UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO
DEPARTAMENTO DE CIÊNCIAS DA INFORMAÇÃO
CURSO DE ARQUIVOLOGIA

GISLENE ANTUNES DE OLIVEIRA

A LEI DE PROTEÇÃO DE DADOS PESSOAIS:

impacto nas pessoas físicas e jurídicas

PORTO ALEGRE
2018

GISLENE ANTUNES DE OLIVEIRA

A LEI DE PROTEÇÃO DE DADOS PESSOAIS:

impacto nas pessoas físicas e jurídicas

Trabalho de Conclusão de Curso (TCC) apresentado como requisito parcial para a obtenção do título de Bacharel em Arquivologia da Faculdade de Biblioteconomia e Comunicação da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Moisés Rockembach

PORTO ALEGRE
2018

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Reitor: Prof. Dr. Rui Oppermann
Vice-Reitora: Prof.ª Dr.ª Jane Fraga Tutikian

FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO

Diretora: Prof.ª Dr.ª Karla Maria Müller
Vice-Diretora: Prof.ª Dr.ª Ilza Maria Tourinho Girardi

DEPARTAMENTO DE CIÊNCIAS DA INFORMAÇÃO

Chefe: Prof.ª Dr.ª Jeniffer Alves Cuty
Vice-Chefe: Prof.ª Dr.ª Eliane Lourdes da Silva Moro

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação

Jacques, Gislene Antunes de Oliveira
A Lei de Proteção de Dados Pessoais: impacto nas pessoas físicas e jurídicas / Gislene Antunes de Oliveira Jacques. -- 2018.
113 f.
Orientador: Moisés Rockembach.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Biblioteconomia e Comunicação, Curso de Arquivologia, Porto Alegre, BR-RS, 2018.

1. Lei de Proteção de Dados Pessoais. 2. Privacidade. 3. Direitos fundamentais. 4. Tratamento de dados pessoais. I. Rockembach, Moisés, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

GISLENE ANTUNES DE OLIVEIRA

A LEI DE PROTEÇÃO DE DADOS PESSOAIS:

impacto nas pessoas físicas e jurídicas

Trabalho de Conclusão de Curso apresentado à Faculdade de Biblioteconomia e Comunicação da Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do grau de Bacharel em Arquivologia.

Aprovado em: ____/_____/_____

BANCA EXAMINADORA

_____
Prof. Dr. Moisés Rockembach – UFRGS
Orientador

_____
Prof.ª Dr.ª Jeniffer Cuty – UFRGS
Examinadora

_____
Prof.ª Marieta Marks Löw – UFRGS
Examinadora

AGRADECIMENTOS

A Deus, por ter mais uma experiência de estudo e crescimento como pessoa.

À Universidade Federal do Rio Grande do Sul, por mais uma oportunidade de me desenvolver como acadêmica e cidadã. E que continue sendo esta Universidade pública, gratuita e de qualidade.

À Fabico, pelos 10 anos de ensino e muito aprendizado primeiro em Biblioteconomia e agora em Arquivologia.

Ao meu orientador, Professor Moisés Rockembach pelos ensinamentos, atenção e auxílio durante a trajetória acadêmica e de orientação.

À Professora Jeniffer Cuty e Professora Marieta Löw que prontamente aceitaram participar desta banca examinadora.

À Professora Ana Regina Berwanger, meu reconhecimento pelo legado transmitido todos estes anos à Arquivologia da UFRGS.

Aos meus nobres colegas que fizeram a Arquivologia ser mais humana e mais forte. Ensinaram-me valores muito importantes de ser membro de uma equipe que se ajuda e compreende o outro com todas as suas dificuldades. Desejo a todos que o caminho seja iluminado e de novas conquistas.

À minha grande amiga e colega, Marilene Flores, que ao longo deste caminho tive oportunidade de conhecê-la e hoje tê-la como amiga e, posso dizer, uma irmã. Muito obrigada por tudo. A verdade sempre prevalece.

À minha mãe que sempre lutou por mim, por minha educação e por me fazer a gostar de estudar.

Ao meu marido, pela ajuda e compreensão todos estes anos.

À minha filha querida, dedico este trabalho e tudo aquilo que eu puder fazer para ajudá-la a crescer como pessoa, como cidadã, como aluna. Ela nasceu conhecendo à Fabico e a UFRGS, e hoje cresce sabendo valorizar a nossa história.

Muito obrigada!

RESUMO

O presente trabalho tem como objetivo apresentar a Lei de Proteção de Dados Pessoais, sancionada no ano de 2018, que regula as ações de coleta e tratamento de dados pessoais realizados por instituições públicas e privadas, com fundamentos específicos que devem ser contemplados como o respeito à privacidade, com vistas a proteger os direitos fundamentais e o desenvolvimento da personalidade da pessoa natural. Analisa a legislação nacional referente à pessoa física e jurídica, os respectivos direitos e deveres, aos quais são contemplados na Constituição Federal de 1988, Código Civil, Código de Defesa do Consumidor, Lei do Marco Civil da Internet e a Lei de Proteção de Dados Pessoais e outras leis que foram citadas ao longo do trabalho. Utiliza os pressupostos metodológicos de abordagem exploratória, explicativa, qualitativa e pesquisa bibliográfica em legislações pertinentes à temática e aos aspectos teóricos conceituais, para compreender o possível impacto da implementação da LPDP nas pessoas físicas e jurídicas. Conclui que as instituições públicas e privadas devem se adequar à lei; os cidadãos poderão solicitar os seus dados pessoais e autorizar o consentimento de uso. Conforme a lei, o tratamento de dados pessoais deverá ser realizado por agentes designados para executar esta função e, com esta perspectiva existe a possibilidade de inserção da área da Arquivologia e dos profissionais arquivistas, neste novo campo de atuação na área da ciência e tecnologia.

