

Lei Geral de Proteção de Dados e GDPR:

histórico, análise
e impactos.

**BAP
TISTA
LUZ**

ADVOGADOS



B/
LUZ

/ Autores

Renato Leite Monteiro

Maria Cecília Oliveira Gomes

Adriane Loureiro Novaes

Gabriela Moribe

Dennys Eduardo Gonsales Camara

Pamela Michelena De Marchi Gherini



/ Prefácio

Até alguns anos atrás, o tema de proteção de dados era marginal às atividades das empresas. Havia a preocupação, evidente, mas não existiam os riscos e exposições que hoje se multiplicam, assim como as regulações nacionais que trazem penalidades cada vez mais severas.

Parte da nossa cultura sempre foi pensar à frente do nosso tempo, tendo a inovação como parte da nossa missão institucional. Além de trabalhar em temas de tecnologia e proteção de dados há mais de dez anos, fomos um dos primeiros escritórios full service a estruturar um time de Data Protection com conhecimento e experiência reconhecida no mercado nacional e internacional, muito antes das principais legislações sobre o tema, como a GDPR e, mais recentemente, a LGPD.

Hoje, o escritório conta com um time de especialistas já preparados a assessorar empresas nacionais e internacionais nos processos mais complexos de conformidade com a lei, assim como questões consultivas, contratuais e litigiosas de diferentes setores da economia, tais como aviação, logística, saúde, financeiro, pagamentos, seguros, varejo, publicidade digital, e-commerce, plataformas online, mobilidade urbana, data brokers, entre outros.

Este estudo é uma pequena demonstração de outra grande característica do nosso escritório. Sempre fomos a favor da democratização do conhecimento e amplo acesso à informação. Várias das nossas iniciativas corroboram essa nossa forma de ver o mundo: **(i) os inúmeros estudos compartilhados amplamente através de nosso site;** **(ii)** Estruturação de uma equipe de **Pesquisa & Desenvolvimento** composta por advogados e estagiários focados em produção de conteúdo jurídico relevante para dentro e fora do escritório; **(iii)** a criação do **Privacy Hub**, iniciativa colaborativa visando conscientizar sobre a importância de proteção de dados para o mercado; **(iv)** o **Espaço Startup**, que permite que empreendedores de todos os tamanhos possam ter acesso, totalmente gratuito, a documentos, contratos, estudos e conteúdo que normalmente seria cobrado, por vezes inviabilizando o seu acesso; e **(v)** as várias associações, do mundo inteiro, com as quais contribuimos ativamente para fomentar o **desenvolvimento de conhecimento**.

Com isso em mente, apresentamos este estudo elaborado pelas áreas de Proteção de Dados e de Pesquisa & Desenvolvimento. Nosso objetivo é contribuir: para o entendimento sobre o desenvolvimento da proteção sobre dados pessoais, elucidando sobre a Lei Geral de Proteção de Dados brasileira, sua relação com a legislação europeia e também as recentes modificações sofridas pela recém-publicada Medida Provisória.

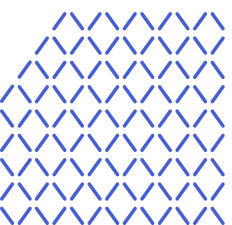
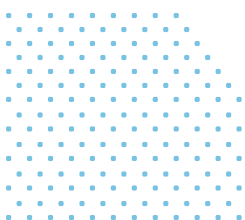
Baptista Luz Advogados

/Resumo

Com a aprovação da Lei Geral de Dados no Brasil (“LGPD”), Lei nº 13.709, de 14 de agosto de 2018, o presente artigo se propõe a descrever o processo e o resultado da criação de uma estrutura normativa que busca harmonizar e ampliar o direito a proteção de dados pessoais no contexto regulatório brasileiro.

Para isso, analisaremos como o direito a proteção de dados pessoais surgiu no mundo e a maneira como gradativamente foi sendo desenvolvida na União Europeia e na América Latina. Nosso escopo de análise se dará entre a LGPD e o Regulamento da União Europeia nº 2016/679, popularmente conhecido como *General Data Protection Regulation* (“GDPR”), que entrou em vigor em 2018.

Buscamos comparar a normatização europeia com a brasileira e compreender o contexto histórico de 2010 a 2018, que culminou com a aprovação da LGPD. Assim, pretendemos entender como esta lei dialogará com as normas setoriais de proteção de dados já existentes no país. Abordaremos também os principais pilares e pontos relevantes da LGPD, a fim de esclarecer a sua importância e seus impactos. Por fim, considerando que também em 2018 entrou em vigor a GDPR, abordaremos de forma superficial alguns pontos de contato entre ambas as normas.



Sumário

06

/ Introdução

- 1.1. Os primeiros passos da Proteção de Dados no mundo
- 1.2. Da consulta pública à sanção presidencial (2010-2018)
- 1.3. Objetivo

13

/ Proteção de Dados: a construção de um direito

- 2.1. Oito anos de debate resultou em uma boa lei?
- 2.2. Como ficam as Leis Setoriais sobre Proteção de Dados no Brasil?

17

/ O Escopo da Lei Geral de Proteção de Dados no Brasil

- 3.1. Dados Pessoais e Categoria de Dados
- 3.2. Bases Legais
- 3.3. Anonimização x Pseudonimização
- 3.4. Compartilhamento de dados
- 3.5. Hipóteses de Exclusão de Dados
- 3.6. Direitos dos Titulares
- 3.7. Transferência internacional de dados
- 3.8. Comunicação de incidente
- 3.9. Padrões de segurança da informação
- 3.10. Sanções
- 3.11. Autoridade Nacional de Proteção de Dados
- 3.12. Relatório de Impacto à Proteção de Dados

40

/ GDPR x LGPD: o que muda com a nova lei brasileira?

- 4.1. Bases legais
- 4.2. Data Protection Officer
- 4.3. Consentimento
- 4.4. Prazo de retenção

/ Conclusão

/ introdução

1.1 Os primeiros passos da proteção de dados no mundo

Ainda que a privacidade seja um direito universal, tratado inclusive no artigo 12 da Declaração Universal dos Direitos Humanos¹, o fato é que a privacidade do indivíduo é um direito relacionado a sua esfera pessoal. A ideia é proteger a vida privada, destacando-a do contato com a esfera pública.

1. ASSEMBLEIA GERAL DA ONU. Resolução 217 A (III). Paris, 10 de dezembro de 1948. Declaração Universal dos Direitos Humanos.

Nesse sentido, após o crescimento e desenvolvimento do cenário tecnológico computacional na década de 60, em 1970 foi instituída a primeira lei estadual de proteção de dados da história, no estado alemão de Hesse, a chamada *Hessisches Datenschutzgesetz*. O Ato de Proteção de Dados de Hesse² foi criado tendo a vista a necessidade de tratar com maior cuidado as informações pessoais de indivíduos armazenadas em meios eletrônicos. A lei, assim, foi pioneira ao tratar da coleta e tratamento de dados de indivíduos, ainda que não o fizesse de maneira objetiva e segmentada.

Alguns anos mais tarde, em 1973, foi aprovada na Suécia a primeira lei nacional de proteção de dados da história, a *Sw. Datalagen* ou o Ato de Dados Sueco³. Assim como a lei de Hesse, a lei sueca tratava da proteção dos dados de maneira genérica, não trazendo, por exemplo, em que situações a coleta de dados poderia ou não ocorrer, dispondo apenas que essa coleta deveria se dar com autorização da agência governamental competente⁴. A lei também não trazia princípios gerais do tratamento de dados pessoais, algo recorrente nas leis modernas sobre o assunto. No entanto, a lei inovou ao trazer o tema da proteção de dados dos cidadãos para a agenda pública de governo.

Seguindo esse movimento, seis anos depois, em 1979 diversas outras nações europeias como França, Alemanha e Dinamarca, já tinham suas próprias legislações de proteção de dados. Estas leis, ainda que muito importantes, eram genéricas, assim como os textos sueco e alemão. Cabe mencionar também que Portugal, Espanha e Áustria chegaram inclusive a considerar a privacidade como um direito fundamental em suas Constituições – o que ilustra muito bem a importância dada por essas nações ao tema,

2. ALEMANHA. *Hessisches Datenschutzgesetz*, de 7 jan. 1999. Disponível em: < <http://www.ess-koeln.de/dokumente/160/151010084004Hessen.pdf> >. Acesso em 29 set. 2018.

3. ÖMAN, Sören. *Implementing Data Protection in Law*. Disponível em: < <http://www.scandinavianlaw.se/pdf/47-18.pdf> >. Acesso em: 18 ago. 2018.

4. *Ibidem*

ainda no final dos anos 70⁵.

No ano de 1981, o Conselho da Europa aprovou a Convenção 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal⁶, por considerar “desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado”. Esse teria sido o primeiro marco legal transnacional sobre proteção de dados. A convenção passou por um recente processo de atualização que culminou com a sua versão modernizada, conhecida como Convenção 108+⁷.

Passadas duas décadas, e com a crescente evolução do cenário tecnológico, as leis de proteção de dados alcançaram mais espaço e começaram a ter um formato mais parecido com o das leis que temos hoje, framework que se consolidou quando a União Europeia, 25 anos depois da Lei de Hesse, promulgou a Diretiva 95/46/CE⁸, em 1995. A norma foi um marco no campo da proteção de dados, pois dispunha sobre o tratamento de dados e direitos dos usuários em todos os países membros do bloco, colocando todos sob a mesma legislação. A Diretiva, além de

5. RUDGARD, Sian. *Origins and Historical Context of Data Protection Law*. Disponível em: <https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf >. Acesso em: 18 ago. 2018.

6. Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 10 jan.1981. Disponível em: <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> >. Acesso em: 21 nov. 2018

7. Council of Europe. *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. 18 maio. 2018. Disponível em: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>. Acesso em: 21 nov. 2018.

8. PARLAMENTO EUROPEU. *Directiva 95/46/CE*. de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao o tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT> >. Acesso em: 18 ago. 2018.

estabelecer como deveria ser feita a coleta e tratamento dos dados, traz os princípios que devem ser seguidos em tais operações, dentre os quais destacam-se o da licitude do tratamento, da limitação dos propósitos, da adequação, da necessidade e da transparência, que visam frear possíveis abusos por parte dos responsáveis pelas mesmas. A Diretiva 95/46/CE vigorou até maio de 2018, quando foi substituída pelo Regulamento nº 2016/679, de 27 de abril de 2016, popularmente conhecido como General Data Protection Regulation (“GDPR”), a nova lei geral de proteção de dados da União Europeia⁹.

A GDPR é enxergada, por muitos, como a mais completa legislação de proteção de dados do mundo¹⁰. Trata-se de uma evolução da Diretiva 95/46/EC, fruto de um longo processo democrático¹¹, seu escopo de aplicação inclui não apenas dados de pessoais naturais localizados na União Europeia, mas todo o fluxo de dados existente nos países membros e nos países ao redor do mundo que possuem pontos de contato com o mercado europeu¹². Os principais avanços da nova lei se dão na

ampliação de direitos dos usuários¹³ e na maior responsabilização das organizações e empresas que realizam o processamento de dados¹⁴.

