita os requisitos, limites e as regras para promoção da transparência das informações, das comunicações e exercício dos titulares dos dados.

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.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 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.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Um ponto de atenção bastante relevante é retratado pelo art. 8º, que é a questão do consentimento. Ao longo dos anos, a necessidade do consentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia. Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para a assegurar a liberdade e a privacidade.

Ao mesmo tempo, as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso, tendo em vista que o desenvolvimento econômico também deve ser garantido a esses sujeitos. Importante destacar que cabe à instituição que realiza o tratamento a capacidade de demonstrar que estava legítima (detinha o registro do consentimento ou se enquadrava nas hipóteses de exceção). Como já observado, considerando o cenário brasileiro de preocupação com segurança, houve um cuidado com a questão de trazer garantias de exceções de consentimento, por exemplo, na situação da proteção do crédito.

O GDPR também pontua a importância primordial do consentimento até mesmo para a garantia da licitude do tratamento de dados a ser realizado ou em realização, como explicitam os artigos 6º e 7º. Nesse mesmo sentido, o regulamento pontua o quão essencial é a identificação do consentimento, tendo em vista que o silêncio ou a omissão não são considerados formas de consentir. Da mesma maneira, o GDPR destaca a liberdade de escolha do titular ante o consentimento, de maneira que a sua recusa ou revogação não lhe pode trazer quaisquer prejuízos.

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:

I – finalidade específica do tratamento;

II – forma e duração do tratamento, observados os segredos comercial e industrial;

III – identificação do controlador;

IV – informações de contato do controlador;

V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º 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.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 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.

O art. 9º prende-se à questão da transparência das informações do tratamento de dados, apontando quais as características relativas ao livre acesso à informação. Nesse sentido, a clara exposição e o fácil acesso relativo à finalidade do tratamento, assim como sua forma, duração, além das informações acerca dos agentes que realizam o tratamento, são elementos essenciais. A gratuidade da consulta a essas informações também é uma garantia importante.

O GDPR também preza pela transparência das informações do tratamento de dados, de maneira que do consentimento do titular até a possibilidade de revogação de tal consentimento o agente tenha a função de oferecer informações claras e de fácil acesso, pontuando ainda que o "consentimento deve ser tão fácil de retirar quanto de dar", conforme o artigo 7º.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador; e

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º 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.

A finalidade apontada pelo controlador para a realização do tratamento de dados deve ser pautada em fundamentações claras e legítimas, e somente os dados real e estritamente necessários devem ser coletados com vistas à garantia do direito a proteção à privacidade do titular. Da mesma maneira, a autoridade nacional deve garantir a

emissão de relatórios relativos ao tratamento e seus impactos e deve respeitar as liberdades do controlador, como o segredo industrial e comercial.

O GDPR destaca essa questão no artigo 6º (1), d, e, f, (3), de maneira que impõe restrições à atuação tanto do sujeito que trata os dados como do Estado que requer a sua verificação/validação.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá 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, este último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (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; ou

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 desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 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.

§ 2º Nos casos de aplicação do disposto nas alíneas a e b do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

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

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I – a portabilidade de dados quando solicitada pelo titular; ou

II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

§ 5º É vedado às operadoras de planos privados de assistência à 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.

A importância do consentimento para a realização do tratamento de dados sensíveis é intrínseca à validade dessa ação, todavia há algumas situações em que tal consentimento pode ser relativizado (excetuado), como pontua o art. 11.

Essas situações são relacionadas ao cumprimento de obrigações legais por parte do controlador, à garantia da segurança do titular, à prevenção à fraude, à execução de políticas públicas, à proteção da vida/incolumidade física, assim como à tutela da saúde. Ainda que o tratamento de dados sensíveis seja realizado mediante a dispensa do consentimento, é obrigação do controlador publicizar essa situação.

Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa.

O GDPR explicita essa preocupação no artigo 9º, afirmando que o consentimento é essencial no tratamento de dados sensíveis, embora haja exceções cujos procedimentos devem respeitar com a mesma seriedade e garantia da segurança ao tratamento. O regulamento europeu ainda pontua que as informações sensíveis que foram tornadas públicas pelo próprio titular também podem ter seu consentimento dispensado.

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º 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.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º 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.

O art. 12 traz em seu texto um ponto de atenção a ser destacado, que dispõe que os dados anonimizados não são considerados dados pessoais. Tal apontamento da LGPD pode gerar margem a interpretação mais subjetiva e a certo grau de insegurança jurídica. Um estudo realizado por um grupo de pesquisadores do Media Lab do Instituto Tecnológico de Massachusetts (MIT) em 2014 apontou[12] que, a partir da criação de

alguns algoritmos matemáticos, é possível identificar uma pessoa baseando-se em seus hábitos de compra[13].

Sendo assim, é importante que o método escolhido pela instituição como processo de anonimização possa demonstrar que impossibilita a sua reversão para aquele que recepcionou o dado classificado como anonimizado, evitando riscos para uma eventual responsabilização futura, ainda mais em discussões em sede judicial de Juizado Especial, com debate de tema consumerista que não permite necessariamente a condução de perícia técnica adequada para o nível de complexidade que a matéria exige. Provavelmente será necessário evoluir para o uso de soluções certificadas para evitar discussões e incertezas na aplicação de soluções de anonimização.

O GDPR adota a mesma postura em seu regulamento, conforme pontua o preâmbulo (26): "Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação".

Art. 13. 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.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

O art. 13 pontua que a regulamentação dos dados não deve ser um impeditivo do incentivo e da produção científica na saúde pública, todavia os mesmos procedimentos de segurança da informação adotados por quaisquer outros institutos e finalidades devem ser observados.

Da mesma forma, as informações pessoais não devem ser publicizadas quando os resultados do estudo ou da pesquisa forem divulgados, haja vista que a privacidade e a

intimidade dos titulares devem ser preservadas. Nesse sentido, a adoção de procedimento de anonimização ou pseudoanonimização dos dados deve ser estimulada sempre que possível nesses casos, na busca da preservação da segurança dos dados pessoais em manuseio.

De maneira semelhante, o GDPR pontua que o tratamento de dados pessoais de interesse público, investigação científica ou histórica, assim como para fins estatísticos, está sujeito a garantias adequadas como a pseudoanonimização, que deve seguir o propósito de proteger os direitos e as liberdade dos titulares de dados, conforme o artigo 89 (1) a (4).

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

---

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 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.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º 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.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas 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.

