março de 2021

Diagnóstico

# Proteção de dados no Brasil

## LGPD: desafios e oportunidades para organizações atuantes no Brasil e Reino Unido


**Autora:** Clarissa Luz

**Colaboradora:** Júlia Ribeiro


Elaborado em parceria entre:

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

FELSBERG ADVOGADOS

# PREFÁCIO

## Por Peter Wilson, British Ambassador to Brazil

A agenda de proteção de dados é extremamente importante para o futuro da cooperação internacional. No contexto atual, a medida em que mais empresas e pessoas se encontram inseridas na produção e processamento de dados, precisamos garantir princípios claros, adequados e transparentes para que todos os envolvidos estejam seguros. Em 2018, o Reino Unido aprovou o Data Protection Act para definir a implementação da General Data Protection Regulation (GDPR), com base na diretriz europeia. Esse foi o marco de um longo processo de adequação interno, que ainda está em andamento e inclui também a discussão sobre o intercâmbio de dados entre países.

Em nossa experiência, a proteção de dados é uma agenda em constante evolução. Certamente não subestimamos esses desafios. 37% das empresas do Reino Unido relataram um incidente de violação de dados a nossa autoridade nacional de proteção de dados, o Information Commissioner's Office (ICO), nos últimos 12 meses.

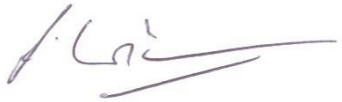
Isso, é claro, está intimamente ligado a questões de segurança cibernética. Uma pequena empresa no Reino Unido é hackeada com sucesso a cada 19 segundos. Cerca de 65.000 tentativas de hackear pequenas e médias empresas (SMBs) ocorrem no Reino Unido todos os dias, cerca de 4.500 das quais são bem-sucedidas.

No Brasil, a legislação de proteção de dados entrou em vigor em 2020, e agora passa por um processo interno de discussão e implementação da legislação. Ainda há um longo caminho pela frente, mas com a instituição da Autoridade Nacional de Proteção de Dados, ANPD, o país tem tudo para estabelecer bases sólidas para uma legislação que proteja os cidadãos e abra portas para parceiros internacionais.

Para apoiar esse processo, temos o orgulho de apresentar este Relatório, financiado pelo governo Britânico em colaboração com a Felsberg Advogados. Nesse documento, é possível acessar as interfaces entre a legislação britânica e a brasileira. Procuramos entender a base legal nacional e internacional para explorar como podemos nos unir para vencer esses desafios.

Tudo isso destaca a importância de aprender uns com os outros e esperamos que o Relatório seja útil para apoiar o Brasil na jornada de adequação à LGPD, além de abrir as portas para o diálogo e troca de experiências com o Reino Unido, reforçando nossa parceria histórica.

Agradeço a todos que colaboraram com esse projeto. À medida que o Brasil continua sua jornada na construção de sua cultura de proteção de dados, esperamos apoiar a promoção de padrões mínimos para um ambiente propício para cidadãos, governo e empresas.



**Peter Wilson**
British Ambassador to Brazil

# Sumário Executivo

O objetivo deste documento é apontar desafios e oportunidades gerados no mercado brasileiro no contexto, notadamente, da nova Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, em vigência desde 18 de setembro de 2020. Esta lei impõe uma nova cultura de proteção a dados pessoais no Brasil e se aplica a quaisquer modelos de negócio ou estruturas que utilizem, ou meramente tenham acesso, a dados pessoais, sejam estes de clientes, parceiros de negócios, prestadores de serviços ou colaboradores.

Inicialmente, trazemos breve levantamento sobre as leis brasileiras no campo da privacidade e proteção de dados pessoais. Em seguida, são apresentados os principais conceitos e aspectos gerais da LGPD e realizada uma análise comparativa entre os critérios legais para o uso de dados por empresas privadas e pelo poder público.

Os impactos da LGPD nas atividades realizadas pelas diferentes áreas de uma empresa, como marketing, recursos humanos e financeiro, são abordados de maneira a facilitar a compreensão das medidas técnicas e administrativas necessárias à conformidade com a referida Lei, em especial tendo em vista os seus principais pilares, a saber, governança corporativa, jurídico e segurança da informação.

O procedimento de adequação à lei não é uma estrada finita, ao contrário, deve ser revisitado para a sua manutenção e correto gerenciamento de riscos. Contudo, isto não significa que as medidas a serem adotadas serão complexas, podendo consistir em atos pontuais, resumidos sempre à real necessidade da organização. Até mesmo porque a ANPD ainda deverá trazer diretrizes para a correta interpretação da LGPD, uma lei genérica e com cláusulas abertas.

As diferenças e aspectos basilares da lei brasileira são analisadas comparativamente à GDPR (Regulamento Geral de Proteção de Dados da União Europeia). Do ponto de vista prático, e para facilitar o *compliance*, demonstramos alguns dos principais ajustes para que empresas já adequadas à GDPR (a exemplo de multinacionais e empresas do Reino Unido ou da União Europeia) tenham um direcional definido sobre quais medidas adotar, objetivamente, para a adaptação de seus procedimentos e estruturas à lei brasileira.

Por fim, o Relatório assinala desafios e oportunidades de mercado gerados a partir de todo o cenário legislativo e de negócios, levantado ao longo deste estudo.

O conteúdo deste documento objetiva auxiliar interessados nos regulamentos de proteção de dados, inclusive profissionais da área, e estruturas corporativas de toda ordem, sejam elas de pequeno, médio ou grande porte, startups, fundações, associações, multinacionais, empresas públicas ou estrangeiras, atuantes no Brasil ou com interesse em oferecer serviços ou produtos neste território.

# Glossário

**ANPD:** Autoridade Nacional de Proteção de Dados do Brasil
**API:** Application Programming Interface
**CNSP:** Conselho Nacional de Seguros Privados
**DPIA:** Data Protection Impact Assessment / Relatório de Impacto de Proteção de Dados (RIPD)
**DPO:** Data Protection Officer / Encarregado pelo Tratamento de Dados Pessoais
**EDPB:** European Data Protection Board
**GDPR:** General Data Protection Regulation of the European Union, (EU)2016/679
**IAPP:** International Association of Privacy Professionals
**IBGE:** Instituto Brasileiro de Geografia e Estatística
**ICO:** Information Commissioner's Office (autoridade de proteção de dados do Reino Unido)
**IGA:** Intra-Group Agreement
**IP:** Protocolo de Internet
**ISO:** International Organization for Standardization
**LGPD:** Lei Geral de Proteção de Dados Pessoais do Brasil, a Lei nº 13.709/2018
**LIA:** Legitimate Interest Assessment / Análise de Legítimo Interesse
**MPDFT:** Ministério Público do Distrito Federal e Territórios
**MPMG:** Ministério Público de Minas Gerais
**OCDE:** Organization for Economic Co-operation and Development
**TISS:** Troca de Informações sobre Seguros de Saúde
**PEC:** Proposta de Emenda à Constituição Federal
**PIA:** Privacy Impact Assessment
**PIX:** sigla usada para definir a política de pagamento instantâneo do BACEN
**PMO:** Project Management Officer
**PROCON:** Programa de Proteção e Defesa do Consumidor
**RIPD:** Relatório de Impacto de Proteção de Dados / Data Protection Impact Assessment (DPIA)
**RoPA:** Record of Processing Activities / Registro dos Processos de Tratamento de Dados Pessoais
**SCC:** Standard Contractual Clauses / Cláusulas Contratuais Padrão
**SENACON:** Secretaria Nacional do Consumidor
**STF:** Supremo Tribunal Federal do Brasil
**STJ:** Superior Tribunal de Justiça do Brasil
**SUSEP:** Superintendência de Seguros Privados
**TJDFT:** Tribunal de Justiça do Distrito Federal e Territórios
**TJMG:** Tribunal de Justiça de Minas Gerais
**TJRJ:** Tribunal de Justiça do Rio de Janeiro
**TJRN:** Tribunal de Justiça do Rio Grande do Norte
**TJSP:** Tribunal de Justiça de São Paulo
**TRT2:** Tribunal Regional do Trabalho da 2ª Região
**TRT3:** Tribunal Regional do Trabalho da 3ª Região
**TRT4:** Tribunal Regional do Trabalho da 4ª Região

# Índice

# 1. Introdução

Dados pessoais podem ser considerados a base para a maioria dos modelos de negócio, porém a forma como as empresas utilizam-nos tem acumulado polêmicas. Justamente pensando em regulamentar o tratamento justo e necessário de dados pessoais, em ambiente físico e online, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, adiante "LGPD") tramitou por oito anos em nosso Legislativo.

Referido diploma legal dispõe que o indivíduo tem o direito à proteção dos seus dados pessoais e tem verdadeiro controle sobre os seus dados pessoais, o que é chamado de *autodeterminação informativa*, ou seja, quais dados circulam a seu respeito e com que finalidade. Seu objetivo, dentre outros, consiste na criação de um cenário de segurança jurídica, com a padronização de normas e práticas para promover a proteção de dados pessoais de todo indivíduo localizado no território brasileiro.

Nesse novo contexto cultural de proteção à privacidade e de oportunidades de mercado, Felsberg Advogados elaborou o presente estudo, por meio de uma análise diagnóstica da legislação e do ecossistema de proteção de dados no Brasil, com foco nos seguintes elementos:

**(i)** **Proteção de Dados no Brasil**: levantamento do atual conjunto de normas brasileiras relacionadas à privacidade e proteção de dados pessoais, em especial nas áreas relevantes de atuação do Governo Britânico; breve síntese dos conceitos e características da LGPD, bem como análise da aplicação da LGPD aos entes federativos do Brasil; e destaques para decisões judiciais brasileiras mais relevantes;

**(ii)** **Implementação da LGPD:** impactos da LGPD em empresas privadas e públicas (como se adequar, duração do procedimento, paralelo à experiência do Reino Unido com a GDPR); medidas de adequação de empresas no Brasil à LGPD; e análise da capacidade e do estágio atual de maturidade das instituições públicas e privadas de segmentos relevantes do mercado, tendo em vista estudos já publicados e o panorama traçado na União Europeia após mais de dois anos da GDPR;

**(iii)** **Comparação entre a GDPR e a LGPD**: comparativo entre a LGPD (Lei Geral de Proteção de Dados) e a GDPR (Regulamento Geral de Proteção de Dados da União Europeia/Reino Unido); e adaptação à LGPD por empresas adequadas à GDPR, bem como efeitos da LGPD nas relações comerciais Brasil-Reino Unido; e

**(iv)** **Desafios e Oportunidades de Mercado:** levantamento e análise das oportunidades de mercado geradas pelos desafios na adequação à LGPD, com foco em possibilidades para a atuação de pessoas e empresas que também operam no Reino Unido.

Os pontos acima serão abordados de forma detalhada a seguir, com o objetivo principal de traçar um relatório diagnóstico sobre os mais relevantes impactos, status atual e expectativa de duração de um procedimento de conformidade à LGPD tendo como plano de fundo os desafios e oportunidades de uma nova cultura à proteção de dados e privacidade, imposta pela legislação atual.

# 2. Proteção de Dados no Brasil

## 2.1. Leis e regulamentos brasileiros relacionados à privacidade e proteção de dados pessoais

No ordenamento brasileiro, antes mesmo da entrada em vigor da LGPD, já havia mais de quarenta dispositivos legais, em normas esparsas, que de alguma forma previam a proteção à privacidade ou critérios para o tratamento de dados pessoais. Como tais normas não eram aplicáveis a todas as pessoas ou a toda natureza de tratamento de dados pessoais, a Lei Geral teve como um dos principais motivos a necessidade de se estabelecer uma norma específica e detalhada sobre o tema de privacidade e proteção de dados, aplicável aos diversos setores, respeitando-se as adequações necessárias à realidade de cada um destes.

Algumas das normas esparsas editadas anteriormente à LGPD encontram-se nos seguintes diplomas legais:

(A) Constituição Federal da República Federativa do Brasil [“Constituição Federal”];
(B) Código Civil brasileiro [Lei nº 10.406/2002 – “Código Civil”];
(C) Código de Defesa do Consumidor [Lei nº 8.078/1990 – “Código de Defesa do Consumidor”];
(D) Marco Civil da Internet [Lei nº 12.965/2014 – “Marco Civil da Internet”];
(E) Código Penal [Decreto-Lei nº 2.848/1940 – “Código Penal”];
(F) regulamentações da Superintendência de Seguros Privados [“SUSEP”] e do Conselho Nacional de Seguros Privados [“CNSP”];
(G) regulamentações para Fintechs, Instituições Financeiras e Meios de Pagamento, inclusive do Banco Central do Brasil [“Banco Central”] e Conselho Monetário Nacional;
(H) regulamentações do Conselho Federal de Medicina, e
(I) resoluções da Agência Nacional da Saúde Suplementar (“Agência Nacional de Saúde”).

A linha do tempo abaixo demonstra a crescente preocupação com a questões de privacidade e/ou proteção a dados pessoais:

## 2.2. LGPD no Brasil

É importante esclarecer que o presente Capítulo não visa trazer todas as características e conceitos da LGPD de maneira exaustiva, tampouco entrar em detalhes sobre a aplicação da LGPD, uma vez que são assuntos tratados em outros tópicos do presente Relatório. Assim, neste Capítulo serão tratadas exclusivamente algumas das principais características da LGPD.

### 2.2.1. Conceitos Gerais da LGPD

Primeiramente, é importante destacar que a LGPD é uma norma principiológica, e não procedimental, o que significa que um dos elementos fundamentais da referida norma são os conceitos por ela definidos.

Nesse sentido, a LGPD estabelece o conceito de dados pessoais, lista as bases legais que autorizam o seu uso, indica os princípios gerais da norma, os principais direitos do titular dos dados pessoais (como acesso, exclusão dos dados e explicação sobre o uso), obrigações e limites para a utilização de tais dados, seja como insumo do modelo de negócio da empresa que coletar ou receber os dados pessoais, seja para atividades relacionadas a seus colaboradores.

Assim, listamos abaixo os principais conceitos estabelecidos pela LGPD, que são fundamentais para a melhor compreensão da referida norma.

#### A. Dados Pessoais e Sensíveis

Como objeto central da LGPD, a delimitação conceitual do que são dados pessoais e dados sensíveis é fundamental para entender o alcance da norma.

O conceito de dados pessoais estabelecido na Lei é expansivo e bastante abrangente, pois inclui informações relacionadas a pessoas físicas (jamais de pessoas jurídicas) *identificadas* ou *identificáveis*. Disso pode-se extrair que (i) dados de pessoas jurídicas não são tutelados pela LGPD, gozando a pessoa jurídica apenas das proteções previstas nas normas esparsas eventualmente aplicáveis à ela (por exemplo, a proteção ao nome, conforme visto no Capítulo 2.1); (ii) será considerado pessoal o dado que, isoladamente ou agregado a outro, permitir a identificação de uma pessoa ou sujeitá-la a determinado estudo de comportamento ou perfil.

Para ajudar na compreensão do termo “dados pessoais”, listamos algumas dessas informações a seguir:

- **dados pessoais:** incluem nome, estado civil, profissão, data de nascimento, CPF, documentos de identidade, endereço, telefone, dados bancários e financeiros, senhas, geolocalização, endereços de e-mails, números de IP, identificação digital, registros de conexão e acesso, cookies, dados para definição de perfil comportamental ou padrões de consumo, entre outros[1]. Também estão englobadas neste conceito as informações pessoais às quais se atribuem técnicas de pseudonimização, conforme definição mais adiante.

Além dos dados pessoais, a Lei define uma outra categoria de informações pessoais considerada especial, para as quais delimita critérios específicos de segurança e tratamento:

- **dados pessoais sensíveis:** são uma categoria especial de informações, para a qual são delimitados critérios específicos de segurança e tratamento. Isso ocorre porque essas informações são capazes de acarretar práticas discriminatórias aos titulares, tais como

[1] Conforme artigos 5º, I, e 12, § 2º da LGPD.

características de saúde, mental, biológica, física, fisiológica, genética, econômicas, culturais, convicções religiosas, filosóficas, morais, políticas, condições e aspectos de rotina e vida, orientação e identificação sexual[2]. O tratamento destes dados acarreta maior risco de alegações por violação legal ou ética.

Por outro lado, existem técnicas que são empregadas de forma a mascarar ou impedir a identificação do titular dos dados. Trata-se de tentativa de diminuição dos riscos de exposição dos dados pessoais ou sensíveis. Se tal técnica permitir a reidentificação do titular dos dados, será uma pseudonimização e a informação ainda estará dentro do escopo de aplicação da LGPD, mantendo-se na categoria de dado pessoal. Caso o dado seja alterado de forma a impedir, de fato, a possibilidade de reidentificação do titular, será um processo de anonimização e a informação perderá a natureza de dado pessoal. A seguir, trazemos mais detalhes a respeito destas duas técnicas:

- **pseudonimização:** dados pseudonimizados ainda são considerados dados pessoais pela Lei. Trata-se de dados que passaram por um processo pelo qual a informação perde a possibilidade de associação, direta ou indireta, a um indivíduo, entretanto, a identificação do indivíduo continua possível pela utilização de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Ou seja, os dados pseudonimizados permanecem dentro do escopo de aplicação da lei, porque há possibilidade do controlador reidentificar o titular por meio do recurso por ele utilizado para "mascarar" a identidade do indivíduo perante terceiros[3]. Assim, dados pseudonimizados permanecem no conceito de dados pessoais.

- **anonimização**: os chamados dados anonimizados passam por técnica que exclui permanentemente seus caracteres identificáveis e impedem a identificação do titular definitivamente, de modo que não mais estarão no escopo de aplicação da LGPD. Portanto, dados anonimizados não são dados pessoais.

Importante destacar que os dados efetivamente anonimizados podem tornar as informações neles contidas imprestáveis, razão pela qual muitas empresas optam por aplicar a técnica de pseudonimização e sujeitarem-se à aplicação da LGPD, que, inclusive, sugere esta técnica para maior segurança da informação tratada[4]. Além disso, a doutrina tem desmistificado há alguns anos a anonimização robusta, ao considerar a crescente possibilidade de reidentificação por ao complementar dados anonimizados com outras informações disponíveis[5]. A diferenciação entre dados *identificados* e *identificáveis*[6], pseudonimizados e anonimizados vem se tornando tarefa cada vez mais árdua, em especial no contexto da chamada "Big Data", consistente no grande volume e variedade de dados. Portanto, a análise do que será considerado dado pessoal deve ser realizada de acordo com o caso específico e tendo em vista a vasta gama de informações públicas disponíveis.

[2] Conforme artigo 5º, II, da LGPD.
[3] Conforme artigo 13, § 4º, da LGPD.
[4] A técnica de anonimização suficiente a excluir os dados do escopo de aplicação da LGPD depende de análise conforme o caso específico e contexto (ver, a este respeito, a opinião do Conselho da Europa, Data Protection Article 29 Working Party — WP29 05/2014. Opinion 5/2014 on Anonymization Techniques. Bruxelas: [s.n.], 2014, p. 6-7. Disponível em: <https://goo.gl/0FQC8c>. Acessado em 15 de novembro de 2020.). O estudo do ICO de novembro de 2012 ajuda a tomar decisões práticas a respeito das técnicas de anonimização, disponível em <https://ico.org.uk/media/1061/anonymisation-code.pdf>. Acessado em 15 de novembro de 2020.
[5] BIONI, Bruno R., *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas*. SP, 2015. p. 74.
[6] Daniel Solove e Paul Schwartz tratam da importância da análise diferenciada sobre cada um desses conceitos, *in verbis*: "an *identifiable* individual when specific identification, while possible, is not a significantly probable event, but there is nonetheless some non-remote possibility of future identification. The risk level for such information is low to moderate. (…) Such nominally identifiable data should be treated the same as identified data.". (SCHWARTZ, Paul M., SOLOVE, Daniel. *The PII problem: Privacy and a New Concept of Personality*. EUA, 2014).