Palavras-chave: Lei de Proteção de Dados Pessoais. Privacidade. Direitos fundamentais. Tratamento de dados pessoais.

ABSTRACT

This paper aims to present the Personal Data Protection Law, enacted in 2018, which regulates the collection and processing of personal data by public and private institutions, with specific grounds that should be considered as respect for privacy, with a view to protecting fundamental rights and developing the personality of the natural person. It analyzes the national legislation regarding the individual and legal, the respective rights and duties, which are contemplated in the Federal Constitution of 1988, Civil Code, Consumer Protection Code, Internet Civil Law and Personal Data Protection Act and other laws that have been cited throughout the work. It uses the methodological assumptions of exploratory, explanatory, qualitative and bibliographic research in legislation pertinent to the thematic and conceptual theoretical aspects, to understand the possible impact of the implementation of Personal Data Protection Act on individuals and legal entities. It concludes that public and private institutions must conform to the law; the citizens can request their personal data and authorize the consent of use. According to the law, the processing of personal data must be carried out by agents appointed to perform this function and, with this perspective, there is the possibility of insertion of the area of Archivology and archivists in this new field of action in the area of science and technology.

Keywords: Law of Protection of Personal Data. Privacy. Fundamental rights. Treatment of personal data.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BBC	British Broadcasting Corporation
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CDC	Código de Defesa do Consumidor
CF	Constituição Federal de 1988
CPF	Cadastro de Pessoa Física
DUDH	Declaração Universal dos Direitos Humanos
GDPR	General Data Protection Regulation
LAI	Lei de Acesso à Informação
LPDP	Lei de Proteção aos Dados Pessoais
MCI	Marco Civil da Internet
ONU	Organização das Nações Unidas
UFRGS	Universidade Federal do Rio Grande do Sul

SUMÁRIO

1 INTRODUÇÃO

Este trabalho teve como objetivo apresentar a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei de Proteção de Dados Pessoais (LPDP), que dispõe sobre o tratamento de dados pessoais, abarcando também os dados pessoais em meios digitais por pessoa natural ou por pessoa jurídica de direito público ou privado. A Lei preconiza a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ainda cabe salientar o impacto desta nova Lei que tem a prerrogativa de expressar as regras sobre o tratamento de dados pessoais que envolvem as pessoas físicas e as instituições públicas e privadas.

Com a premissa da publicação da LPDP e de todas as diretrizes elencadas pode-se preconizar um novo campo de atuação aos arquivistas. A Lei refere-se ao tratamento de dados pessoais com especificação de determinadas operações que pressupõem à área arquivística como coleta, produção, classificação, acesso, reprodução, transmissão, processamento, arquivamento, eliminação, avaliação, comunicação, transferência e difusão de informações. Porém ainda não existe nenhuma orientação de autoridades do meio arquivístico para proceder ou inserir às atividades desempenhadas pelos profissionais da área.

Como a Lei foi sancionada em agosto de 2018, com vigência em 18 meses, ainda não houve tempo hábil para a difusão deste novo instrumento legal e a inserção de novas demandas às práticas arquivísticas. É importante salientarmos, que não existe nenhuma menção ao Arquivista ou à área da Arquivologia. Também não existe nenhuma referência na Lei de Acesso à Informação – LAI (2011) aos Arquivistas, mas suas atuações são pautadas em grande parte à essa Lei.

Salientamos a importância da LPDP para a área da Arquivologia e o potencial de agregar novas demandas. Sobretudo sobre a formação dos arquivistas que não somente devem ser custodiadores de informação em suportes de papel, mas também adequar-se às perspectivas de paradigmas que envolvam a ciência e a tecnologia.

No segundo capítulo apresentamos a conceituação de alguns termos e contextualização em alguns ordenamentos legais e jurídicos referentes à pessoa física e jurídica. Apresentamos também as premissas de direitos e deveres destas pessoas e a posição do Estado como definidor de regras fundamentadas em instrumentos

legais como citada a Constituição Federal de 1988; o Código de Defesa do Consumidor (1990); a Lei de Acesso à Informação - LAI (2011) e a Lei do Marco Civil da Internet (2014). Identificamos a legislação pertinente ao tema e toda a trajetória de previsão legal que foram importantes para compreender a evolução das leis, de acordo com as necessidades que foram surgindo ao longo do tempo. O Marco Civil serviu de base para a compreensão da Lei de Proteção de Dados Pessoais que foi sancionada para estabelecer uma série de regras para organizações que atuam no Brasil e terão que segui-la para permitir ao cidadão mais controle sobre os seus dados pessoais e aos referentes ao sigilo de comunicações e à privacidade.

No terceiro capítulo apresentamos a metodologia utilizada na pesquisa com base na abordagem exploratória, explicativa, bibliográfica e qualitativa em legislações pertinentes à temática e aos aspectos teóricos conceituais, com vistas a compreender o possível impacto da implementação da LPDP nas pessoas físicas e jurídicas.

No quarto capítulo apresentamos a Lei de Proteção de Dados Pessoais (LPDP) com as suas principais diretrizes que fundamentaram a publicação e a alteração da Lei nº 12.965, de 23 de abril de 2014, que é denominada como Lei do Marco Civil na Internet (MCI). Mas também discorremos sobre a importância deste instrumento legal, o primeiro no mundo com abordagem referente aos princípios e regras, direitos e deveres dos usuários, provedores de serviços e conteúdos no uso da internet no país.

A partir de 2018, quando foi sancionada a LPDP, estabeleceu-se um prazo de 18 meses para a adaptação de pessoas físicas e jurídicas, com vistas a contemplar as considerações fundamentadas nesta Lei. Portanto, somente entrará em vigor em 2020, um tempo razoável para que pessoas físicas e jurídicas se adaptem e cumpram as normativas elencadas referente à proteção de dados pessoais.