Saindo do âmbito europeu e ingressando no cenário da América do Sul, verifica-se que dos 12 países pertencentes ao continente, apenas Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai e Guiana Francesa possuem leis gerais para a proteção dos dados dos titulares. O Brasil passou a fazer parte deste rol com a aprovação da Lei nº 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados (“LGPD”). Ainda dentro do contexto sul-americano, vale ressaltar que o Equador¹⁵, Bolívia¹⁶, Venezuela¹⁷ e Guiana¹⁸ possuem, também, leis setoriais sobre proteção de dados, restando o Suriname como único país do continente que ainda não possui leis sobre o tema.

9. Para uma visão mais completa do histórico de leis de proteção de dados acesse: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

10. ALBRECHT, Jan Philipp. How the GDPR Will Change the World. Disponível em: < https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf > Acesso em: 18 ago. 2018.

11. EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. Disponível em: < https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en >. Acesso em: 18 ago. 2018.

12. EUROPEAN COMMISSION. Who does the data protection law apply to? Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en >. Acesso em: 19 ago. 2018.

13. Segundo a LGPD, os direitos dos titulares de dados possuem fundamento em direitos fundamentais de liberdade, intimidade e privacidade, previstos em nossa Constituição e, por isso, sua aplicação se dará sempre na maior medida possível. Assim, em termos gerais e que serão aprofundados ao longo deste artigo, são direitos dos titulares de dados, em relação aos dados de quem forem titulares: conhecimento da existência de tratamento dos dados; possibilidade de acesso e exclusão de dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; portabilidade, mediante requisição expressa; informação das entidades públicas e privadas com as quais o controlador compartilhou os dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento, a qualquer tempo, para o tratamento de dados.

14. INFORMATION COMMISSIONER'S OFFICE. Guide to the *General Data Protection Regulation* (GDPR). Disponível em: < <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> >. Acesso em: 19 ago. 2018.

15. OEA. Desarrollos Normativos por País – Equador. Disponível em: < http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_ecuador.asp >. Acesso em: 19 ago. 2018.

16. RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación- Bolívia. Disponível em < <http://www.redipd.org/legislacion/bolivia-ides-idphp.php> >. Acesso em: 12 nov. 2018.

17. RED IBEROAMERICANA DE PROTECCION DE DATOS. Legislación- Venezuela. Disponível em < <http://www.redipd.org/legislacion/venezuela-ides-idphp.php> >. Acesso em: 12 nov. 2018.

18. A Guiana possui leis setoriais de proteção de dados como o Statistics Act 1965 e o Access to Information Act 2011.

Na Argentina, a *Ley de Protección de los Datos Personales*¹⁹, ou Lei de Proteção de Dados Pessoais, de outubro de 2000, traz disposições e princípios gerais relativos à proteção de dados. Ela traz em seu corpo os direitos dos titulares dos dados, a responsabilidade das organizações que realizam o tratamento dos mesmos, sanções aplicáveis e medidas de proteção. Cabe mencionar que a Argentina e o Uruguai são hoje os únicos países sul-americanos considerados com níveis adequados de proteção de dados pela União Europeia²⁰. Como veremos adiante, essa classificação é importantíssima no contexto da GDPR. Países com tais “níveis adequados” podem mais facilmente realizar a transferência internacional de dados para países sob a jurisdição da GDPR. A Lei Argentina passa, atualmente, por um processo de modernização que irá aproximá-la com o regulamento europeu²¹.

No Chile, há a *Ley de Protección de Datos de Carácter Personal*²², ou Lei de Proteção de Dados de Carácter Pessoal, de agosto de 1999. O dispositivo garante direitos aos “titulares” dos dados tratados (as pessoas a quem os dados se referem), como o direito à correção e exclusão dos dados, assim como obrigações, como a limitação do uso dos dados coletados

.....
19. ARGENTINA. Ley N° 25.326, de 4 de outubro de 2000. Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Disponível em: <<http://www.oas.org/es/sla/ddi/docs/A7%20ley%20protecci%C3%B3n%20de%20datos.pdf>>. Acesso em: 19 ago. 2018.

20. EUROPEAN COMMISSION. Adequacy of the protection of personal data in non-EU countries. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>. Acesso em: 19 ago. 2018.

21. FERNANDEZ, Diego. Argentina’s new Bill on Personal Data Protection. Disponível em: <<https://iapp.org/news/a/argentinanew-bill-on-personal-data-protection/>>. Acesso em: 19 ago. 2018

22. CHILE. Ley n° 19628, de 28 de agosto de 1999. Protección de datos de carácter personal. Disponível em: <<http://www.oas.org/es/sla/ddi/docs/CH3%20Ley%2019628%20Proteccion%20de%20Datos%20de%20Car%C3%A1cter%20Personal.pdf>>. Acesso em: 19 ago. 2018.

ao propósito informado pelo responsável por seu tratamento.

Na Colômbia, vigora a *Ley Estatutaria n° 1581*²³ de 2012, pela qual se ditam as disposições gerais de proteção de dados pessoais neste país. Esta traz informações detalhadas acerca dos princípios que regem o tratamento dos dados, direitos dos titulares e responsabilidade das organizações responsáveis por esse tratamento.

No Peru, desde julho de 2011, vigora a *Ley de Protección de Datos Personales*²⁴. A lei peruana, assim como, as outras leis mencionadas, traz os princípios do tratamento dos dados pessoais, os direitos do titular, as obrigações do titular e do responsável pelo tratamento, o funcionamento dos bancos de dados e de uma autoridade de caráter nacional para a proteção de dados, assim como sanções administrativas a serem aplicadas ao responsável pelo tratamento.

No Uruguai entrou em vigor em 2011 a *Ley de Protección de Datos Personales y Acción de Habeas Data*²⁵. A lei que coloca o Uruguai como um dos únicos países sul-americanos a dispor de níveis adequados de proteção de dados de acordo com a Comissão Europeia²⁶,

.....
23. COLOMBIA. Ley Estatutaria N° 1581, de 17 de Outubro de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Disponível em: <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>>. Acesso em: 19 ago. 2018.

24. PERU. Ley n° 29733, de 03 de julho de 2011. *Ley de protección de datos personales*. Disponível em: <<http://www.oas.org/es/sla/ddi/docs/P6%20Ley%2029733%20de%20protecci%C3%B3n%20de%20datos%20personales.pdf>>. Acesso em: 19 ago. 2018.

25. URUGUAI. Ley n° 18.331, de 18 de agosto de 2008, Protección de datos personales y acción de “habeas data”. Disponível em: <<http://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20y%20Acci%C3%B3n%20de%20Habeas%20Data.pdf>>. Acesso em 20 ago. 2018.

26. EUROPEAN COMMISSION. Adequacy of the protection of personal data in non-EU countries. How the EU determines if a non-EU has an adequate level of protection. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>. Acesso em 28 set. de 2018.

além da Argentina, institui os princípios que regem o tratamento de dados e direitos e deveres de titulares e responsáveis pelo tratamento, além de estabelecer a criação de um órgão de controle governamental.

O Paraguai não tem uma lei geral de proteção de dados, como a dos outros países já listados, contando apenas com um dispositivo genérico sobre o tema. A *Ley n° 1.682 que Reglamenta la Información de Carácter Privado*²⁷, aborda de maneira ampla quais dados podem ser tratados e como além de estabelecer sanções para as organizações que descumpram tais disposições.

1.2. Da consulta pública à sanção presidencial (2010-2018)

Constatando a necessidade de ser construída uma agenda de debates sobre proteção de dados no Brasil, o Ministério da Justiça redigiu um Anteprojeto de Lei de Proteção de Dados (“APLPD”) e o ofereceu para consulta e comentários públicos no ano de 2010, quando foi criado um blog sobre proteção de dados e disponibilizado uma Consulta Pública sobre o tema, ambos hospedados no site “culturadigital.br”²⁸.

A consulta, que teve duração de 4 meses, recebeu comentários de diferentes setores da sociedade, formando assim um contingente multissetorial de contribuições. Vale ressaltar que, à época, este anteprojeto foi bastante associado à discussão pública acerca do Marco Civil da Internet, naquele momento ainda em processo de debate, recebendo

27. PARAGUAI. *Ley n° 1682*, de 16 de janeiro de 2001. Que reglamenta la información de carácter privado. Acesso em: < http://www.redipd.org/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf>. Acesso em: 20 ago. 2018.

28. Link para acesso ao site: <http://culturadigital.br/dados-pessoais/blog/2010/12/15/marco-normativo-de-privacidade-e-protecao-de-dados-pessoais-esta-em-debate-participe/>

algumas vezes, por esse motivo, o nome de “Marco Legal da Proteção de Dados”²⁹. Com os primeiros comentários ao APLPD, foi feito um esboço do que viria a se tornar o futuro texto da LGPD, 8 anos mais tarde.

Dois anos depois dessa primeira consulta pública, em 13 de junho de 2012, o Deputado Milton Monti propôs na Câmara dos Deputados o Projeto de Lei n° 4060 de 2012³⁰ (“PL 4060/12”), que dispunha sobre o tratamento de dados pessoais e dava outras providências, tendo como fonte primária de inspiração a própria consulta pública promovida pelo Ministério da Justiça.

O PL 4060/12 que foi protocolado na Câmara sem muito alarde, só teve andamento em 2013³¹, quando o analista de sistemas Edward Snowden denunciou uma série de irregularidades e práticas de vigilância em escala global promovidas pela Agência Nacional de Segurança (“NSA”), órgão vinculado ao governo norte americano³². A repercussão do caso foi enorme, e envolvia tanto vigilância em massa de usuários das redes quanto a chefes de estado de outros países – fato este que, inclusive, levou o Brasil a se pronunciar internacionalmente sobre o tema³³. Diante desse cenário, e sendo o PL 4060/12 o único sobre proteção de dados à época existente no País, acabou sendo pautado para debate

29. CULTURA DIGITAL. Diretrizes para a Discussão sobre o Marco Normativo de Privacidade e Proteção de Dados. Disponível em: < <http://culturadigital.br/dadospessoais/diretrizes-e-terminos-de-uso/>>. Acesso em: 20 ago. 2018.

30. BRASIL. Câmara dos Deputados. Projeto de Lei n° 4060 de 2012. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>>. Acesso em: 20 ago. 2018.

31. Ibidem

32. GIDDA, Mirren. Edward Snowden and the NSA files – timeline. *The Guardian*. 21 aug. 2013. Disponível em: < <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>>. Acesso em: 20 ago. 2018.

33. NAKAGAWA, Fernando; GUIMARÃES, Mariana. Imprensa internacional destaca ‘duro ataque’ de Dilma à espionagem dos EUA. *O Estado de São Paulo*. 24 set. 2013. Disponível em: <<https://politica.estadao.com.br/noticias/geral,imprensa-internacional-destaca-duro-ataque-de-dilma-a-espionagem-dos-eua,1078297>>. Acesso em: 20 ago. 2018.

pela Comissão Parlamentar de Inquérito da Espionagem no Senado Federal³⁴.