### B. Tratamento de Dados

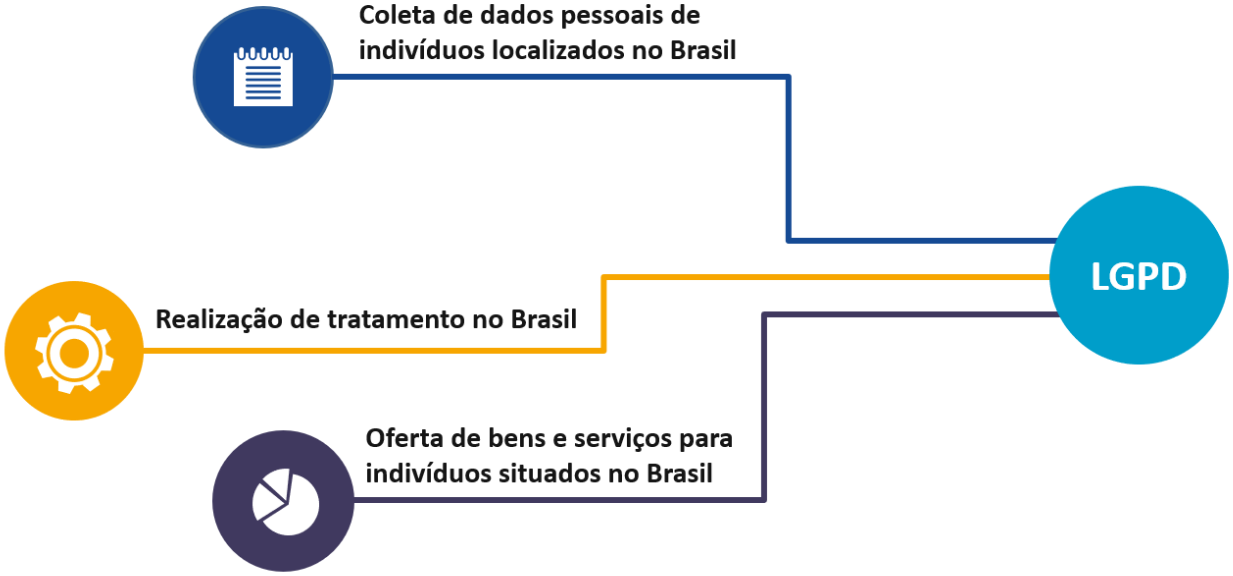
O tratamento, por sua vez, é definido como qualquer tipo de processamento de dados pessoal, indicado em um rol não taxativo[7] da Lei que inclui mais de vinte verbos, a exemplo de coleta, uso, armazenamento, compartilhamento e transferência. A LGPD, portanto, é aplicável a quaisquer dessas inúmeras atividades de tratamento de dados pessoais ou sensíveis, sejam realizadas no contexto profissional ou comercial por pessoas jurídicas ou físicas, de direito público ou privado, em meio digital ou físico (online ou offline).

### C. Escopo de Aplicação

Quanto ao escopo de aplicação, a LGPD define as situações específicas dos tratamentos que devem cumprir seus dispositivos legais[8], a saber:

- atividades de tratamento realizadas no território brasileiro;
- atividades de tratamento que ofereçam bens ou serviços a indivíduos localizados no território brasileiro (ainda que a sede da empresa esteja situada fora do Brasil), e
- as atividades de tratamento de dados pessoais que tenham sido coletados no Brasil.

Ou seja, a LGPD é aplicável nas hipóteses identificadas no esquema gráfico a seguir:




### D. Rede Atuante no Tratamento: Agentes (Controlador e Operador), Titular, DPO e ANPD

O quadro a seguir ilustra a rede atuante no tratamento de dados:

[7] Conforme artigo 5º, X, da LGPD.
[8] Conforme o artigo 3º da LGPD.


De acordo com a norma, há dois agentes na relação de tratamento de dados incluídos na cadeia de responsabilidades, quais sejam[9]:

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões sobre os *meios* e *finalidades* para as quais os dados são tratados; e

- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador deverá agir sempre de acordo com o quanto contratado, ou será responsabilizado.

Em relação à responsabilidade dos agentes de tratamento, a LGPD prevê a responsabilidade solidária dos agentes envolvidos no tratamento de dados em casos de incidente de segurança da informação, uso indevido ou em excesso, acesso por terceiro não autorizado, ou outros atos em violação à lei.

A LGPD determina, ainda, que (i) "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo"[10]; (ii) o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador[11]; e (iii) os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente[12].

Considerando os riscos da responsabilização solidária, é de suma importância a celebração de contratos formais entre esses agentes com a adição de cláusulas de proteção de dados; para os contratos celebrados antes da lei, deve-se adotar aditivos contratuais para a inclusão dessas cláusulas. Na contratação entre os agentes, devem ser consignadas as obrigações de segurança e medidas técnicas e administrativas a serem adotadas, sendo que, em geral, garante-se ao controlador o direito de realizar auditoria técnica em relação ao operador para confirmar se os critérios determinados no contrato estão sendo cumpridos. Tais precauções poderão isentar o controlador de responsabilidades ou facilitar eventual ação de regresso (ou seja, direito do controlador de exigir ao operador que o indenize pelos danos experimentados) caso o

[9] Conforme artigo 5º, VI, VII e IX, da LGPD.
[10] Conforme artigo 42 da LGPD.
[11] Conforme artigo 42, parágrafo primeiro, I, da LGPD.
[12] Conforme artigo 42, parágrafo primeiro, II, da LGPD.

operador viole as premissas relacionadas aos dados tratados com base no contrato celebrado entre essas partes.

Além dos agentes, a LGPD prevê a participação de outras figuras no fluxo de tratamento de dados pessoais, quais sejam:

- **Titular dos dados pessoais:** pessoa física a quem se referem os dados pessoais objeto do tratamento. Vale ressaltar que, apesar da LGPD não se aplicar a dados relativos a pessoas jurídicas, tais como CNPJ, nome da empresa, telefone da empresa, a empresa terá acesso a dados de contato de seus próprios funcionários e de representantes dessas pessoas jurídicas, tais como nome, e-mail de contato e logs de acesso a algum sistema da empresa, portanto até mesmo empresas B2B (*business to business*), ou seja, que possuem como clientes apenas PJs, também deverão se adequar à LGPD;

- **Encarregado pelo Tratamento de Dados Pessoais (denominado na GDPR como "DPO" - *Data Protection Officer*):** pessoa física ou jurídica indicada, obrigatoriamente, pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (conforme definida abaixo)[13]. Sua identidade deverá ser divulgada publicamente, preferencialmente no site do controlador. A LGPD não determinou quais serão as prerrogativas do DPO, mas apenas quatro atividades que lhe cabem, a seguir expostas: (i) aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares[14]. A doutrina, seguindo a linha da GDPR, vem construindo a interpretação de que o DPO deverá ter independência funcional e alçada para tomar decisões dentro da estrutura da empresa.

- **Autoridade Nacional de Proteção de Dados ("ANPD"):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional[15]. A ANPD poderá solicitar ao controlador relatório de impacto à proteção de dados quando o tratamento se fundamentar no interesse legítimo[16], a ser elaborado durante o processo de adequação à LGPD, quando necessário.

## 2.2.2. Características Gerais da LGPD

### A. Princípios legais

Por ser uma lei principiológica e não procedimental, os dez princípios elencados no artigo 6º fazem parte dos pilares da LGPD e devem orientar qualquer operação realizada com dados pessoais, de modo que todos os seguintes princípios devem ser sempre e concomitantemente observados:

[13] Conforme artigo 5º, VIII, da LGPD.
[14] Conforme artigo 41, §2º, da LGPD.
[15] Conforme artigo 5º, XIX, da LGPD.
[16] Conforme artigo 10, §3º, da LGPD.

| Princípios legais - LGPD | |
|---|---|
| **Princípio da Finalidade** | O tratamento de dados pessoais deve atender a propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado o tratamento posterior de forma incompatível com essas finalidades. |
| **Princípio da Adequação** | O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular. |
| **Princípio da Necessidade** | O tratamento de dados pessoais deverá ser limitado ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular, garantindo também que tais informações sejam armazenadas pelo menor tempo possível. |
| **Princípio do Livre Acesso** | Aos titulares deverá ser garantida a consulta facilitada e gratuita quanto à forma e à duração do tratamento, bem como a integralidade de seus dados pessoais; |
| **Princípio da Qualidade dos Dados** | Aos titulares deverá ser garantida a exatidão, a clareza, a relevância e a atualização dos dados pessoais. |
| **Princípio da Transparência** | As informações sobre o tratamento e atuação do controlador e/ou operador devem ser claras, precisas e facilmente acessíveis, respeitados os segredos comercial e industrial. |
| **Princípio da Segurança** | Os agentes de tratamento devem adotar medidas técnicas e organizacionais aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. |
| **Princípio da Prevenção** | Devem ser adotadas medidas técnicas e organizacionais a fim de prevenir a ocorrência de danos envolvendo dados pessoais. |
| **Princípio da Não Discriminação** | As atividades de tratamento de dados pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos. |
| **Princípio da Responsabilização e Prestação de Contas** | Os agentes de tratamento devem armazenar os registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados, comprovando sua eficácia e eficiência. |

### B. Bases legais autorizadoras do tratamento

Atendidos os dez princípios supra citados, observe-se que o tratamento de dados pessoais deverá ser justificado em uma das dez bases legais dispostas no art. 7º (para dados pessoais) e/ou em uma das oito bases legais do art. 11 (para dados pessoais sensíveis, identificadas no rol a seguir com um asterisco*). Destacamos que o consentimento é apenas uma dessas bases legais, inexistindo qualquer critério de

hierarquia entre as hipóteses a seguir. Somente será lícito o tratamento e sua respectiva finalidade se devidamente enquadrados em uma dessas hipóteses autorizadoras:

| Bases legais autorizadoras do tratamento - LGPD | |
|---|---|
| **Consentimento** | É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O uso dessa hipótese deve ser observado com especial atenção, uma vez que há possibilidade de revogação a qualquer tempo pelo titular. No caso de consentimentos para dados sensíveis, este deverá ser, ainda, específico e destacado do consentimento geral. Além disso, enquanto o consentimento referente a dados de crianças (consideradas assim aquelas de até 12 (doze) anos incompletos, conforme Estatuto da Criança e do Adolescente do Brasil) deve ser concedido por um dos pais ou responsável legal, maiores de 12 (doze) anos poderão consentir, desde que entendam do que se trata o termo de consentimento. Por essa razão o documento deve ser dotado de linguagem clara e acessível. |
| **Cumprimento de obrigação legal ou regulatória** | Caso exista uma previsão legal expressa ou contida em regulamento específico, que determine ou autorize o tratamento de dados pessoais, esta hipótese poderá ser utilizada pelo controlador/operador para justificar o processamento ou armazenamento de dados pessoais. Ainda assim, o controlador deverá respeitar o princípio da transparência e comunicar ao titular se seus dados serão compartilhados com órgãos controladores, para fins de cumprimento da(s) obrigação(ões) legal(is) ou regulatória(s) em questão. |
| **Execução de políticas públicas** | A administração pública, para fins de execução de políticas públicas, poderá realizar o tratamento e o compartilhamento de dados, prevalecendo assim o interesse público sobre o privado. |
| **Realização de estudos por órgão de pesquisa** | De modo consistente com os fundamentos da LGPD, em especial os que se relacionam à liberdade de expressão, de informação, de comunicação e de opinião, bem como o desenvolvimento tecnológico e a inovação, a realização de estudos por órgãos de pesquisa é uma das bases legais para o tratamento de dados pessoais. |
| **Execução contratual** | Justificará o tratamento quando o processamento dos dados pessoais for necessário para a execução do contrato (como dados de prestadores de serviços) ou, ainda, se os dados pessoais forem necessários para a execução de procedimentos preliminares ao contrato (a exemplo de informações pessoais de um currículo de candidato. |
| **Exercício regular de direitos em processo judicial, administrativo ou arbitral** | O tratamento de dados pessoais também é lícito, no caso de finalidade do exercício regular de direitos em processo judicial, administrativo ou arbitral. Esta hipótese tem especial importância em nosso país, pois há um excesso de leis e regulamentos, além de extrema judicialização, portanto grande parte das atividades realizadas com dados pessoais se utilizará desta hipótese para o armazenamento de dados por tempo superior ao término da relação com o titular. |
| **Proteção da vida ou da incolumidade física** | Quando o tratamento de dados tiver por finalidade proteger a vida ou a incolumidade física do próprio titular ou de terceiro não haverá necessidade de obtenção de consentimento para a realização do tratamento. Esta hipótese poderá ser empregada, por exemplo, em casos de dados específicos de saúde dos funcionários da empresa, se minimizados e em respeito à finalidade. |
| **Tutela da saúde** | Esta hipótese é aplicada pelos profissionais de saúde, entidades sanitárias e empresas do setor de saúde suplementar. |
| **Legítimo interesse** | Poderá ser utilizado se as hipóteses previstas nos itens “ii”, “v” ou “vi” acima não forem aplicáveis. A LGPD não estabeleceu quais seriam esses “interesses legítimos”, por isso determinou o limite em respeito aos direitos e liberdades fundamentais do titular, que deverão sempre prevalecer. Sendo assim, este tratamento deve ser realizado somente se estritamente necessário e proporcional (ou |

| | |
|---|---|
| | seja, deve ser feito o teste de proporcionalidade). A empresa deverá, obrigatoriamente, elaborar um documento denominado Análise de Legítimo Interesse (denominado na União Europeia como Legitimate Interest Assessment, ou "LIA"). A LGPD não traz maiores explicações sobre esta base legal, porém é possível que as diretrizes europeias guiem a sua interpretação no Brasil enquanto a ANPD não regulamenta a matéria. A este respeito, cabe destacar que a LGPD possibilitar expressamente o uso do legítimo interesse como base autorizadora para apoio e promoção das atividades do controlador, sendo possível a sua aplicação para fins de marketing. |
| **Proteção ao Crédito** | O tratamento de dados pessoais para fins de proteção do crédito é possível e amplamente utilizado por instituições financeiras. Como o Código de Defesa do Consumidor já prevê a possibilidade de criação de banco de dados e cadastros de consumidores para esta finalidade, já era utilizado para justificar o tratamento de acordo com esta finalidade. Contudo, passa a ter maior aplicação e utilidade para empresas que tratam dados de indivíduos que não são seus consumidores diretos, para este mesmo fim. |
| **Fraude** | Aplicável apenas a dados sensíveis. Trata-se de base legal autorizadora do tratamento dessas informações de categoria especial somente quando indispensável para garantir a prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. |

O correto entendimento das possíveis bases legais para o tratamento de dados pessoais é importante não só para a formação da cultura de privacidade e proteção aos dados, mas também pela necessidade e obrigatoriedade do registro de toda e qualquer operação de tratamento pela empresa, requisito este explorado no Capítulo 4 abaixo no contexto das medidas de adequação à LGPD.

### C. Direitos dos titulares de dados

A LGPD garante, ainda, novos direitos aos titulares de dados, que deverão ter suas solicitações respondidas pelos controladores dos dados pessoais no prazo legal de 15 (quinze) dias. O operador deverá cooperar com o controlador, bem como informá-lo se eventualmente receber qualquer solicitação dos titulares, mas não está sujeito a esta obrigação. Tais direitos são[17]:

| Direitos dos titulares de dados - LGPD | |
|---|---|
| **Confirmação da existência de tratamento** | É direito do titular saber se existe o tratamento de seus dados pessoais. |
| **Acesso aos Dados** | Ao titular é garantido acesso a todo e qualquer dado pessoal de sua titularidade que seja tratado pelo agente de tratamento. |
| **Correção de dados incompletos, inexatos ou desatualizados** | Ao titular também é garantida, além do acesso, a correção dos dados pessoais que estejam incompletos, inexatos ou desatualizados. Esse dispositivo é uma ampliação de direito semelhante já previsto no Código de Defesa do Consumidor, conforme explicado no Capítulo 2.1. |

[17] Conforme artigos 17 a 20 da LGPD.

| | |
|---|---|
| **Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD** | Se houver coleta de dados desnecessários, excessivos ou que estejam sendo tratados em desconformidade com as regras definidas na LGPD, o titular poderá solicitar a anonimização, o bloqueio ou a eliminação desses dados. |
| **Portabilidade para outro fornecedor de serviço ou produto** | Garante a portabilidade dos dados para outro fornecedor de serviço ou produto. Para tanto, a Lei exige apenas que o titular formalize a requisição de forma expressa. Atualmente, trata-se de direito com grande dificuldade de concretização, tendo em vista as plataformas diversas utilizadas pelas empresas e a impossibilidade de transferência em formato útil. |
| **Eliminação dos dados tratados com base no consentimento** | O tratamento de dados pessoais pode ser encerrado a pedido expresso do titular. No entanto, este pedido deverá ser analisado pelo agente, pois em muitos casos haverá obrigação legal/regulatória de armazenamento por tempo superior, a exemplo de dados dos colaboradores da empresa para fins de comprovação de recolhimento do FGTS, ou, ainda, de exercício de defesa em futuro processo legal, entre outros. O agente, portanto, deve estar preparado para justificar, com base em seus registros prévios das operações de dados, a possibilidade de retenção e informar o titular a respeito, quando de sua solicitação. |
| **Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados** | O titular pode exigir informações, e o agente deve ter transparência prévia, sobre entidades públicas e privadas com as quais compartilha as informações de tais indivíduos. |
| **Informação sobre a possibilidade de não fornecer consentimento, desde que justificado** | Ao titular devem ser prestadas informações sobre a possibilidade de não fornecer o consentimento para que os seus dados pessoais sejam tratados, bem como das possíveis consequências que advirão de sua recusa. Essa regra reforça o princípio da transparência e autodeterminação informativa, e estabelece um dever de cooperação, na medida em que impõe ao controlador a obrigação de prover informações essenciais para que ocorra uma escolha refletida e consciente do titular dos dados a respeito do fornecimento ou não do consentimento quando esta for a base legal escolhida pela empresa. |
| **Revogação do consentimento** | É direito do titular, mediante requerimento expresso, revogar seu consentimento. Se assim solicitado, o agente deverá obstar qualquer operação relacionada ao uso de tais dados pessoais (por exemplo, envio de comunicações e ações de marketing). Este é um dos motivos pelo qual a base legal do consentimento geralmente é a mais complexa de gerir. |
| **Revisão de decisões automatizadas** | O titular tem o direito de solicitar ao agente de tratamento a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. |

Se o agente não for o controlador, este deverá comunicar tal fato imediatamente ao titular e indicar, sempre que possível, o agente responsável; se for controlador, deverá responder a solicitação em até 15 (quinze) dias com declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial. Para a minimização de riscos e proteção à empresa, é altamente recomendável que os agentes de tratamento armazenem todo o histórico de solicitação.

É importante ressalvar, entretanto, que tais direitos não são absolutos e poderão ser afastados se colidirem com outras garantias, como o sigilo de informações ou segredos comercial e industrial, conforme previsto em lei, ou no caso de obrigações legais de retenção ou necessidade de armazenamento para eventual defesa em processos judiciais, administrativos ou arbitrais, que poderão justificar recusa a pedidos de exclusão dos dados.

### D. Sanções

A LGPD prevê sanções para os casos de descumprimento das normas nela previstas, por meio das disposições do artigo 52, que podem ser aplicadas tanto ao controlador quanto ao operador, considerando a análise do caso concreto. As sanções previstas na LGPD possuem diversos níveis de gravidade, sendo elas:

| | |
|---|---|
| **Advertência** | Advertência, com indicação de prazo para a adoção de medidas corretivas; |
| **Multas** | Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil no último ano, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; |
| | Multa diária, limitada a R$ 50.000.000,00 (cinquenta milhões de reais), como forma de forçar o cumprimento da determinação da ANPD; |
| **Publicização** | Publicização da informação, de modo a dar publicidade e conhecimento público a respeito de alguma violação às normas da LGPD (efeito reputacional); |
| **Bloqueio** | Bloqueio dos dados pessoais a que se refere a infração até a sua regularização, ou seja, uma limitação temporária à atividade de tratamento de dados até que se corrija a infração; e |
| **Eliminação** | Eliminação dos dados pessoais a que se refere a infração, ou seja, a exclusão definitiva dos dados pessoais relacionados à infração. |

Em contrapartida, a LGPD também determina alguns critérios a serem observados pela ANPD antes de decidir a sanção a ser aplicada, o que pode transformar uma possível multa em uma advertência, a depender do caso[18]. Tais critérios incluem a gravidade e natureza das infrações dos direitos afetados, a boa-fé do infrator e medidas adotadas para a minimização dos danos.

### E. Obrigações de Medidas de Segurança.

Por fim, a LGPD estabelece que os agentes devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Deve-se, assim, garantir a segurança eletrônica, manutenção de softwares devidamente atualizados, redes seguras, confidencialidade, integridade, além de disponibilidade imediata das informações pessoais coletadas, caso solicitadas pelo cliente.

Em caso de incidentes de segurança, o controlador deverá comunicar à ANPD e o titular o fato, caso este possa acarretar risco ou dano relevante ao titular dos dados pessoais. Essa comunicação deverá ser realizada em prazo razoável e pelo Encarregado, seguindo o procedimento estabelecido na LGPD.

[18] Conforme artigo 52, parágrafo 1º, da LGPD.