No quinto capítulo abordamos os possíveis impactos da LPDP nas pessoas físicas e jurídicas e o impacto nas atividades dos setores públicos e privados no tratamento dos dados pessoais apresentados em sítios eletrônicos; portais de transparência; fluxos de comunicações que podem desrespeitar o sigilo e a privacidade individual.

A partir de uma reflexão inicial sobre o tema foi possível a determinação do problema de pesquisa:

Quais são os possíveis impactos que a Lei de Proteção de Dados Pessoais acarretará nas pessoas físicas e jurídicas?

A delimitação do problema oportunizou a elaboração dos objetivos:

Objetivo Geral:

Analisar o impacto da Lei de Proteção de Dados Pessoais nas pessoas físicas e jurídicas.

Objetivos Específicos:

a) apresentar a Lei de Proteção de Dados Pessoais e a Lei de Acesso à Informação;
b) conceituar e delimitar pontos relevantes referentes à Lei de Proteção de Dados Pessoais;
c) identificar as alterações ocorridas em outras legislações em decorrência da Lei de Proteção de Dados Pessoais;
d) descrever o possível impacto da Lei de Proteção de Dados Pessoais;
e) identificar o campo de atuação para o arquivista através da Lei de Proteção de Dados Pessoais.

2 CONTEXTUALIZAÇÃO TEÓRICA E LEGAL

Antes de adentrar no cerne do objeto deste trabalho cabe, primeiramente, conceituar alguns termos e contextualizá-los em alguns ordenamentos legais e jurídicos.

No âmbito jurídico, o termo pessoa física é denominado também de “pessoa natural” o que remete à representação jurídica de um indivíduo que possui capacidade para adquirir direitos e assumir obrigações, relacionado ao momento do nascimento (BRASIL, 2002).

O termo pessoa natural configura que todo ser humano tem direitos e deveres, dotado de personalidade envolvendo a questão moral e sua posição como consumidor e em sua atuação como cidadão no Estado (BRASIL, 2002).

Com intuito de estabelecer a aquisição da personalidade jurídica de uma pessoa natural, ou seja, a capacidade de adquirir direitos e deveres, o Código Civil estabeleceu no seu art. 2º que: “A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro” (BRASIL, 2002). O que identifica a capacidade do indivíduo de garantir seus próprios direitos e, por consequência, cumprir seus deveres.

No artigo 1º do Código Civil (2002) “Toda pessoa é capaz de direitos e deveres na ordem civil”. Mas, não existe o pressuposto concreto de que ela pode exercer a capacidade por si própria, o que demanda análise sobre este fator de forma mais abrangente.

A dotação de personalidade está relacionada com a capacidade de direito e de fato. A capacidade de direito é a forma como a pessoa física pode adquirir os seus direitos ou assumir obrigações (DICIONÁRIO JURÍDICO ONLINE, 2018). A capacidade de fato é o momento quando a pessoa física passa a exercer os seus direitos e demais responsabilidades pertinentes. A relação de capacidade é conduzida a garantir que o cidadão possua os direitos e que tenha a responsabilidade civil sobre seus atos (DICIONÁRIO JURÍDICO ONLINE, 2018).

Em outro aspecto, o indivíduo pode não se encontrar apto para exercer a sua capacidade e não a exercer de forma autônoma, denominada como incapacidade jurídica. São denominados os absolutamente incapazes:

> Art. 3º São absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 (dezesseis) anos.
>
> Art. 4º São incapazes, relativamente a certos atos ou à maneira de os exercer:
>
> I - os maiores de dezesseis e menores de dezoito anos;
> II - os ébrios habituais e os viciados em tóxico;
>
> III - aqueles que, por causa transitória ou permanente, não puderem exprimir sua vontade;
>
> IV - os pródigos. (BRASIL, 2002).

Segundo o Código Civil (2002), a pessoa jurídica é uma expressão reconhecida pela justiça, com obrigações e deveres. Assim como, configura uma unidade jurídica que resulta de uma coletividade humana ordenada, podendo ser privada ou pública, com características e finalidades específicas.

> Art. 40. As pessoas jurídicas são de direito público, interno ou externo, e de direito privado.
>
> Art. 41. São pessoas jurídicas de direito público interno:
>
> I - a União;
>
> II - os Estados, o Distrito Federal e os Territórios;
>
> III - os Municípios;
>
> IV - as autarquias, inclusive as associações públicas;
>
> V - as demais entidades de caráter público criadas por lei.
>
> Parágrafo único. Salvo disposição em contrário, as pessoas jurídicas de direito público, a que se tenha dado estrutura de direito privado, regem-se, no que couber, quanto ao seu funcionamento, pelas normas deste Código.
>
> Art. 42. São pessoas jurídicas de direito público externo os Estados estrangeiros e todas as pessoas que forem regidas pelo direito internacional público.
>
> Art. 43. As pessoas jurídicas de direito público interno são civilmente responsáveis por atos dos seus agentes que nessa qualidade causem danos a terceiros, ressalvado direito regressivo contra os causadores do dano, se houver, por parte destes, culpa ou dolo.
>
> Art. 44. São pessoas jurídicas de direito privado:

> I - as associações;
>
> II - as sociedades;
>
> III - as fundações;
>
> IV - as organizações religiosas;
>
> V - os partidos políticos;
>
> VI - as empresas individuais de responsabilidade limitada. (BRASIL, 2002).

Ao retornar ao termo capacidade, se pode afirmar que essa constitui-se à medida dessa personalidade em exercer relações jurídicas. Estas não se relacionam somente com a transformação em pessoa jurídica, mas a todas as relações de consumo. A pessoa, ao estabelecer relação jurídica, está relacionada também com ser consumidor. Do Código de Defesa do Consumidor (CDC), Lei nº 8.078/1990, se pode extrair alguns conceitos.