Na Comissão, foram promovidas audiências públicas sobre o tema³⁵, indicando que essa era uma das formas de promover a privacidade e a proteção de dados dos cidadãos, assim como uma maneira de evitar práticas de vigilância estatal praticadas por outros países.

Passado o ano de 2013, o tema de proteção de dados acabou não avançando de maneira significativa. A retomada da pauta ocorreu em 2015, quando o Ministério da Justiça promoveu a segunda consulta pública sobre o anteprojeto da lei de proteção de dados, também na plataforma da “culturadigital.br”³⁶.

Nesta segunda consulta, houve um contingente muito maior de contribuições e sugestões de alteração na redação do texto pelos diferentes setores da sociedade³⁷. A partir dessas recomendações, o Ministério da Justiça, próximo ao término do primeiro mandato da presidenta Dilma Rousseff, protocolaram o Projeto de Lei, que recebeu então o número 5276/16 (“PL 5276/16”).

Por possuir um texto mais completo, o PL 5276/16³⁸ acabou avançando mais rapidamente que os demais. Essa completude se deu pelo volume de audiências públicas realizadas para ouvir e debater o tema com representantes de todos os setores da sociedade brasileira, bem como de atores internacionais convidados para expor sobre o tema.

Impulsionado pela entrada em vigor da GDPR no dia 25 de maio de 2018³⁹, a Câmara e o Senado decidiram unir forças para que o texto do PL 5276/16, considerado o mais completo fosse apresentado como texto substitutivo ao PL 4060/12. Este, no caso, tinha prioridade de tramitação na Câmara por ter sido proposto 4 anos antes do PL 5276/16. Uma vez apensados, a nova versão foi colocada em pauta no plenário da Câmara dos Deputados no dia 29 de maio de 2018 e foi aprovado em 20 minutos por unanimidade⁴⁰. Após a aprovação do texto na Câmara, seguiu para o Senado Federal e lá recebeu identificação de Projeto de Lei da Câmara 53 de 2018 (“PLC 53/2018”)⁴¹.

No dia 03 de julho de 2018, o texto foi colocado em pauta na Comissão de Assuntos

34. BRASIL. Senado Federal. Disponível em: <<https://legis.senado.leg.br/comissoes/comissao;jsessionid=779DDBC-421C9E4637D209B7050309322?0&codcol=1682>>. Acesso em 4 jan. 2018.

35. BRASIL. Câmara dos Deputados. Projeto de Lei nº 4060 de 2012. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>>. Acesso em: 20 ago. 2018.

36. BRASIL, Emanuelle. Consulta pública será base para projeto de lei sobre proteção de dados pessoais. Câmara dos Deputados. 28 jan. 2015. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html>>. Acesso em: 20 ago. 2018.

37. MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. Jota. 14 jul. 2018. Disponível em: <<https://www.jota.info/opiniao-e-analise/columnas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>>. Acesso em: 20 ago. 2018.

38. BRASSCOM - ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES. Contribuições à Comissão Especial – Dados Pessoais da Câmara dos Deputados sobre a Lei de Tratamento e Proteção de Dados Pessoais. Jun. 2017. Disponível em: <<http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/Brasscom.pdf>>. Acesso em: 20 ago. 2018.

39. GOMES, Helton Simões. Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda. G1. 25 maio. 2018. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>>. Acesso em: 20 ago. 2018.

40. MENDES, Laura Schertel; DONEDA, Danilo. Lei de proteção de dados não pode morrer na praia. FOLHA. Disponível em: <<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>>. Acesso em: 24 ago. 2018.

41. BRASIL. Câmara dos Deputados. Projeto de Lei da Câmara nº 53, de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>>. Acesso em: 24 ago. 2018.

Econômicos (“CAE”) do Senado Federal, recebendo a relatoria do Senador Ricardo Ferraço, então relator do PLS 330/2013, projeto de lei geral que tramitava em paralelo no Senado Federal⁴². Com alguns pedidos de emenda com poucas alterações substanciais ao texto, foi considerado em boas condições para ser colocado em pauta para votação. Na mesma sessão, foi aprovado e recebeu requerimento de urgência para ser incluído na pauta do plenário do Senado Federal⁴³. Em 10 de julho de 2018, após forte pressão da sociedade civil e de outros setores, o PLC foi pautado no plenário do Senado Federal, onde foi votado e aprovado por unanimidade⁴⁴. Após isso, foi encaminhado para sanção presidencial, que se deu em 14 de agosto de 2018, com alguns vetos⁴⁵, principalmente no que se refere aos artigos 55 a 59 que constituíam e organizavam a Autoridade Nacional de Proteção de Dados (“ANPD”) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, sob a justificativa de que havia vício de iniciativa, ou seja, a entidade não poderia ser criada por uma lei de iniciativa do poder legislativo, e sim teria que ser criada por iniciativa normativa oriunda do poder executivo.

Por fim, em 27 de dezembro de 2018, foi editada a Medida Provisória nº 869 (“MP nº 869/18”), publicada no Diário Oficial da União em 28 de dezembro de 2018, que promoveu alterações no texto sancionado e também criou a ANPD. Medidas Provisórias

.....
42. BRASIL. Senado Federal. Projeto de Lei do Senado nº 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>>. Acesso em: 24 ago. 2018.

43. BRASIL. Senado Federal. Senadores aprovam urgência para proposta que muda tributação de aplicativos de transporte. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2018/05/23/senadores-aprovam-urgencia-para-proposta-que-muda-tributacao-de-aplicativos-de-transporte>>. Acesso em: 24 ago. 2018.

44. MENDES, Laura Schertel; DONEDA, Danilo. Lei de proteção de dados não pode morrer na praia. FOLHA. Disponível em: <<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilo-doneda-lei-de-protacao-de-dados-nao-pode-morrer-na-praia.shtml>>. Acesso em: 24 ago. 2018.

45.

têm aplicação imediata, mas dependem de aprovação do Congresso Nacional para transformação definitiva em lei e posterior sanção presidencial caso seu conteúdo seja alterado, o que será melhor desenvolvido adiante.

Essa construção histórica das leis de proteção de dados no mundo, especificamente no continente europeu e sul-americano, entre 1970 e 2018, demonstra alguns pontos importantes. O primeiro é a trajetória do desenvolvimento de um direito específico para a proteção de dados dos titulares, abrangendo meios online e offline, e o segundo demonstra o volume de leis já existentes, bem como o fato de a primeira lei ter sido aprovada em 1970 na Alemanha, evidenciando os quase 50 anos de atraso legislativo sobre o tema em solo brasileiro.

Após 48 anos da existência da primeira lei de proteção de dados no mundo, o Brasil passa a ter a sua lei geral de proteção de dados. Com a aprovação da LGPD, há forte expectativa de uma promoção maior de direitos e garantias para os cidadãos, no meio online e offline, de forma a, espera-se, resguardar direitos individuais e fomentar a inovação por meio do estabelecimento de regras claras, harmônicas e transparentes.

1.3. Objetivo

Para descrever o processo e o resultado da criação de uma estrutura normativa no contexto brasileiro, vamos analisar como a LGPD dialoga com as normas setoriais de proteção de dados já existentes no país. Abordaremos também os principais pilares e pontos relevantes da LGPD, a fim de esclarecer a sua importância e no que ela gera impacto. Por fim, considerando que também em 2018 entrou em vigor a GDPR, abordaremos de forma superficial alguns pontos de contato entre ambas as normas.

/Proteção de Dados: a construção de um direito

2.1. Oito anos de debate resultou em uma boa lei?

Os 8 anos que separam a publicação da primeira consulta pública e a aprovação da LGPD foram marcados por intensos debates, os quais contaram com a participação de membros dos mais diversos setores da sociedade. A preocupação em aprimorar a lei pode ser observada diante do fato de que as discussões para o desenvolvimento da redação dos textos dos PLs 4060/12 e 5276/16 contaram com 2 consultas públicas e 13 audiências públicas⁴⁶. Durante o mesmo período tramitava um outro Projeto de Lei no Senado, o PLS 330/13. Este contou com apenas 2 audiências públicas e acabou sendo arquivado posteriormente⁴⁷.

46. BRASIL. Câmara dos Deputados. PL 4060/12 - Tratamento e Proteção de Dados Pessoais – Reuniões Anteriores. Disponível em: <<http://www2.camara.leg.br/atividadelegislativa/comissoes/comissoes-temporarias/especiais/55aleislatura/pl-4060-12-tratamento-e-protecao-de-dadospessoais>>. Acesso em 23 jul. 2018.

47. BRASIL. Senado. Projeto de Lei do Senado nº 330, de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>>. Acesso em: 24 ago. 2018.

Esses anos de debates e construção legislativa demonstram que todo esse percurso foi um grande processo de amadurecimento sobre a matéria de proteção de dados no Brasil⁴⁸. As audiências públicas desempenharam um papel importante nesse cenário. Tais eventos contaram com a participação de acadêmicos, representantes do terceiro setor, iniciativa privada, governo e até mesmo representantes da União Europeia, os quais foram convidados para falar sobre suas experiências no processo legislativo que culminou com a aprovação da GDPR. A presença de tais representantes tornou possível que os parlamentares que eram responsáveis pelos projetos de lei em questão os conduzissem munidos de riquíssima informação.⁴⁹

Tais discussões permitiram que os parlamentares produzissem diversos relatórios sobre o tema, além de emendas aos projetos de lei tratados (foram 11 emendas apenas ao PL 5276/16⁵⁰), o que permitiu, no geral, uma lei bastante completa e a par dos altos padrões de qualidade tacitamente impostos pela discussão internacional sobre o tema. Contudo, as alterações trazidas pela posterior MP nº 869/18 podem ter enfraquecido determinados pontos da LGPD quando comparado aos padrões internacionais, como veremos adiante.

48. BIONI, Bruno. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. Jota. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>>. Acesso em: 23 jul. 2018

49. CÂMARA DOS DEPUTADOS. PL 4060/12 - Tratamento e Proteção de Dados Pessoais - Reuniões Anteriores. Disponível em: <<http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais>>. Acesso em 23 jul 2018.

50. BRASIL. Câmara dos Deputados. Projeto de Lei nº 5276 de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>>. Acesso em: 23 jul. 2018.

Com forte inspiração na GDPR, conforme constou em muitos dos diversos relatórios apresentados durante a tramitação do PL 4.060/12 na Câmara e posteriormente no Senado⁵¹, o texto, em seus 65 artigos, tentou se aproximar, a sua própria maneira, da legislação europeia.

A lei brasileira inova ao trazer para o cenário jurídico pátrio questões não satisfatoriamente endereçadas por outras leis setoriais de proteção de dados existentes no Brasil. Citamos, por exemplo, uma definição mais exata sobre o conceito de dados pessoais, uma previsão expressa das bases legais que autorizam o tratamento de tais dados, uma previsão de processamento de dados públicos, a criação de uma Autoridade Nacional de Proteção de Dados, sanções, etc. Nos itens seguintes, detalharemos as principais inovações trazidas pela LGPD.