## 2.2.3. Quadro resumo

A fim de facilitar a compreensão das peculiaridades da LGPD já expostas acima, sintetizamos adiante os principais pontos trazidos pela LGPD, que são relevantes para todos os projetos de adequação e, ainda, para a conscientização sobre o tema:

Principais pontos da LGPD:

**Intuito da LGPD**
Proteção aos direitos fundamentais de liberdade e privacidade dos indivíduos (art. 1º). Maior propriedade aos titulares sobre os seus dados pessoais

**ANPD**
A Autoridade Nacional de Proteção de Dados é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional (art. 5º, XIX)

**Incidentes de Segurança**
O controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança, envolvendo dados pessoais, que possa acarretar risco ou dano relevante aos titulares (art. 48)

**Bases Legais**
Além do consentimento, a LGPD traz outras 10 bases legais que autorizam o tratamento de dados pessoais, sem qualquer nível de hierarquia entre elas (art. 7º)

**Dados Sensíveis e de Menores**
A LGPD traz regras criteriosas e bases legais específicas para o tratamento de dados sensíveis, assim como de informações pessoais de crianças e adolescentes (arts. 11 e 14)

**Princípios**
A legislação é principiológica, razão pela qual elenca em seu art. 6º os 10 princípios a serem observados nas operações de tratamento, dentre eles: transparência, finalidade, necessidade e adequação (art. 6º)

**Aplicabilidade da LGPD**
Qualquer operação de tratamento independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que atendidos os requisitos dos incisos I, II e III do art. 3º

**RIPD**
A ANPD poderá determinar ao controlador que elabore um relatório de impacto (RIPD), inclusive sobre operações realizadas com dados sensíveis, observados os segredos comercial e industrial (art. 38)

**Sanções**
As sanções administrativas previstas na LGPD incluem multa de até 2% do faturamento anual da PJ, grupo ou conglomerado no Brasil, limitada a R$ 50 milhões por infração (art. 52)

**Mapeamento de Dados**
O art. 37 determina ao controlador e ao operador que mantenham o registro das operações de tratamento de dados pessoais realizadas em sua estrutura, especialmente quando baseadas no legítimo interesse

**Direitos dos Titulares**
A LGPD prevê diversos direitos aos titulares, inclusive acesso, portabilidade, exclusão, revogação do consentimento etc. (art. 18)

**Encarregado / DPO**
A LGPD determina a indicação do Encarregado pelo Tratamento de Dados Pessoais (DPO), que consiste na(s) pessoa(s), física ou jurídica, responsável por ser o elo de comunicação entre controlador, titular e ANPD (art. 41)

## 2.2.4. LGPD e o Poder Público

A previsão de regras para o tratamento de dados pessoais pelo Poder Público foi alvo de grandes discussões quando da construção do projeto de lei que em seguida culminaria na LGPD. Aqueles que defendiam que tal lei não deveria ser aplicável ao Poder Público argumentavam que, para desempenhar suas funções, o Estado e os demais entes da Administração Pública precisam fazer uso massivo de dados pessoais dos cidadãos e, caso houvesse a previsão de novas regras aplicáveis a tal processamento, o Poder Público estaria sujeito a responsabilidades de forma desmedida diante de suas necessidades de processamento.

Entretanto, embora o Estado necessite tratar dados pessoais em larga extensão para executar políticas públicas e cumprir com suas competências ou atribuições legais, visando o interesse público do Estado, chegou-se ao consenso de que o Poder Público não poderia coletar, processar e armazenar indiscriminadamente tamanha base de dados pessoais sem o mínimo de regulação quanto ao seu compartilhamento e eventuais responsabilidades. Assim, a redação final da LGPD acabou por atribuir diversas obrigações ao Poder Público em relação ao tratamento de dados pessoais, conforme melhor explicado abaixo.

### A. Tratamento de Dados Pessoais Pelo Poder Público

O estabelecimento das regras de tratamento de dados pessoais pelas pessoas jurídicas de direito público no cenário da LGPD está intrinsicamente ligada aos preceitos já estabelecidos pela Lei nº 12.527/2011 ("Lei de Acesso à Informação") e das normas esparsas já tratadas no Capítulo 2.1 deste documento.

Neste contexto, a LGPD primeiramente determinou quais são as entidades públicas sujeitas às regras, a saber[19]:

(i) os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo (incluindo as Cortes de Contas), e Judiciário e do Ministério Público; e

(ii) as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Há, ainda, a previsão de que o tratamento de dados pessoais feito por tais entidades públicas deverá atender suas respectivas finalidades públicas, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

(i) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e

(ii) seja indicado um Encarregado quando realizarem operações de tratamento de dados pessoais.

Destaca-se que as formas em que serão feitas a publicidade das operações de tratamento mencionadas no item (i) acima serão definidas pela ANPD.

Com relação aos prazos e procedimentos para exercício dos direitos dos titulares dos dados pessoais, ª LGPD traz tratamento diferente daqueles impostos às pessoas jurídicas de direito privado, devendo ser observado o disposto em legislação específica, como a Lei nº 9.507/1997 (Lei do Habeas Data), a Lei nº 9.784/1999 (Lei Geral do Processo Administrativo), e a Lei nº 12.527/2011 (Lei de Acesso à Informação).

A LGPD também determina que as empresas públicas e as sociedades de economia mista que atuarem em regime de concorrência (ou seja, para fins comerciais e/ou mercadológicos) terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado, enquanto aquelas que estiverem operacionalizando

[19] Conforme artigo 23 da LGPD.

políticas públicas, no âmbito de sua execução, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público[20].

Por sua vez, os dados constantes de bases do Poder Público deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vista a facilitar tanto a prestação dos serviços públicos quanto o acesso do público em geral à tais informações[21]. Entende-se por interoperabilidade a característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. No que diz respeito à previsão dos dados estarem estruturados, a LGPD entende que os dados devem estar organizados para serem acessados e tratados com maior eficiência. A forma com que o Poder Público fará isso está amplamente disposto no Decreto nº 10.406 /2019 e na Resolução nº 2/2020, adiante explicadas.

O uso compartilhado de dados pessoais pelo Poder Público também deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados na própria LGPD[22], exceto nas seguintes situações expressamente previstas pela LGPD, nas quais o Poder Público poderá transferir dados pessoais de suas bases para entidades privadas:

(i) casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527/2011 (Lei de Acesso à Informação);

(ii) casos em que os dados forem acessíveis publicamente;

(iii) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; e

(iv) na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Com relação à exceção prevista no item (iii) acima, a despeito de ser possível a transferência, sua utilização para finalidade diversa da original demanda a obtenção de nova base legal de tratamento previstas na LGPD. Além disso, vale ressaltar que tais contratos e convênios deverão ser comunicados à ANPD.

Ainda em relação ao compartilhamento de dados, a LGPD determina que as organizações de direito público só poderão compartilhar ou comunicar dados pessoais a empresas de direito privado mediante consentimento do titular[23], exceto nos seguintes casos:

(i) dispensa de consentimento previstas na LGPD[24];
(ii) uso compartilhado de dados em que será dada publicidade, nos termos a serem estabelecidos pela ANPD; e
(iii) exceções para o compartilhamento de dados explicadas acima.

[20] Conforme artigo 24 da LGPD.
[21] Conforme artigo 25 da LGPD.
[22] Conforme artigo 26 da LGPD.
[23] Conforme artigo 27 da LGPD.
[24] Tais dispensas estão previstas no artigo 7º da LGPD.

É importante destacar, também, que o tratamento de dados pessoais pelo Poder Público, assim como por empresas privadas, independe do consentimento do titular quando for indispensável para a execução de políticas públicas legalmente previstas[25]. Contudo, conforme já explicado acima, esta hipótese não se aplica a empresas públicas e sociedades de economia mista que atuem em regime de concorrência, uma vez que estas têm o mesmo tratamento dispensado às pessoas jurídicas de direito privado.

Em relação à função da ANPD perante o Poder Público, esta poderá (i) solicitar informações sobre o tratamento de dados pessoais às entidades do Poder Público, assim como informações específicas sobre os dados em si; (ii) emitir parecer técnico complementar para garantir o cumprimento da LGPD; (iii) propor diretrizes para correção de violações de dados, quando estas acontecerem por causa de tratamentos de dados pessoais feitos por órgãos públicos[26]; interferir na atuação do Poder Público quando houver infração à LGPD, enviando informe com medidas cabíveis, para solicitar a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para o tratamento de dados pessoais.

Por fim, também caberá à ANPD estabelecer regra específica para as pessoas jurídicas de direito público requererem à ANPD a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional[27].

### B. Quadro Comparativo

Em complemento às regras específicas referentes à aplicação da LGPD ao Poder Público, sintetizamos, abaixo, as principais diferenças da aplicação da LGPD entre o setor privado e público:

| Principais pontos da LGPD: | Aplicação: Setor Privado x Setor Público |
|---|---|
| Conceito de Dados Pessoais e Dados Pessoais Sensíveis | Mesma aplicação. |
| Conceito de Controlador e Operador | Mesma aplicação. |
| Demais Definições | Mesma aplicação. |
| Aplicabilidade dos Princípios | Mesma aplicação. |

[25] Conforme artigo 11, II, b, LGPD.
[26] Conforme artigos 29 e 30 da LGPD.
[27] Conforme artigo 33 da LGPD.

| | |
|---|---|
| **Bases Legais** | Diferença no Setor Público: possibilidade do tratamento e uso compartilhado de dados com base na necessidade à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres[28].<br>Possível aplicação das bases legais referentes à prevenção de fraudes e irregularidades, ou proteção da segurança ou integridade do titular (sem especificação de se tratar de dados sensíveis, o que, espera-se, será regulamentado pela ANPD)[29]. |
| **Tratamento de Dados Sensíveis** | Diferença no Setor Público: aplicação da hipótese de tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis e regulamentos[30]. |
| **Observância dos Direitos dos Titulares** | Mesma aplicação, exceto no que diz respeito ao prazo para atendimento das solicitações dos titulares, conforme abaixo:<br>(i) para o Setor Privado, o atendimento deve ser imediato ou em até 15 (quinze) dias, contado da data do requerimento do titular; e<br>(ii) para o Setor Público: Os prazos e procedimentos para exercício dos direitos do titular observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507/1997 (Lei do Habeas Data), da Lei nº 9.784/1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527/2011 (Lei de Acesso à Informação). |
| **Armazenamento dos dados** | Diferença no Setor Público: os dados deverão ser mantidos em formato interoperável e estruturado para uso compartilhado, conforme previsto em legislações específicas.<br>Por outro lado, no Setor Privado os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso[31] e portabilidade. |
| **Transferência Internacional de Dados** | Diferença no Setor Público: pessoas jurídicas de direito público podem requerer à ANPD a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional[32]. |
| **Indicação de DPO** | Mesma aplicação. |

[28] Previsto no artigo 7º, III, da LGPD.
[29] Previstas no artigo 26, § 1º, da LGPD.
[30] Previsto no artigo 11, II, "b", da LGPD.
[31] Conforme artigo 19, §1º, da LGPD.
[32] Conforme artigo 33 da LGPD.

| | |
|---|---|
| **Notificação de Incidentes** | Mesma aplicação. |

Finalmente, com relação ao poder para legislar sobre matérias atinentes à privacidade e à proteção de dados, vale frisar que a PEC nº 17/2019, em trâmite no Congresso brasileiro, mencionada no item 2.1.A acima,[33] possui entre suas finalidades[34] o escopo de definir como competência privativa da União o poder para legislar sobre tais assuntos.

A tentativa de alteração da Constituição Federal garantiria maior segurança jurídica à aplicação da LGPD de forma a manter unidade e regulamentação uníssona por todos os entes federativos do Brasil, em especial tendo em vista que alguns Municípios, como Vinhedo (Estado de São Paulo)[35] e João Pessoa (Estado da Paraíba), publicaram Leis Municipais com regras específicas sobre o tratamento de dados pessoais[36].

## 2.3. Decisões Judiciais e Aplicações de Multas no Brasil

A ANPD possui a função específica de fiscalizar o cumprimento da LGPD e zelar pela proteção de dados pessoais e privacidade, assim como editar normas e diretrizes para assessorar na interpretação da Lei, tendo sido oficialmente constituída em 6 de novembro de 2020 por meio da publicação de ato Presidencial que nomeou os cinco membros do primeiro Conselho Diretor, inclusive o Diretor-Presidente, dando-se início à estrutura regimental prevista no Decreto nº 10.474/2020. Até a elaboração deste estudo não foram definidos todos os profissionais que ocuparão os demais cargos de sua estrutura; no entanto, seu funcionamento independe desta definição e pode se iniciar a qualquer momento. O site da ANPD, inclusive, já se encontra no ar, podendo ser consultado através do link: https://www.gov.br/anpd/pt-br.

Além disso, não obstante o fato de as sanções administrativas previstas na LGPD[37] terem sua vigência iniciada somente em agosto de 2021, isto não afasta a plena possibilidade de aplicação de multas e indenizações por violação à LGPD, sendo que, nestes casos, tais multas e indenizações serão mensuradas com base em outros diplomas legais, como Código Civil e Código de Defesa do Consumidor.

Nesse sentido, sanções já têm sido aplicadas em decorrência de violações à privacidade ou tratamento indevido de dados pessoais por meio de demandas individuais ajuizadas por titulares de dados, ou a partir de fiscalização por órgãos específicos, a exemplo do Ministério Público, Secretaria Nacional do Consumidor

[33] O andamento da tramitação de referida norma está disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acessado em 16.11.2020.
[34] Conforme Proposta de Emenda à Constituição nº 17/2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=5DF9E8A0C078EABE984D8B72570144DB.proposicoesWebExterno2?codteor=1773684&filename=PEC+17/2019>. Acessado em 16.11.2020.
[35] Lei Complementar (Vinhedo) nº 161/2018 <https://www.legiscompliance.com.br/legislacao/norma/200#:~:text=Disp%C3%B5e%20sobre%20o%20tratamento%20de,privado%20no%20Munic%C3%ADpio%20de%20Vinhedo.&text=DE%2005.07.2018-,Disp%C3%B5e%20sobre%20o%20tratamento%20de%20dados%20pessoais%20por%20pessoa%20jur%C3%ADdica,privado%20no%20Munic%C3%ADpio%20de%20Vinhedo>. Acessado em 17.11.2020.
[36] Lei Municipal nº 13.697/2019 <https://leismunicipais.com.br/a/pb/j/joao-pessoa/lei-ordinaria/2019/1369/13697/lei-ordinaria-n-13697-2019-dispoe-sobre-a-politica-municipal-de-protecao-de-dados-pessoais-e-da-privacidade-no-ambito-da-administracao-publica-direta-no-municipio-de-joao-pessoa-pb-e-da-outras-providencias>. Acessado em 17.11.2020.
[37] Previstos nos artigos 52 e seguintes da LGPD.

("Senacon"), Instituto Brasileiro de Defesa do Consumidor, Programa de Proteção do Consumidor ("Procon"). Os casos de maior relevância no Brasil até o momento são os seguintes:

- **Drogaria Araújo**: um dos casos de maior valor foi a aplicação de multa à Drogaria Araújo em montante superior a R$ 7.000.000,00 (sete milhões de reais). A condenação foi aplicada pelo Procon-MG, órgão integrante do Ministério Público de Minas Gerais (MPMG), em dezembro de 2018. A decisão se baseou nos dispositivos do Código de Defesa do Consumidor ao entender que, ao ter condicionado descontos ao fornecimento do CPF do consumidor no ato da compra sem oferecer informação clara e adequada sobre abertura de cadastro do consumidor, ou seja, sem transparência quanto ao uso dessas informações. Em seguida, no mês de fevereiro de 2019, foi celebrado um Termo de Ajustamento de Conduta entre as partes que impôs diversas obrigações de segurança à Drogaria e dever de informação aos consumidores, em caso de descumprimento ao acordo, a Drogaria Araújo estará sujeita a multa que poderá variar entre R$ 10.000,00 (dez mil reais) e R$ 50.000,00 (cinquenta mil reais);

- **Decolar.com**: em 2018 teve-se conhecimento que a Decolar.com estaria oferecendo reservas a preços diferentes dependendo da localização do consumidor, identificado por intermédio do *Internet Protocolo – IP*, prática conhecida como *geo pricing.* Além disso, a Decolar.com também estaria ocultando a disponibilidade de acomodações a consumidores brasileiros em favor de consumidores estrangeiros, conduta denominada *geo blocking.* Ambas as práticas discriminam consumidores em razão de sua localização geográfica. O Departamento de Proteção e Defesa do Consumidor (DPDC), órgão do Ministério da Justiça, entendeu pela condenação da Decolar.com devido à violação da legislação consumerista, determinando o pagamento de multa no valor de R$7.500.000,00 (sete milhões e quinhentos mil reais) e cessação das atividades condenadas, sob pena de suspensão da atividade e retirada do site do ar.

- **Banco Inter S.A.:** o Ministério Público do Distrito Federal e Territórios ("MPDTF") instaurou, em 2018, ação civil pública por danos morais coletivos contra o Banco Inter, pelo vazamento de dados pessoais dos correntistas do banco. Ainda no inquérito civil instaurado pelo mesmo órgão, o Banco Inter tentou se eximir da responsabilidade sobre o incidente de segurança, afirmando que, apesar dos dados pessoais dos clientes terem vazado, não houve comprometimento de tais dados e, portanto, prejuízo a seus clientes. Na ação proposta, o MPDFT solicitou a condenação do Banco Inter ao pagamento de indenização no valor total de R$10.000.000,00 (dez milhões de reais); porém o Banco Inter e o MPDFT entraram em acordo para o pagamento de R$1.500.000,00 (um milhão e quinhentos mil reais), sendo (i) R$1.000.000,00 (um milhão de reais) destinados a instituições públicas que combatem crimes cibernéticos; e (ii) o restante, ou seja, R$500.000,00 (quinhentos mil reais), a instituições de caridade. As informações do processo, bem como as premissas do acordo firmado entre as partes, permanecem em sigilo.

- **Ns2.Com Internet S.A. – Netshoes:** em 2019, a Netshoes foi alvo de duas condenações por incidentes de segurança e violação de sigilo de dados pessoais, sendo uma no TJMG e outra no MPDFT. Ambas as condenações dizem respeito ao ataque cibernético sofrido pela Netshoes em 2018, no qual foram clonados e divulgados os dados pessoais de mais de 2.000.000 (dois milhões) de clientes da empresa, gerando o comprometimento de dados pessoais. Foi celebrado um Termo de Ajustamento de Conduta ("TAC") entre a Netshoes e o MPDTF para pagamento de indenização por danos morais coletivos causados pelo incidente de segurança. No TAC ficou acordado o pagamento de R$ 500.000,00 (quinhentos mil reais) a título de indenização, além do comprometimento da Netshoes em implementar medidas adicionais ao seu Programa de Proteção de Dados, quais sejam: (i) gerenciamento de riscos e vulnerabilidades no portal Netshoes; (ii) ações de adequação à LGPD; (iii) atualização contínua de sua Política de Segurança Cibernética; (iv) realização de esforços de orientação a consumidores, para aumentar o nível de conhecimento sobre os riscos cibernéticos e

medidas de proteção de seus dados pessoais, por meio de campanha de conscientização; (v) disseminação ao mercado das melhores práticas para privacidade e proteção de dados pessoais, por meio da participação em fóruns e eventos especializados, e (f) difusão de boas práticas de proteção dos dados. O descumprimento de qualquer das obrigações acordadas no TAC poderá implicar à Netshoes a imediata propositura de ação cível pública para reparação por danos morais coletivos no valor de R$ 10.000.000,00 (dez milhões), além de propositura de ação cível pública para reparação por danos patrimoniais causados no valor de R$ 85.000.000,00 (oitenta e cinco milhões de reais), que representaria R$ 5,00 (cinco reais) por titular do dado pessoal comprometido.

- **Cia. Hering**: em agosto de 2020, a Senacon aplicou multa no valor aproximado de R$ 58.000,00 (cinquenta e oito mil reais) à Cia. Hering, grande varejista de artigos de vestuário, pela utilização de tecnologia de reconhecimento facial com a coleta de dados biométricos (dados sensíveis) dos consumidores em uma loja situada no bairro do Morumbi, na cidade de São Paulo, Estado de São Paulo, o que foi feito sem o consentimento prévio, expresso, específico e destacado dos titulares, em violação ao disposto pela LGPD. Entretanto, não há muitos detalhes em relação a tal decisão, uma vez que ainda não foi disponibilizada ao público.

- **Serasa Experian**: a líder em serviços de informação no Brasil foi suspensa liminarmente de comercializar irregularmente dados pessoais de consumidores brasileiros. A Serasa oferecia os serviços "Lista Online" e "Prospecção de Clientes", que consistiam em bases de dados personalizadas, contendo informações como CPF, nome, endereço, telefones, sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagens de risco, para fins de captação de novos clientes a terceiros interessados. Estima-se que o universo de clientes era de 150.000.000 (cento e cinquenta milhões) titulares de CPFs, e o custo do serviço para cada titular era de R$ 0,98.

- **Cyrela Brasil Reality S/A Empreendimentos e Participações:** a construtora foi, em setembro de 2020, condenada a pagar R$10.000,00 (dez mil reais) por ter compartilhado dados pessoais de um cliente com outras empresas, além de abster-se de repassar ou conceder a terceiros, a título gratuito ou oneroso, dados pessoais, financeiros ou sensíveis titularizados pelo cliente, sob pena de multa de R$300,00 (trezentos reais) por contato indevido. Uma das maiores empresas brasileiras no ramo imobiliário, sediada em São Paulo e com operação em outros 16 estados e até no exterior, a empresa foi acionada pela justiça brasileira através de um consumidor, que após comprar um imóvel com a construtora, passou a receber ofertas promocionais de empresas parceiras da Cyrela, sem que houvesse, por parte da construtora, a informação de com quem os dados pessoais do cliente haviam sido compartilhados, deixando o cliente sujeito ao contato de diversas empresas de outros ramos empresariais para ações marketing/promocionais. De acordo com a decisão do TJSP, a Cyrela foi além do que previa o contrato de compra e venda do imóvel, celebrado com o cliente, violando, portanto, as disposições da LGPD.