Os dados relacionados a menores de idade estão classificados em uma categoria de dados especiais (pois exigem um tratamento diferenciado em termos de cuidados). As informações relativas a dados pessoais de crianças e adolescentes devem observar o consentimento de pelo menos um dos pais ou responsáveis legais.

Da mesma maneira, devem obedecer ao princípio da finalidade e transparência. Merece destaque a preocupação do regulamento em assegurar que o consentimento

recebido realmente adveio dos responsáveis/pais do menor. Isso porque o ambiente digital possibilita inúmeros meios de burlar os procedimentos de identificação; dessa forma, cabe aos controladores garantir que o consentimento é real e válido.

Ao mesmo tempo, nas situações em que é necessário o contato com os pais ou responsáveis da criança/adolescente, é possível realizar a coleta de dados independentemente de consentimento, porém esse dado deve ser utilizado somente dentro de seu propósito e não pode ser armazenado. Dessa forma, são garantidos o acesso ao dado e a proteção da informação coletada, assim como seu uso e propósito imediato.

O GDPR pontua as condições relativas à coleta de dados de crianças e adolescentes no artigo 8º, destacando a necessidade de proteção especial dos dados pessoais desses indivíduos. Um aspecto diferencial do regulamento europeu é o apontamento de que, no que concerne à oferta direta de serviços, é lícito o consentimento dado por parte de uma pessoa com pelo menos 16 anos, sendo que indivíduos com menos 16 anos devem ter o consentimento submetido aos pais ou responsáveis legais, e, dependendo do país, essa idade pode ser até de 13 anos (não inferior a 13). Ou seja, dependendo do país, pode o jovem dar o próprio consentimento a partir de 13 anos ou a partir de 16 anos (ou precisar do consentimento dos pais para tanto). Jovens com menos de 13 anos sempre precisarão do consentimento dos pais.

Seção IV
Do Término do Tratamento de Dados

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 conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Conforme dispõe a LGPD, um dos requisitos de validade do tratamento de dados é o limite de atuação do procedimento, e tal ideia é relativa tanto ao limite de informações a serem coletadas quanto à finitude do procedimento no tempo.

Isso quer dizer que o tratamento não deve ser realizado por tempo indeterminado. O término do tratamento de dados deve seguir alguns requisitos básicos, dos quais se destacam a verificação do alcance da finalidade do processo, o término do prazo

estimulado ao tratamento, a revogação do consentimento do titular e a determinação da autoridade nacional.

O GDPR pontua no preâmbulo (39) a importância da limitação e imposição de prazos ao tratamento de dados, de maneira que tais aspectos têm vinculação direta com a finalidade do procedimento. Uma diferença do documento em relação à lei brasileira diz respeito à vinculação dos prazos à necessidade do processo, sendo que a limitação de tempo obriga o controlador a realizar o apagamento ou a revisão dos dados coletados. O artigo 13 (2) a recomenda que prazos sejam determinados de acordo com a finalidade do tratamento.

Art. 16. 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:

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 nesta Lei; ou

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

Um dos aspectos vinculados ao tratamento dos dados é que, assim que o seu procedimento chega ao fim, os dados coletados devem ser apagados, salvo nas condições pontuadas no art. 16.

Claramente, a intenção das instituições é preservar a manutenção da base de dados pessoais, evitando as hipóteses de eliminação sempre que possível, visto que há um alto valor na preservação da informação. O descarte pode e deve ocorrer, já que é um direito, mas será observado se recairá alguma previsão de justificativa legal de retenção que permita a manutenção do dado por um prazo até a sua eliminação definitiva (se esta vier a ocorrer).

Grande parte do trabalho recairá sobre a análise da possibilidade de apagamento ou retenção. O direito ao apagamento (direito ao esquecimento) e o direito à portabilidade dos dados pessoais são os dois direitos com maior impacto sobre a operação de gestão do ciclo de vida dos dados pessoais nas organizações. E, devido à necessidade de continuar com a informação, surge a oportunidade da aplicação da anonimização como último recurso viável.

No preâmbulo (39) do regulamento europeu GDPR pontua-se: "A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica". Os arts. 16 e 17 também indicam a possibilidade de retificação das

informações em tratamento, assim como o seu apagamento a partir da ausência da finalidade, revogação do consentimento do titular, tratamento realizado de maneira ilícita e obrigações jurídicas.

Capítulo III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Um dos objetivos da LGPD é assegurar a proteção e o livre desenvolvimento da personalidade da pessoa natural. É possível relacionar essa garantia da pessoa natural à titularidade de seus dados à inviolabilidade de sua vida privada, pontuada por meio do art. 5º, X[14], da Constituição Federal e do art. 21 do Código Civil[15], haja vista que as informações pessoais da pessoa fazem parte de sua privacidade, ainda mais no contexto digital.

Art. 18. 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 o disposto nesta 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 no art. 16 desta 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 do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I – comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º 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, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

§ 7º 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.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

O direito dos titulares dos dados de livre acesso às informações relativas ao tratamento é reiterado de maneira enumerativa no art. 18, cuja preocupação é garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade.

Da mesma forma, a liberdade de revogar o consentimento e requerer o apagamento dos dados é reafirmada como reflexo da liberdade de escolha da pessoa, de forma que – assim como o consentimento – a revogação deve ser expressa. Novamente, o texto da lei reitera que os dados anonimizados não recebem o direito ao mesmo tratamento dos dados pessoais.

A questão da portabilidade de dados pessoais é por certo um dos direitos ainda com maior margem de discusão em termos de executividade do rol de direitos do art. 18. Foi muito acertada a atualização da LGPD ao deixar claro que há o limite do segredo comercial e industrial e há que se diferenciar o que são dados pessoais do titular (fornecidos por ele) do que é o aprendizado oriundo da relação de clientela, que inclusive compõe o fundo de comércio das empresas e é, portanto, um ativo empresarial.

O GDPR pontua nos artigos 12, 13, 14, 15, 22 e 34 os direitos e as garantias dos titulares de dados. Nos artigos 16 e 17, o regulamento europeu menciona o direito de retificação e o direito a ser esquecido, uma garantia com expansão já apontada por Rolf Weber em seus estudos acerca dos impactos da tecnologia na compreensão e expansão dos direitos humanos[16].

Também merece destaque a importância, trazida pelo § 6º, de se limitar a comunicação aos demais agentes de tratamento com os quais tenha realizado compartilhamento de dados, exceto se esta comunicação for comprovadamente impossível ou implicar esforço desproporcional.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I – em formato simplificado, imediatamente; ou

II – 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, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para esse fim; ou

II – sob forma impressa.