O artigo 2º do CDC dispõe que “consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final”; o parágrafo único do artigo 2º do CDC somente faz uma equiparação ao termo consumidor “a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo”; o artigo 17 do CDC também por equiparação afirma que todas as vítimas do dano causado pelo fato do produto e do serviço são consideradas consumidoras. E, por fim o artigo 29 do CDC indica que são equiparadas a consumidor todas as pessoas, determináveis ou não, expostas às práticas comerciais e que, por isso, fazem jus à proteção contratual.

Reza no art. 6º do CDC os direitos básicos do consumidor:

> I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;
>
> II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações;
>
> III - a **informação adequada e clara** sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;

> IV - **a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;** (grifo nosso)
>
> V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas;
>
> VI - **a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos**; (grifo nosso)
>
> VII - o acesso aos órgãos judiciários e administrativos com vistas à prevenção ou reparação de danos patrimoniais e morais, individuais, coletivos ou difusos, assegurada a proteção Jurídica, administrativa e técnica aos necessitados;
>
> VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências;
>
> (...)
>
> X - a adequada e eficaz prestação dos serviços públicos em geral. (BRASIL, 1990).

Os dados pessoais dos consumidores encontram-se em banco de dados ou cadastros físicos. Esses bancos de dados ou cadastros se referem a uma forma abrangente às modalidades de armazenamento de informações (PINHEIRO, 2012). O CDC garante proteção ao cidadão contra a violação desses dados.

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> Parágrafo 1. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> Parágrafo 2. A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> Parágrafo 3. O consumidor, sempre que encontrar inexatidão em seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

> Parágrafo 4. Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> Parágrafo 5. Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. (BRASIL, 1990).

Antes de dar continuidade com as relações jurídicas, as pessoas e ao consumidor, é importante percorrer um caminho sobre direitos e a informação em uma relação diferente que a existente entre consumidor e vendedor/fornecedor, facilitando desta forma o entendimento das novas relações de consumo existentes na atualidade onde se utiliza a internet.

Inicia-se essa trajetória pela Declaração Universal dos Direitos Humanos (DUDH), da Organização das Nações Unidas (1948), que prevê em seu art. 19º que “Todo ser humano tem direito à liberdade de opinião e de expressão; esse direito inclui a liberdade de ter opiniões sem sofrer interferência e de procurar, receber e divulgar informações e ideias por quaisquer meios, sem limite de fronteiras” (ONU, 1948).

O Brasil assinou vários atos internacionais que deram reconhecimento à importância de garantir e proteger o direito à informação. Dentre eles, podemos citar o Pacto Internacional dos Direitos Civis e Políticos em 1966; a Declaração Interamericana de Liberdade de Expressão no ano 2000 e a Convenção das Nações Unidas contra a Corrupção em 2003 que traz em seus artigos 10º e 13º que cada Nação-Estado deverá:

> [...] tomar as medidas necessárias para aumentar a transparência em sua administração pública [...] procedimentos ou regulamentos que permitam aos membros do público em geral obter [...] informações sobre a organização, funcionamento e processos decisórios de sua administração pública [...]. (ONU, 2003).

A Constituição Federal de 1988 quando trata dos Princípios Fundamentais traz nos incisos de seu artigo primeiro alguns fundamentos:

> I - a soberania;
>
> II - a **cidadania**;
>
> III - a **dignidade da pessoa humana**;
>
> IV - os valores sociais do trabalho e da livre iniciativa;

> V - o pluralismo político. (BRASIL, 1988).
>
> (Grifo nosso)

E de seu art. 3º os Objetivos Fundamentais da República Federativa do Brasil:

> I - construir uma **sociedade livre, justa e solidária**;
>
> II - garantir o desenvolvimento nacional;
>
> III - erradicar a pobreza e a marginalização e **reduzir as desigualdades sociais e regionais**;
>
> IV - **promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.** (BRASIL, 1988).
>
> (Grifo nosso)

Na Constituição de 1988 foi apresentada uma ação denominada de *habeas data*, que possibilita e assegura “o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público” (BRASIL, 1988). Os órgãos públicos devem permitir o acesso a informações de interesse particular, coletivo ou geral, de acordo com a demanda preconizante.

Ainda na CF/1988 importante destacar alguns dos incisos do art. 5º dos direitos e deveres individuais e coletivos, que se relacionam e corroboram com a Declaração Universal e, que se preconiza por ser um dispositivo de internacionalização dos direitos humanos e no seguimento de orientações sobre um conjunto de valores universais que atua como regulador dos direitos e garantias fundamentais dos cidadãos.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> I - homens e mulheres são iguais em direitos e obrigações, nos termos desta Constituição;
>
> II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;
>
> III - ninguém será submetido a tortura nem a tratamento desumano ou degradante;
>
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
>
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias;

(...)

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(...)

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

(...)

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

(...)

XXVII - aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar;

(...)

XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor;

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

XXXIV - são a todos assegurados, independentemente do pagamento de taxas:

a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder;

b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal;

(...)

XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;

XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;

(...)

LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;

> LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;
>
> LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;
>
> (...)
>
> LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;
>
> (...)
>
> LXXII - conceder-se-á *habeas data:*
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [...]. (BRASIL, 1988).

Em quase todos os seus capítulos e seções, a CF/1988 traz especificações sobre o direito à informação, inserindo assim para toda a estrutura da Administração Pública: Poder Legislativo, Judiciário e Executivo, o dever de dar acesso à informação como um ato democrático, de exercício da cidadania, de prestação de contas e de respeitos aos direitos humanos (BERNADES, 2015).

Em 2012 entrou em vigor a Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação (LAI), que tem como propósito regulamentar o direito constitucional de acesso dos cidadãos às informações públicas no país, trazendo vários conceitos e princípios que norteiam o direito de acesso à informação.