Além disso, em breve consulta a sites de reclamações consumeristas brasileiros, como o Reclame Aqui (https://www.reclameaqui.com.br/), utilizando o termo "LGPD" na consulta, nota-se o crescente número de pedidos de titulares de dados pessoais ao cumprimento de seus direitos previstos na LGPD, o que deve resultar, em breve, em centenas ou milhares de ações judiciais relacionadas ao tema.

Nesse contexto, pesquisamos em Tribunais de Justiça brasileiros, a fim de identificar situações de condenação, seja na esfera administrativa ou judicial, de empresas dos mais variados setores da economia, inclusive relacionados às áreas de atuação do Governo Britânico, como comércio e saúde, e sintetizamos, abaixo, os principais casos analisados:

| Setor | Empresa | Infração | Data da decisão | Indenização / Multa | Nº do processo | Autor da Ação |
|---|---|---|---|---|---|---|
| Vendas On-Line e Varejo | Mercado Livre.Com Atividades De Internet Ltda. e Mercadopago.Com Representações Ltda. ("Mercado Livre") | Comercialização indevida maciça de dados pessoais de brasileiros por intermédio da plataforma do Mercado Livre, por usuário vendedor de produto anunciante na plataforma. Além de multa ao anunciante, o Mercado Livre foi condenado por afronta aos artigos 2º, I, e 44 da LGPD. | 15/10/2020 | Obrigação de suspensão de anúncio da plataforma e fornecimento dos dados cadastrais do anunciante. | 0733785-39.2020.8.07.0001 (TJDFT) | MPDFT |
| | Decolar.com Ltda. | Discriminação de preço e disponibilidade de hospedagem em hotéis com base na origem geográfica e/ou nacionalidade dos consumidores ("Geo-Pricing" e "Geo-Blocking"), em afronta aos artigos 6º, II e IV, e 39, II, V, IX e X. | 18/06/2018 | R$ 7.500.000,00 | Processo nº 08012.002116/2016-21 (Senacon) | Outro legitimado |
| | Ns2.Com Internet S.A. - Netshoes | Violação de sigilo de dados por ataque cibernético, em afronta ao artigo 14 do Código de Defesa do Consumidor. | 25/10/2019 | R$ 15.000,00 | 5127059-44.2018.8.13.0024 - Usar o código nº: 19102602120600000000089048321 (TJMG) | Titular |
| | | Incidente de segurança que gerou o comprometimento de dados pessoais de clientes, em afronta ao artigo 7, I, VII, do Marco Civil da Internet | 16/01/2019 | R$ 500.000,00 | 08190.044813/18-44 - TAC n. 01/2019 (MPDFT) | MPDFT |
| | Cia. Hering | Uso de tecnologias de tecnologias de reconhecimento facial sem consentimento dos consumidores, em afronta ao artigo 5º, X, da Constituição Federal. | 14/08/2020 | R$ 58.767,00 | 08012.001387/2019-11 (Senacon) | Outro legitimado |
| Telefonia | Telefônica Brasil S.A. e Nextel Telecomunicações Ltda. | Portabilidade de linha telefônica a outra operadora sem solicitação prévia, com compartilhamento indevido de dados pessoais a terceiro, em afronta ao artigo 14 do Código de Defesa do Consumidor. | 15/10/2020 | R$ 7.000,00 | 1005860-19.2020.8.26.0016 (TJSP) | Titular |

| Setor | Empresa | Infração | Data da decisão | Indenização / Multa | Nº do processo | Autor da Ação |
|---|---|---|---|---|---|---|
| | Lenovo Tecnologia (Brasil) Limitada | Compartilhamento indevido de dados pessoais, em afronta ao artigo 14 do Código de Defesa do Consumidor. | 03/09/2020 | R$ 6.000,00 | 0000633-07.2017.8.07.0014 (TJDFT) | Titular |
| **Construção** | Cyrela Brasil Reality S/A Empreendimentos e Participações | Compartilhamento indevido de dados pessoais a terceiro, em afronta ao artigo 6, I e II, da LGPD. A Cyrela compartilhou os dados de seus clientes com terceiros sem informá-los previamente a respeito. | 02/10/2020 | R$ 10.000,00 | 1080233-94.2019.8.26.0100 (TJSP) | Titular |
| **Seguradora** | 24 (vinte e quatro) seguradoras e/ou entidades de classe de mercado de seguradoras | Compartilhamento indevido de dados pessoais a terceiro, em afronta ao artigo 198 do CTN e artigo 13-A da Lei 11.442/2007 | 25/09/2020 | R$ 1.000.000,00 | 0000241-06.2013.5.04.0802 (TRT4) | Outro legitimado |
| **Metrô** | Companhia Do Metropolitano De São Paulo - Metrô | Apresentação de Análise de Impacto de Proteção de dados e outros, com fundamento no artigo 5º, XVII, 7 da LGPD. | 20/02/2020 | Obrigação de fazer. | 1006616-14.2020.8.26.0053 (TJSP) | DPSP |
| **Universidade** | Universidade Norte Do Paraná-Unopar | Desvio de finalidade e uso indevido de dados pessoais, em afronta ao artigo 6, I e II da LGPD. | 14/10/2019 | R$ 5.000,00 | 0848344-52.2018.8.20.5001 (TJRN) | Titular |
| **Produtos Farmacêuticos** | Drogaria Araújo S/A | Condicionamento de descontos ao fornecimento do CPF do consumidor no ato da compra, sem oferecer informação clara e adequada sobre abertura de cadastro do consumidor, em afronta ao artigo 13, I e XIII do Código de Defesa do Consumidor. | 03/12/2018 | R$ 7.137.721,55 | 0024.18.002027-3 (MPMG) | Outro legitimado |
| **Serviços de Informação** | Serasa S.A. | Comercialização indevida maciça de dados pessoais de brasileiros por meio dos produtos “Lista Online” e “Prospecção de Clientes”, em afronta aos artigos 7º e 8º da LGPD. | 23/11/2020 | Obrigação de suspensão da comercialização indevida de dados pessoais de brasileiros por meio dos produtos “Lista Online” e Prospecção de Clientes”. | 0749765-29.2020.8.07.0000 (TJDFT) | MPDFT |

| Setor | Empresa | Infração | Data da decisão | Indenização / Multa | Nº do processo | Autor da Ação |
|---|---|---|---|---|---|---|
| Banco | HSBC Bank Brasil S.A. - Banco Múltiplo | Cláusula abusiva para compartilhamento de dados pessoais com terceiros, com finalidade distinta da finalidade original e sem opção de descadastramento pelo titular de dados, em afronta aos artigos 51, §1º, I, II, III e 6, IV do Código de Defesa do Consumidor. | 30/11/2017 | R$ 1.000,00 | 1.348.532 (STJ) | Outro legitimado |
| | Banco Santander (Brasil) S/A | Vazamentos de dados pessoais utilizados fraudulentamente por terceiros perante outras entidades bancárias, em afronta ao artigo 14 do Código de Defesa do Consumidor. | 30/05/2017 | R$ 6.000,00 | 1050922-66.2016.8.26.0002 (TJSP) | Titular |
| | Banco Inter S.A. | Vazamento de dados pessoais de mais de 19 mil correntistas, em afronta ao artigo 14 do Código de Defesa do Consumidor. | 18/12/2018 | R$ 1milhão de reais para doação a instituições públicas de combate a crimes cibernéticos e R$ 500mil para instituições de caridade | 0721831-64.2018.8.07.0001 (TJDFT) | MPDFT |
| | Município de Capitólio (MG) | Divulgação indevida de dados pessoais, além dos exigidos pela Lei da Transparência, em afronta ao artigo 5º, X, da Constituição Federal. | 07/08/2018 | R$ 5.000,00 | 0011653-85.2017.5.03.0101 (TRT3) | Titular |

Em comparação com o que ocorre no cenário europeu, conforme será destacado no Capítulo 4.1.3 abaixo, cujas normas de proteção de dados são mais maduras, os casos listados acima não sejam numerosos; apesar disso, a tendência é que, com a entrada em vigor da LGPD, haja um aumento expressivo desse número, uma vez que existe no Brasil uma cultura de excessivas ações judiciais. Além disso, espera-se que a morosidade no início das atividades da ANPD contribua para a existência de decisões judiciais diversas em relação a uma mesma matéria prevista na LGPD, uma vez que a LGPD é uma norma principiológica, que contém cláusulas abertas e que aguarda regulamentação pela ANPD.

Dessa forma, caso a ANPD não inicie sua atuação rapidamente e comece a fiscalizar e emitir diretrizes sobre os aspectos controvertidos da LGPD, a expectativa é que se enfrente um cenário de excesso de litígios, competências concorrentes controvertidas de órgãos públicos e decisões conflitantes, com o inevitável aumento nos riscos das atividades de empresas que tratam dados pessoais.

Recentemente, o Supremo Tribunal Federal (STF) suspendeu a eficácia da Medida Provisória nº 954/2020, a qual obrigava as empresas de telefonia ao compartilhamento de dados pessoais de seus clientes com o

IBGE[38]. Trata-se, portanto, de decisão relevantíssima no contexto de privacidade e proteção de dados do Brasil, uma vez que restou expressamente reconhecida a proteção de dados pessoais e a autodeterminação informativa como direitos fundamentais autônomos, extraídos do texto constitucional. Assim, consagrou-se, ainda que indiretamente, a garantia fundamental à proteção de dados pessoais.

Nesse diapasão, conclui-se pela necessidade de adoção do máximo de medidas possíveis para a conformidade das empresas às LGPD, como uma das únicas formas de mitigação dos riscos inerentes a resultados inesperados em demandas judiciais dessa natureza.

[38] Tal questão foi discutida na ADI 6387 MC-Ref/DF, Rel. Min. ROSA WEBER, julgada pelo Tribunal Pleno no STF em 7 de maior de 2020, conforme acórdão publicado em 12 de novembro de 2020. Veja o argumento utilizado em referida decisão: "de sorte que eu lavro uma ementa concordando inteiramente com o brilhante voto da Ministra Rosa Weber, que foi cirúrgica num momento tão complexo para fazer esse cotejo entre essa liberdade de informação que municia a estatística e, de outro lado, a privacidade pessoal, para, concordando com Sua Excelência, reitero, a Ministra Rosa Weber, assentar, em primeiro lugar, que a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana, conforme foi muito bem destacado já, digamos assim, pela Ministra Rosa Weber e já no primeiro voto, o do Ministro Alexandre de Moraes".

# 3. Impactos e Medidas de Adequação

## 3.1. Impactos Gerais da LGPD nas Empresas e seus Setores Internos

Não obstante a existência de normas esparsas sobre o tema, conforme explicado no Capítulo 2.1 acima, a ausência, até recentemente, de uma lei consolidada de privacidade e proteção de dados no Brasil fez com que, por muito tempo, grande parte das empresas tratassem dados pessoais sem observar critérios específicos de segurança da informação ou garantir transparência aos titulares.

O advento da LGPD, desde a publicação de seu texto até a sua entrada em vigor, foi, e continua sendo, objeto de intensos debates entre o Poder Público, representantes de empresas do setor privado e a sociedade em geral. A inexistência de uma cultura de proteção a dados pessoais e à privacidade, com exceção do setor financeiro e sua pretérita e consolidada regulamentação específica, em grande parte anterior à publicação da LGPD, trouxe incertezas a todos os setores da economia, sejam estes órgãos públicos ou empresas do setor privado.

A indecisão político-administrativa sobre diversos pontos da LGPD e seus reais impactos econômicos fez com que até mesmo a sua entrada em vigor foi cercada de controvérsias e discussões.

Com a entrada em vigor da LGPD em 2020 após sucessivas discussões sobre sua prorrogação, empresas tiveram que iniciar procedimentos de adequação e despender investimento considerável em meio à pandemia do COVID-19, o que possivelmente afetou o orçamento anual e as previsões para o exercício seguinte. Isso porque os dois anos que transcorreram entre a publicação da LGPD e sua entrada em vigor, fez com que muitas empresas, especialmente do setor privado, desacreditassem que a LGPD alteraria os parâmetros do tratamento de dados pessoais no Brasil e adiarem ao máximo a adequação aos seus requisitos.

Há, também, o risco de excesso de judicialização e decisões judiciais conflituosas no que tange à interpretação da Lei, conforme detalhado no Capítulo 2.3. acima, o que contribui para dificultar o provisionamento de despesas relacionadas a esta matéria pelas empresas sujeitas à adequação à LGPD.

Além disso, emergiu no meio das discussões envolvendo a adequação das empresas à LGPD um novo evento que atraiu a atenção do Poder Público e da sociedade em geral, que o ataque cibernético sofrido pelo Superior Tribunal de Justiça (e outros órgãos públicos) no início de novembro de 2020, o que resultou na suspensão de prazos processuais e indisponibilidade de acesso à sua base de dados.

Entretanto, independentemente da discussão sobre a possível responsabilização de empresas pela violação às normas de proteção de dados, não se pode ignorar que a adequação à LGPD tem um importante reflexo no mercado, uma vez que gera um diferencial competitivo, aumenta a relevância e credibilidade da empresa adequada às suas regras no mercado e amplia as chances de captação de clientes e de investidores, que sentem mais segurança em aportar valores devido à proteção garantida aos dados pessoais tratados.

Um dos pontos mais importantes da conformidade de empresas à LGPD refere-se à criação de estruturas de governança corporativa para o tratamento dos dados pessoais.

Por ser uma lei mais principiológica que a GDPR, conforme será melhor explicado no Capítulo 4.1 abaixo, e não trazer detalhes procedimentais em seu texto, uma vez que tais procedimentos deverão ser regulamentados pela ANPD, eventual responsabilidade será mensurada primordialmente conforme as medidas de segurança e mitigação de riscos adotadas e comprovadas pela empresa (o chamado “princípio da *accountability*”, abarcado tanto pela LGPD como pela GDPR).

Isso porque inevitavelmente a LGPD impõe mudanças nas principais áreas e departamentos das empresas públicas e privadas, tais como recursos humanos, marketing, comercial, financeiro, tecnologia e segurança da informação, dentre outras. Esse procedimento de revisão de atividades internas, ao qual se costuma referir como "adequação", acaba criando oportunidades de negócios para facilitar a adequação dessas atividades, no sentido de garantir o exercício regular dos direitos dos titulares de dados, evitar incidentes de segurança e violações aos preceitos da LGPD.

O trabalho de adequação começa com o engajamento direto dos funcionários, com a finalidade de aumentar a aderência à LGPD dentro do ambiente e rotina de negócios, assim como conscientizá-los da importância da conformidade. As empresas precisarão colocar a proteção de dados no centro de suas decisões de negócio, incluindo a execução de avaliações de impacto de proteção de dados.

Conforme já mencionado, os impactos da conformidade atingem as mais diversas áreas das empresas e encontram-se resumidamente destacados a seguir, considerando-se a divisão setorial interna a qual as empresas normalmente estão sujeitas:

| | **IMPACTOS DA LGPD NOS SETORES INTERNOS DAS EMPRESAS** |
|---|---|
| **Impacto no Departamento de Tecnologia e Segurança da Informação** | É importante, até mesmo para a organização interna da empresa, que se documente e relate o fluxo dos dados pessoais transitados em sistemas da empresa, de modo que se saiba todo o seu fluxo e ciclo de vida desde a coleta, local de armazenamento, quem e como poderá acessá-los, com quem são compartilhados etc.<br>A depender do modelo de negócio, as áreas de tecnologia/segurança da informação poderão ser o cerne das medidas de adequação, a exemplo de plataformas que oferecem serviços e produtos a partir de estudos de comportamento de indivíduos realizados por meio de algoritmos e inteligência artificial. Para cada finalidade de uso dos dados deverá ser aplicada uma base legal adequada e, se não for possível justificar o seu processamento, os dados possivelmente deverão ser excluídos. Este departamento pode e deve ajudar a adequação, protegendo os dados contra acessos não autorizados, automatizando o gerenciamento dos dados dos usuários e de APIs, garantir a aplicação e desenvolvimento de um programa de segurança da informação robusto, com maior segurança aos dados, e possuir um procedimento para resposta a incidentes de segurança. |
| **Impacto no Departamento Comercial** | Estratégias que transformam rapidamente potenciais clientes em clientes efetivos são consideradas as melhores dentro da realidade atual das atividades comerciais. Porém, a lei traz algumas mudanças para o setor, principalmente na maneira de conduzir a prospecção. Nessa linha, a lista de potenciais consumidores que já manifestaram interesse no produto ou serviço (leads) compradas, por exemplo, deverá ser utilizada com base em uma das hipóteses autorizadoras para o tratamento de dados pessoais e em atenção aos princípios legais estabelecidos pela LGPD.<br>Ao cumprir a LGPD, o setor tende a atender rapidamente seus indicadores-chaves de performance de vendas, gerar leads de qualidade, alcançar mais clientes em potencial, destruir dados inexpressivos ou desnecessários e, por fim, obter taxas de fechamento mais altas. Trata-se, portanto, de uma mudança |

| | |
|---|---|
| | cultural de descarte de bases de dados desqualificadas para obter uma maior qualidade, demonstrada inclusive em estudo da Cisco de janeiro de 2020 , segundo o qual o retorno sobre o investimento em privacidade pode atingir um valor equivalente a quase o triplo do montante gasto na adequação da empresa. |
| **Impacto no Departamento de Recursos Humanos**  | O departamento de RH costuma tratar elevado número de informações pessoais e até mesmo sensíveis, uma vez que coleta e armazena dados de todos os colaboradores, candidatos a vagas de emprego, contratados e ex-colaboradores.<br>**Na contratação**:<br>Dados obtidos em processos de recrutamento e seleção, por exemplo, precisarão ser justificados em uma das bases legais autorizadoras da LGPD, a exemplo do consentimento ou legítimo interesse, de acordo com o caso concreto.<br>Destaca-se ser recorrente o compartilhamento de dados de colaboradores com terceiros, como para a terceirização da folha de pagamento. Todo empregador deverá informar com transparência, disponibilizando aviso de privacidade claro e detalhado sobre como os dados de seus funcionários serão utilizados, para quais finalidades, por quais motivos serão compartilhados e transmitidos a empresas terceiras, mantendo a atualização constante dessa política interna.<br>**Na demissão**:<br>O empregador deverá manter inúmeros dados pessoais dos empregados desligados, conforme previsto na própria legislação trabalhista e regulamentos setoriais. Esses dispositivos devem ser observados e registrados, criando-se ainda uma política de retenção de dados para que não estes sejam armazenados em excesso, de forma descuidada, tampouco excluídos em violação à legislação. |
| **Impacto no Departamento de Marketing**  | A coleta de dados deve ser relevante e necessária para a finalidade estabelecida. Isso significa que, por exemplo, se a empresa estiver executando uma campanha, só poderá usar as informações que receber para essa finalidade, sendo vedada a utilização para qualquer outro fim que não tenha sido informado ao titular ou cuja expectativa do titular de receber esse tipo de campanha não exista.<br>Apesar de não impor consentimentos para promoção e ações de marketing, a LGPD determina a garantia de “saída” (a chamada opção de “opt-out”, que significa o descadastramento de determinada lista de divulgação/promoção) em todas as comunicações. Na prática, contudo, espera-se que haja muitas demandas por consumidores desavisados no sentido de solicitar comprovação de que consentiram em serem contatados pelas empresas.<br>Ainda, de acordo com a LGPD, o banco de dados construído antes da entrada em vigor da LGPD (dados legados) deverá ser reavaliado para garantir a verificação dos requisitos da LGPD, bem como para atribuir a base legal correspondente ao tratamento e observar os princípios da Lei. |

| | |
|---|---|
| **Impacto no Departamento Financeiro** $ | O departamento financeiro possui grande quantidade de dados pessoais e deverá garantir a segurança de todos os colaboradores. Um dos principais pontos é a necessidade de atenção ao arquivamento de informações, certificando-se de que os registros arquivados permaneçam inalterados e sejam destruídos após um período de retenção definido (que será estabelecido na Política de Retenção de Dados, que deverá ser criada).<br>No processo de conformidade com a LGPD, o departamento financeiro precisa estar atento à responsabilidade, transparência, assim como à implementação de medidas técnicas e organizacionais necessárias para responder de forma adequada às solicitações dos titulares de dados, com base em seus direitos assegurados por lei. Deve-se saber, ainda, que tais direitos não são ilimitados e precisam ser analisados conforme o caso. |

Pelo exposto, e conforme demonstrado, o impacto da LGPD nas empresas vai muito além da implementação de políticas e procedimentos internos, sendo necessária a construção de um programa de governança em privacidade e proteção de dados robusto, que garanta a efetividade das medidas com a conscientização de colaboradores e parceiros, internos e externos.