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

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

A garantia da facilidade do acesso e de claros dispositivos de comunicação entre o titular dos dados e os agentes do tratamento de dados deve ser observada, de maneira que o princípio da transparência e a boa-fé estejam presentes ao longo do processo.

O GDPR pontua esse aspecto nos artigos 12 (2), 14 e 15, dispondo que o procedimento deve ser facilitado, rápido e transparente.

Art. 20. O titular dos dados tem direito a solicitar a 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.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Este é um artigo mais polêmico, visto que envolve as situações de uso de métodos automatizados de análise de dados, como ocorre, por exemplo, em processos de seleção (análise de volume de informações de perfis de candidatos) e também na concessão de crédito (na análise de score). Claramente, devido ao volume, o uso de robôs é uma forma de melhoria da análise (aplicação de métodos de analytics com big data).

Sendo assim, apesar de a lei prever que o titular pode requerer que seja revisto, muito provavelmente será aplicada a mesma fórmula de análise (algoritmo), mas esclarecido por uma pessoa o processo utilizado para alcançar o resultado. Há que se ter um

cuidado, pois há a liberdade de contratar entre as partes e há o segredo de negócios, direitos esses também presentes e protegidos no ordenamento jurídico vigente nacional e também nos demais países.

O GDPR reserva os artigos 21 e 22 para garantir o direito à oposição do titular a decisões relacionadas ao tratamento de seus dados, inclusive em relação à definição de perfis que produzam efeitos na vida do titular.

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Como explicitado, o consentimento do titular ao tratamento de seus dados pessoais não deve lhe onerar de forma alguma, por isso as informações coletadas não devem ser utilizadas em prejuízo do titular.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Assim como pontua o art. 5º, XXXIV[17], da Constituição Federal, todos devem ter assegurado o seu direito de acesso à justiça e defesa de seus direitos.

O GDPR pontua no artigo 13 (2) d que o responsável pelo tratamento deve garantir ao titular o direito de apresentar reclamação junto a uma autoridade de controle.

Capítulo IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

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

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;

II – (VETADO); e

III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e

IV – (VETADO).

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei n. 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei n. 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade pública e o interesse público[18] para a realização de tratamento de dados.

Diferentemente das empresas privadas, as instituições públicas poderão seguir os prazos e procedimentos apontados pelas Leis n. 9.507, de 12 de novembro de 1997 (Lei d o Habeas Data), n. 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) e n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). No caso das empresas públicas, o art. 173 da Constituição[19] lhes garante tratamento igual ao reservado às empresas privadas.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

O art. 24 pontua a base constitucional do tratamento diferenciado das empresas públicas. O que se quis foi dar uma diferenciação sobre o tratamento de dados pessoais nas instituições públicas, já se vislumbrando situações futuras relacionadas inclusive ao atendimento de outras legislações, como a Lei de Acesso à Informação.

Art. 25. Os dados deverão 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.

As técnicas de manutenção dos dados em tratamento são especificadas no caso das instituições públicas, de maneira que a sua estruturação e organização devem visar à execução das políticas públicas e à prestação de serviços.

Art. 26. 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, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I – em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II – (VETADO);

III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;

IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

V – 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.

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Cabe ao Poder Público a garantia de que o uso compartilhado de dados segue os propósitos especiais que concernem à execução das políticas públicas e que, ao mesmo tempo, a ponderação entre a necessidade da publicidade das informações disponíveis ao acesso garante que os direitos dos titulares sejam respeitados. Da mesma forma, a transferência dos dados pessoais às entidades privadas é vetada, com exceção das situações em que os dados são acessíveis publicamente ou em que a execução de um serviço ou medida o exigir.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I – nas hipóteses de dispensa de consentimento previstas nesta Lei;

II – nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III – nas exceções constantes do § 1º do art. 26 desta Lei.

Art. 28. (VETADO).

Aqui se quis permitir que haja a interconexão das bases de dados públicas e privadas que ocorrem atualmente, já justificadas nas hipóteses de exceção de consentimento da legislação de proteção de dados pessoais, como para a proteção do crédito, proteção da saúde, da segurança pública.

Art. 29. A autoridade nacional poderá 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 e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

A autoridade nacional – a ser criada – responsável pela fiscalização do tratamento de dados pessoais possui caráter autônomo, em virtude disso pode aplicar seus

procedimentos fiscalizantes também ao Poder Público.

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Conforme as necessidades do cumprimento do seu exercício, é possível a expansão das normas da LGPD para garantir que as atividades de comunicação e uso compartilhado de dados sejam efetivas e seguras.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Os órgãos públicos estão sujeitos às medidas administrativas específicas; em virtude disso, cabe à autoridade nacional garantir que medidas cabíveis e proporcionais sejam adotadas quando da violação do tratamento de dados pessoais nos órgãos públicos.

Conforme aponta Celso Antônio Bandeira de Mello[20], os órgãos públicos estão no âmbito do regime administrativo, logo estão sujeitos às normas e aos parâmetros deste, e consequentemente respondem administrativa e não judicialmente, daí a necessidade de tratamento específico dentro dos limites das normas administrativas.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Este artigo prevê a necessidade de as instituições públicas preverem o impacto de privacidade no âmbito da administração pública, especialmente em setores como da Saúde, o que por certo terá um grande impacto e exigirá muitas implementações e uma política pública para adequação e conformidade do setor público à nova regulamentação.

O que se quer evitar é ter uma legislação que seja eficaz apenas no setor privado e não consiga ser implementada no setor público.

Capítulo V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I – para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II – quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III – 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;

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

V – quando a autoridade nacional autorizar a transferência;

VI – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII – quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII – 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; ou

IX – quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Seguindo os parâmetros lançados pelo GDPR, a adoção da lei brasileira traz a previsão – inevitável – dos fluxos transfronteiriços de dados pessoais, de maneira que os países passíveis desse tipo de transação devem oferecer a garantia da proteção dos dados pessoais em mesmo grau que a LGPD prevê.

Isso significa que o Brasil segue o movimento europeu de padronização internacional do fluxo de dados, assim como de proteção dessas informações, de maneira a garantir que o desenvolvimento tecnológico e econômico possa continuar seu acelerado e complexo processo, sem que com isso direitos e garantias fundamentais sejam relativizados ou violados.