2.2. Como ficam as leis setoriais sobre proteção de dados no Brasil?

A preocupação com a privacidade e a proteção de dados no Brasil surge de forma embrionária com a entrada em vigor do Código Penal, em 1940. Em seu artigo 151, o código prevê a proibição de se violar correspondência alheia. Ainda que não trate exatamente da proteção de dados, o artigo é um marco por tratar, pela primeira vez em texto legal, do direito à privacidade.

A Constituição Federal de 1988 também teve certa preocupação com o tema ao prever, em seu artigo 5º, inciso X, a inviolabilidade da intimidade e da vida

51. BRASIL. Senado. Projeto de Lei do Senado nº 4.060, de 2012. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750>. Acesso em 26 set. de 2018.

privada, assegurando ainda o direito a indenização pelo dano material ou moral decorrente de sua violação. A constituição ainda garante a inviolabilidade das comunicações em trânsito, que somente podem ser interceptadas por meio de ordem judicial.

A primeira lei brasileira a de fato tratar da proteção de dados e direitos relativos a este é o Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990 ("CDC"). O dispositivo regula as relações entre consumidores e fornecedores, estabelecendo obrigações e direitos para ambos os lados. Os dados consumeristas são tema do artigo 43, que dá aos consumidores o direito de ter acesso e a corrigir informações referentes a si mesmo, entre outras disposições. O CDC foi complementado pela Lei do Cadastro Positivo, Lei 12.414/2012, que criou um microsistema de proteção de dados no contexto das relações de consumo, mais especificamente dados de adimplência e modelagem de crédito, e trata sobre temas como princípio da finalidade, necessidade e até mesmo de revisão de decisões automatizadas.

Diversas leis setoriais que abordavam, de alguma forma, a proteção de dados, foram criadas no legislativo brasileiro. Tais leis tratam, por exemplo, de dados relacionados à saúde, ao mercado financeiro, ao direito penal e até mesmo às atividades do setor público.

No campo da saúde, destacam-se a Resolução nº 1.821/07 do Conselho Federal de Medicina, que dispõe sobre prontuário eletrônico e proteção de dados médicos, e a Resolução da Agência Nacional de Vigilância Sanitária - ANVISA da Diretoria Colegiada nº 44/2009, que dispõe sobre boas práticas farmacêuticas para prestação desses serviços, inclusive o uso de dados.

No mercado financeiro, podem ser observadas a Lei Complementar nº 105, de 10 de janeiro de 2001, que trata do sigilo das operações de instituições financeiras, e a Portaria nº 5/2002 da Secretaria de Direito Econômico do Ministério da Justiça, que tornou abusivas as cláusulas em contratos de consumo que autorizam o envio de dados pessoais sem consentimento prévio.

No âmbito do Direito Penal, o principal exemplo é a recente Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, que tornou crime a invasão de dispositivos informáticos. Outro importante exemplo é a Lei nº 9.296, de 24 de julho de 1996, que tornou crime a interceptação telefônica sem autorização judicial.

Já no setor público, o principal destaque é a Lei nº 12.527, de 18 de novembro de 2011 ("Lei de Acesso à Informação"), de extrema importância por garantir aos cidadãos o acesso a dados públicos nas três esferas governamentais.

No mundo online, da Internet, a Lei nº 12.965, de 23 de abril de 2014, ("Marco Civil da Internet"), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, é considerada, junto com o Decreto 8.771/2016, que a regulamentou, um microsistema de proteção de dados no contexto de tratamento de dados por meio da Internet. O Marco Civil, traz, por exemplo, como base legal única, a necessidade de consentimento expresso para o tratamento de dados pessoais, os quais foram conceituados pelo decreto.

Além de leis setoriais como as mencionadas, já existe no Brasil lei municipal e projetos de lei municipal específicos sobre proteção de dados. O principal exemplo é a Lei Complementar nº 161, de 12 de julho de 2018 do município de Vinhedo, São Paulo, mas também há em Campinas e São Paulo

projetos de lei com o mesmo objetivo – garantir a proteção dos dados dos cidadãos desses municípios.

Com a entrada em vigor da Lei Geral de Proteção de Dados, muito se questiona sobre a situação de tais leis de proteção de dados no Brasil. Nesse cenário, a LGPD pode ser vista como uma diretiva geral para a proteção de dados no Brasil. Isso significa que a nova lei busca não substituir as que existem atualmente, mas estabelecer regras e princípios gerais para que as mesmas possam ser cumpridas de uma maneira mais benéfica para os titulares dos dados pessoais. Naturalmente, caso se verifiquem contradições entre essas leis e a LGPD, as regras clássicas para decisão entre contradições jurídicas deverão ser aplicadas.



/ O Escopo da Lei Geral de Proteção de Dados no Brasil

Após analisar o histórico europeu e sul-americano de proteção de dados, vamos explorar, de maneira específica, os institutos mais importantes presentes em nossa Lei Geral de Proteção de Dados.

Assim, em primeiro lugar, importa ressaltar que a LGPD possui aplicação extraterritorial⁵², ou seja, até mesmo entidades sem presença física no Brasil, podem estar sujeitas a ela.

São fatores que determinam a incidência da LGPD, como regra geral, (i) que a operação do tratamento se dê em território nacional; ou (ii) que o intuito deste tratamento seja oferecer bens ou serviços ou, simplesmente, se deem sobre dados de indivíduos localizados no território nacional; ou, por fim (iii) que os dados pessoais objeto do tratamento tenham sido coletados no território nacional⁵³.

52. As exceções estão descritas nos incisos do artigo 4º da Lei 13.709 de agosto de 2018.

53. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 3º, incisos I, II e III.

3.1. Dados pessoais e categoria de dados

Nossa legislação define dado pessoal como a “informação relacionada à pessoa natural identificada ou identificável⁵⁴”. Ou seja, qualquer informação que, isolada ou associada a outras, permite identificação de uma pessoa natural. A abrangência da definição é uma maneira de enquadrar mais informações nessa categoria, aumentando o escopo de aplicação da lei.

Uma das categorias de dados presente na lei são os dados pessoais sensíveis. A LGPD indica que dados pessoais sensíveis são aqueles sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural⁵⁵”. A nomenclatura “sensíveis” advém do fato de que essas informações podem sujeitar os seus titulares às práticas discriminatórias e, por isso, o tratamento de tais dados deve observar bases legais mais restritivas e padrões de segurança mais elevados.

A terceira e última categoria abordada pela lei é a dos dados anonimizados. Tratam-se de dados sobre um titular “que não possa ser identificado, utilizando-se meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;⁵⁶”. Dados anonimizados não estariam sujeitos às regras da lei caso não possam ser reidentificados⁵⁷, incentivando inovações como internet das coisas e inteligência artificial. Mais adiante abordaremos com mais detalhes o processo de anonimização.

54. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso I.

55. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso II.

56. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso III.

57. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 12, *caput*.

3.2. Bases legais

A LGPD possui 10 bases legais para a coleta e o processamento de dados. Bases legais são hipóteses pelas quais a legislação permite que seja realizado o tratamento de dados pessoais. Antes, no Brasil, existiam poucas bases legais expressamente previstas em lei, tais como: consentimento, interesse público e obrigação legal. Com a LGPD, o leque de bases legais aumentou, tornando o tratamento de dados, possivelmente, mais flexível do que os realizados com base somente nas leis nacionais vigentes.

Para que seja realizado o tratamento dos dados pessoais de forma legítima e lícita, é preciso observar os princípios gerais⁵⁸ e bases legais específicas, que dependem da categoria de dados em questão.

A LGPD apresenta 10 hipóteses que permitem o tratamento dos dados pessoais, sendo o consentimento do titular somente uma delas. Esse consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular⁵⁹. Também vale destacar que, em caso de consentimento escrito, ele deverá constar em cláusula destacada no contrato⁶⁰ e que

58. Os princípios se encontram no *caput* e nos 10 incisos do artigo 6 da LGPD. Eles seriam a boa-fé, a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

59. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, *caput*.

60. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º.

o ônus da prova de consentimento cabe ao controlador⁶¹. Além disso, o titular dos dados tem o direito, de forma gratuita e facilitada, de revogar o seu consentimento⁶².

Assim, no conjunto, as bases legais são: (i) o consentimento do titular⁶³; (ii) o cumprimento de obrigação legal ou regulatória pelo controlador⁶⁴; (iii) a execução de políticas públicas⁶⁵; (iv) a realização de estudos⁶⁶ por órgãos de pesquisa⁶⁷; (v) a execução de contrato de qual seja parte o titular⁶⁸; (vi) o exercício regular de direito em processo judicial, administrativo ou arbitral⁶⁹; (vii) a proteção da vida⁷⁰; (viii) a tutela da saúde⁷¹; (ix) o legítimo interesse⁷²; e, por fim, (x) a proteção ao crédito⁷³.

Importante pontuar que o instituto do legítimo interesse do controlador dos dados está presente na legislação. Dessa forma, o controlador poderá fundamentar o tratamento dos dados para finalidades legítimas observadas em situações concretas, independente do consentimento do titular, uma vez que todas as bases legais são independentes entre si e nenhuma

prepondera sobre a outra⁷⁴.

Para os dados pessoais sensíveis, as regras são mais restritivas em comparação aos dados pessoais “comuns”. No caso do consentimento do titular, ele deve ser feito de forma específica e destacada para as finalidades de tratamento descritas⁷⁵, comportando exceções para o seu tratamento sem consentimento, apenas quando esse dado for indispensável para a execução das atividades destacadas na lei⁷⁶.

Outra categoria de dados que possui base legal destacada são os dados pessoais de crianças, assim categorizadas como aquelas cuja idade seja até 12 anos. O consentimento para tratamento deverá ser específico e em destaque e deverá ser realizado por um dos pais ou responsável legal⁷⁷. O tratamento de dados pessoais de adolescentes, ou seja, àqueles superiores à 12 anos, tem que ser feito no seu melhor interesse, respeitando as bases legais e os princípios relativos à dados pessoais.

3.3. Anonimização x Pseudonimização

Outro ponto presente na LGPD é a diferenciação entre dados anonimizados e os pseudonimizados. Como já observamos anteriormente, os dados anonimizados são aqueles que não podem identificar o titular utilizando meios técnicos razoáveis e disponíveis na época de seu tratamento. Por esse motivo eles não são considerados dados pessoais e essa impossibilidade de identificação retira os dados anônimos do escopo da LGPD.

Por outro lado, os dados pseudonimizados são aqueles sujeitos ao tratamento que

61. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §2º.

62. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §5º.

63. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso I.

64. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso II.

65. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso III.

66. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso IV.

67. A definição de órgão de pesquisa se encontra no artigo 5º, XVII.

68. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso V.

69. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso VI.

70. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso VII.

71. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso VIII.

72. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso IX.

73. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso X.

74. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 10, incisos I e II.

75. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, inciso I.

76. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, inciso II, itens a, b, c, d, e, f e g.

77. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 14, §1º.

são aqueles sujeitos ao tratamento que impossibilita a associação a um indivíduo, salvo pelo uso de informação adicionalmente mantida em separado pelo controlador⁷⁸. Em nossa LGPD, os dados pseudonimizados só podem ser utilizados na realização de pesquisas em saúde pública, observando as regras do artigo 13 e seus parágrafos.