## 3.2. Medidas de Adequação à LGPD

### 3.2.1. Vantagens da conformidade à LGPD

Conforme ilustrado abaixo, o Brasil tem se destacado nos rankings de países que mais sofreram ciberataques, ocupando a primeira posição na América Latina e a terceira posição mundial. Os alvos dos cibercrimes vão desde os usuários até os sistemas de grandes empresas, governos e instituições públicas, tornando investimentos em segurança não apenas recomendados, mas extremamente necessários para proteger informações pessoais e sensíveis, individuais e coletivas, e evitar custos e impactos de ciberataques, para além das possíveis multas da LGPD.

Nesse contexto, o dever de adoção de medidas capazes de adequar às empresas à LGPD pode alterar substancialmente a estrutura e rotina de atividades dentro das empresas. Apesar do trabalho intensificado, tal conformidade traz vantagens financeiras (como destacado no estudo da Cisco supra mencionado) e reputacionais, a saber:

| | **VANTAGENS DA CONFORMIDADE À LGPD** |
|---|---|
| **Segurança Jurídica** | Segurança jurídica para o tratamento dos dados pessoais, a partir da elaboração dos relatórios de atividades e de impacto, por exemplo, a fim de cumprir os requisitos necessários a serem apresentados à ANPD, além da criação de um cenário de respostas a incidentes de segurança que evite denegrir a imagem da empresa; |

| | |
|---|---|
| **Oportunidades de Negócios**  | Oportunidades de negócios, na medida em que a tendência do mercado é o compartilhamento de dados e, com isso, impõe-se ao parceiro de negócios a comprovação de que seus procedimentos de adequação estão em andamento ou já foram concluídos, inclusive por meio de cláusulas inseridas nos contratos de modo a garantir o direito de realizar auditorias na empresa contratante e/ou contratada, conforme o caso. A atenção e preparo para a conformidade com a LGPD tende a trazer benefícios nacionais e internacionais, uma vez que desde maio de 2018 se verifica a imposição de medidas de conformidade à GDPR por empresas da União Europeia. Além disso, a partir do momento em que o Brasil adota parâmetros considerados seguros para a proteção dos dados, há diminuição dos custos de transação na celebração de contratos com partes de diferentes países e evita-se que autoridades de outros países imponham obstáculos à contratação, por residentes de tais países, de prestadores de serviços localizados no Brasil; |
| **Credibilidade**  | Credibilidade, que poderá ser um diferencial perante a concorrência, principalmente aos olhos dos consumidores que, com a crescente cultura de privacidade trazida pela LGPD, estão cada vez mais cientes e preocupados com o tratamento de seus dados, e buscarão empresas atentas ao cumprimento da LGPD e de seus direitos, na qualidade de titulares; |
| **Economia**  | Economia, ao desenvolver novos produtos e serviços adequados à LGPD desde a sua concepção (*"Privacy by Design" /"Default"*) e evitar novos investimentos na adaptação posterior aos preceitos da LGPD. |

As vantagens e necessidade de adequação valem tanto para os setores público como privado, pois ambos tratam dados pessoais para a prestação de seus serviços e estão diretamente ligados aos indivíduos que os contratam ou que fazem uso desses serviços.

## 3.2.2. Adequação à LGPD

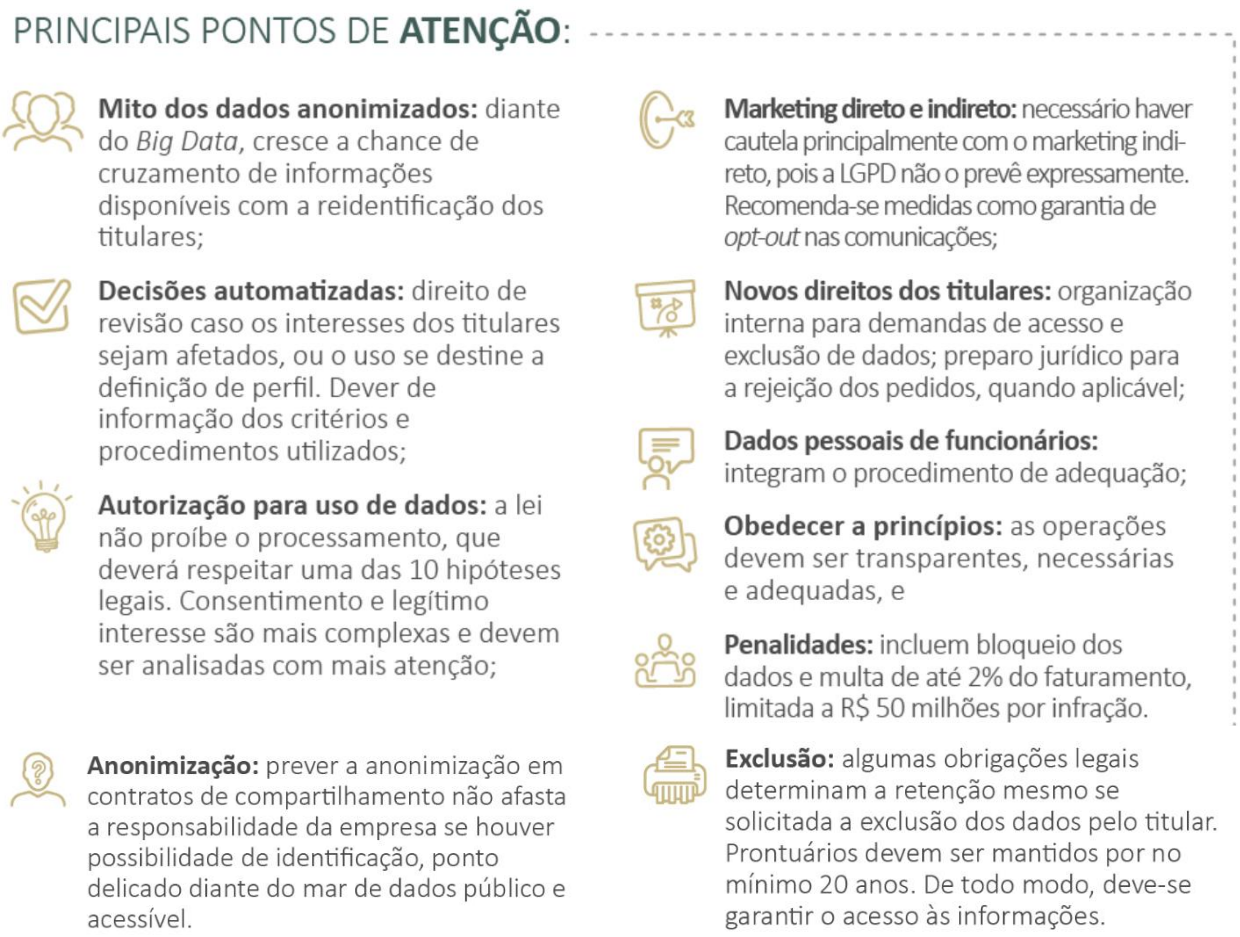
Inicialmente, destaca-se que o procedimento de adequação à LGPD não deve seguir padrões ou planos *"one size fits all"* (ou seja, as empresas não devem utilizar planos que sejam preparados indistintamente, para que sejam aplicáveis a quaisquer empresas). O *roadmap* precisa ser construído de acordo com as reais necessidades, modelo de negócio, prioridades e ambições da empresa que busca a adequação. A abordagem deve ser adaptável e flexível, de forma a criar estratégias personalizadas e holísticas à empresa.

Antes de se falar em método de adequação, deve-se ter em mente os princípios historicamente aceitos em relação ao tratamento de dados e privacidade em nível internacional, mais presente aos países membros da Organização para a Cooperação e Desenvolvimento Econômico (*Organisation for Economic Co-operation and Development* – OCDE). Embora o Brasil ainda não seja parte integrante do grupo, as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ao lado da *Council of Europe's Convention* 108, formam a base da Diretriz de Proteção de Dados da União Europeia ("*EU Data Protection Directive*") e da GDPR. Nesse sentido, e tendo em mente que os princípios adotados pela LGPD são exatamente os mesmos da GDPR, segue-se a mesma base elaborada pela OCDE.

Nesse contexto, pode-se realizar um programa de conformidade econômico e enxuto, pois a LGPD, ao contrário da GDPR, não é procedimental, mas eminentemente principiológica, e caberá à ANPD elaborar diretrizes claras, detalhadas e específicas. O procedimento, ademais, não se esgota em si mesmo, tampouco se encerra após o *roadmap*. Isto se deve tanto ao fato de que novas regulamentações devem ser criadas, como pelo fato de que a empresa é viva e muda constantemente seus negócios, processos de tratamento de dados, colaboradores, desenvolve produtos e serviços e diretrizes, de modo que se deve monitorar constantemente o trabalho de conformidade.

Embora inexistam diretrizes brasileiras, as metodologias internacionais podem ser utilizadas para a escolha dos critérios de adequação, sempre levando em consideração uma abordagem com base no risco (*risk-based approach*), a exemplo do método detalhado em um dos mais importantes livros do gênero, o *Privacy Program Management*, da International Association of Privacy Professionals (IAPP)[39], assim como as diretrizes fundamentais do ICO (*Information Commissioner's Office*, a autoridade supervisora do Reino Unido), e as do Centre for Information Policy Leadership Accountability Framework[40].

Abaixo, os principais pontos de atenção que devem ser considerados pelas empresas durante o processo de adequação:




[39] "Privacy Program Management: Tools for Managing Privacy Within Your Organization", Russel Densmore, 2nd ed., 2019, IAPP.

[40] Disponíveis em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> e <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020__v2.0.pdf>. Acessado em 15 de novembro de 2020.

## 3.2.3. Etapas do Procedimento de Conformidade

Considerando que o procedimento de adequação deve ser determinado com base nas características específicas de cada empresa, as etapas de adequação dependerão das reais necessidades e realidade da empresa, seja ela pública ou privada. A seguir, ilustra-se um exemplo de *roadmap* de adequação. As etapas do modelo abaixo poderão variar, ou até mesmo ocorrer de forma concomitante tendo em vista as medidas mais urgentes a serem adotadas:


Passamos a descrever as etapas que normalmente são sugeridas de forma geral para a minimização de riscos em relação ao tratamento de dados pessoais. Para facilitar a compreensão dessas etapas, aglutinamos algumas das fases da ilustração acima.

### A. Workshop de Conscientização e Impacto

A etapa inicial do procedimento de conformidade à LGPD tem o escopo de impactar os colaboradores, com uma aula para provocar a conscientização sobre os impactos da lei no negócio, familiarizar os colaboradores com os termos e regras e informá-los sobre o método de trabalho a ser implementado e o papel de cada colaborador em tal processo de conformidade. Por meio desses ensinamentos, estabelece-se uma cultura de privacidade imediata e os colaboradores começam a observar com mais cuidado o uso de dados pessoais em suas atividades de rotina. Aproveita-se, ainda, para informar como será realizado o procedimento de adequação, os papeis dos colaboradores nas medidas de implementação, como deverão responder os questionários e entrevistas iniciais, entre outros aspectos. Na sequência, faz-se uma reunião inicial e definem-se os papéis principais na estrutura da governança em privacidade e proteção de dados da empresa, importantes no curso do procedimento e para além de sua conclusão, de forma a manter a empresa em conformidade:

| | MEDIDAS INICIAIS DE ADEQUAÇÃO |
|---|---|
| **Gerente do Projeto** | O gerente do projeto (*Project Management Officer* - **PMO**) será o responsável pela comunicação entre a empresa e os responsáveis pelo programa de adequação (escritório de advocacia, por vezes em conjunto |

| | |
|---|---|
| | com uma empresa de segurança da informação para análise e treinamento específicos sobre tecnologia e segurança cibernética). O PMO também será o líder do projeto na empresa no sentido de assessorar qualquer comunicação interna, entre as áreas, diretoria e lideranças do projeto; |
| **Encarregado pelo Tratamento de Dados** | O Encarregado (**DPO**, definido com mais detalhes no Capítulo 2.2), servirá para fiscalizar e garantir a conformidade da empresa em relação a assuntos relacionados à privacidade e proteção de dados, bem como garantir o cumprimento das políticas e procedimentos relacionados ao tema, assim como gerir o programa de adequação, além de aprovar produtos, soluções, sistemas, práticas de negócio etc., cujo risco seja baixo ou médio; |
| **Comitê de Privacidade** | O Comitê de Privacidade, geralmente, se já houver Comitês de segurança, tecnologia, compliance ou riscos, estes poderão ser utilizados para facilitar a estruturação do Comitê de Privacidade, o qual servirá para debater questões relacionadas à privacidade com os líderes das áreas mais críticas da empresa, acompanhar indicadores e fatores de melhoria ao programa de adequação. Este Comitê servirá, ainda, para aprovar soluções, produtos, práticas de negócio, sistemas etc., cujo risco de privacidade seja classificado como alto, e |
| **Privacy Champions** | Os ***Privacy Champions***, pontos focais do DPO em cada uma das áreas críticas da empresa, no que se refere ao tratamento de dados pessoais. São treinados, assim como o DPO, para manter a adequação da empresa e assessorar os colaboradores de sua área nas rotinas de atividades realizadas com dados pessoais, facilitando a comunicação com o DPO. Não possuem poder decisório. Realiza o levantamento de informações sobre os projetos da área, para auxílio no preparo de Relatórios de Impacto à Proteção de Dados, quando necessário. |

### B. Mapeamento de Dados

A LGPD determina ao controlador e ao operador a manutenção do registro das operações de tratamento de dados pessoais realizadas, especialmente (mas não apenas) quando baseadas em legítimo interesse[41]. Para cumprir esta obrigação, esta etapa objetiva identificar os processos de negócio e de tratamento de dados pessoais, os fluxos e ciclos de vida de tais dados dentro e fora da empresa (informações acessadas, coletadas, usadas, transferidas, armazenadas ou compartilhadas), inclusive as relações comerciais com fornecedores e parceiros e as políticas de privacidade e segurança vigentes. Adicionalmente, realiza-se a:

- elaboração do Registro das Operações de Tratamento (*Record of Processing Activities* - RoPA), conforme o modelo do Anexo A, que deverá ser preenchido pelo escritório responsável pelo procedimento de adequação, após questionários e entrevistas realizadas com os colaboradores das áreas-chave da empresa, ou seja, os que mais realizam atividades de tratamento de dados pessoais em sua rotina de trabalho e estão ativamente envolvidos no fluxo dos dados tratados pela empresa

[41] Conforme artigo 37 da LGPD.

(a serem selecionados de acordo com a estratégia do procedimento, a empresa, modelo de negócio, estrutura interna, áreas, produtos e serviços oferecidos no mercado, entre outros fatores);

- análise jurídica dos processos de tratamento de dados, inclusive a avaliação da possibilidade de manutenção de tais atividades em vista das bases legais da LGPD e a possibilidade e conveniência de exclusão desses dados. Destaca-se a importância do exame da legitimidade e validade de cada um desses processos em vista dos princípios legais[42], tempo de armazenamento, categoria dos dados (pessoais ou sensíveis), finalidades, critérios para transferência internacional e compartilhamento, adoção de boas práticas de governança[43];

- avaliação dos critérios de segurança da informação nos processos; e

- análise de riscos e levantamento de lacunas referentes aos processos.

Em alguns casos específicos de tratamento de dados em larga escala pode-se realizar a etapa de descobrimento de dados (*Data Discovery*) antes do mapeamento. Para tanto, uma consultoria de tecnologia oferece software, a ser acessado a partir dos sistemas da empresa, para o levantamento automático dos dados pessoais de suas bases estruturadas e não estruturadas, o que é feito por meio de algoritmos e inteligência artificial. Entretanto, é importante destacar que esse serviço pode resultar em falsos positivos/negativos e atingir valores consideráveis.

Para fins de cálculo da média de valores e tempo, informamos que esta etapa costuma durar em torno de um mês em uma empresa de médio porte.

### C. Análise de *Gaps*, Avaliação de Riscos (*Risk Assessment*), Revisão e Diagnóstico

Esta etapa consiste em identificar os pontos de atenção relacionados às atividades realizadas com dados pessoais pelas áreas da empresa e seus colaboradores, dentro do fluxograma levantado na etapa de mapeamento. Deve-se analisar as lacunas e avaliar os riscos no contexto desses processos de tratamento de informações pessoais. Elabora-se, então, o diagnóstico da empresa com base no que foi analisado, e aponta-se os documentos e contratos a serem revisados. Além disso, nesta etapa:

- análise do impacto da estrutura da organização, a disparidade de processos e avalia-se seus impactos;

- análise de lacunas e levantamento de riscos e vulnerabilidades em procedimentos e documentos, como políticas, governança, regulamentos e regulação incidentes, procedimentos, cláusulas de proteção de dados, contratos (com clientes, parceiros, fornecedores de serviços e produtos, acordos empregatícios, terceiros que acessam dados pessoais e sensíveis, *intergroup* ou *intercompany agreements* etc.), gerenciamento de consentimentos, meios adotados para a garantia dos direitos de titulares, elaboração de Relatórios de Impacto de Proteção de Dados ("DPIA" ou "RIPD") e aplicação do *Privacy by Design*, gerenciamento de incidentes, inclusive notificação a titulares e ANPD, procedimentos e instrumentos para transferência internacional[44], e

- Elabora-se o plano de ação para a implementação das políticas, medidas técnicas e organizacionais de privacidade, proteção de dados e segurança da informação.

[42] Nos termos do artigo 6º da LGPD.
[43] Conforme artigo 50 da LGPD.
[44] Conforme Capítulo X da LGPD.

Esta etapa costuma durar em torno de um mês e meio em uma empresa de médio porte.

### D. Elaboração e Implementação

O conteúdo desta etapa dependerá das fases anteriores e poderá ser desenvolvido concomitantemente com outras etapas, em especial tendo em vista a urgência da adequação após a entrada em vigor da LGPD.

A implementação deve ser planejada e elaborada de forma a contemplar medidas jurídicas, organizacionais e técnicas de acordo com as regras de privacidade e setoriais aplicáveis. A implementação deve priorizar os riscos e seguir uma estratégia direcionada a manter a maior quantidade de dados possível, contanto que a LGPD seja respeitada. Em geral, incluem-se os seguintes passos nesta etapa:

- elaboração de contratos e cláusulas (aditivos) de proteção de dados para documentos e relações jurídicas analisadas anteriormente, inclusive políticas de privacidade e termos de uso para plataformas e websites;

- se necessário, elaboração de Análises de Legítimo Interesse (LIA – *Legitimate Interest Assessment*) e/ou DPIA;

- treinamentos de empregados e, eventualmente, de parceiros de negócios, de forma a mitigar os riscos de responsabilização da empresa por erros de tais parceiros;

- assessoramento ao cliente na criação de uma estrutura de governança responsável pela continuidade do projeto e pela implementação da nova cultura, assim como para possibilitar um método PDCA (*Planning, Doing, Checking, and Acting*); e

- Definição de estruturas para o gerenciamento de consentimentos e cumprimento aos pedidos de titulares no exercício de seus direitos (se aplicáveis), procedimentos para transferência internacional, administração e notificação de incidentes e indicação de DPO (segundo a LGPD, é possível a indicação de equipe, pessoa física ou jurídica).

Esta etapa costuma se iniciar em paralelo à etapa de mapeamento, tendo em vista a urgência das empresas ainda não adequadas à LGPD, em implementar medidas e adequar documentos. Esta fase costuma demorar em torno de três meses em uma empresa de médio porte.

### E. Monitoramento

De tempos em tempos será necessário realizar o monitoramento da conformidade para que se observem e se mantenham as políticas, métodos e medidas implementadas. Trata-se de etapa importante em decorrência de eventuais modificações nos modelos de negócios, processos, contratação de funcionários, desenvolvimento de novos produtos/serviços. O monitoramento poderá englobar:

- a manutenção de inventário de dados e mecanismos de transferência;
- a manutenção de políticas de proteção de dados e privacidade;
- a manutenção da conscientização dos colaboradores e treinamentos, riscos de segurança da informação, riscos de terceiros e alertas/notificações;
- o monitoramento de novas práticas operacionais;
- a elaboração ou monitoramento de programa de gerenciamento sobre perda de dados;

- o monitoramento de regulamentos elaborados pelas autoridades, e
- a verificação das garantias de respostas corretas a incidentes de segurança e de privacidade.

Destaca-se que o monitoramento é de extrema relevância porque as regras e critérios de privacidade e proteção de dados nacionais, além de novas, estão constantemente evoluindo. Ademais, como cabe à ANPD a criação de diretrizes e interpretação da LGPD, é possível que a empresa venha a ter que alterar qualquer política ou prática estabelecida inicialmente.

Assim, conforme explicitado neste Capítulo, o procedimento de adequação visa a gerar engajamento na empresa no sentido de implementar uma cultura de proteção a dados e segurança das informações para a manutenção das práticas e políticas adotadas no curso das etapas de adequação. Consequentemente, torna-se vital que a empresa contrate especialistas competentes com larga experiência na área, dispostos a atuar diante dos obstáculos previstos, principalmente porque a interpretação da LGPD encontra-se pendente de análise por parte das autoridades relevantes.