O preâmbulo (5), (6), (116) e o artigo 4 (23) pontuam que a proteção de dados não deve prejudicar o desenvolvimento econômico e tecnológico no contexto global, mas que a promoção da garantia de proteção aos tratamentos dos dados deve ser eficaz e real, conforme reitera o artigo 56 (1) ao destacar que a autoridade de controle tem competência de ação no tratamento de dados transfronteiriços.

Nesse contexto, é importante pontuar que, ainda que o ambiente digital aponte-se

como naturalmente internacional, a soberania das nações deve ser respeitada. A atuação dos órgãos/cortes internacionais pode ser aumentada e expandida com essa nova realidade.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará 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 nesta Lei;

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; e

VI – outras circunstâncias específicas relativas à transferência.

Ainda na busca da criação de um padrão internacional de proteção aos dados pessoais, a imposição de métodos avaliativos da autoridade nacional em face dos países estrangeiros e organismos internacionais mostra-se necessária.

O GDPR pontua em seu artigo 44 a necessidade de adequação das transferências além das fronteiras da União aos padrões e às garantias instituídas pelo regulamento.

Art. 35. 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, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Verifica-se que a imposição de uma padronização do modelo de cláusulas contratuais que devem ser observadas pelas instituições, quer seja em suas relações corporativas globais, quer seja em seus códigos internos e certificados, demonstra que as novas regulamentações visam assegurar que os preceitos legais e os princípios, direitos, garantias e deveres trazidos pela lei sejam observados e pactuados em toda a cadeia de

valor do negócio, ou seja, que as regras fiquem claras e sejam disseminadas também por meio da governança dos contratos entre as partes. Esta é uma estratégia normativa para gerar caráter vinculante propondo clausulado padronizado já a partir da própria legislação. Isso tem sido observado na técnica de redação inclusive de órgãos regulatórios, como o Banco Central, por exemplo com a Resolução 4.658/2018 sobre contratação de serviços na nuvem, que também traz artigos específicos que tratam sobre cláusulas contratuais obrigatórias e vinculantes[21].

A mesma ideia é explorada pelo GDPR no artigo 47, que destaca que cabe à Autoridade Supervisora aprovar regras/padrões corporativos que devem ser específicos quanto à sua estrutura e aos contatos de grupo empresarial, de forma que as transferências de dados serão feitas com base nos princípios propostos pelo regulamento e deverão ter caráter juridicamente vinculante.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

Ainda tomando por base o princípio da transparência, que é o principal princípio da regulamentação de proteção de dados pessoais, quaisquer mudanças relacionadas às garantias fornecidas deverão ser comunicadas à autoridade nacional competente.

Capítulo VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Para o controle e a transparência das ações e do cumprimento dos propósitos do tratamento de dados, cabe ao controlador e ao operador documentar as operações realizadas durante o processo de tratamento de dados pessoais.

Os artigos 24 (1) e 30 do GDPR apontam que, além da necessidade de documentação dos processos, a revisão e a atualização dos procedimentos adotados devem ser observadas de acordo com as necessidades que se apresentem.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de

regulamento, observados os segredos comercial e industrial.

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

A força de ação dos órgãos reguladores é bastante pontuada também no GDPR, de modo que o regulamento europeu – nos artigos 24, 25 e 42 – dispõe que a proteção de dados deve ser realizada desde a concepção do tratamento (by design) e que as certificações e o cumprimento dos códigos de conduta são medidas de verificação de que o controlador está cumprindo com suas obrigações.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Este artigo traz a vinculação entre controlador e operador, visto que a regulamentação de proteção de dados pessoais tem o condão de estabelecer uma responsabilidade solidária do controlador para com o operador a partir do contrato entre eles, considerando que quem detém o consentimento do titular é o controlador e, portanto, continua a ser o que fica responsável pelo que ocorre no ciclo de vida dos dados pessoais na gestão e governança do negócio.

Art. 40. A autoridade nacional poderá 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.

Devido ao poder de fiscalização das autoridades nacionais, é relevante pontuar que a instituição de padrões de ação por esses órgãos facilita o cumprimento das normas. Este artigo tem implementação pendente da criação da ANPD.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações da autoridade nacional e adotar providências;

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

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

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO).

A imputação da necessidade de um encarregado principal por parte do controlador em face das atividades e ações relativas ao tratamento de dados busca garantir que as informações fiquem centralizadas e que o controlador se certifique de que a aplicação das normas receberá efetiva validação. Esse encarregado pode ser qualquer tipo de pessoa, seja ela física ou jurídica, seja ela contratada interna ou terceirizada, e a lei não trouxe qualquer requisito de formação específica como ocorre com o Regulamento GDPR.

O GDPR pontua no artigo 27 a necessidade de indicação de um representante na União quando o controlador ou o processador não estiverem estabelecidos dentro da União. E os artigos 37 a 39 descrevem as situações em que o responsável pelo tratamento e o subcontratante devem designar um encarregado para a proteção de dados. Em verdade, todas as atividades do encarregado (pela LGPD) ou do DPO (pelo GDPR) demonstram muito mais um serviço do que a atividade de uma única pessoa.

A experiência tem mostrado que as habilidades necessárias para execução de todas as atividades do Encarregado (DPO) são híbridas, ou seja, exigem tanto conhecimento da própria legislação como também sobre atendimento e relacionamento com titulares (que podem ter dois tipos de perfis principais: o de consumidor final e o de funcionário, em que os canais de diálogos normalmente são atendidos ou por uma Ouvidoria ou SAC ou então por um RH ou Canal de Denúncias). Além disso, também deve ter conhecimentos técnicos, especialmente de ciber segurança e se possível de governança de dados. Logo, poderíamos agrupar as ações do Encarregado em pelo menos 4 grupos distintos: a) atendimento de Titulares (para dentro e para fora); b) relacionamento com Autoridades (Legal Affairs); c) orientação sobre Proteção de Dados Pessoais (suporte para implementação e manutenção da conformidade e campanhas educativas); e d) resposta a incidentes (contenção, mitigação e liçoes aprendidas).

Analisando todo esse escopo, podemos identificar alguns perfis muito afins a essa função, como do Compliance, da Auditoria, do Jurídico, do Security Officer, da área de Riscos. Por isso, muitas instituições têm constituído um comitê e têm também contato com alguma consultoria externa (DPO as a service ou on demand).

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. 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.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I – 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, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter 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.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Assim como no GDPR, artigos 24, 25 e 26, a lei brasileira traz em sua previsão o caráter solidário da responsabilização do controlador e do operador.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

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

III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Mediante a apresentação de provas suficientes que isentem de responsabilidade os agentes do tratamento de dados (que são o controlador e/ou o operador), a mesma isenção de responsabilidade lhe deverá ser garantida.