> Art. 3° Os procedimentos previstos nesta Lei destinam-se a assegurar o **direito fundamental de acesso à informação** e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
>
> I - observância da **publicidade** como preceito geral e do sigilo como exceção;
>
> II - divulgação de **informações** de interesse público, independentemente de solicitações;
>
> III - utilização de meios de **comunicação** viabilizados pela tecnologia da **informação**;
>
> IV - fomento ao desenvolvimento da cultura de **transparência** na administração pública;

> V - desenvolvimento do **controle** social da administração pública. (BRASIL, 2011) (Grifo nosso).

Cabe destacar a mudança de paradigma em relação à transparência pública ao definir que o acesso é a regra e o sigilo, a exceção.

O Decreto nº 7.724/2012 regulamenta a LAI no âmbito do Poder Executivo Federal para orientar os seus órgãos e entidades. Os demais poderes, estados e municípios publicaram sua própria regulamentação tendo como base a LAI. Através da LAI surgem outros termos importantes formadores de princípios e relacionados à transparência e à informação, quais sejam:

- Transparência ativa e Transparência passiva;
- Abertura de dados;
- Governo aberto;
- Informação primária e Informação relativa;
- Autoridade de monitoramento;
- Gestão da informação.

De acordo ao Dicionário Michaelis, transparência significa "(...) limpidez. É a qualidade do que é transparente (que se pode ver através, que é evidente ou que se deixa transparecer)".

Segundo Braga (2011, p. 12) a transparência:

> [...] é um componente do Controle Interno Administrativo ou Controle Primário, como elemento que possibilita um melhor acompanhamento dos processos pelo próprio gestor, conduzindo a eficiência da gestão e o acesso aos direitos sociais. (BRAGA, 2011, p. 12).

No Quadro 1 encontram-se alguns termos e seus conceitos extraídos da Lei de Acesso a Informação (LAI):

Quadro 1 - Conceitos extraídos da LAI

INFORMAÇÃO	Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
DOCUMENTO	Unidade de registro de informações, qualquer que seja o suporte ou formato.
INFORMAÇÃO PESSOAL	Aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.
INFORMAÇÃO SIGILOSA	Aquela relacionada à pessoa natural identificada ou identificável.
TRATAMENTO DA INFORMAÇÃO	Conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento,

	eliminação, avaliação, destinação ou controle da informação.
DISPONIBILIDADE	Qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.
AUTENTICIDADE	Qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema.
INTEGRIDADE	Qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino.
PRIMARIEDADE	Qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Fonte: Lei de Acesso à Informação. Adaptada pela autora (2018).

A Lei de Acesso à Informação (LAI) brasileira também estabeleceu os seguintes princípios a partir do Artigo 19 da Declaração Universal de Direitos Humanos (ONU, 1948):

> **1. Princípio da publicidade máxima**: a abrangência do direito à informação deve ser ampla no tocante ao espectro de informações e órgãos envolvidos, bem como quanto aos indivíduos que poderão reivindicar esse direito;
> **2. Princípio da transparência ativa e a obrigação de publicar**: os órgãos públicos têm a obrigação de publicar informações de interesse público, não basta atender apenas aos pedidos de informação. O ideal é que a quantidade de informações disponibilizadas proativamente aumente com o passar do tempo;
> **3. Princípio da abertura de dados**: estímulo à disponibilização de dados em formato aberto;
> **4. Princípio da promoção de um governo aberto**: os órgãos públicos precisam estimular a superação da cultura do sigilo e promover ativamente uma cultura de acesso. É preciso que todos os envolvidos na gestão pública compreendam que a abertura do governo é mais do que uma obrigação, é também um direito humano fundamental e essencial para a governança efetiva e apropriada;
> **5. Princípio da criação de procedimentos que facilitem o acesso:** os pedidos de informação devem ser processados mediante procedimentos ágeis, de forma transparente e em linguagem de fácil compreensão, com a possibilidade de apresentação de recurso em caso de negativa da informação. Para o atendimento de demandas de qualquer pessoa por essas informações, devem ser utilizados os meios de comunicação viabilizados pela tecnologia da informação. (ONU, 1948).

A Lei de Acesso à Informação preconiza a obrigatoriedade de órgãos públicos, de forma proativa, divulgarem informações gerais ou coletivo. Quando as informações de interesse coletivo, mesmo que não tenham sido solicitadas são fornecidas é

denominada de transparência ativa, devido a possibilidade do órgão público de permear a iniciativa de divulgar informações aos cidadãos.

> Art. 3°. Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
>
> ----------
>
> II - divulgação de informações de interesse público, independentemente de solicitações;
>
> ----------
>
> Art. 8°. É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas. (BRASIL, 2011).

Em contrapartida, a transparência passiva se verifica quando determinado órgão é demandando pela sociedade para prestar informações de interesse geral ou coletivo e, que não estejam amparadas por sigilo.

> Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1° desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida. (BRASIL, 2011).

Tanto na Constituição, na Lei de Acesso à Informação como na Lei de Transparência foram oferecidas resistências por parte principalmente do setor público e seus servidores, que estavam acostumados a reter informações como se fossem seus proprietários. Havia uma cultura do segredo, como se as informações abertas pudessem oferecer riscos. Também houve resistência em relação à demanda de trabalho que poderia acarretar (SEABRA; CAPANEMA; FIGUEIREDO, 2013).

As instituições públicas tiveram que se adequar não somente na mudança de mentalidade de seus servidores, mas também em termos de tecnologia. Os portais de transparência e de acesso à informação começaram a surgir e fazer parte do dia a dia das instituições e dos cidadãos.

Os cidadãos em tudo que solicitavam baseavam seus pedidos na Lei de Acesso e na Lei da Transparência. Mas muitas vezes essas solicitações eram negadas por estarem enquadradas como informação sigilosa. As situações de sigilo de

informações são elencadas no Art. 23 da LAI, como àquelas que demandam a segurança do indivíduo, da sociedade e os pressupostos relacionados à soberania nacional.

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
>
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações. (BRASIL, 2011).