Por fim, mesmo que o procedimento geralmente possa ser o mesmo para empresas privadas e públicas, destaca-se que a LGPD prevê regras específicas direcionadas ao Poder Público, conforme já explicado no Capítulo 2.2.2.

# 4. LGPD e GDPR

## 4.1. Contexto Histórico do Regulamento Geral de Proteção de Dados da União Europeia (GDPR)

### 4.1.1. Razões que levaram a União Europeia a pensar em proteção de dados

Durante o início dos anos 1970, houve um aumento no uso de computadores para processar informações sobre indivíduos (ou dados pessoais). O progresso rápido no campo do processamento eletrônico de dados e o primeiro aparecimento de computadores mainframe[45] permitiram que a administração pública e grandes empresas criassem amplos bancos de dados para melhorar a coleta, o processamento e o compartilhamento de informações pessoais.

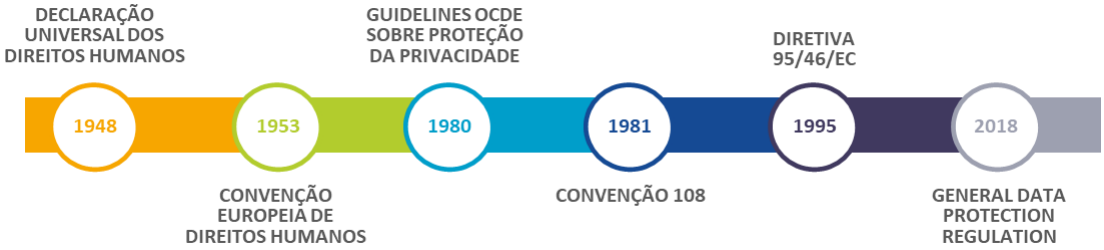
Além disso, o comércio transfronteiriço, facilitado pela Comunidade Econômica Europeia (CEE), incentivou o aumento no compartilhamento de informações, e a combinação entre o uso dos computadores e o desenvolvimento das telecomunicações abriu novas oportunidades para o processamento de dados em escala internacional.

Embora esses desenvolvimentos tenham oferecido vantagens consideráveis em termos de eficiência e produtividade, eles também deram origem a preocupações de que tais avanços teriam um impacto adverso sobre a privacidade dos indivíduos, o que seria agravado quando as informações pessoais fossem transferidas em âmbito internacional.

Assim, dentro do sistema jurídico de cada Estado-membro da União Europeia, já havia regras destinadas a proteger as informações pessoais antes da promulgação da GDPR, como leis sobre privacidade, sigilo e confidencialidade. No entanto, foi observado que o armazenamento automatizado de informações pessoais e o aumento do comércio transfronteiriço exigiam novos padrões que, ao mesmo tempo, permitissem aos indivíduos exercerem controle sobre suas informações pessoais e o livre fluxo internacional de informações necessárias para apoiar o comércio internacional.

O desafio era enquadrar esses padrões de uma forma que mantivesse um equilíbrio entre as preocupações em um nível nacional em relação à liberdade pessoal e privacidade e a capacidade de apoiar o comércio livre no nível da CEE.

Destacamos as principais normas que antecederam a promulgação da GDPR na Europa e já previam proteção aos dados pessoais e à privacidade:




[45] Disponível em: <https://www.tecmundo.com.br/supercomputadores/58611-computadores-mainframes-decada-1980-falta-imagens.htm>. Acessado em 7 de dezembro de 2020.

## 4.1.2. GDPR

Em resposta às preocupações com a falta de unicidade dos Estados-membros com a Diretiva de 1995, a Comissão Europeia lançou uma revisão do então cenário jurídico sobre proteção de dados em 2009 e, em 2010, definiu uma estratégia para fortalecer as regras de proteção de dados. Isso resultou em uma proposta da Comissão Europeia, em janeiro de 2012, para uma reforma abrangente da Diretiva, sob a forma de um regulamento geral de proteção de dados (ou seja, a GDPR), que imporia um único conjunto de regras em toda a União Europeia.
Os regulamentos emitidos pela Comissão Europeia, Parlamento Europeu e Conselho da União Europeia, como é o caso da GDPR, são obrigatórios em sua integralidade e se aplicam diretamente a todos os Estados-membros após a sua entrada em vigor, sem a necessidade de transposição para o direito nacional, de modo que o objetivo de ter sido publicado um regulamento em vez de uma diretiva era maximizar a consistência da abordagem entre os Estados-membros da União Europeia. No entanto, a GDPR permite que os Estados-membros promulguem regras mais específicas em algumas situações, o que permite que haja divergências de abordagem entre os Estados-membros sobre como a GDPR é implementada na prática.

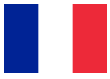
Assim, a GDPR foi concebida para criar um *framework* de proteção de dados forte e mais coerente, para proporcionar maior confiança à economia, inclusive digital, e o desenvolvimento do mercado interno.

## 4.1.3. Aplicações de multas no cenário Europeu

Diferentemente do que ocorre no Brasil, conforme já explicado no Capítulo 2.3 acima, desde a entrada em vigor da GDPR já foram aplicadas mais de 450 (quatrocentas e cinquenta) penalidades a empresas de diversos setores, porém apenas 50 (cinquenta) dessas penalidades chegaram a valores superiores a € 100.000,00 (cem mil euros).

Até o momento, os valores das contribuições pecuniárias variaram entre € 28,00 (vinte e oito euros), aplicada para a Google Ireland Ltd., e € 50.000.000,00 (cinquenta milhões de euros), aplicada para a Google Inc. No total, estima-se que a soma de todas as multas aplicadas já tenha excedido € 220.000.000,00 (duzentos e vinte milhões de euros).

Neste contexto, para referência, elaboramos o quadro abaixo com as 10 (dez) maiores multas já aplicadas no âmbito da GDPR:

| Maiores multas - GDPR | | | | | |
|---|---|---|---|---|---|
| **#** | **Empresa** | **Jurisdição** | **Data** | **Artigos violados (GDPR)** | **Multa** |
| **1.** | Google Inc. |  | 21.01.2019 | Arts. 5º, 6º, 13 e 14. | € 50.000.000,00 |
| **2.** | H&M Hennes & Mauritz Online Shop A.B. & Co. KG |  | 01.10.2020 | Arts. 5º e 6º. | € 35.258.708,00 |

| | | | | | |
|---|---|---|---|---|---|
| **3.** | TIM – Telecom Provider |  | 15.01.2020 | Arts. 5º, 6º, 17, 21 e 32. | € 27.800.000,00 |
| **4.** | British Airways |  | 16.10.2020 | Arts. 5 (1) f) e 32. | € 22.046.000,00 |

É importante destacar que, mesmo nos casos acima, que representam as maiores violações de dados da Europa dos últimos anos, diversas atenuantes foram consideradas para diminuir as multas esperadas. Por exemplo, no caso H&M (caso número 2 da tabela acima), que consistiu na coleta de dados sensíveis de seus funcionários, a autoridade nacional alemã (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) declarou que as tentativas de reparação de conduta, incluindo a comunicação da infração e a indenização aos funcionários, foram encaradas positivamente. Já nos casos julgados pela autoridade italiana (Garante per la Protezione dei Dati Personali - GPDP) foram consideradas atenuantes a cooperação na investigação, adoção de medidas técnicas e organizacionais que confiram um controle maior dos dados aos titulares, reforço de medidas de segurança para acesso às bases de dados da empresa etc.

## 4.2. Comparativos entre LGPD e GDPR

A LGPD baseou-se, e muitos dos seus fundamentos encontram respaldo, na GDPR. Se, por um lado, ambas as legislações se assemelham em muitos aspectos, por outro (e ao contrário do que alguns dizem e pensam), essas normas possuem algumas diferenças marcantes e notáveis, que expomos a seguir:

### A. Bases Legais

Uma das principais diferenças entre as citadas leis é a variedade de bases legais que autorizam o tratamento de dados pessoais e de dados sensíveis. Na GDPR, há seis bases legais autorizadoras do tratamento de dados pessoais (quais sejam, consentimento, execução de contrato, cumprimento de obrigação legal/regulatória, legítimo interesse, políticas públicas e proteção da vida – conforme artigo 6º da GDPR), enquanto na LGPD, em seu artigo 7º, podemos identificar dez bases legais que, igualmente e sem posição de hierarquia, autorizam o tratamento de dados pessoais (quais sejam, consentimento, cumprimento de obrigação legal/regulatória, execução de políticas públicas, estudos por órgão de pesquisa, execução de contrato, exercício regular de direitos, proteção da vida, tutela da saúde, legítimo interesse e proteção do crédito). O quadro resumo abaixo sintetiza as principais diferenças das bases legais previstas pela LGPD e pela GDPR para o tratamento dessa categoria de informações:

| **Bases Legais: Dados Pessoais** | | |
|---|---|---|
| | **LGPD** | **GDPR** |
| **Consentimento**  | Se utilizada esta base legal, o consentimento do titular dos dados deve ser livre, informado e inequívoco, para finalidades determinadas. | Se utilizada esta base legal, o consentimento para o tratamento de dados pessoais deve ser concedido para um ou mais fins específicos. |
| **Cumprimento de obrigação legal ou regulatória** | Para o cumprimento de obrigação legal ou regulatória pelo controlador. | Quando o tratamento é necessário para o cumprimento de obrigação legal a qual o controlador está sujeito. |

| | | |
|---|---|---|
| | | |
| **Execução de políticas públicas** | Realizada pela administração pública quando o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. | Realizada pela Administração Pública quando o tratamento é necessário para o desempenho de uma tarefa realizada no interesse público ou no exercício de autoridade investida no controlador. |
| **Realização de estudos por órgão de pesquisa** | Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais | |
| **Execução contratual** | Quando o tratamento é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. | Quando o tratamento é necessário para a execução de um contrato do qual o titular dos dados seja parte, ou para adotar medidas a pedido do titular dos dados antes de celebrar um contrato. |
| **Exercício regular de direitos em processo judicial, administrativo ou arbitral** | Para o exercício regular de direitos em processo judicial, administrativo ou arbitral | |
| **Proteção da vida ou da incolumidade física** | Para a proteção da vida ou da incolumidade física do titular ou de terceiro. | O tratamento é necessário para proteger os interesses vitais do titular dos dados ou de outro indivíduo. |
| **Tutela da saúde** | Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária | |
| **Legítimo interesse** | Quando o tratamento é necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. O legítimo interesse do controlador somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: (i) apoio e promoção de atividades do controlador; e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais. | Quando o tratamento é necessário para os fins e interesses legítimos perseguidos pelo controlador ou por terceiros, exceto quando tais interesses são anulados pelos interesses ou direitos e liberdades fundamentais do titular dos dados, que requerem a proteção de dados pessoais, em particular quando o titular dos dados é uma criança. |
| **Proteção ao Crédito** | Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente | |

Do mesmo modo, a LGPD também possui bases legais diversas da GDPR no que se refere às hipóteses autorizadoras do tratamento de *dados sensíveis*. A atenção a este aspecto é fundamental para se evitar penalidades por tratamento ilícito dessa categoria especial de dados, cujos critérios são ainda mais rigorosos se comparados aos referentes a dados pessoais.

Observa-se que, se determinada empresa estiver adequada à GDPR e, sem se atentar às diferenças entre este regulamento e a LGPD, acabar por justificar o uso de dados de saúde de seus funcionários com base no *legítimo interesse*, terá assumido um risco demasiadamente alto, pois tal hipótese é proibida no Brasil, uma vez que não consta no rol de bases legais de dados sensíveis da LGPD. Nesse sentido, sintetizamos abaixo as diferenças entre as bases legais previstas para tratamento de dados sensíveis:

| **Bases Legais: Dados Sensíveis** | | |
|---|---|---|
| | **LGPD** | **GDPR** |
| **Consentimento** | Se utilizada esta base legal, o titular dos dados, ou seu responsável legal no caso de se tratar de criança, deve consentir, de forma específica e destacada, para finalidades específicas. | Se utilizada esta base legal, o titular dos dados deve consentir explicitamente para o tratamento de tais informações para um ou mais finalidades específicas. |
| **Cumprimento de obrigação legal ou regulatória** | O tratamento é indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador. | O tratamento é necessário para efeitos de cumprimento das obrigações e exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados no domínio do emprego e da segurança social e do direito de proteção social, na medida em que é autorizado pela legislação da União ou do Estado-Membro ou por uma convenção coletiva nos termos da legislação do Estado-Membro, desde que preveja salvaguardas adequadas dos direitos fundamentais e dos interesses do titular dos dados. |
| **Execução de políticas públicas** | O tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos. | O tratamento é necessário por razões de interesse público na área de saúde pública, como proteção contra problemas graves ameaças transfronteiriças à saúde ou garantia de elevados padrões de qualidade e segurança dos cuidados de saúde e medicamentos, produtos ou dispositivos médicos, com base na legislação da União ou dos Estados-Membros, desde que contenham disposições adequadas e específicas medidas para salvaguardar os direitos e liberdades do titular dos dados, em particular o sigilo profissional. |
| **Realização de estudos por órgão de pesquisa** | Quando o tratamento é indispensável para a realização de estudos por órgão de pesquisa, devendo-se garantir, sempre que possível, a anonimização dos dados pessoais sensíveis. | O tratamento é necessário para fins de arquivo de interesse público, pesquisa científica ou histórica, ou estatísticos, com base na legislação da União ou dos Estados-Membros, que devem ser proporcionais ao objetivo prosseguido, respeitar o conteúdo essencial do direito à proteção de dados e prever disposições adequadas e medidas específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados. |

| | | |
|---|---|---|
| **Exercício regular de direitos em processo judicial, administrativo ou arbitral**  | Quando o tratamento é indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral. | O tratamento é necessário para o estabelecimento, exercício ou defesa de ações judiciais ou sempre que os tribunais atuam na sua capacidade judicial. |
| **Proteção da vida ou da incolumidade física**  | Quando o tratamento é indispensável para a proteção da vida ou da incolumidade física do titular ou de terceiros. | O tratamento é necessário para a proteção dos interesses vitais do titular dos dados. |
| **Tutela da saúde**  | Quando o tratamento é indispensável para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. | O tratamento é necessário para efeitos de medicina preventiva ou ocupacional, para a avaliação da capacidade de trabalho do funcionário, diagnóstico médico, prestação de cuidados de saúde ou assistência social ou tratamento ou gestão dos sistemas e serviços de saúde ou de assistência social com base na legislação da União ou dos Estados-Membros, ou nos termos de um contrato com um profissional de saúde. |
| **Fraude**  | O tratamento é indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos dos titulares e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. | O tratamento é realizado, no curso das atividades legítimas do agente de tratamento com salvaguardas adequadas, por uma fundação, associação ou qualquer outra entidade sem fins lucrativos com finalidade política, filosófica, religiosa ou sindical, e sob a condição de que o tratamento diga respeito exclusivamente aos membros ou ex-membros do órgão ou a pessoas que tenham contato regular com ele, em conexão com seus objetivos, e que os dados pessoais não sejam divulgados fora desse corpo sem o consentimento dos titulares dos dados. |
| **Interesse Público**  | | O tratamento é necessário por razões de interesse público substancial, com base na legislação da União ou dos Estados-Membros, que devem ser proporcionais ao objetivo perseguido, respeitar a essência do direito à proteção de dados e prever disposições adequadas e medidas específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados. |
| **Dados tornados públicos pelo Titular**  | | O tratamento diz respeito a dados pessoais manifestamente tornados públicos pelo titular dos dados |

## B. Prazo para Resposta às Solicitações de Titulares

Outra diferença marcante e de fundamental importância entre a LGPD e a GDPR é o prazo para responder a solicitações feitas pelos titulares de dados: na GDPR, o controlador deve fornecer informações sobre as medidas tomadas em relação a uma solicitação feita pelo titular dos dados sem atrasos indevidos, no prazo de um mês após a recepção da solicitação, prorrogável por dois meses adicionais, se necessário, a depender da complexidade e do número de pedidos, e o controlador deve informar o titular dos dados sobre qualquer prorrogação no prazo de um mês a partir do recebimento da solicitação, juntamente com as razões para o

atraso (artigo 12 (3) da GDPR). Nesse sentido, vemos que a GDPR não diferencia os prazos para o atendimento aos direitos dos titulares; ou seja, independentemente da solicitação feita pelo titular, o prazo será o mesmo.

Por sua vez, a LGPD, em seu artigo 19, estabelece que o prazo para resposta à solicitação dos titulares nos pedidos de confirmação de existência de tratamento e acesso é imediato, se em formato simplificado, ou de quinze dias, se em formato completo, devendo indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial. Para as demais solicitações feitas com base nos direitos previstos pelo artigo 18 da LGPD, a legislação é silente quanto ao prazo de resposta. Por conta disso, enquanto não há qualquer posicionamento por parte da Autoridade Nacional de Proteção de Dados ("ANPD"), recomendamos que seja dado o mesmo tratamento aos demais direitos dos titulares. Importante ressaltar que tal entendimento pode vir a ser alterado após a manifestação da ANPD.
A tabela comparativa abaixo ilustra, de forma mais visual, os prazos para resposta às solicitações de titulares na LGPD e na GDPR:

| Procedimentos para Respostas às Solicitações de Titulares | |
|---|---|
| **LGPD** | **GDPR** |
| O controlador deve responder às solicitações de confirmação de existência de tratamento e acesso aos dados pessoais:<br><br>(i) imediatamente, se em formato simplificado, ou<br><br>(ii) em 15 dias, mediante declaração clara e completa indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, sob reserva do sigilo comercial e industrial. | As solicitações devem ser respondidas:<br><br>(i) sem atrasos indevidos; e<br>(ii) dentro de 1 mês a partir do recebimento.<br><br>O prazo pode ser estendido para 2 meses adicionais devido à complexidade e quantidade de solicitações. |

## C. DPO

Em relação ao cargo do DPO, ambas as legislações apresentam diferenças significativas. Na GDPR, os controladores e operadores devem indicar um DPO em circunstâncias específicas, como: (i) no caso de autoridade pública; (ii) caso haja monitoramento de dados em larga escala; ou (iii) no caso de tratamento de categorias especiais de dados em larga escala. Um grupo econômico pode nomear o mesmo DPO, desde que ele(a) seja facilmente acessível por qualquer entidade do grupo. Além disso, a GDPR estabelece que o DPO deve atuar com independência e reportar ao nível mais alto de gestão da sociedade.

Por sua vez, na LGPD, o DPO deve ser indicado por todo e qualquer operador ou controlador, independentemente da quantidade, categoria ou finalidade do tratamento de dados. O DPO, atualmente, pode ser uma ou mais pessoas físicas, ou até mesmo uma pessoa jurídica. Cabe à ANPD divulgar normas complementares sobre as situações de sua dispensa. A LGPD, ao contrário da GDPR, não estabelece explicitamente a obrigatoriedade de independência do DPO em relação à empresa a qual ele representa. Segue tabela comparativa com os principais pontos de diferença:

| DPO | |
|---|---|
| **LGPD** | **GDPR** |

| | |
|---|---|
| Os controladores e operadores devem indicar um DPO, que pode ser uma pessoa física ou jurídica.<br><br>A LGPD não limita a nomeação do DPO em circunstâncias específicas, cabendo à ANPD divulgar normas complementares sobre as situações em que poderá ser dispensada a indicação de tal pessoa, em função da natureza e do porte da entidade ou do volume das operações de processamento de dados. | Os controladores e operadores devem indicar um DPO em circunstâncias específicas, como:<br><br>(i) caso seja autoridade pública;<br>(ii) caso monitore dados em larga escala;<br>(iii) caso trate categorias especiais de dados pessoais em larga escala.<br><br>Além disso, um grupo de empresas pode nomear um mesmo DPO, desde que este seja facilmente acessível por cada estabelecimento. A GDPR estabelece, ainda, a necessidade de independência na atuação do DPO. |

## D. Incidentes de Segurança Envolvendo Dados Pessoais

Outra diferença marcante entre a LGPD e a GDPR refere-se às ações/medidas a serem tomadas em caso de incidente de segurança envolvendo dados pessoais. Na GDPR, caso constatada uma violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, se possível, em 72 (setenta e duas) horas após ter tomado conhecimento do incidente, notificar a violação de dados pessoais à autoridade de supervisão competente, a menos que da violação de dados pessoais seja improvável resultar risco para os direitos e liberdades dos titulares de dados. Caso a notificação à autoridade seja feita após o prazo de 72 (setenta e duas) horas, esta deve ser acompanhada da justificativa do atraso. Como visto, a comunicação sobre o incidente deve ser comunicada apenas à autoridade supervisora, inexistindo obrigatoriedade de comunicação aos titulares.

Por outro lado, a LGPD determina que o controlador informe à ANPD e aos titulares dos dados da ocorrência de um incidente de segurança, desde que tal incidente possa causar riscos ou danos relevantes aos titulares dos dados. A comunicação será feita em prazo razoável, conforme definido pela ANPD. Ou seja, no caso da LGPD, caso o incidente não possa causar qualquer tipo de risco ou dano relevantes aos titulares de dados, não será necessária a comunicação à ANPD ou aos titulares. Por outro lado, caso exista risco ou dano relevantes, a comunicação deverá ser feita em prazo razoável, sem qualquer informação sobre o que seria considerado um prazo razoável.