Art. 44. 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, entre as quais:

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.

Parágrafo único. 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 desta Lei, der causa ao dano.

Este artigo traz as condições de demonstração da ilicitude do tratamento de dados pessoais, assim como ocorre com o artigo 6º do GDPR, que pontua as condições de

licitude do tratamento de dados pessoais.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Dependendo do tipo de violação de direitos do titular serão aplicadas penalidades conforme já previsto na legislação consumerista (Código de Defesa do Consumidor) e/ou pela regra geral do Código Civil Brasileiro (arts. 186, 187 e 927[22]).

Capítulo VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

No âmbito da promoção da segurança da informação, os processos e procedimentos devem assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, ao longo de todo o ciclo de vida do dado.

Dessa maneira, para que o tratamento de dados pessoais seja assegurado de maneira eficiente e suficiente, cabe aos agentes responsáveis por esse tratamento a adoção de medidas de segurança técnicas adequadas e específicas para esse tipo de procedimento.

No artigo 5º do GDPR, são descritos os princípios relacionados ao processamento de dados pessoais desde a sua criação até a minimização dos dados, instituindo-se até um ciclo de vida dos dados. O artigo 32 reitera a necessidade de adoção de medidas técnicas e organizacionais adequadas e que assegurem um nível de segurança satisfatório ao risco.

Art. 47. 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 nesta Lei em relação aos dados pessoais, mesmo após o seu

término.

Devido à responsabilidade solidária das ações imputadas durante o processo de tratamento de dados, a segurança dos procedimentos deve ser assegurada por todos os agentes, sendo fundamental a preservação da trilha de auditoria para fins de apuração.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

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; e

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

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I – ampla divulgação do fato em meios de comunicação; e

II – medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será 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.

Como reflexo da boa-fé, transparência e responsabilização dos atos dos agentes, a comunicação pelo controlador da ocorrência de incidentes de segurança durante o processo de tratamento de dados é essencial.

O GDPR destaca a importância dessa ação no artigo 33 e ainda aponta que a notificação deve ocorrer sem demora injustificada e sempre que possível em até 72 horas após ter conhecimento do ocorrido.

Art. 49. 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 nesta Lei e às demais normas regulamentares.

Qualquer procedimento, sistema ou equipamento necessário durante o tratamento de dados deve seguir os mesmos requisitos de segurança mínimos exigidos pela lei; de outra maneira, ficaria impossível garantir a plena eficácia das medidas adotadas.

O artigo 32 do GDPR aponta as providências mínimas que devem ser adotadas para garantir a segurança do tratamento.

Seção II
Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam 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.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão 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.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados 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, poderá:

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; e

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 desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

A instituição de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção dos dados pessoas sejam efetivados.

Conforme os artigos 40, 41, 42 e 43, as medidas de boas práticas envolvem um sistema amplo e complexo de relações e previsões como instituição de mecanismos de educação e prevenção em face da segurança da informação, atuação de organismos de certificação e treinamento de equipes junto à atuação das autoridades supervisoras.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

O estímulo da adoção de mecanismos de controle interno e instituição de padrões técnicos de garantia de segurança à informação também deve ser realizado pela autoridade competente. A implementação adequada deste artigo está pendente da criação da ANPD.

Capítulo VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

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 – 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 na Lei n. 8.078, de 11 de setembro de 1990, e em legislação específica.

§ 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 n. 8.112, de 11 de dezembro de 1990, na Lei n. 8.429, de 2 de junho de 1992, e na Lei n. 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 n. 7.347, de 24 de julho de 1985, e a Lei n. 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.

A imputação de sanções administrativas faz com que os entes responsáveis pelo tratamento de dados pessoais atentem-se à garantia da segurança das informações que estão utilizando.

Dessa forma, observa-se que a LGPD busca estimular a aplicação de seus dispositivos

em caráter preventivo.

As sanções vão desde advertências até a imputação de multa simples – que pode chegar a 2% do faturamento, cujo valor fica limitado a um total de R$ 50 milhões – e diária, além da suspensão das atividades relativas ao banco de dados.

O artigo 84 do GDPR também aponta que cabe aos Estados--Membros o estabelecimento de regras para a aplicação de sanções, que devem ser efetivas, proporcionais e dissuasivas.

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.

Cabe à autoridade nacional responsável a análise do caso e proporcional aplicação das medidas de sanção.

A aplicação deste artigo está pendente da constituição da ANPD, apesar de a vigilância e a fiscalização da lei poderem ser realizadas pelo Ministério Público até que a Autoridade seja constituída.

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.

Observando o princípio constitucional da proporcionalidade[23], a imputação das sanções deve sempre observar a proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal no momento do exercício de suas funções. Por certo, as novas leis que tratam de matéria relacionada à proteção de direitos no âmbito da transformação digital das instituições possuem um altíssimo impacto nos modelos de negócios. Desse modo, uma forma de fazer com que sejam observadas é prever penalidades bem altas. No entanto, por serem regras que se aplicam a qualquer perfil de empresa, seja ela uma startup, seja uma grande multinacional, privada ou instituição pública, de qualquer setor da economia, há que se considerar uma dosagem na aplicação

das punições, sob pena de inviabilizar a pequena empresa ou mesmo os projetos de maior inovação que tendem a assumir mais riscos operacionais. Além disso, o fiscalizador da nova regulamentação também deve levar em consideração alguns critérios que possam agravar ou amenizar a aplicação da sanção, visto que a possibilidade de ocorrência de uma violação de dados a partir de uma violação de segurança é altíssima no contexto digital atual, até por uma grande carência de investimentos no combate ao crime organizado que opera na Internet e que já se utiliza de recursos sofisticados para atacar indivíduos e instituições de todo e qualquer porte. Portanto, mesmo que um controlador ou operador esteja seguindo todas as melhores práticas e aplicando todos os controles, ainda assim, pode haver a infração e o incidente de vazamento de dados pessoais. Logo, por tudo isso, no caso da regulação das infrações envolvendo o tratamento de dados, tal postulação constitucional permanece válida. Importante destacar que o princípio da proporcionalidade ou razoabilidade é amplamente apontado pela doutrina e jurisprudência nacional como uma derivação do art. 5º, V, da Constituição Federal, sendo muito vinculado ao exercício do direito administrativo. Como a regulação dos dados pessoais será efetuada por uma agência nacional, a aplicação das sanções deve seguir os mesmos nortes e princípios do direito administrativo.