A Lei da Transparência e a LAI surgiram com a explosão informacional, quando o uso da internet e de tecnologias já faziam parte do dia a dia da população como o acesso aos *blogs*, sítios de internet, portais empresariais, redes sociais, celulares, etc.

Inúmeros serviços e produtos cresciam e crescem exponencialmente através de empresas com diversas soluções de publicidade, *marketing*, comunicação, aplicativos de conversas instantâneas com qualquer pessoa em qualquer lugar do mundo, dentre outras tecnologias e soluções.

Após aproximadamente 18 anos de Internet no Brasil surge a Lei nº 12.737, aprovada em 2012 que realiza alterações no Código Penal e é conhecida popularmente como Lei “Carolina Dieckmann”. Essa Lei tipificou vários dos crimes de natureza on-line (cibernética) bem como delitos informáticos.

O nome “midiático” da Lei foi em função de um caso pessoal ocorrido com a atriz Carolina Dieckmann. A atriz teve seu e-mail invadido e o autor teve acesso a fotografias de foro íntimo. O autor da invasão chantageou a atriz exigindo dinheiro para não publicar as fotografias nas redes sociais (SILVA, 2014).

Diante de um cenário de acesso amplo à informação, a Lei nº 12.737/2012 é considerada como um dos primeiros procedimentos com o objetivo de estabelecer segurança jurídica para a vida privada on-line.

A importância não se deve somente à Lei em si, mas por despertar maior interesse na Internet e considerá-la um campo importante que deveria ser regulamentado e fazer parte do ordenamento jurídico. Com a Lei, as alterações no Código Penal dizem respeito à violação de equipamentos e sistemas com a intenção de destruir dados ou informações, ou somente deixá-los vulneráveis. A tipificação independe de que a violação tenha acontecido com os equipamentos ou sistemas conectados à internet.

As alterações preveem penas mais graves à invasão para obter informações das comunicações privadas, de informações sigilosas e de segredos comerciais ou industriais. Com agravamento da pena se essas informações forem divulgadas, transmitidas on-line ou comercializadas.

A Lei acarretou outros problemas relacionados à dependência de perícia e de pessoas capacitadas para identificar se houve crime ou não. Também de advogados e juízes conhecedores não somente de legislação, mas também de informática, tecnologias e termos relacionados a este ambiente virtual. Além disso as tecnologias mudam a cada instante e a adaptação e aperfeiçoamentos tanto da lei como do ordenamento jurídico e dos julgamentos devem ser constantes.

Retornando à questão das relações com o consumidor, na atualidade pensar em consumidor não mais significa relações de compra em uma loja física, pois as tecnologias e a internet abriram frente para novas relações jurídicas de comércio e serviços.

Como meio de regulação foi criado o Marco Civil da Internet (MCI) através da Lei nº 12.965/2014 que teve como objetivo estabelecer princípios, garantias, deveres para o uso da Internet no Brasil e determina que estas diretrizes sejam abrangentes à atuação da União, dos Estados, dos Municípios e do Distrito Federal.

O MCI surge por não haver normas jurídicas específicas vigentes no país que se referissem às questões sobre relações sociais na internet e que viessem ao encontro do disposto de forma mais ampla na CF/1988, Código Civil e Código Penal.

Com a explosão de acesso à rede, a invasão de privacidade se tornou um problema e o MCI tem como finalidade regimentar as normas de comportamento dos usuários na rede. O MCI, também é conhecido como “Constituição da Internet” (TOMASEVICIUS FILHO, 2016).

> Art. 2° A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> I - o reconhecimento da escala mundial da rede;
>
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> III - a pluralidade e a diversidade;
>
> IV - a abertura e a colaboração;
>
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - a finalidade social da rede. (BRASIL, 2014).

Foi a primeira lei no mundo a fundamentar e disciplinar sobre os direitos e deveres dos usuários da rede com ênfase na liberdade de expressão, no exercício da cidadania em meios digitais, mas também, sobre a proteção da privacidade, a proteção dos dados pessoais e da preservação de garantia de neutralidade da rede (SANTOS, 2016).

> Art. 3° A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014).

As novas tecnologias e o uso da rede permitiram a transmissão de informações constante em diversas esferas, tanto a pública quanto a privada; possibilitando a transformação das atividades destes setores. Entretanto, a privacidade se tornou muito “frágil” diante destas novas tecnologias, que possibilitaram o alcance de muitas formas de detalhamento de informações acerca do indivíduo.

O conceito de privacidade atrelado aos recursos tecnológicos não apenas se insere no direito de a pessoa preferir se reservar ou não expor informações sobre si mesma, mas a forma como o tratamento das informações é publicada em bancos de dados e sítios de transparência pública (AJURIS, 2014).

Desde o início da implantação da LAI e do MCI existiu o questionamento sobre a disponibilização de informações de caráter pessoal em sítios de transparência pública e/ou banco de dados. Muitos dados e informações pessoais foram disponibilizados de forma gratuita e aberta à ampla consulta. Estes foram agregados à alta tecnologia de capacidade de armazenamento de dados, os quais geraram problemas em relação a possibilidade de cruzamento de dados pessoais, de exposição da imagem do indivíduo e da violação de privacidade.

> Art. 7° O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]. (BRASIL, 2014).

O Artigo 7º da Lei nº 12.965/2014 do Marco Civil na Internet foi criado como um mecanismo para garantia dos direitos dos usuários de internet, em especial, o direito à privacidade, a intimidade, a vida privada e o direito de se isolar. Além de fundamentar, o direito de impedir que outros tenham acesso a informações pessoais; a preservação do sigilo das comunicações e dos registros armazenados e o não fornecimento de informações coletadas a terceiros.

Este dispositivo expressa semelhança com o Art. 5º, inciso XII da CF/88 que assegura a questão sobre o direito à privacidade nas comunicações:

> é inviolável sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988).