Neste caso, podemos pontuar que os dados anonimizados, caso não seja possível a sua reidentificação através de meios razoáveis, podem ser utilizados de maneira ampla, enquanto os dados pseudonimizados só podem ser utilizados para fins científicos bastante restritos.

Além disso, a lei não obriga a anonimização, mas sim apenas indica quando possível que isso seja feito, isso significa que se “A” é uma empresa que trabalha operando seus serviços com bases em CPF, e precisa desse identificador para poder gerar um target, ou realizar enriquecimento de dados, por exemplo, ela não poderá anonimizar a sua base de dados, porque isso inviabilizaria os seus serviços, mas poderá tão somente, pseudonimizar e criptografar os dados, a fim de mitigar riscos associados a possíveis incidentes.

Portanto, é importante mensurar essa diferença, a fim de compreender tecnicamente e dentro do escopo da lei, o contexto da base de dados de um órgão público ou empresa e assim traçar medidas de como implementar medidas técnicas de pseudonimização.

3.5. Compartilhamento de dados

A LGPD define o uso compartilhado de dados como:

78. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 13, §4º.

“...comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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;”⁷⁹.

Para o compartilhamento dos dados pessoais é preciso ter uma base legal adequada ao contexto do tratamento⁸⁰. É importante que o controlador tenha rastreabilidade dos dados pessoais que transfere aos seus parceiros, pois os titulares possuem os direitos de saber com quem e para quais finalidades seus dados foram compartilhados⁸¹, assim como, de que suas demandas por correção, eliminação, anonimização ou bloqueio de dados sejam replicadas àqueles que obtiveram os dados compartilhados.

Importante pontuar que o Poder Público possui maiores liberdades na seara de compartilhamento de dados entre órgãos da Administração Pública. Por exemplo, maior liberdade para o compartilhamento de dados sensíveis⁸², estruturação de dados pessoais para uso compartilhado⁸³, entre outros. Contudo, vale ressaltar que o Poder Público só pode compartilhar dados mediante uma previsão legal específica, que apresente finalidades específicas para esse compartilhamento, atendendo ao princípio da finalidade e legalidade, como é o caso das Lei de Lavagem de Dinheiro, Lei de Combate

79. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso XVI.

80. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, §5º. Apesar deste parágrafo falar em consentimento específico, e após em dispensa do consentimento, aqui houve uma atecnia legislativa. O compartilhamento pode ser feito com fundamento em qualquer uma das bases legais do referido artigo.

81. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 9, incisos V e VII, e artigo 18, inciso VII.

82. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 23, caput.

83. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 24, Parágrafo Único.

às Organizações Criminosas e Lei de Acesso à Informação. Sempre respeitando o princípio da necessidade e da proporcionalidade no momento da coleta dos dados.

Com a nova redação dada à LGPD pela Medida Provisória nº 869/18, o compartilhamento de dados sensíveis de saúde também passa a ser possível para a prestação de serviços de saúde suplementar, como operadoras de planos de saúde⁸⁴.

Por fim, além das regras já dispostas na LGPD, a Autoridade Nacional de Proteção de Dados (a "ANPD") poderá estabelecer normas complementares sobre o uso compartilhado de dados pessoais⁸⁵. Como será melhor explicado nos itens 3.11 e 3.12, a ANPD terá como função fiscalizar o cumprimento das disposições presentes na LGPD, bem como aplicar as sanções cabíveis no caso de infração de uma ou mais delas⁸⁶.

3.6. Hipóteses de exclusão de dados

A "eliminação" é um termo definido na LGPD como: "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado"⁸⁷. Além disso, o termo eliminação é utilizado como uma modalidade de tratamento de dados⁸⁸.

Os titulares dos dados pessoais possuem o direito de exigir, a qualquer momento e mediante requisição, a eliminação de dados desnecessários, excessivos ou

em desconformidade com a LGPD⁸⁹, podendo inclusive solicitar a eliminação de dados tratados originalmente com seu consentimento⁹⁰.

Além disso, os dados pessoais devem ser eliminados pelo controlador, após o término de seu tratamento⁹¹. Esse término é observado nas seguintes hipóteses taxativas dos incisos do artigo 21 da LGPD:

*"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. 14 desta Lei, resguardado o interesse público; ou
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei."*⁹²

O direito à exclusão dos dados pessoais, no entanto, não é absoluto. A exclusão, ou cancelamento dos dados, requerida pelo titular dos dados é baseada na revogação de seu consentimento⁹³. Caso exista uma outra base legal, que não o consentimento, que autorize a manutenção dos dados, a empresa poderá continuar o tratamento até que a finalidade desta outra base legal seja atingida. Ou seja, uma vez que o armazenamento dos dados é uma hipótese de tratamento destes, é necessário ter uma base legal para ela, seja o consentimento ou alguma outra das previstas na LGPD. Outras exceções que autorizam a manutenção dos dados pessoais são sua utilização para o cumprimento da

84. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, Parágrafo 4º, inciso II.

85. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 30, caput.

86. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 52, caput.

87. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5, inciso XIV.

88. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5, inciso X.

89. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, inciso IV.

90. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, inciso VI.

91. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 16.

92. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 15.

93. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 15, inciso III.

lei ou de regulação; para estudo por órgão de pesquisa; para transferência a terceiros respeitando os dispositivos da LGPD; e para uso exclusivo pelo controlador, desde que os dados estejam anonimizados⁹⁴.

3.7. Direitos dos titulares

A LGPD busca assegurar a toda pessoa natural a titularidade de seus dados pessoais, além de garantir os seus direitos fundamentais de liberdade, intimidade e privacidade⁹⁵. Além disso, há uma série de direitos específicos que estão indicados ao longo dos artigos 18 e 20 da lei. Dentre eles podemos classificar primeiramente os chamados “direitos ARCO”, que garantem aos titulares: (i) acesso; (ii) retificação; (iii) cancelamento (chamado aqui de eliminação); e (iv) oposição ao processamento de seus dados pessoais (art. 18, incisos II, III, VI e §2º).

Além destes direitos, a LGPD garante também aos titulares a: (v) confirmação da existência de tratamento; (vi) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; (vii) portabilidade dos dados; (viii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (ix) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (x) a revogação do consentimento (art. 18, I, IV, V, VII, VIII e IX).

Além desses direitos, é possível inferir mais um no artigo 20, o qual trata sobre: (xi) revisão de decisão automatizada que, com as mudanças trazidas pela MP nº 869/18 na LGPD, não precisa ser realizada por

pessoa natural⁹⁶.

Nesse sentido, segue abaixo uma breve explicação e exemplos sobre alguns desses direitos:

Requisição de acesso aos seus dados pessoais. Este direito permite que o titular possa requisitar e receber uma cópia dos seus dados pessoais.

Requisição de retificação dos dados pessoais. Este direito permite que o titular a qualquer momento possa solicitar a correção e/ou retificação dos seus dados pessoais, caso ele identifique que alguns deles estão incorretos.

Requisição de exclusão dos dados pessoais. Este direito permite que o titular possa solicitar a exclusão dos seus dados pessoais. Todos os dados coletados deverão ser excluídos, salvo se houver qualquer outra razão para a manutenção deles, como eventual obrigação legal de retenção de dados ou necessidade de preservação destes para resguardo de direitos do operador ou controlador.

Oposição a um processamento de dados. O titular tem o direito de contestar onde e em que contexto os agentes de tratamento estão tratando os seus dados pessoais para diferentes finalidades. E poderá se opor em relação a uma finalidade ou todas. Em alguns casos é possível demonstrar que os agentes possuem motivos legítimos para processar os dados pessoais, os quais podem se sobrepor aos direitos dos titulares, já que nesses casos podem ser essenciais para o fornecimento do produto e/ou serviço.

Restringir o processamento dos dados

96. Vale lembrar que a MP 869/18 trouxe outras mudanças significativas neste artigo 20 da LGPD, retirando: (i) a possibilidade do titular dos dados requisitar informações sobre os critérios e os procedimentos utilizados para a decisão automatizada; e (ii) a possibilidade da ANPD realizar auditoria para verificar eventuais aspectos discriminatórios realizados por processos algorítmicos; mudanças que impactam diretamente no princípio da transparência e o direito à explicação.

94. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 16, incisos I, II, III e IV.

95. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 17.

personais. Este direito permite que o titular peça aos agentes de tratamento para suspender o processamento de seus dados pessoais nos seguintes cenários: (a) se o titular quiser que os agentes estabeleçam a precisão dos dados; (b) quando o titular precisar que sejam mantidos os dados mesmo se os agentes não precisarem mais deles, conforme necessário, para estabelecer, exercer ou defender reivindicações legais; ou (c) nos caso em que o titular se opôs ao uso de seus dados, mas os agentes precisam verificar se tem motivos legítimos para usá-los.

Titular solicitar a portabilidade dos dados pessoais para ele ou para terceiros. Ele permite que o titular requisite que seus dados sejam disponibilizados em um formato estruturado e interoperável, que facilite a transferência para outros fornecedores de produtos ou serviços, de forma similar como já é feito entre as operadoras de telefonia no Brasil, através da Resolução 460/2007 da Anatel.

Direito de retirar o consentimento a qualquer momento. O titular tem o direito de retirar o seu consentimento, no entanto, isso não afetará a legalidade de qualquer processamento realizado antes disso acontecer. Dependendo do contexto se o titular retirar o seu consentimento, talvez não seja possível aos agentes de tratamento fornecer determinados produtos e serviços. E se for este o caso, eles precisam avisar o titular no momento em que isso ocorrer.

Solicitação por parte do titular de revisão de decisões. Outro importante direito dos titulares é o de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de seus dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definição de perfis pessoais, profissionais, de consumo e de crédito e/ou

os aspectos de sua personalidade⁹⁷. Com as mudanças trazidas pela MP 869/18 na LGPD, tal revisão não precisa mais ser realizada por uma pessoa natural.

3.8. Transferência internacional de dados

A transferência internacional de dados é aquela na qual os dados pessoais são transferidos para país estrangeiro ou organismo internacional do qual o país seja membro⁹⁸, sendo também a transferência internacional uma forma de tratamento de dados pessoais⁹⁹.

A transferência internacional só é permitida quando realizada para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado¹⁰⁰. A adequação será avaliada pela ANPD¹⁰¹ e levará em consideração, por exemplo, as normas gerais e setoriais da legislação em vigor no local de destino, a natureza dos dados, a observância dos princípios e direitos dos titulares da LGPD, a adoção de medidas de segurança previstas em regulamento, entre outras.

Outra autorização de transferência internacional se dá quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, direitos do titular e regime de proteção previstos na LGPD por diversas formas, como cláusulas contratuais específicas ou padronizadas, normas corporativas globais ou selos, certificados e

97. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 20, caput.

98. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5, inciso XV.

99. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5, inciso X.

100. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 33, inciso I.

101. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 34, caput.

códigos de conduta¹⁰².