A regulamentação europeia (GDPR) também postula tal critério no artigo 83, em que são apontadas as condições gerais para a imputação de sanções administrativas, com destaque para o artigo 83 (1): "Cada autoridade de controlo assegura que a aplicação de coimas nos termos do presente artigo [...] em cada caso individual, efetiva, proporcionada e dissuasiva".

Capítulo IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei n. 13.853, de 2019)

§ 1º 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. (Incluído pela Lei n. 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei n. 13.853, de 2019)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei n. 13.853, de 2019)

I – Conselho Diretor, órgão máximo de direção; (Incluído pela Lei n. 13.853, de 2019)

II – Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei n. 13.853, de 2019)

III – Corregedoria; (Incluído pela Lei n. 13.853, de 2019)

IV – Ouvidoria; (Incluído pela Lei n. 13.853, de 2019)

V – órgão de assessoramento jurídico próprio; e (Incluído pela Lei n. 13.853, de 2019)

VI – unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei n. 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea f do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores – DAS, no mínimo, de nível 5. (Incluído pela Lei n. 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei n. 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei n. 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei n. 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-E. 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. (Incluído pela Lei n. 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei n. 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei n. 12.813, de 16 de maio de 2013. (Incluído pela Lei n. 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei n. 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei n. 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei n. 13.853, de 2019)

I – zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei n. 13.853, de 2019)

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 desta Lei; (Incluído pela Lei n. 13.853, de 2019)

III – elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

V – apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei n. 13.853, de 2019)

VI – promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei n. 13.853, de 2019)

VII – promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

IX – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei n. 13.853, de 2019)

X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

XII – elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei n. 13.853, de 2019)

XV – arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei n. 13.853, de 2019)

XVI – realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei n. 13.853, de 2019)

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 o previsto no Decreto-lei n. 4.657, de 4 de setembro de 1942; (Incluído pela Lei n. 13.853, de 2019)

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 a esta Lei; (Incluído pela Lei n. 13.853, de 2019)

XIX – garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n. 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei n. 13.853, de 2019)

XX – deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei n. 13.853, de 2019)

XXI – comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei n. 13.853, de 2019)

XXII – comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei n. 13.853, de 2019)

XXIII – articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei n. 13.853, de 2019)

XXIV – implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei n. 13.853, de 2019)

§ 1º 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, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei n. 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei n. 13.853, de 2019)

§ 3º 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 desta Lei. (Incluído pela Lei n. 13.853, de 2019)

§ 4º A ANPD manterá 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. (Incluído pela Lei n. 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei n. 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma

agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei n. 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei n. 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei n. 13.853, de 2019)

I – as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei n. 13.853, de 2019)

II – as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei n. 13.853, de 2019)

III – os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei n. 13.853, de 2019)

IV – os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei n. 13.853, de 2019)

V – (VETADO); (Incluído pela Lei n. 13.853, de 2019)

VI – os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei n. 13.853, de 2019)

VII – o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei n. 13.853, de 2019)

Art. 56. (VETADO).

Art. 57. (VETADO).

A Autoridade Nacional de Proteção de Dados Pessoais foi constituida com a Lei n. 13.853/2019 de maneira a que a LGPD possa ter o mesmo nível de adequação do Regulamento GDPR.

Seção II
Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

---

Art. 58. (VETADO).

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: (Incluído pela Lei n. 13.853, de 2019)

I – 5 (cinco) do Poder Executivo federal; (Incluído pela Lei n. 13.853, de 2019)

II – 1 (um) do Senado Federal; (Incluído pela Lei n. 13.853, de 2019)

III – 1 (um) da Câmara dos Deputados; (Incluído pela Lei n. 13.853, de 2019)

IV – 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei n. 13.853, de 2019)

V – 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei n. 13.853, de 2019)

VI – 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei n. 13.853, de 2019)

VII – 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei n. 13.853, de 2019)

VIII – 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei n. 13.853, de 2019)

IX – 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei n. 13.853, de 2019)

X – 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei n. 13.853, de 2019)

XI – 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei n. 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei n. 13.853, de 2019)

§ 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. (Incluído pela Lei n. 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei n. 13.853, de 2019)

I – serão indicados na forma de regulamento; (Incluído pela Lei n. 13.853, de 2019)

II – não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei n. 13.853, de 2019)

III – terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei n. 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei n. 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei n. 13.853, de 2019)

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; (Incluído pela Lei n. 13.853, de 2019)

II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei n. 13.853, de 2019)

III – sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei n. 13.853, de 2019)

IV – elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei n. 13.853, de 2019)

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

Art. 59. (VETADO).

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade foi constituído pela Lei n. 13.853/2019. É muito importante que os membros do Conselho sejam experts no tema de proteção de dados pessoais e também sobre a sua aplicação nos diferentes setores da sociedade, visto que há muitas particularidades que precisarão ser consideradas na implementação da legislação e para seu contínuo aperfeiçoamento. Além disso, o Brasil precisa se manter competitivo e atraente para os investidores estrangeiros, bem como promover um ambiente que fomente inovação tecnológica.

Quanto mais heterogêneo puder ser sua composição, melhor, incluindo especialistas técnicos, jurídicos, econômicos, cientistas de dados e comunicadores.

Capítulo X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

"Art. 7º .....

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16 .....

II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Devido ao fato de a LGPD trazer em seu corpo legislativo algumas novidades conceituais e mesmo procedimentais em relação ao tratamento de dados pessoais, é necessário atualizar o Marco Civil da Internet nas partes que concernem às atualizações.

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, 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 LGPD previu o procedimento para que haja alcance e aplicação extraterritorial e tenha efeitos internacionais.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei n. 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei n. 10.861, de 14 de abril de 2004 .

A aplicação deste artigo está sujeita à constituição da ANPD.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

A aplicação deste artigo está sujeita à constituição da ANPD.

Art. 64. Os direitos e 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.

É muito importante que a LGPD seja aplicada de forma especial no tocante à matéria de proteção de dados pessoais, não excluindo a aplicação das demais leis de forma complementar ou subsidiária, sejam nacionais ou tratados internacionais, que devem ser interpretados de maneira harmoniosa e integradora.