Conforme o Art. 60, inciso IV da CF/88 os direitos e as garantias são denominados de cláusulas pétreas. Este dispositivo apresenta a impossibilidade de abolir, reduzir a eficácia e não permite a discricionariedade judicial referente aos direitos e garantias individuais, ou seja, qualquer ato em desconformidade com o texto poderia ser considerado inconstitucional (WOLOSZYN, 2014).

> [...] a disposição constitucional, ao mesmo tempo que garante a inviolabilidade da correspondência, dos dados, a das comunicações telegráficas e telefônicas, abre uma única exceção, relativa a estas últimas. Isso quer dizer, no nosso entender, que com relação às demais formas indicadas pela Constituição (correspondência, dados e comunicações telegráficas) a inviolabilidade é absoluta. A posição da Constituição não é a melhor, levando a consequência da impossibilidade de se legitimar, por lei, a apreensão da correspondência, dos dados a do conteúdo das comunicações telegráficas, mesmo em caso de particular gravidade. (GRINOVER, 1994, p. 154).

Há um contraponto constitucional na parte final do inciso que apresenta exceções de inviolabilidade do sigilo dos dados e das comunicações telefônicas para fins de investigação criminal ou instrução processual.

Não havendo previsão constitucional para quaisquer outros tipos de inviolabilidade ocasiona uma lacuna para interpretação. Nos casos previstos a inviolabilidade é considerada absoluta e, nos casos em que não há previsão pode ocorrer a violabilidade, pois o que não estiver previsto em lei não é considerado ilegal

se for cometido por pessoa física ou jurídica de direito privado. Em se tratando de pessoa jurídica de direito público somente pode agir de acordo com o que está previsto em lei.

Importante salientar que ao não haver previsão em lei não é ilegal, podendo ir somente para a seara da moralidade e da ética. Essas lacunas fazem com que leis específicas sejam demandadas.

O Artigo 10 da Lei nº 12.965/2014 versa sobre a guarda e a disponibilização de registros, que devem primar sobre o atendimento da preservação da intimidade, honra da parte direta ou indiretamente envolvidas.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (BRASIL, 2014).

O conteúdo das comunicações privadas somente pode ser disponibilizado através de ordem judicial; o provedor responsável pela guarda dos dados poderá auxiliar no fornecimento de informações, em casos, em que seja solicitada a identificação do usuário para fins judiciais.

Os dados pessoais devem ser tratados com medidas de segurança e sigilo e que respeitem o direito de privacidade e confidencialidade, assim como atender estes direitos aos prestadores de serviços quando ocorrem solicitações judiciais.

O Artigo 11 da Lei do Marco Civil da Internet (MCI) faz menção sobre a coleta, armazenamento de registro, dados pessoais com ênfase aos direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (BRASIL, 2014).

O que caracteriza essa Lei é que apenas faz citação sobre a proteção de dados pessoais, mas não apresenta aprofundamentos. Não regulamenta as punições e sanções para quem descumprir os parâmetros legais referentes ao uso e disseminação de dados pessoais e/ou objetivando interesses de terceiros de qualquer natureza sem respeitar os interesses do próprio indivíduo titular dos dados pessoais. Não há na Lei previsão de consentimento formal do titular para o uso de seus dados com finalidade estabelecida, clara e objetiva.

Para tanto, foi criada e regulamentada a Lei de Proteção de Dados Pessoais (LPDP), nº 13.709/2018 que dispõe sobre a matéria inclusive em meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, para fins de proteger os direitos fundamentais como liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3 METODOLOGIA

A pesquisa caracterizou-se por ser de natureza exploratória, explicativa, bibliográfica e qualitativa. A pesquisa exploratória tem como finalidade desenvolver, esclarecer, modificar os conceitos e o aprimoramento de ideias; com a aproximação do problema para deixá-lo mais explícito e possibilitar a construção de hipóteses (GIL, 2002).

Segundo Marconi e Lakatos (2003, p. 187),

> [...] são estudos exploratórios que têm por objetivo descrever completamente determinado fenômeno, como, por exemplo, o estudo de um caso para o qual são realizadas análises empíricas e teóricas. Podem ser encontradas tanto descrições quantitativas e/ou qualitativas quanta acumulação de informações detalhadas como as obtidas por intermédio da observação participante. Dá-se precedência ao caráter representativo sistemático e, em consequência, os procedimentos de amostragem são flexíveis.

A partir destas características elencadas foi possível desenvolver também a abordagem explicativa que tem como princípio “identificar os fatos que determinam e contribuem para a ocorrência de fenômenos” (GIL, 2002, p. 43). O aprofundamento do tema abordado, proporcionou um maior entendimento da realidade, visto que, explica a razão e os desdobramentos para compreensão de todo o contexto apresentado ao longo do trabalho.

As estratégias de pesquisa adequadas auxiliam na aplicação de mais de um procedimento metodológico, insere a possibilidade de aumento de detalhes e interpretações, maior precisão e objetividade na apresentação de resultados. Este tipo de pesquisa permitiu a realização de pesquisa bibliográfica acerca do problema proposto para o desenvolvimento deste trabalho.

A partir dos objetivos específicos foram pesquisadas as temáticas identificadas como relevantes à construção do *corpus* teórico.

> A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Boa parte dos estudos exploratórios pode ser definida como pesquisas bibliográficas. (GIL, 2002, p. 44).

O desenvolvimento da pesquisa fundamentou-se na pesquisa em materiais bibliográficos; em *sites* de revistas científicas; no Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES); no Repositório Digital da UFRGS - LUME e em base de dados para a contemplação de referencial teórico e metodológico.

A pesquisa qualitativa não está atrelada à representatividade numérica, mas ao examinar o entendimento de um contexto, grupo social, de uma organização e outros. A abordagem não pressupõe um único modelo de pesquisa, abrange pressupostos para elencar metodologias de outras ciências (GOLDENBERG, 1997).