Elaboramos uma tabela comparativa para simplificar a compreensão deste ponto:

| **Procedimentos em Caso de Incidentes de Segurança** | |
|---|---|
| **LGPD** | **GDPR** |
| O controlador deve informar à ANPD e os titulares dos dados da ocorrência de um incidente de segurança que possa causar riscos ou danos relevantes aos titulares dos dados. A comunicação será feita em prazo razoável, conforme definido pela ANPD. | Em caso de violação de dados pessoais, o controlador deve, sem demora injustificada e, se possível, no mais tardar em até 72 (setenta e duas) horas após ter tomado conhecimento, notificar a violação de dados pessoais à autoridade de supervisão competente, a menos que a violação de dados pessoais seja improvável resultar em risco para os direitos e liberdades das pessoas singulares.<br><br>Se a notificação à autoridade não for feita no prazo de 72 horas, deve ser acompanhada da justificação do atraso. |

## E. Diferenças entre Legítimo Interesse e Consentimento

Por fim, importante mencionar as diferenças existentes entre as bases legais do legítimo interesse e consentimento em ambas as legislações. Em relação ao legítimo interesse, a LGPD estabelece que este somente poderá ser utilizado como fundamento para finalidades legítimas consideradas situações concretas, que incluem, mas não se limitam a: (i) apoio e promoção de atividades do controlador; e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais[46]. Inclusive, a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. Nesse sentido, tendo em vista a ausência de explicações detalhadas sobre essa base legal, entendemos que sua aplicação pode ser bastante abrangente, desde que utilizadas com cautelas e sempre em benefício dos titulares e garantidos seus direitos e liberdades.
Quanto ao legítimo interesse previsto pela GDPR, o ICO, autoridade nacional do Reino Unido, já se manifestou sobre o assunto[47] no seguinte sentido:

- Os interesses legítimos são a base legal mais flexível para o tratamento de dados, porém pode-se presumir que sempre será a mais apropriada;
- É provável que tal base legal seja mais apropriada na utilização dos dados dos titulares da maneira que eles razoavelmente esperariam e que tenham um impacto mínimo na privacidade, ou quando há uma justificativa convincente para o tratamento;
- Se a empresa optar por se basear em legítimo interesse assumirá responsabilidade extra para considerar e proteger os direitos e interesses dos titulares;
- As autoridades públicas só podem utilizar o interesse legítimo como base legal se o tratamento for feito por um motivo legítimo que não o desempenho de suas tarefas como autoridade pública;
- Existem três elementos essenciais na base do legítimo interesse, que exigem:
  - A identificação de um interesse legítimo;
  - A demonstração de que o tratamento é necessário; e
  - O equilíbrio com os interesses, direitos e liberdades dos titulares.
- O legítimo interesse pode ser do controlador ou de terceiros, que podem incluir interesses comerciais, interesses individuais ou benefícios sociais mais amplos;
- O tratamento deve ser necessário; se for possível alcançar razoavelmente o mesmo resultado de outra forma menos invasiva, o legítimo interesse não se aplicará;
- É necessário equilibrar os interesses do controlador com os dos titulares, de modo que, se eles não esperarem razoavelmente o tratamento, ou se isso puder causar danos injustificados aos titulares, os seus interesses provavelmente se sobreporão aos interesses legítimos do controlador ou do operador, conforme o caso;
- É necessário manter um registro de sua avaliação de interesses legítimos (LIA) para ajudá-lo a demonstrar conformidade, se necessário; e
- É necessário incluir detalhes de seus interesses legítimos nos avisos de privacidade.

Portanto, é possível observar que o legítimo interesse, na GDPR, além de ser mais detalhado quanto à sua forma de utilização e hipóteses em que não deve ser utilizado, já foi objeto de opinião específica por parte das autoridades, notadamente do ICO. Por outro lado, no Brasil ainda se aguarda um posicionamento da

[46] Conforme artigo 10 da LGPD.
[47] Disponível em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>. Acessado em 16 de novembro de 2020.

ANPD a esse respeito, a fim de esclarecer a forma de utilização correta dessa base legal e evitar qualquer tipo de prejuízo tanto aos titulares quando aos agentes de tratamento.

Por sua vez, em relação à base legal do consentimento, a GDPR diz que este deve ser livre, específico, informado e inequívoco, por meio de uma declaração ou por uma ação afirmativa clara. Da mesma forma, a LGPD indica que o consentimento deve ser livre, informado, inequívoco e, em situações específicas, no caso de tratamento de dados pessoais sensíveis ou de crianças, deve ser específico e em destaque. Portanto, quanto às características do consentimento, ambas as legislações seguem o mesmo raciocínio.

**COOKIES:** Por outro lado, diferentemente do que acontece no Brasil, na Europa existe também a Diretriz 2002/58/EC, a chamada *E-Privacy Directive* (Diretiva da Privacidade Eletrônica), também conhecida como *Cookie Law* (Lei dos Cookies), que dispõe sobre o tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrônicas. De acordo com tal norma, o consentimento deve ser coletado sempre que houver tratamento de dados a partir do uso de cookies, de modo que deve ser solicitado ao titular de dados o seu consentimento livre, informado e inequívoco quando de seu acesso a um site que se utiliza de cookies de marketing, performance, funcionais etc. Esta previsão inexiste no Brasil e, enquanto não houver diretrizes específicas sobre o tema por parte da ANPD, a base legal do legítimo interesse pode legitimar o tratamento de dados pessoais feito a partir de cookies, sendo, por ora, afastada a necessidade de coleta de consentimento contanto que as políticas de privacidade do website tragam transparência e informações a respeito de seu processamento e do método empregado.

Assim, conforme exposto acima, as diferenças entre a LGPD e a GDPR são relevantes e qualquer omissão ou erro poderá causar um dano à empresa. Portanto, as peculiaridades da LGPD e o alto grau de risco aos agentes de tratamento merecem atenção especial.

## 4.3. Da GDPR à LGPD: ajustes necessários e efeitos nas relações comerciais

No Capítulo anterior, apresentamos algumas das principais diferenças entre a LGPD e a GDPR, pois, apesar de tais normas geralmente serem referidas como similares, é possível verificar a existência de diversas particularidades. Neste contexto, analisaremos a seguir como essas diferenças devem ser observadas no procedimento de adequação das empresas já adaptadas à GDPR.

De início, vale mencionar que os efeitos da LGPD nas relações comerciais entre Brasil e Reino Unido foram positivos às empresas que saíram à frente e se posicionaram como adequadas a ambas as normas (GDPR e LGPD), pois os contratantes dessas duas localidades passaram a exigir cláusulas de proteção de dados com garantia de conformidade, inclusive com possibilidade de auditoria para constatação de cumprimento contratual e segurança da informação.

Algumas das empresas situadas no Brasil com atuação internacional, em especial as subsidiárias de multinacionais, empenharam-se em adotar medidas de adequação à GDPR quando de sua entrada em vigor, em 25 de maio de 2018, e agora buscam ajustar-se à LGPD.

Nesses casos, como as duas normas apresentam diversas similaridades, tais como princípios legais, direitos de titulares e algumas das obrigações e bases legais previstas, a adequação de tais empresas será simplificada, uma vez que, ao estarem adequadas à GDPR, necessitarão de adequações pontuais para a conformidade com a LGPD.

Normalmente, essas empresas focam e se limitam a adotar medidas de tecnologia da informação (por exemplo, com a alteração de softwares para obedecer aos critérios de segurança de ISOs 27001, 27002, 27701 etc.) e revisar alguns contratos internacionais (ex.: *Intra-Group Agreements* (IGAs)), a fim de que estes estejam adequados à GDPR. Todavia, a conformidade à LGPD ultrapassa medidas pontuais como estas. Em verdade, a análise de quais providências serão necessárias para complementar o trabalho de conformidade à GDPR deverá levar em consideração as especificidades da LGPD e demais normas aplicáveis para o correto ajuste ao ordenamento nacional, assim como a cultura à privacidade dos colaboradores localizados no Brasil, suas rotinas de atividades e os fluxos de dados desenvolvidos nesta localidade, que muitas vezes ocorre de forma diversa às operações realizadas na União Europeia.

Ou seja, a conformidade à GDPR não garante a adequação à LGPD.

De acordo com a nossa experiência, as seguintes medidas costumam ser as mais indicadas para complementar eventuais adequações à GDPR já adotadas:

(i) **Conscientização e treinamentos**: muitas dessas empresas sequer realizaram uma palestra de conscientização de seus colaboradores a respeito da LGPD, tampouco os treinaram com ações educativas para que estejam aptos a cumprir os procedimentos obrigatórios da LGPD, especialmente aqueles que são diferentes da GDPR, como prazos e forma de resposta a solicitações de titulares e quando e de que forma comunicar a ANPD e titulares sobre incidentes de segurança. Sem tal providência não será possível incorporar uma nova cultura de privacidade e proteção de dados e mitigar riscos de governança;

(ii) **revisão do RoPA**: o registro das atividades realizadas com dados pessoais deve ser feito para fins de cumprimento ao artigo 37 da LGPD. Se a empresa mapeou esses fluxos e se pautou pela GDPR, esta deverá rever a planilha para adequação das bases legais àquelas previstas na LGPD, tendo em vista as hipóteses adicionais e as diferenças entre as bases legais da GDPR e da LGPD, conforme explicado acima, além de verificar se as atividades desempenhadas fora do Brasil são as mesmas e, em caso negativo, avaliar a necessidade de elaboração de um novo RoPA, especifico e com as particularidades das atividades desenvolvidas no Brasil. Destaque-se que, no Brasil, muitas das atividades serão justificadas com base em obrigação legal, como em relações de trabalho, em que regras legais específicas do Brasil exigem o armazenamento de dados por dezenas de anos. Eventuais incorreções no RoPA podem acarretar a responsabilização da empresa, como poderá ocorrer no caso de exclusão indevida de dados;

(iii) **revisão de contratos, documentos e políticas**: planos de resposta a incidentes, como mencionado no item acima, são diferentes daqueles elaborados para a conformidade à GDPR. Da mesma forma, políticas de privacidade internas, externas, avisos de tratamento de dados aos colaboradores, cláusulas de contratos empregatícios, contratos entre agentes de tratamento, como prestadores e clientes, e também IGAs, devem ser ajustados para atenderem aos critérios de transferência internacional de dados estabelecidos na LGPD;

(iv) **governança corporativa**: as alterações e normas relacionadas à LGPD deverão ser acompanhadas e as rotinas de atividades monitoradas, pois não existe término ao procedimento de adequação à LGPD. Além de ser uma lei que aguarda diretrizes para ser interpretada, deve-se acompanhar e eventualmente treinar colaboradores e parceiros no sentido de manter as atividades com o menor risco possível, de acordo com as constantes mudanças no cenário jurídico incidente; e

(v) **nomeação do Encarregado pelo Tratamento de Dados Pessoais**: diferentemente da GDPR, que qualifica e caracteriza o *Data Protection Officer* (DPO) de maneira muito mais detalhada,

restringindo a atuação deste profissional em função que acarrete conflito de interesse, entre outras disposições, a LGPD é bastante sucinta e genérica ao dispor sobre tal profissional, como já exposto no Capítulo 2.2.1., item D. A LGPD estabelece que os agentes de tratamento deverão indicar o Encarregado pelo tratamento de dados pessoais, disponibilizando publicamente a sua identidade e as suas informações de contato, de forma clara e objetiva, preferencialmente no seu website[48]. Além disso, a LGPD indica que as atividades do Encarregado consistem em: (a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (b) receber comunicações da autoridade nacional e adotar providências; (c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares[49]. Por fim, a LGPD garante à ANPD o estabelecimento de normas complementares sobre a definição e as atribuições do Encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados[50].

A adequação à LGPD está baseada em três pilares principais, a saber, governança, jurídico e segurança/tecnologia da informação, sendo a governança um dos meios fundamentais para a diminuição de riscos. Tanto assim que a LGPD elenca medidas a serem incluídas no programa de governança em privacidade, a ser desenvolvido pela empresa, e antecipa a possibilidade de prestação de contas à ANPD sobre a efetividade dessas medidas[51]. Há, ainda, a necessidade de se manter o programa de privacidade devidamente atualizado mediante avaliações periódicas e com contínuo monitoramento das ações adotadas, podendo, inclusive, ser uma das atribuições do Encarregado a garantia de conformidade e o monitoramento do programa de privacidade construído ao longo do projeto de adequação.

Apesar de ser um viés fundamental, a grande maioria das empresas multinacionais já adequadas ao regulamento europeu de proteção de dados não adotou medidas de governança suficientes para garantir o cumprimento a este pilar da LGPD.

A importância de um programa de governança de privacidade é ainda mais clara quando se observa que um dos maiores riscos de responsabilização da empresa consiste em ações indevidas adotadas por seus próprios colaboradores. Com treinamentos de segurança e manutenção de programas corporativos de conformidade, riscos gerados por fatores humanos, que costumam ser responsáveis pela maioria dos incidentes cibernéticos, podem ser mitigados, assim como corrigidos equívocos comuns e dificilmente constatados, como compartilhamentos indevidos ou acessos por áreas que não teriam necessidade de coletar determinadas informações.

Não há dúvidas, portanto, que a mera adequação a GDPR necessitará ser complementada, seja com medidas jurídicas, de tecnologia e segurança da informação, ou de programas de governança corporativa e riscos.

Com relação à transferência internacional de dados, ainda há certa incerteza na União Europeia por conta da decisão do caso *Schrems II*[52], contudo recentemente foram divulgadas versões iniciais (*draft*) de novas

[48] Conforme artigo 41, § 1º da LGPD.
[49] Conforme artigo 41, § 2º da LGPD.
[50] Conforme artigo 41, § 3º da LGPD.
[51] Conforme artigo 50, I, d LGPD.
[52] O caso *Schrems II*, julgado em julho de 2020 pelo Tribunal de Justiça da União Europeia, declarou inválido o mecanismo de transferência internacional denominado *Privacy Shield*, até então utilizado para viabilizar transferências internacionais de dados pessoais entre União Europeia e Estados Unidos. Nessa mesma decisão, o Tribunal manteve válidas as transferências realizadas com base nas SCC, contudo, para a utilização deste mecanismo, deve-se examinar tanto os termos do contrato como as condições de privacidade e proteção a dados pessoais no país

Cláusulas Contratuais Padrão (*Standard Contractual Clauses* - SCCs), pela Comissão Europeia, a qual revisou as versões anteriores, dos idos de 2001/2004, sendo que estas atualizadas devem ser publicadas no segundo semestre de 2021.

Essa situação também pode significar uma boa oportunidade para efetuar transferências com maior segurança entre Brasil e Reino Unido, pois, ao participar ativamente do processo interpretativo da LGPD, atualmente incipiente no Judiciário, e da elaboração das primeiras diretrizes a respeito do tema, que possivelmente começarão por parte da estruturada ANPD nos próximos meses, será possível manter um certo pioneirismo nas relações que estão sendo construídas no momento atual entre ambos os países.

Além disso, em relação à transferência internacional de dados pessoais para países que não pertencem à União Europeia, a Comissão Europeia tem o poder de determinar, com base no artigo 45 da GDPR, se um país fora da União Europeia possui um nível adequado de proteção de dados. Por conseguinte, a adoção de uma decisão de adequação envolve: (i) uma proposta da Comissão Europeia; (ii) a opinião do EDPB; (iii) a aprovação de representantes de países da União Europeia; e (iv) a adoção da decisão pela Comissão Europeia.

Assim, o país estrangeiro ou organismo internacional que desejar receber os dados pessoais transferidos por países da União Europeia deverá demonstrar a capacidade de assegurar-lhes o mesmo grau de proteção previsto na GDPR.

Até agora, a Comissão Europeia reconheceu que Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça e Uruguai fornecem proteção adequada. Há negociações em andamento com a Coreia do Sul nesse sentido. No caso do Brasil, aqueles que pretenderem transferir dados deverão adotar uma das medidas previstas no artigo 46 da GPDR.

Destaca-se a análise realizada pelo Instituto de Tecnologia e Sociedade (ITS-Rio), de autoria do Professor Mario Viola, cujos principais argumentos estão transcritos abaixo[53]:

> "Mas, se por um lado deve ser compreendida a imperiosa necessidade de circulação internacional dos dados pessoais como um pressuposto de existência de uma economia que se apresenta cada dia mais globalizada, por outro é preciso reconhecer que assegurar um adequado grau de proteção a esses dados que serão objeto de transferência internacional é uma preocupação justificável e que existe antes mesmo das disposições da GDPR e da LGPD.
>
> Desde 1980 a OCDE já havia publicado as suas diretrizes relativas à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais[54], o que demonstra que a preocupação com a proteção dos dados pessoais é algo que não reprime, ao revés, fomenta, o desenvolvimento de um ambiente econômico saudável.
>
> Nesse sentido, é inegável o relevo da questão, pois eventual reconhecimento de que a LGPD garante ao Brasil um grau de proteção aos dados pessoais equivalente ao estatuído pela GDPR, permitirá que haja o livre fluxo de dados com a União Europeia, com potencial impacto econômico positivo, já que a economia relacionada ao mercado de dados deverá representar 5,4% do PIB da União Europeia até o ano de 2025[55].

de destino, cujas regras nesse campo devem garantir o mesmo nível de proteção da GDPR. Esta decisão poderá impactar a forma de condução desta matéria pela ANPD.

[53] Disponível em <https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acessado em 7 de dezembro de 2020.

[54] Disponível em <http:// www.oecd.org/sti/ieco - nomy/15590254.pdf>. Acessado em 7 de dezembro de 2020.

[55] Disponível em <https://europa. eu/rapid/press-release_IP19-2749_pt.html>. Acessado em 7 de dezembro de 2020.

> E a relevância do assunto poderá ser ainda maior caso venha a prosperar o recém anunciado Acordo de Associação Mercosul — União Europeia, que é baseado no "diálogo político, cooperação e livre comércio"[56]. Ou seja, o fluxo de dados pessoais entre empresas e até mesmo entre os governos do Brasil e dos países da União Europeia será fundamental para permitir um pleno aproveitamento da abertura comercial que se avizinha.
>
> Entretanto, mesmo o eventual (mas indesejado) insucesso na concretização do acordo entre o Bloco Sul-Americano e o Europeu não retirará do tema a importância que ele tem. Frisa-se as exportações brasileiras para a União Europeia somaram US$ 42 bilhões no último ano (2018), o que indica se tratar de um mercado proeminente, a merecer a devida atenção.
>
> Os ganhos econômicos, todavia, não podem e não devem ser enxergados como o elemento principal dessa equação. Os benefícios de um ambiente seguro para o tratamento de dados pessoais significam a proteção do próprio ser humano, visto que "a tutela jurídica da intimidade (e, também, da privacidade) constitui — qualquer que seja a dimensão em que se projete — uma das expressões mais significativas em que se pluralizam os direitos da personalidade"[57].
>
> Logo, obter o reconhecimento de adequação da LGPD à GDPR é medida que poderá resultar em ganhos econômicos e sociais que não podem ser desprezados."

Portanto, a transferência internacional merece destaque e deve ser viabilizada com a maior urgência possível, justamente visando possibilitar a concretização de diversos negócios, inclusive quando falamos no cumprimento de tratados de cooperação internacional.

Já em relação ao Brasil, a ANPD deverá analisar o nível de proteção de dados do país estrangeiro em consideração a: (i) normas gerais e setoriais do país de destino; (ii) natureza dos dados; (iii) observância dos princípios gerais de proteção de dados e direitos dos titulares previstos na LGPD; (iv) adoção de medidas de segurança previstas em regulamento; (v) existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e (vi) outras circunstâncias específicas relativas à transferência[58].

Enquanto a ANPD não se manifestar sobre o assunto, pode-se afirmar que, pelo fato da LGPD ter sido, em muitos aspectos, baseada na GDPR, e por todo o histórico e cultura de privacidade e proteção de dados, presente ao menos desde o ano 1970 na Europa, certamente o compartilhamento de dados pessoais entre o Brasil e países da União Europeia (incluindo o Reino Unido) estará adequado, sem a necessidade de adoção de qualquer outra medida prevista no artigo 33, inciso II da LGPD.

Por outro lado, quando estivermos diante da necessidade de adoção de SCCs ou de IGAs, é possível determinar que, no mínimo, as seguintes disposições devem estar presentes nesses documentos:

- **Intra-Group Agreements (IGAs)**: documentos corporativos de transferência intergrupo (i) quem são as partes envolvidas na transferência internacional; (ii) as definições que serão utilizadas no documento; (iii) o objeto e a duração do acordo; (iv) a natureza e a finalidade do tratamento, as categorias de dados pessoais e titulares de dados; (v) a obrigação de cada uma das partes, de quem compartilha os dados internacionalmente e de quem os recebe; e (vi) o dever de cooperação com as respectivas autoridades de proteção de dados; e

[56] Disponível em <http://www. itamaraty.gov.br/ima - ges/2019/2019_07_03_-_ Resumo_Acordo_Mercosul_UE.pdf>. Acessado em 7 de dezembro de 2020.
[57] Trecho do voto vencido proferido pelo Ministro Celso de Mello, do Supremo Tribunal Federal, no julgamento do RE 601.314/SP.
[58] Conforme artigo 34 da LGPD.