A transferência também poderá ocorrer quando for necessária para cooperação jurídica internacional, importante para a proteção da vida do titular ou de terceiros, autorizado pela ANPD, por compromissos internacionais de cooperação, para execução de política pública, fornecimento de consentimento específico para a transferência internacional, que deve se dar de forma destacada para o titular¹⁰³, entre outras¹⁰⁴.

3.9. Comunicação de incidente

Na ocorrência de algum incidente de segurança com os dados pessoais que possa acarretar risco ou danos aos titulares, tais como vazamento dos dados ou uso inadequado destes, o controlador deverá comunicá-los e à ANPD¹⁰⁵.

A ANPD irá estabelecer prazo razoável para comunicar o incidente, que deverá conter no mínimo¹⁰⁶:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – as 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 incidente”

A ANPD, levando em consideração a gravidade do incidente, poderá determinar ao controlador providências como a ampla divulgação do ocorrido ou adoção de medidas que mitiguem ou revertam o incidente¹⁰⁷.

3.10. Padrões de segurança da informação

O Decreto nº 8.771, de 11 de maio de 2016, regulamenta o Marco Civil da Internet e apresenta, em seu artigo 13, diretrizes para desenvolvimento de padrões de segurança que devem ser observados por provedores de conexão e aplicação. Essas diretrizes são: o estabelecimento de controle estrito sobre o acesso dos dados, a previsão de mecanismo de autenticação de registros, a criação de inventário detalhado de acesso e o uso de técnicas de inviolabilidade dos dados.

A LGPD apresenta novas regras sobre padrões de segurança da informação. Os agentes de tratamento devem adotar medidas de segurança técnica e administrativa para proteger os dados pessoais tratados¹⁰⁸.

102. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 33, inciso II.

103. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 33, incisos de III até VIII.

104. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 33, inciso IX e Artigo 7º, incisos II, V e VI.

105. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 48, caput.

106. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 48, §1º.

107. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 48, §2º.

108. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 46, caput.

Esses padrões devem ser adotados desde a fase inicial da concepção do produto ou serviço. O instituto do “privacy by design”, que internacionalmente se consagrou por meio da GDPR, acaba encontrando, por esse dispositivo, sua concretização em nosso ordenamento jurídico.

A ANPD desempenha funções importantes nessa seara. Ela poderá dispor sobre padrões mínimos de privacidade de acordo com a natureza das informações tratadas¹⁰⁹, poderá dispor sobre padrões e técnicas para o processo de anonimização¹¹⁰, sugerir a adoção de padrões e boas práticas para tratamento de dados pessoais pelo Poder Público¹¹¹, entre outros.

Importante mencionar que a iniciativa privada também pode estabelecer boas práticas e padrões de segurança da informação¹¹². Ao desenvolver esses padrões, a LGPD aponta os itens mínimos que devem ser observados, determinando que quem queira apresentar iniciativas:

“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 objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente que lhe assegure mecanismos de participação;

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;”

Deve-se lembrar que estes são os requisitos mínimos. Naturalmente, as empresas podem adotar padrões mais rigorosos de segurança, ou mesmo procurarem estar de acordo com normas internacionais como a GDPR.

3.11. Sanções

A LGPD prevê uma série de sanções administrativas, que devem ser aplicadas pela ANPD. Elas seriam¹¹³:

109. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 46, §1º.

110. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 12, §3º.

111. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 32, *caput*.

112. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 50.

113. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 52.

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 regularização da atividade de tratamento pelo controlador;
VI – eliminação dos dados pessoais a que se refere a infração;”

Para definição da sanção aplicável, a ANPD utilizará como parâmetro¹¹⁴ a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, a extensão do dano, a cooperação do infrator, comprovação de utilização de mecanismo capazes de minimizar os danos, a adoção de políticas de boas práticas e governança e a pronta adoção de medidas corretivas.

Por fim, a ANPD poderá, por regulamento próprio, definir as metodologias que orientarão o cálculo do valor-base das sanções administrativas relativas a infrações à LGPD, que deverá ser objeto de consulta pública¹¹⁵.

3.12. Autoridade Nacional de Proteção de Dados

Como já brevemente mencionado, no projeto

114. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 52, §1º, incisos de I até X.

115. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 53, caput.

de lei aprovado pelo Congresso Nacional, a ANPD seria uma autarquia vinculada ao Ministério da Justiça. No entanto, os artigos referentes a sua criação¹¹⁶, presentes no PLC 53/2018, foram vetados na fase de sanção presidencial. A justificativa central deste veto foi a de que a instituição da ANPD através da LGPD apresentaria vício de iniciativa, tendo em vista que sua criação seria de competência do Poder Executivo¹¹⁷, segundo Michel Temer¹¹⁸.

Sendo assim, em 27 de dezembro de 2018, o então Presidente Michel Temer editou a MP nº 869/18, publicada no Diário Oficial da União em 28 de dezembro de 2018, que, além de promover determinadas alterações no texto sancionado da LGPD, também criou a ANPD como sendo um órgão da administração pública federal direta e vinculado diretamente à Presidência da República^{119 120}.

De acordo com o texto da MP nº 869/18, a ANPD será composta por seis departamentos, destacando-se o Conselho Diretor, o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, o órgão de assessoramento jurídico e as unidades especializadas¹²¹, que provavelmente irão atuar de forma distribuída pelo país.

O Conselho Diretor será composto por cinco diretores, dos quais um será o Diretor Presidente¹²². Os membros do Conselho serão nomeados diretamente pelo Presidente

116. BRASIL. Câmara dos Deputados. Projeto de Lei da Câmara nº 53, de 2018. Artigo 55 e seguintes.

117. Sancionada com vetos lei geral de proteção de dados. *Senado Notícias*. 15 ago. 2018. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais>>

118. *Ibidem*.

119. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-A.

120. A MP 870/2019, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, também a ANPD como sendo um órgão integrante da Presidência da República, em seu artigo 2º, inciso VI.

121. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-B.

122. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-D, caput.

da República para cargos de comissão¹²³, e selecionados por meio de métricas objetivas¹²⁴. Além disso, o mandato dos membros do Conselho Diretor será de 04 anos¹²⁵, sendo certo que as primeiras nomeações terão prazos diferenciados, de acordo com o que for estabelecido no ato da nomeação¹²⁶.

Já o Conselho Nacional de Proteção de Dados Pessoais e Privacidade será composta por 23 membros, com composição multissetorial¹²⁷. Basicamente, o Conselho Nacional será um órgão consultivo, sem poder sancionatório ou investigativo, acessório à ANPD, que auxiliará na elaboração da Política Nacional de Proteção de Dados Pessoais e na atuação da ANPD. O Conselho Nacional deverá elaborar relatórios para averiguar as ações da Política Nacional, podendo também elaborar estudos, realizar debates e audiências públicas sobre temas correlatos à privacidade e proteção de dados, além de disseminar conhecimento para a população em geral¹²⁸. No que se refere às competências da ANPD¹²⁹, destacamos o zelo pela proteção de dados pessoais, fiscalizar e aplicar sanções, entre diversas outras funções citadas anteriormente¹³⁰. Em resumo, é um órgão regulador com funções regulamentares, fiscalizatórias, sancionadora e disciplinadora que terá atuação abrangente, lidando com órgãos públicos e privados que realizem tratamento de dados pessoais.

Por fim, vale lembrar que as Medidas Provisórias têm aplicação imediata, mas

.....
123. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-D, §1º.

124. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-D, § 2º.

125. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-D, § 3º.

126. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-D, §4º.

127. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 58-A

128. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 58-B, incisos I a V.

129. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-J, incisos I a XVI.

130. A ANPD é citada em nossos itens de Transferência Internacional de Dados, Comunicação de Incidentes, Padrões de Segurança da Informação e Sanções.

dependem de aprovação do Congresso Nacional para transformação definitiva em lei e posterior sanção presidencial caso seu conteúdo seja alterado. Desta forma, tais alterações trazidas pela MP 869/18 na LGPD podem perder a eficácia se rejeitadas pelo Congresso Nacional ou perder a validade se passado seu prazo de vigência sem aprovação da conversão em lei da MP pelo Congresso Nacional.

3.13. Relatório de Impacto à Proteção de Dados e Processo de Conformidade

O relatório de impacto à proteção de dados é conceituado na LGPD¹³¹ como o documento do controlador que tem por objetivo mapear todos os processos de tratamento de dados pessoais realizados pela organização que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos.

A LGPD dispõe que a ANPD poderá solicitar ao controlador a elaboração, apresentação e publicação do relatório de impacto à proteção de dados em diferentes momentos^{132 133}. E a partir da construção do relatório é possível visualizar o mapa de dados da empresa e identificar os riscos existentes no fluxo de dados. Assim o documento se torna uma fase importante para o processo de demonstração de conformidade com a Lei.

Ocorre que, diante da ausência temporária de uma autoridade brasileira, a qual muito além do papel fiscalizador, tem por objetivo contribuir para a melhoria do ecossistema de proteção de dados no Brasil, fica difícil

.....
131. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso XVII.

132. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 10, parágrafo 3º e Artigo 38, parágrafo único.

133. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 38.

elaborar um relatório de impacto, sem a própria autoridade indicar quais são as metodologias e padrões que deveriam ser utilizados no momento da elaboração dele.

Assim, diante dessa ausência de recomendações, empresas e organizações que desejam iniciar o processo de conformidade com a LGPD podem se valer das metodologias aprovadas por legislações e autoridades de proteção de dados estrangeiras enquanto esse tema ainda não é definido no Brasil. Tendo em vista que a LGPD se inspirou, e muito, na legislação europeia da GDPR, é possível buscar metodologias e formatos já adotados no cenário europeu como parâmetro para estruturação e aplicação do relatório de impacto à proteção de dados.

A ideia de se elaborar um relatório de impacto à proteção de dados, emergiu na Diretiva da União Europeia, de 1995, com o Privacy Impact Assessment (“PIA”). O PIA buscava endereçar riscos e mitigadores relativos à privacidade dos indivíduos, contudo, não abordava algumas questões específicas de proteção de dados. Isso mudou com a entrada em vigor da GDPR, que introduziu o Data Protection Impact Assessment (“DPIA”), trazendo metodologias e requisitos para a elaboração do documento, além de tornar obrigatória a sua elaboração em diversas hipóteses como no caso de processamento de dados em larga escala e quando há monitoramento de acessos públicos.

Com a criação e constituição da ANPD, o relatório de impacto à proteção de dados possivelmente ganhará forma e desenho, a fim de estruturar metodologias definidas e estabelecer critérios mínimos para a sua elaboração. Enquanto a ANPD não é constituída, ainda é preciso recorrer aos melhores modelos no cenário internacional para que seja possível fazer o assessment, elaborar o relatório e demonstrar conformidade com a lei.

Desta forma, o DPIA se tornou um instrumento que permite uma fotografia do status de conformidade regulatória da instituição as leis de proteção de dados, incluindo a LGPD, a GDPR e leis setoriais. Após esta fotografia, é possível identificar o que é preciso ser feito para atingir a conformidade. Isso pode incluir a revisão de processos, elaboração de políticas, revisão de contratos, indicação de times de supervisão, além de aplicação de metodologias de proteção de dados desde a concepção, conhecida como privacy by design.