Art. 65. Esta Lei entra em vigor:

I – dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e

II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

O prazo previsto pela LGPD é considerado curto em termos de realidade brasileira, mesmo com a prorrogação ocorrida que ampliou de 18 meses para 24 meses, ficando o prazo equivalente ao do GDPR, que também adotou o prazo de dois anos – 25 de maio de 2016 a 25 de maio de 2018 – para que empresas, governo e sociedade civil tomassem conhecimento e implementassem medidas necessárias ao cumprimento de suas disposições. Esta é uma legislação de alto impacto econômico e social e que eleva o custo Brasil, exigindo uma política pública para ser implementada.

REFERÊNCIAS

AGÊNCIA BRASIL. Legislação de proteção de dados já é realidade em outros países. 2018. Disponível em: <http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>. Acesso: em abr. 2019.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 7. ed. São Paulo: Saraiva, 2018.

BOURBON, Maria João. Parlamento aprova nova lei nacional de proteção de dados. Expresso, 2019. Disponível em: <https://expresso.pt/economia/2019-06-14-Parlamento-aprova-nova-lei-nacional-de-protecao-de-dados>. Acesso em: jun. 2019.

BRASIL. Comissão mista destinada a emitir parecer sobre a Medida Provisória n. 869, de 28 de dezembro de 2018. Poder Executivo, 2019.

BRASIL. Redação Final da Medida Provisória n. 869-B, de 2018 – Projeto de Lei de Conversão n. 7, de 2019. Câmara dos Deputados, 2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1756651>. Acesso em: maio 2019.

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Poder Executivo, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm>. Acesso em: maio 2019.

BRASIL. SENADO. 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/10/02/congresso-conclui-analise-de-vetos-sobre-protecao-de-dadosHYPERLINK "https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1756651">. Acesso em: out. 2019.

BRASIL. [CONGRESSO NACIONAL] Veto n. 24/2019. 2019. Disponível em: <https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445HYPERLINK "https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1756651">. Acesso em: out. 2019.

BRASIL [Casa Civil]. Constituição da República Federativa do Brasil de 1988. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: ago. 2018.

_____. Decreto n. 7.962, de 15 de março de 2013. Brasília, 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em: ago. 2018.

_____. Lei n. 8.078, de 11 de setembro de 1990. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm>. Acesso em: ago. 2018.

_____. Lei n. 10.406, de 10 de janeiro de 2002. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: ago. 2018.

_____. Lei n. 12.965, de 23 de abril de 2014. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: ago. 2018.

CONSTANTIN, Lucian. Relatório constata mais de 59 mil notificações de violação do GDPR. Computer World, 2019. Disponível em: <https://computerworld.com.br/2019/02/10/relatorio-constata-mais-de-59-mil-notificacoes-de-violacao-do-gdpr/>. Acesso em: abr. 2019.

CRIADO, Miguel Ángel. Quatro compras com o cartão bastam para identificar qualquer pessoa. El País, jan. 2015. Disponível em: <https://brasil.elpais.com/brasil/2015/01/29/ciencia/1422520042_066660.html>. Acesso em: ago. 2018.

DLA PIPER. Data Protection Laws of the World – full handbook. 2019. Disponível em: <www.dlapiperdataprotection.com>. Acesso em: abr. 2019.

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO. Autoridade Nacional de Proteção de Dados – ANPD. Disponível em: <https://www.fiesp.com.br/agenda/seminario-autoridade-nacional-de-dados-pessoais-anpd/>. Acesso em: abr. 2019.

FRANÇA, Philip Gil. Interesse público, um conhecido conceito "não determinado". Direito do Estado, n. 249, 2016. Disponível em: <http://www.direitodoestado.com.br/colunistas/phillip-gil-franca/interesse-publico-um-conhecido-conceito-nao-indeterminado>. Acesso em: ago. 2018.

GIANNELLINI, Luiz Fernando Salles. As inovações da Lei Geral de Proteção de Dados. Estadão, 2018. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/as-inovacoes-da-lei-geral-de-protecao-de-dados/>. Acesso em: abr. 2019.

GUIDI, Felipe. Modelos regulatórios para a proteção de dados pessoais. Instituto de Tecnologia e Sociedade do Rio, 2017. Disponível em: < https://itsrio.org/wp-

content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: abr. 2019.

GUIMARÃES, António. Passado um ano, Portugal finalmente aprova lei de proteção de dados. 4gnews, 2019. Disponível em: <https://4gnews.pt/passado-um-ano-portugal-finalmente-aprova-lei-de-protecao-de-dados/>. Acesso em: jun. 2019.

IRLANDA. Data Protection Commission. Disponível em: <https://www.data protection.ie/>. Acesso em: ago. 2019.

LEMOS, Ronaldo et al. GDPR: a nova legislação de proteção de dados pessoais da Europa. Jota, maio, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Acesso: em ago. 2018.

MELLO, Celso Antônio Bandeira de. Curso de direito administrativo. 33. ed. São Paulo: Malheiros Editores, 2018.

OHM, Paul. Broken Promisses of Privacy: responding to the surprising failure of anonymization. UCLA Law Review, p. 1701-76, 2010. Disponível em: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1016&context=hightechevents>. Acesso em: ago. 2018.

REANI, Valéria. Como a GDPR nos ensina o compliance de medidas protetivas da privacidade. Conjur, jun. 2018. Disponível em: <https://www.conjur.com.br/2018-jun-15/valeria-reani-gdpr-compliancede-medidas-protetivas>. Acesso em: ago. 2018.

SERVIÇO NACIONAL DE PROCESSAMENTO DE DADOS. Congresso aprecia veto sobre revisão de decisões automatizadas. 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/congresso-aprecia-veto-ao-artigo-20-da-lgpd>. Acesso em: out. 2019.

SOLERE, Bertrand de. A Lei Geral de Proteção de Dados (LGPD). Solere, 2018. Disponível em: <https://solere-avocats.fr/blog/loi-protection-donnees-personnelles/>. Acesso em: abr. 2019.

TI INSIDE ONLINE. Mudanças na LGPD podem gerar insegurança jurídica no mercado, afirma advogada. TI Inside Online, 2019. Disponível em: <https://tiinside.com.br/tiinside/26/09/2019/mudancas-na-lgpd-podem-gerar-inseguranca-juridica-no-mercado-afirma-patricia-peck/>. Acesso em: out. 2019.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-

content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: ago. 2018.

WEBER, Rolf. The right to be forgotten: more than a Pandora's Box? JIPITEC, 2011. Disponível em: <https://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf>. Acesso em: ago. 2018.

1 Alterado pela MP n. 869/2018, que ampliou em mais 6 meses, totalizando 24 meses, e com última redação dada pela Lei n. 13.853/2019: "Art. 65. Esta Lei entra em vigor: I – dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos".