- **Cláusulas Contratuais Padrão (SCCs)**: (i) quem são as partes envolvidas na transferência internacional; (ii) as definições que serão utilizadas no documento; (iii) detalhes da operação de transferência de dados pessoais; (iv) a obrigação de cada uma das partes, de quem compartilha os dados internacionalmente e de quem os recebe; (v) cláusula de delimitação de responsabilidade; e (vi) o dever de cooperação com as respectivas autoridades de proteção de dados;

Outra questão que merece atenção das empresas já adequadas à GDPR é a utilização da base legal de legítimo interesse para basear a transferência internacional de dados pessoais. Enquanto a GDPR autoriza o emprego desta base como mecanismo de transferência internacional e dados, tal possibilidade inexiste em nossa lei. A LGPD contém um rol taxativo de hipóteses autorizadoras desse tratamento internacional de dados e nenhum deles cita o legítimo interesse[59]. Portanto, as empresas adequadas à GDPR e que eventualmente tenham utilizado tal base legal para transacionar dados pessoais com outros países, não poderão se valer dessa hipótese no Brasil e deverão, por mais este motivo, revisar o RoPA, IGAs e SCCs para adequá-los à LGPD.

Finalmente, no que se refere às relações comerciais entre Brasil e Reino Unido, não se pode afastar o grande benefício da entrada em vigor da LGPD, pois finalmente o Brasil aderiu à lista de mais de 100 (cem) países com um regulamento específico para proteger dados pessoais e privacidade, sendo o Reino Unido um dos expoentes no tema. Além de sua histórica cultura legislativa a respeito, o ICO é uma das autoridades de proteção de dados mais ativas do mundo no sentido de criar diretrizes detalhadas, aprofundadas, facilitar o acesso a estas e permitir a adequação e interpretação da norma por parte de titulares e agentes de tratamento.

[59] Conforme artigo 33 da LGPD.

# 5. Desafios e Oportunidades de Mercado

Um dos maiores desafios relacionados à entrada em vigor da LGPD no Brasil sem dúvida consiste na necessidade de adequação à norma com investimentos em meio à pandemia do Covid-19, impondo-se a compreensão e cumprimento de uma nova realidade cultural, com obrigações, direitos, princípios e conceitos em sua maioria distintos das imposições legais no *status quo*.

Outros fatores complexos e igualmente desafiantes são a realidade brasileira de excesso de litígios, a tendência de decisões judiciais conflitantes, a atuação concomitante de órgãos fiscalizadores como MPDFT, Senacom e Procon, com a consequente e já conhecida insegurança jurídica.

Não menos importante são a tardia formação da ANPD e a necessidade de publicação urgente de suas diretrizes sobre diversos artigos da LGPD que demandam mais detalhes sobre forma de cumprimento e aplicabilidade; alguns deles incluem as bases legais adequadas para o tratamento de dados de adolescentes, as medidas necessárias para a adequação de micro e pequenas empresas, assim como de startups, além de cláusulas contratuais modelo (SCCs) como garantia da transferência internacional facilitada de dados pessoais entre os países.

Mais um desafio a ser enfrentado refere-se ao fato de que o País é um dos que mais sofrem ataques cibernéticos no mundo, atingindo a 3ª posição. A certeza dos incidentes e das falhas de segurança nos sistemas impõem investimentos em melhoria técnica e treinamentos de políticas de segurança e de resposta a incidentes. As empresas que não estiverem adequadas estarão sujeitas a maior mácula e denegrimento de sua imagem e marca perante o mercado.

Nessa mesma linha de raciocínio, em 04 de janeiro de 2021 foi publicado o relatório elaborado pela *Eurasia Group*[60], uma das maiores consultorias de riscos geopolíticos do mundo, com um levantamento cuidadoso sobre os 10 (dez) principais riscos para o referido ano, sendo que dois dos maiores possuem relação direta com a área: dificuldades na *livre transferência internacional de dados* (5º risco da lista) e *problemas cibernéticos*, como ataques digitais para quebra de confidencialidade entre governos e falta de segurança no constante desenvolvimento de dispositivos tecnológicos e seu uso crescente (6º da lista).

O quinto risco acima mencionado, denominado "Global Data Reckoning", aponta que os obstáculos ao livre fluxo de dados através das fronteiras afetarão os modelos de negócios dependentes dessa transferência internacional facilitada e acarretando problemas para a economia global. Segundo prevê tal relatório, "o crescente protecionismo e soberania de dados se espalharão para as moedas digitais e fintechs nesse ano também. Isso será alimentado por preocupações em Bruxelas, Washington e dentro de órgãos de fiscalização financeiros internacionais, como o FMI, no sentido de que a inovação está ultrapassando a regulamentação e os governos reagirão fortemente para evitar a perda do controle de seu monopólio sobre os dados do setor financeiro".

Se há riscos, há oportunidades. Nota-se que a referida publicação menciona a competição estratégica entre os Estados Unidos e a China, as iniciativas de localização de dados ("data localization") desenvolvidas na Índia, e os debates constantes na Europa, aonde os dados se tornaram uma questão de soberania nacional. Presume-se, assim, que a criação de soluções para esses riscos e problemas será a grande oportunidade de crescimento no mercado.

[60] O relatório da Eurasia Group está disponível em <https://www.eurasiagroup.net/issues/top-risks-2021>. Acessado em 05 de janeiro de 2021.

Conforme explicado no Capítulo 2.1, a LGPD não foi a primeira norma a tratar de proteção de dados no Brasil, sendo possível identificar dezenas de dispositivos legais referentes a essa matéria na legislação brasileira. Entretanto, é inegável que foi a partir da publicação da LGPD, em 2018, que houve um crescimento expressivo de atividades relacionadas à área de proteção no Brasil, criando-se nossas oportunidades de mercado e um novo segmento de atuação profissional especializada, tanto para empresas quanto para prestadores de serviços.

Com a entrada em vigor da LGPD em 2020, a expectativa é de crescimento ainda maior dessa nova área no Brasil, uma vez que as empresas, públicas e privadas, conforme explicado no Capítulo 3, precisarão estar adequados à LGPD, o que exige a atuação coordenada de diversos profissionais durante a fase de conformidade e no posterior monitoramento desse procedimento, bem como da indicação de DPOs para tais empresas.

Há outros dados que corroboram a expectativa de que o desenvolvimento da nova área de proteção de dados no Brasil seja promissora, quais sejam: (i) a Associação Internacional de Profissionais de Privacidade (*International Association of Privacy Professionals* – IAPP) indicou o Brasil como o país com o maior crescimento de profissionais associados, uma vez que somente entre 2018 e 2019 foram mais de 300 (trezentos) novos membros; (ii) há um elevado número de advogados no Brasil que podem se dedicar à nova área, uma vez que se estima que, em 2019, havia mais de 1.100.000 (um milhão e cem mil) de advogados inscritos na Ordem dos Advogados do Brasil[61]; e (iii) há diversas iniciativas com soluções tecnológicas relacionadas à área de proteção de dados têm se multiplicado no Brasil, quase na mesma progressão de membros da IAPP.

Nesse sentido, algumas startups passaram a atuar no Brasil nos últimos 2 (dois) anos, no segmento de privacidade e proteção de dados, com o objetivo de trazer soluções inovadoras para alguns dos problemas e desafios enfrentados na área, incluindo-se empresas brasileiras e subsidiárias de empresas constituídas em outros países

É neste contexto que se passa a analisar oportunidades pontuais de negócios relacionados à proteção de dados no Brasil, com foco em possibilidades para a atuação de pessoas e empresas que também operam no Reino Unido.

## A. Intercâmbio de autoridades

É inegável que a maturidade da legislação e da prática de proteção de dados do Reino Unido poderá ser de grande valia para o desenvolvimento da área de proteção de dados no Brasil, inclusive no que se refere ao aperfeiçoamento da LGPD.

Isso porque, especialmente até que a ANPD passe a atuar ativamente na regulamentação da proteção de dados no Brasil, o Reino Unido pode assumir uma postura colaborativa com as autoridades brasileiras e auxiliar na elaboração e revisão de normas relacionadas à LGPD, contribuindo para a eliminação de lacunas normativas, interpretação de dispositivos legais e criação de uma cultura de proteção de dados no Brasil.

Tal atuação do Reino Unido decorrer de um intercâmbio de agentes reguladores com o Brasil, para que aqueles agentes atuantes no Reino Unido possam vir ao Brasil e os agentes brasileiros possam ficar um tempo no Reino Unido, a fim de permitir a troca de experiências e a melhor compreensão do funcionamento das normas de proteção de dados em ambos os países.

[61] Tal pesquisa está disponível em <https://migalhas.uol.com.br/quentes/312946/brasil-tem-um-advogado-para-cada-190-habitantes>. Acessado em 16 de novembro de 2020.

Uma das principais vantagens de tal intercâmbio de autoridades e troca de experiências é a diminuição dos custos de transação das transações envolvendo empresas do Brasil e do Reino Unido e do custo de adequação regulatória de subsidiárias do Reino Unido que venham a ser constituídas no Brasil, uma vez que haverá uma maior harmonização entre as normas de ambos os países.

## B. Intercâmbio de profissionais

O crescimento da área de proteção de dados no Brasil vem acompanhado de um aumento nas oportunidades de negócios relacionadas à prestação de serviços na área de proteção de dados, seja para viabilizar a adequação das empresas à LGPD, seja para manter o constante monitoramento da conformidade, incluindo a indicação e manutenção de um DPO, que, conforme já explicado, pode ser tanto uma pessoa física quanto pessoa jurídica.

Comprovando essa tendência, foi publicado um artigo em outubro de 2020 pela IAPP[62], no qual se estimou a necessidade de contratação de aproximadamente 50.000 (cinquenta mil) DPOs no Brasil nos próximos meses. Destaca-se que, em outro artigo do mesmo veículo, indicou-se que, em apenas um ano após a entrada em vigor da GDPR na União Europeia, mais de 500.000 (quinhentas mil) organizações registraram DPOs na União Europeia.

Assim, indicamos a seguir três serviços que tendem a apresentar um crescimento expressivo no Brasil nos próximos meses, em decorrência da entrada em vigor da LGPD.

### a. DPO as a Service

A LGPD, assim como a GDPR, permite que as empresas contratem terceiros para exercerem a função de DPO, o que se convencionou chamar de *DPO as a Service*. Tal prática permite às empresas o acesso a uma equipe de especialistas em privacidade e proteção de dados atuando como seu DPO e evita a sobrecarga dos recursos internos e nomeação de pessoas não qualificadas para o cargo. Assim, considerando que o DPO pode ser uma pessoa jurídica, empresas do Reino Unido que prestem tais serviços podem expandir suas atividades para o Brasil e oferecer o *DPO as a Service* para a empresas brasileiras, sendo que, nessa hipótese, contariam com a expertise já adquirida durante os anos de vigência da GDPR, apesar das especificidades da norma brasileira.

A decisão pela contratação de um DPO externo cabe à empresa, que deverá analisar, conjuntamente, os três pontos a seguir para concluir por qual caminho optar:

(i) **Expertise e qualificação dos colaboradores internos**: o DPO deve ter uma ampla gama de conhecimentos e habilidades multifuncionais, como experiência e conhecimento das leis de privacidade e proteção de dados aplicáveis ao negócio que representa; conhecimento da estratégia de negócios; experiência com treinamentos e campanhas de conscientização cultural; e capacidade de representar a empresa perante o público e reguladores.

Isso porque poucos indivíduos possuem todos esses requisitos dentro da própria empresa, e se têm, são provavelmente diretores ou estão em nível de gerência da empresa e, por isso, já possuem muitas responsabilidades acumuladas e não tem disponibilidade para gerenciar uma nova iniciativa como essa. Assim, a contratação de DPO as a Service vem para oferecer um suporte multifuncional para a empresa, gerindo o programa de privacidade de forma eficaz,

[62] Disponível em: https://iapp.org/news/a/study-lgpd-likely-to-require-at-least-50000-dpos-in-brazil-alone/>. Acessado em 15 de novembro de 2020.

através de um time de especialistas em privacidade e proteção de dados em tempo integral, que já possuem vasta experiência em gestão e execução de programas de privacidade.

(ii) **Independência e conflitos de interesse**: apesar de a LGPD não estabelecer a obrigatoriedade de independência, limitando-se a exigir a criação de uma ouvidoria, que será encarregada pela comunicação entre titulares de dados, empresa e ANPD, como regra geral o DPO atuaria de maneira independente e livre de conflito de interesses. Como algumas empresas não conseguiriam cumprir um requisito de independência devido às especificidades de seu quadro de colaboradores, o DPO as a Service se torna um produto interessante, especialmente porque o DPO externo claramente é independente e não conflita com outros interesses internos da empresa, assemelhando-se ao papel de auditores, consultores e advogados externos. Como a ANPD terá a função de complementar a LGPD no que se refere às funções do DPO, é possível que o caráter de independência seja ainda exigido no Brasil, o que provavelmente causaria um aumento no número de vagas e oportunidades da área.

(iii) **Custos**: os custos relacionados à contratação de um DPO externo podem ser elevados, considerando principalmente que esse tipo de serviço começou recentemente a ser oferecido no Brasil. Com a recente entrada em vigor da LGPD, muitas empresas ainda estão no início de seus procedimentos de adequação e tendem a analisar em breve o custo-benefício e a viabilidade da nomeação de um DPO interno ou a contração de um DPO as a Service. Dessa forma, é provável que este serviço tenha uma alta demanda nos próximos meses/anos, especialmente para atuação em empresas com times mais concisos, para os quais a dificuldade de se encontrar pessoas que se encaixam no perfil desejado é ainda maior. Além disso, devido à demanda, esse tipo de serviço tende a ter um custo variável a depender do tipo de atuação do DPO externo, o qual poderá ser geral ou especializado (*on demand*).

### b. Legal Services

Devido às especificidades da LGPD, as empresas precisarão ser assessoradas por profissional especializado, capaz de orientar corretamente o processo de conformidade com as leis de privacidade e proteção de dados, bem como prestar assistência para classificação e orientação de respostas à incidentes de segurança. A princípio, tais serviços serão prestados por advogados habilitados no Brasil, que deverão, ainda, cuidar dos litígios provenientes de eventuais problemas com o tratamento e manuseio dos dados pessoais.

Entretanto, especialmente para as empresas multinacionais, transferência internacional de dados e no caso de celebração de contratos por partes de diferentes países (incluindo o Reino Unido), será necessária a atuação conjunta entre advogados com conhecimento tanto da LGPD quanto da GDPR. Além disso, a experiência dos advogados que já atuam com a GDPR é de extrema importância para o desenvolvimento e interpretação das normas aplicáveis ao Brasil, de modo que há a possibilidade de uma postura colaborativa também entre advogados do Brasil e do Reino Unido.

## C. Outros prestadores de serviços

Como se verifica, as oportunidades de negócios que devem surgir no Brasil incluem empresas que prestem serviços relacionados a soluções tecnológicas, compliance, *accountability*, tecnologia, segurança da informação, riscos etc.

Cita-se, por exemplo, a atuação da empresa One Trust, considerada a principal plataforma de privacidade do mundo e que já tem prestado serviços relacionados à proteção de dados no Brasil. Nesse sentido, é importante também destacar que 7 (sete) empresas britânicas são credenciadas como *Official Training*

*Partners* no IAPP, enquanto no Brasil o número cai para apenas dois, o que demonstra o grande potencial de sinergia entre a experiência de empresas britânicas e as necessidades de crescimento do Brasil.

Um serviço que tende a ser cada vez mais requisitado no Brasil, também, é o *Assessment Manager*, que realiza a automatização de diferentes funções de um programa de privacidade, desde a operacionalização de avaliações de impacto de privacidade e localização de lacunas de risco até a entrada de dados e relatórios. Atualmente existem no máximo três plataformas que realizam esta função no Brasil; entretanto, nenhuma delas possui a expertise dos softwares europeus.

Entretanto, é importante destacar que, tanto para a atuação de profissionais quanto de empresas do Reino Unido no Brasil será necessário o conhecimento/adequação de seus serviços às exigências específicas da LGPD. Apesar disso, conforme já explicado no Capítulo 4 acima, como as duas normas possuem diversos pontos de contato, tal adaptação não tende a representar custos elevados ou demandar um longo tempo para adequação.

Deve-se ter em mente a necessidade de unir a experiência do Reino Unido na área com as especificidades da nossa cultura e diploma legal. Se as iniciativas caminharem em conjunto, pode-se criar produtos realmente únicos, com experiência em privacidade, cultura híbrida e técnica jurídica específica e local.

# 6. Conclusão

Diante da realidade de um mundo hiperconectado e uma economia nutrida por dados pessoais, a privacidade se tornou líquida na mesma medida em que o controle sobre as nossas informações pessoais se diluiu, como atesta Zygmunt Bauman. Nesse contexto, a **LGPD** e à **GDPR** são fundamentais para que não se perca de vista a privacidade e a proteção aos dados pessoais.

Toda empresa deve se adequar ao regulamento incidente e o fato de uma empresa estar em conformidade com à GDPR não afasta a necessidade de adotar mecanismos específicos para se ajustar à LGPD, caso processe dados de indivíduos localizados no Brasil, ou lhes ofereça serviços ou produtos.

Como se viu neste estudo, para a adequação com menor risco aos agentes controladores ou operadores dos dados, deve-se observar fatores específicos como a estrutura corporativa, modelo de negócio, produtos desenvolvidos, público-alvo e áreas de atuação. A empresa é um organismo vivo, portanto o procedimento de adequação não é um fim, mas um meio; as etapas a serem implementadas permanecerão como métodos a serem mantidos e revisitados. O mapeamento dos dados, etapa inicial do procedimento, é apenas um retrato daquele momento da empresa e deverá ser reelaborado ou alterado de acordo com as novas realidades ou produtos que surgirem. Elucidamos estes pontos ao explicar sobre o método de adequação *tailor-made* e suas implicações em diversos setores da empresa.

Os casos judiciais brasileiros compilados neste Relatório demonstram que a LGPD não tardou a ser suscitada em ações judiciais. Em apenas um mês de sua vigência, o MPDFT propôs a primeira ação civil pública com base em violações contra a referida lei; desde então, diversas demandas judiciais foram apresentadas e os consumidores têm apostado em seus direitos como titulares de dados pessoais para publicar reclamações contra empresas omissas ou negligentes.

Em meio ao inevitável crescimento da judicialização, a **ANPD** finalmente foi estruturada,, elaborou sua primeira orientação educacional sobre a Lei, revelou um de seus papeis fundamentais para além de zelar pela proteção a dados pessoais, i.e., editar normas e trazer orientações simplificadas, e ainda publicou um programa de temas a serem objeto de diretrizes para os próximos meses

Ainda que seja altamente desafiante às empresas a garantia de adequação à LGPD em meio à pandemia do Covid-19, não se pode afastar de vista as inegáveis oportunidades que caminham junto com este novo cenário.

A Lei pode ser vista como um valor positivo para a empresa.

Muito embora os fatores mais mencionados ao se falar da LGPD se resumam ao elevado valor das sanções e excesso de demandas judiciais, a visão de uma legislação meramente punitiva não se adequa às suas reais oportunidades. Com efeito, o Brasil passa a ter uma chance considerável de ser reconhecido como uma jurisdição adequada para o livre fluxo de dados pessoais com a União Europeia e possivelmente Reino Unido, o que contribuiria para incrementar parcerias de negócio, internacionalizar empresas nacionais, facilitar o ingresso no mercado brasileiro e garantir maior competitividade.

Adicione-se que a obrigação de tecnicidade aos agentes, DPOs, empresas, legaltechs, *players* e demais profissionais atuantes no ramo da privacidade no Brasil abre espaço à expertise e prática dos concorrentes do Reino Unido no setor, seja mediante treinamentos direcionados, ou por investimento e internacionalização de iniciativas na área de privacidade, inclusive soluções tecnológicas para adequação automatizada, seguros e prevenção de riscos cibernéticos, e atendimento a direitos de titulares de forma facilitada.

Não se pode finalizar este Relatório sem repisar o fato de que neste novo cenário, os indivíduos passam a valorizar com tenacidade seus direitos na qualidade de titulares das informações pessoais, buscam com maior propriedade o cumprimento às obrigações legais inerentes a esta proteção o que causa um efeito viral da lei e termina por impor, entre empresas, cláusulas de proteção a dados pessoais em conformidade com a LGPD. Invariavelmente, esses fatores impulsionam que as empresas adequadas à LGPD obtenham maior credibilidade perante parceiros e clientes, conquistem espaço com maior facilidade em relação à concorrência e não percam oportunidades de negócios.

Portanto, conclui-se que os desafios enfrentados com a mudança cultural no Brasil no que tange à privacidade e proteção a dados pessoais, além das implicações e investimentos no procedimento de adequação em si, não se sobrepõem às diversas oportunidades de mercado.