/ GDPR x LGPD: o que muda com a nova lei brasileira?

A comparação entre a GDPR e a LGPD é uma questão de grande valor prático. Vale destacar que a GDPR pode se aplicar às empresas brasileiras, tendo em vista que seu escopo territorial abrange dados coletados de pessoais naturais que se encontram na União Europeia¹³⁴. Portanto, surge o questionamento: é possível estar de acordo com ambas as leis?

Para respondermos a essa pergunta, se faz necessária a comparação dos elementos principais de ambos os textos legais. Afinal, as legislações possuem normas inconciliáveis ou é possível estar em conformidade com ambas as normativas?

134. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 3º

4.1. Bases legais

A LGPD apresenta 10 bases legais¹³⁵ para tratamento legítimo dos dados pessoais, enquanto que a GDPR se limita a 6¹³⁶. Passaremos a comparar as bases previstas em ambas leis.

O consentimento é uma base legal que se encontra em ambas as normativas^{137 138}. Sobre esse ponto, as normas apresentam algumas semelhanças, tais como: o consentimento por escrito deverá constar em cláusula apartada das demais^{139 140}; a prova do consentimento é um ônus do controlador/responsável^{141 142}, entre outras. Uma importante diferença entre as normas é que a GDPR não caracteriza como “livre” o consentimento quando este se mostra como um requisito para a prestação de um serviço¹⁴³, enquanto a LGPD apenas destaca que o titular dos dados pessoais deve ser informado quando o tratamento de dados é condição para obtenção de um produto ou serviço¹⁴⁴.

Por sua vez, o tratamento de dados pessoais para exercício de funções de interesse

.....
135. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º.

136. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 6º.

137. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 6º, 1.

138. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso I.

139. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 7º, 2.

140. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §1º.

141. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 7º, 1.

142. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §2º.

143. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 7º, IV.

144. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 9º, §3º.

público^{145 146} possui importantes diferenças. A primeira delas é que a GDPR, em seu considerando 31¹⁴⁷, afirma que o tratamento pautado nessa base legal não implica que as autoridades possam compartilhá-los entre si; enquanto a LGPD permite tal compartilhamento no próprio inciso que trata dessa base legal¹⁴⁸, contanto que se atente às finalidades específicas de execução de políticas públicas nos termos do artigo 26.

Ainda, com as alterações trazidas pela MP nº 869/18 na LGPD, o rol de exceções ao compartilhamento de dados pessoais pelo Poder Público com entes privados ficou ampliado, sendo possível realizar tal transferência quando¹⁴⁹: (i) houver a execução descentralizada de atividade pública que exija a transferência; (ii) o ente privado tiver indicado um encarregado; (iii) quando houver previsão legal ou em instrumentos jurídicos administrativos; (iv) quando a transferência for para fins de prevenção à fraude, segurança e integridade do titular dos dados; e (v) dados forem publicamente acessíveis.

Outro ponto importante sobre esse assunto é que a LGPD permite que o tratamento de dados pela administração pública pode estar respaldado em contratos, convênios e instrumentos congêneres, dando uma abertura maior do que a GDPR.

O legítimo interesse do controlador é uma base legal presente em ambas as normas, limitada pelos direitos e liberdades fundamentais

.....
145. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Artigo 6º, 1 e).

146. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso III.

147. As considerações dentro de uma norma legal visam apresentar as prerrogativas para melhor interpretação dos artigos de uma determinada lei.

148. Ainda sobre esse tema, o artigo 25 da LGPD afirma que “os dados pessoais tratados pelo Poder Público deverão ser mantidos em formato interoperável e estruturados para uso compartilhado...”. BRASIL. Lei nº 13.709, de 14 de agosto de 2018.

149. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 26, §1º, incisos I a VI.

dos titulares dos dados^{150 151}. No entanto, também há divergências. A LGPD não permite o tratamento de dados sensíveis, de crianças e a transferência internacional fundamentada pelo legítimo interesse. Ainda, a LGPD não faz maiores considerações sobre se essa base legal poderia ser aplicada para ente público no bojo de suas atividades, não havendo uma limitação expressa, como na GDPR¹⁵².

Vale ressaltar que a LGPD apresenta algumas regras específicas sobre o tratamento com base em legítimo interesse. No caso, os dados pessoais deverão ser estritamente necessários para a finalidade pretendida quando tratados por meio de legítimo interesse, além de dever ser garantida a transparência aos titulares para a utilização de dados por essa base legal¹⁵³. É necessário aplicar um teste de proporcionalidade que leva em consideração a legitimidade da finalidade, a possibilidade de existir uma outra base legal mais adequada, além das expectativas do titular dos dados, dentro do contexto de tratamento, além da necessidade de aplicação de salvaguardas que visem mitigar eventuais danos aos titulares.

Sobre as bases legais a seguir não há nenhuma diferença substancial entre as normativas: execução de um contrato na qual o titular seja parte^{154 155}, para cumprimento de obrigação

legal pelo controlador^{156 157}, proteção de interesses vitais do titular ou de terceiros^{158 159}.

Esgotadas as bases legais presentes na GDPR, ainda se faz necessário observar se ela, de alguma forma, remete às outras 4 bases legais presentes na LGPD, quais sejam: (i) a realização de estudos por órgão de pesquisa, (ii) exercício regular em processo judicial/administrativo/arbitral, (iii) para a tutela da saúde em procedimentos realizados por profissionais da saúde e sanitários e (iv) a proteção do crédito.

No contexto da realização de estudos por órgão de pesquisa, a GDPR determina que os Estados-Membros devem conciliar as normas que garantem a liberdade de expressão acadêmica com o direito à proteção de dados pessoais, podendo criar exceções para garantir o equilíbrio desses direitos fundamentais¹⁶⁰. A lei também prevê que o titular tenha a possibilidade de limitar o seu consentimento a determinadas categorias ou projetos de pesquisa específicos¹⁶¹.

A GDPR trata o exercício ou defesa de um direito em um processo judicial como uma hipótese em que o tratamento dos dados pessoais pode ser menos restrito, embora não seja em si uma base legal. Os direitos do titular de exigir que seus dados sejam apagados ou retificados, ou que o seu tratamento seja limitado, podem ser reduzidos se o tratamento for necessário para a defesa ou exercício

.....
150. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º, 1 f).

151. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso IX.

152. "O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica." UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º.

153. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 10, §1º e 2º.

154. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso V.

155. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º, 1 b).

.....
156. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso II.

157. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º, 1 c).

158. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, inciso VII.

159. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º, 1 d).

160. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Considerando (153).

161. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Considerando (33).

de direitos em um processo judicial¹⁶². Essa hipótese também pode permitir que dados pessoais sejam transferidos a países terceiros ou organizações internacionais cujo nível de proteção de dados não seja assegurado pela Comissão Europeia¹⁶³.

A GDPR não considera a tutela da saúde em procedimentos realizados por profissionais da saúde e sanitários um fundamento legal para o tratamento de dados, mas aborda o tema ao endereçar dados sensíveis, uma vez que os dados de saúde fazem parte de tal categoria especial de dados pessoais, que, como vimos, exigem um padrão maior de segurança. Os Estados-Membros podem também impor novos limites e condições para o tratamento de dados relativos à saúde¹⁶⁴.

Por fim, não há, na GDPR, considerações específicas sobre uma base legal que tenha por finalidade a proteção do crédito. O lastro na legislação europeia seria, provavelmente, o legítimo interesse ou a execução de contrato.

4.2. Data Protection Officer

O Data Protection Officer (“DPO”), na GDPR, ou “encarregado”, na LGPD, é a figura responsável por auxiliar o controlador no cumprimento das obrigações legais de proteção de dados, por meio de monitoramento, aconselhamento, etc.¹⁶⁵ ¹⁶⁶ Também vale destacar que ambas as normas possibilitam que as autoridades reguladoras apresentem novos regulamentos

sobre os encarregados¹⁶⁷ ¹⁶⁸.

Ainda, após as alterações trazidas pela MP nº 869/18 na LGPD, o encarregado não precisa mais ser uma pessoa natural, abrindo espaço para a possibilidade de indicação de pessoas jurídicas, ou comitês, ou grupos de trabalho, que podem exercer tais funções. Assim, atualmente, ambas as normas possibilitam que o DPO e/ou encarregado seja um empregado da empresa (pessoa natural) ou um terceiro prestador de serviços (pessoa jurídica)¹⁶⁹ ¹⁷⁰.

Mesmo que a figura exista e exerça funções similares em ambas as normativas, várias diferenças podem ser destacadas.

A GDPR apresenta maior quantidade de tarefas para o DPO. Por exemplo, ele se manifestará na notificação de incidente¹⁷¹ ¹⁷², no desenvolvimento do DPIA¹⁷³ e nas consultas prévias realizadas perante a autoridade reguladora de proteção de dados¹⁷⁴.

Além disso, a GDPR apresenta preocupações específicas com o papel do DPO dentro da governança do controlador onde atua. O DPO não poderá receber instruções sobre o exercício de suas funções, nem poderá ser destituído ou penalizado por conta delas. O

162. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Considerando (65) e artigo 18º, 2.

163. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 49º, 1.e).

164. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 9º.

165. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 41, §2º.

166. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 39º.

167. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 41, §3º.

168. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 47º, 1 h).

169. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso VIII (Redação dada pela MP 869/18).

170. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 37º.

171. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 13º, 1 b) e artigo 14º, 1 b).

172. Na LGPD a identificação do DPO é obrigatória nos termos do artigo 41, §1º.

173. O DPIA se trata de um instituto presente na GDPR, em seu artigo 35º. Ele consiste em uma análise de quanto a implementação de uma nova tecnologia de tratamento de dados pode implicar em risco para direitos e liberdades dos titulares. A participação do DPO nesse procedimento é prevista no artigo 35º, 2.

174. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 36º, 3 d).

DPO deverá reportar-se diretamente ao mais alto nível de responsabilidade pelo tratamento de dados dentro da estrutura organizacional da empresa¹⁷⁵.

Por fim, uma diferença muito importante sobre as duas leis se trata da necessidade de um DPO. Enquanto a GDPR aponta a diversas atividades que requerem a atuação de um DPO na empresa¹⁷⁶, a LGPD aponta que todo e qualquer controlador deve indicar um encarregado de maneira genérica¹⁷⁷. Assim, enquanto a GDPR apresenta balizas mais claras de quando deve-se indicar um DPO, a LGPD torna a obrigação genérica, de forma que provavelmente será aplicada para controladores de todos os tamanhos, hipótese que poderá ser alvo de regulação posterior pela Autoridade Nacional de Proteção de Dados, que poderá, inclusive, trazer situações de dispensa.

4.3. Consentimento

O consentimento é uma base legal presente em ambas as normativas^{178 179}, sendo, inclusive, bem próximas as definições utilizadas^{180 181} por cada uma delas.

Outras características muito similares entre as normativas, de forma que não merecem

175. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 38º, 3.

176. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 37.

177. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 41.

178. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 13, inciso I.

179. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 6º, 1 a).