2 Disponível em: <https://iapp.org/resources/article/data-protection-authority/>. Acesso em: 4 jan. 2020.

3 Disponível em: < https://ico.org.uk/>. Acesso em: 4 jan. 2020.

4 "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor."

5 "Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: [...] VII – utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor."

6 "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; [...] III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; [...]."

"Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil."

7 "Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I – construir uma sociedade livre, justa e solidária; II – garantir o desenvolvimento nacional;"

"Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: [...] II – prevalência dos direitos humanos;"

"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo--se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]."

"Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social: [...] XXVII – proteção em face da automação, na forma da lei; [...]."

"Art. 219. O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal. Parágrafo único. O Estado estimulará a formação e o fortalecimento da inovação nas empresas, bem como nos demais entes, públicos ou privados, a constituição e a manutenção de parques e polos tecnológicos e de demais ambientes promotores da inovação, a atuação dos inventores independentes e a criação, absorção, difusão e transferência de tecnologia."

8 "(1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. [...].

9 (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares. [...]

(13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros. [...]."

"Artigo 1º Objeto e objetivos [...] 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais."

10 "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil."

11 Diversos cientistas têm apontando que os processos de anonimização são repletos de problemas e que os dados, uma vez considerados anônimos, podem ser reidentificados de maneira relativamente simples. Paul Ohm realizou um interessante estudo sobre o tema em 2010, chamado de "Broken Promisses of Privacy: responding to the surprising failure of anonimization", no qual dá alguns exemplos dos problemas relativos à anonimização de dados pessoais.

12 Informações de Miguel Ángel Criado, do El País, por meio da matéria: "Quatro compras com o cartão bastam para identificar qualquer pessoa", publicada em 30 de janeiro de 2015, no site do jornal.

13 Tal identificação foi possível a partir da utilização de uma média de quatro transações aliados ao dia e à loja em que o consumo foi realizado; isso levanta ainda mais uma polêmica acerca da anonimização e a sua validade real: dados anonimizados isoladamente, quando agrupados, podem gerar a reversão do procedimento de anonimização?

14 "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

15 "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

16 Para mais aprofundamento acerca do direito de ser esquecido, consultar o texto "The Right to Be Forgotten: More than a Pandora's Box?", de Rolf Weber.

17 "Art. 5º [...] XXXIV – são a todos assegurados, independentemente do pagamento de taxas: a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal."

18 Nas palavras de Philip Gil França, "O interesse público pode ser compreendido como produto das forças de uma dada sociedade (jurídicas, políticas, econômicas, religiosas, dentre outras) concretizadas em certo momento e espaço que exprime o melhor valor de desenvolvimento de um maior número possível de pessoas dessa mesma sociedade. Então, alcançar esse produto, considerando as forças de uma sociedade, é o dever primordial do Estado, conforme o art. 3º da CF. Assim exposto, conclui-se, neste primeiro momento, que interesse público possui relevância jurídica quando é passível

19 de determinação e concretização – do contrário, trata-se de discurso vazio e sem força jurídica vinculante. Fato que, por si, afasta a ideia de conceito jurídico indeterminado, muitas vezes vinculado à concepção de interesse público.

Assim definido, urge raciocinar que a atuação estatal – em destaque, da Administração Pública – precisa estar intimamente conectada com a realização e a promoção de um interesse público concreto, ou concretizável". Ver "Interesse público, um conhecido conceito 'não indeterminado'", de Philip França.

"Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei. § 1º A lei estabelecerá o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre: I – sua função social e formas de fiscalização pelo Estado e pela sociedade; II – a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários; III – licitação e contratação de obras, serviços, compras e alienações, observados os princípios da administração pública; IV – a constituição e o funcionamento dos conselhos de administração e fiscal, com a participação de acionistas minoritários; V – os mandatos, a avaliação de desempenho e a responsabilidade dos administradores. § 2º As empresas públicas e as sociedades de economia mista não poderão gozar de privilégios fiscais não extensivos às do setor privado. § 3º A lei regulamentará as relações da empresa pública com o Estado e a sociedade. § 4º A lei reprimirá o abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros. § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular."

20 Ver o Curso de direito administrativo, de Celso Antônio Bandeira de Mello.

21 Resolução Bacen 4.658/2018: "Art. 17. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever: I – a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; II – a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I; III – a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes; IV – a obrigatoriedade, em caso de extinção do contrato, de: a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante; e b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea a e a confirmação da integridade e da disponibilidade dos dados recebidos; V – o acesso da instituição contratante a: a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III; b) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas d e e; e c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12,

inciso II, alínea f ; VI – a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição; VII – a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações; VIII – a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e IX – a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor. Parágrafo único. O contrato mencionado no caput deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil: I – a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada; e II – a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que: a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante".

22 "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

[...]

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo."

23 Luís Roberto Barroso (2018, p. 293-294) explica o desenvolvimento do princípio da proporcionalidade afirmando que o "princípio da razoabilidade ou da proporcionalidade, no Brasil, tal como desenvolvido por parte da doutrina e, também, pela jurisprudência, inclusive do Supremo Tribunal Federal, é o produto da conjugação de ideias vindas de dois sistemas diversos: (i) da doutrina do devido processo legal substantivo do direito norte-americano, onde a matéria foi primeiramente tratada; e (ii) do princípio da proporcionalidade do direito alemão". O Supremo Tribunal Federal reitera essa posição, conforme a decisão proferida no RE 374.981-RS (Informativo n. 381 STF): "O princípio da proporcionalidade – que extrai a sua justificação dogmática de diversas cláusulas constitucionais, notadamente aquela que veicula a garantia do substantive due process of law – acha-se vocacionado a inibir e a neutralizar os abusos do poder público no exercício de suas funções, qualificando-se como parâmetro de aferição da própria constitucionalidade material dos atos estatais. A norma estatal, que não veicula qualquer conteúdo de irrazoabilidade, presta obséquio ao postulado da proporcionalidade, ajustando-se à cláusula que consagra, em sua dimensão material, o princípio do substantive due process of law (art. 5º, LIV). Essa cláusula tutelar, ao inibir os efeitos prejudiciais decorrentes do abuso de poder legislativo, enfatiza a noção de que a prerrogativa de legislar outorgada ao Estado constitui atribuição jurídica essencialmente limitada, ainda que o momento de abstrata instauração normativa possa repousar em juízo meramente político ou discricionário do legislador".