180. "Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;". UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 4º, 11.

181. "XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidade determinada;". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso XII.

maiores considerações, são: o ônus do controlador na prova de consentimento do titular^{182 183}, a necessidade do consentimento por escrito se encontrar em cláusula contratual destacada e específica^{184 185}, o direito de retirada do consentimento^{186 187}, o consentimento para o tratamento de crianças e ser oferecido por seus responsáveis^{188 189} e o consentimento ser uma das poucas bases legais para tratamento de dados pessoais sensíveis^{190 191}.

Um ponto relevante apresentado pela GDPR se relaciona com as decisões individuais automatizadas. Os titulares possuem o direito de não ficarem sujeito às decisões tomadas, exclusivamente, com base no tratamento automatizado que o afetem de maneira significativa¹⁹². Essa regra não se aplica quando o tratamento se der com base no consentimento do titular dos dados sobre esse tipo de tratamento, em casos nos quais o tratamento seja necessário para a execução de um contrato no qual o titular faça parte ou o tratamento for autorizado pelo Estado-

182. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 7º, 1.

183. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §2º.

184. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 7º, 2.

185. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §1º.

186. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 7º, 3.

187. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 8º, §5º.

188. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 8º, 1.

189. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 14, §1º.

190. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 9º, 2 a).

191. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, inciso I.

192. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 22º, *caput*.

Membro da UE¹⁹³.

A LGPD, por outro lado, garante ao titular o direito de ter seus dados revisados quando tratados por meio automatizado¹⁹⁴, independente da base legal que autorizar o tratamento - não havendo as exceções presentes na GDPR. Vale ressaltar ainda que, com as mudanças trazidas pela MP n° 869/18 à LGPD, não é mais necessário que a revisão de decisões automatizadas se dê por pessoa natural.

4.4. Prazo de retenção

Tanto a GDPR quanto a LGPD estabelecem limites e restrições quanto ao armazenamento e tratamento de dados pessoais atrelados ao atingimento de sua finalidade.

Na GDPR, tais limites estão presentes no Artigo 5º, que estabelece que o tratamento dos dados será limitado à finalidade para qual os mesmos foram coletados¹⁹⁵. Quanto ao prazo máximo de retenção, a lei europeia não faz menção a um período específico, deixando apenas claro que tal prazo deverá limitar-se ao tempo necessário para atingir a finalidade para a qual os dados foram coletados e estão sendo processados.

Assim como a GDPR, a LGPD traz a preocupação em limitar a retenção dos dados apenas àquilo estritamente necessário para seu tratamento. A LGPD também não traz um prazo fixo para a retenção dos dados tratados, mas estabelece, em seu Artigo 16, que os “dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades”. Observa-se, dessa forma, que o prazo de retenção de dados na LGPD está condicionado

à necessidade dos mesmos para a finalidade declarada pelo responsável pelo tratamento, e que, uma vez utilizados para tal finalidade, devem ser excluídos de seus servidores.

193. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 22, 2,a), b) e c).

194. BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Artigo 20, *caput* e §1º

195. UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. General Data Protection Regulation. Artigo 5º, 1 b).



/ Conclusão

A construção histórica das leis de proteção de dados pelo mundo (principalmente nos continentes europeu e sul-americano, entre 1970 e 2018) demonstra que o desenvolvimento do direito específico para a proteção de dados não é algo recente, apesar de ter ganhado os noticiários após a aprovação e entrada em vigor da GDPR. Além disso, é surpreendente o volume de leis já existentes que foram criadas a partir de 1970 quando a primeira delas foi aprovada na Alemanha. Isso demonstra que apesar do Brasil ter tomado um passo necessário com a aprovação da LGPD o fez com quase 50 anos de atraso.

Com esta aprovação há forte expectativa de uma promoção maior de direitos e garantias para os cidadãos no meio online e offline, de forma a, espera-se, resguardar direitos individuais e fomentar a inovação por meio do estabelecimento de regras claras, harmônicas e transparentes, seguindo uma tendência mundial de tutela destes direitos.

Os 8 anos de debates e construção legislativa demonstram que todo esse percurso foi um grande processo de amadurecimento sobre a matéria de proteção de dados no Brasil. Tanto é que durante este período foram avaliados vários projetos de lei distintos até que optassem por dar sequência ao que deu origem à LGPD.

As audiências públicas desempenharam um papel importante. Tais eventos contaram com a participação de acadêmicos, representantes do terceiro setor, iniciativa privada, governo e até mesmo representantes da União Europeia, os quais foram convidados para falar sobre suas experiências no processo legislativo que culminou com a aprovação da GDPR. A presença de tais representantes tornou possível que os parlamentares que eram responsáveis pelos projetos de lei em questão os conduzissem munidos de riquíssima informação.

A LGPD pode ser vista como uma diretiva geral para a proteção de dados no Brasil. Isso significa que a nova lei busca não substituir as que existem atualmente, mas estabelecer regras e princípios gerais para que as mesmas possam ser cumpridas de uma maneira mais benéfica para o cidadão. Naturalmente, caso se verifiquem contradições entre essas leis e a LGPD, as regras clássicas para decisão entre contradições jurídicas deverão ser aplicadas.

A lei brasileira inovou ao trazer para o cenário jurídico nacional questões não satisfatoriamente endereçadas por outras leis setoriais de proteção de dados existentes no Brasil. Um exemplo, conforme abordamos, é uma definição mais exata sobre o conceito de dados pessoais, uma previsão expressa das bases legais para o processamento de dados, uma previsão de processamento de dados públicos, sanções e até a criação de uma Autoridade Nacional de Proteção de Dados, que acabou sendo feita em momento posterior através da edição da MP nº 869/18 publicada no Diário Oficial da União em 28 de

dezembro de 2018.

A LGPD possui 10 bases legais para a coleta e o processamento de dados, o que por si foi uma inovação importante já que antes no Brasil existiam poucas bases legais expressamente previstas em lei, tais como: consentimento, interesse público e obrigação legal. Com a LGPD, o leque de bases legais aumentou, e se tornou mais flexível do que outras leis gerais sobre proteção de dados no mundo.

Outras inovações importantes, são, por exemplo, para que seja realizado o tratamento dos dados pessoais de forma legítima e lícita, é preciso observar princípios gerais e bases legais específicas, que dependem da categoria de dados em questão. Outro ponto presente na LGPD é a diferenciação entre dados anonimizados e os pseudonimizados. Assim, podemos pontuar que os dados anonimizados possuem maior gama de utilização, enquanto os dados pseudonimizados só podem ser utilizados para fins científicos bastante restritos, diferente do que ocorria anteriormente.

Outro ponto relevante da norma é que a transferência internacional de dados passa a ser autorizada quando realizada para países, organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ou quando necessários para cooperação judicial internacional. Em outras situações, é necessário observar o instrumento jurídico adequado para a transferência específica.

Por fim, a comparação entre a GDPR e a LGPD é uma questão de grande valor prático. Vale destacar que a GDPR pode se aplicar a empresas brasileiras, tendo em vista que seu escopo territorial abrange qualquer dado coletado de pessoais naturais que se encontram na União Europeia. Portanto, muitas das semelhanças entre ambas as normas auxiliam no compliance das empresas que atuarem ao mesmo tempo no escopo da GDPR e da LGPD.

A GDPR tem apenas 6 bases legais. O fato da LGPD possuir um número maior não necessariamente significa que a proteção fornecida pela legislação brasileira seja superior. Inclusive, apesar de muito da LGPD ter sido baseada na GDPR, podemos afirmar a GDPR é mais completa e detalhista, por possuir, por exemplo, um texto vestibular que auxilia na interpretação mais profunda da norma.

Apesar da LGPD só entrar em vigor 24 meses após a data de sua publicação, em 16 de agosto de 2020¹⁹⁶, o número de mudanças que ela propõe coloca um desafio importante para o setor no Brasil, principalmente no que se refere a adequação dos meios de coleta e tratamento de dados. Além do aspecto ético ligado à forma que empresas lidam com dados, é importante ter em mente que as sanções em caso de descumprimento da norma são bastante altas, demonstrando a importância do bem jurídico sendo tutelado e a necessidade dos atores do setor se prepararem para uma nova realidade regulatória.

Para auxiliar no processo de conformidade, entidades públicas e privadas podem se valer de várias metodologias, dentre elas o Relatório de Impacto à Proteção de Dados, também conhecido por DPIA, que apesar de ser um instrumento para mensuração impacto de práticas de tratamento de dados no titulares, se tornou um instrumento que permite uma fotografia do status de conformidade regulatória da instituição as leis de proteção de dados, incluindo a LGPD, a GDPR e leis setoriais. Após esta fotografia, é possível identificar o que é preciso ser feito para atingir a conformidade. Isso pode incluir a revisão de processos, elaboração de políticas, revisão de contratos, indicação de times de supervisão, além de aplicação de

metodologias de proteção de dados desde a concepção, conhecida como *privacy by design*.

Além disso, é possível encarar a adequação, a conformidade com a LGPD como um grande diferencial competitivo, uma vez que uma das possíveis consequências do processo é o fortalecimento da confiança do titular dos dados com o ente que os trata. Isso pode acarretar uma melhora na reputação e na imagem da empresa perante o mercado e do ente público perante a sociedade.

Diante de tudo isso, é possível afirmar que a Lei Geral de Proteção de Dados, assim como a GDPR, terá um impacto na sociedade como um todo como poucas leis antes tiveram, devido a sua natureza horizontal e transversal. Importante sempre lembrar que ao mesmo tempo que a lei visa garantir ao titular, uma proteção maior no uso de seus dados pessoais, ela visa, também, fomentar o desenvolvimento econômico, tecnológica e a inovação. Tais prismas devem orientar a interpretação de lei por completo. Somente desta forma a vontade do legislador, e da sociedade, serão alcançadas.

.....
[196. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 65 \(Redação dada pela MP 869/18\). Vale lembrar que, no que se refere à ANPD, a Lei somente entrará em vigor no dia 28 de dezembro de 2018.](#)



Sobre Baptista Luz Advogados

Com mais de uma década de atuação, nossa especialidade é apresentar soluções efetivas e ideias inovadoras para as questões jurídicas de nossos clientes, parceiros e empreendedores.

Com profissionalismo e experiência, nosso escritório oferece assessoria legal de alta qualidade por meio de atendimento personalizado, em que o cliente recebe todo o suporte necessário com precisão e clareza.

Siga-nos nas redes sociais



BRASIL

São Paulo

Rua Ramos Batista, 444 / 2º Andar
Vila Olímpia / São Paulo / SP / Brasil
tel +55 11 3049 7950

Florianópolis

Rodovia SC 401, Km 4 / Saco Grande /
Florianópolis / SC
tel +55 48 3036 0294

Londrina

Rua Ayrton Senna da Silva, 300 /
Sala 1801, Torre 1 / Gleba Palhano
Londrina / PR
tel +55 43 3367 7050

USA

Miami

78 SW 7th Street Suite 500
Miami / FL 33130 / US
tel +1 (786) 622 2002

Acesse nosso site:
en.baptistaluz.com.br