Neves (1999, p. 1) identifica que a “pesquisa qualitativa busca compreender e manifestar o sentido dos fenômenos do mundo social, para minimizar a distância entre sujeito e objeto, entre teoria e dados, entre contexto e ação”. O estudo qualitativo foi realizado através de pesquisa no sítio eletrônico do “Portal oficial da República do Brasil” (Planalto) referente à busca de legislação pertinente sobre os assuntos desenvolvidos.

Após a coleta de informações, foram realizadas análises sobre a Constituição Federal (CF); Lei de Acesso à Informação (LAI); Lei de Transparência; Lei do Marco Civil da Internet (MCI) e a Lei de Proteção de Dados Pessoais (LPDP). Assim como, uma análise comparativa sobre as diferenças entre os pressupostos elencados nas leis referente à privacidade, proteção de dados pessoais, proteção das comunicações, honra e imagem.

Neste contexto, foram apresentados os comparativos que proporcionaram a análise do impacto da Lei de Proteção de Dados Pessoais nas pessoas físicas e pessoas jurídicas. Além disso, em como estas duas pessoas devem atuar na proteção de dados pessoais para preservar a privacidade e a imagem dos indivíduos, conforme preconiza a Lei que tem como objetivo garantir os direitos e deveres do cidadão.

Para por fim, refletir sobre o impacto nas atividades dos setores públicos e privados no tratamento da informação apresentada em sítios eletrônicos; portais de transparência; fluxos de comunicações que podem desrespeitar o sigilo e a privacidade individual.

4 A LEI DE PROTEÇÃO DE DADOS PESSOAIS

No dia 14 de agosto de 2018 ocorreu a aprovação da Lei nº 13.709, conhecida como Lei de Proteção de Dados Pessoais (LPDP), que dispõe sobre o tratamento de dados pessoais abarcando também os dados pessoais em meios digitais.

O termo “dados pessoais” se refere as informações pessoais relacionadas à pessoa natural identificada ou identificável, e “tratamento de dados” a todas as operações realizadas com os dados pessoais, quais sejam, coleta, classificação utilização, acesso, reprodução, processamento, armazenamento, eliminação, controle da informação (BRASIL, 2018).

Para melhor entendimento dos termos tratados a própria lei traz em seu Art. 5º várias definições e para melhor dispô-los considera-se melhor a criação de um quadro com esses conceitos:

Quadro 2 - Definição de dados

CONCEITO	DEFINIÇÃO
DADO PESSOAL	Informação relacionada a pessoa natural identificada ou identificável.
DADO PESSOAL SENSÍVEL	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
DADO ANONIMIZADO	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
BANCO DE DADOS	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
TITULAR	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
OPERADOR	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
ENCARREGADO	Pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.
AGENTES DE TRATAMENTO	O controlador e o operador.

TRATAMENTO	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
ANONIMIZAÇÃO	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
CONSENTIMENTO	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
BLOQUEIO	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
ELIMINAÇÃO	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
TRANSFERÊNCIA INTERNACIONAL DE DADOS	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
USO COMPARTILHADO DE DADOS	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
ÓRGÃO DE PESQUISA	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico
AUTORIDADE NACIONAL	Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Fonte: Lei de Proteção de Dados Pessoais. Adaptada pela autora (2018).

A LPDP afeta a pessoa natural e a pessoa jurídica de direito público e privado, e provoca modificações principalmente no Marco Civil da Internet. Seu objetivo é o de "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Diante de um cenário mundial de criações de leis relacionadas à proteção de dados e de casos de repercussão mundial de vazamentos de dados tanto de pessoas naturais como de pessoas jurídicas, o Brasil viu-se no dever de regular também através de legislação própria.

Em meados dos anos 90, a União Europeia começou a normatizar a proteção de dados, porém com um objetivo mais calcado na unificação de regras relacionadas à proteção de dados dos países pertencentes ao bloco europeu. A Diretiva de Proteção de Dados Pessoais na União Europeia como era chamada na época ocorreu no início do uso da Internet não prevendo todas as relações de consumo por meio digital (PEZZI, 2007).

Em 2012, o esboço de uma nova lei estava sendo criado e, em 2016, uma nova lei foi elaborada, porém somente implementada em maio de 2018 sob o nome de Regulamento Geral de Proteção de Dados, ou GDPR sigla em inglês para *General Data Protection Regulation.* O GDPR influenciou não somente a União Europeia, mas também vários outros lugares do mundo (GOMES, 2018).

O prazo para implementação de dois anos a partir do ano que foi elaborada coincidiu com um dos maiores escândalos da história sobre vazamento de dados envolvendo a rede social *Facebook* e a empresa *Cambridge Analytica*. Em abril de 2018, Mark Zuckerberg, fundador e diretor executivo do *Facebook*, teve que dar explicações no Congresso norte-americano (BBC, 2018).

De acordo com o Jornal da "*British Broadcasting Corporation"* - BBC (2018) a *Cambridge Analytica*, pivô do escândalo, é uma empresa de análise de dados e a mesma que trabalhou na campanha eleitoral de Donald Trump nas eleições. A BBC afirma também, tendo como fonte o jornal "*The Guardian*", que essa mesma empresa foi contratada para colaborar na campanha da saída do Reino Unido da União Europeia (Brexit).

A acusação em ambos os casos e negada pela *Cambridge Analytica* é que essa teria comprado informações de usuários do *Facebook* sem autorização e depois

utilizado para criar um sistema que conseguia entender as preferências dos usuários e influenciar suas escolhas nas urnas.

Na época a política do *Facebook* permitia a coleta de dados por terceiros, mas era proibida a venda e seu uso para propaganda. Para driblar essa regra a *Cambridge* munida dos dados dos usuários criou um aplicativo em que disponibilizava um teste de personalidade. Os usuários ao completá-lo estavam, sem saber, informando suas preferências e depois, sem se dar por conta, recebiam notícias e propagandas que influenciassem o seu voto. Um dos grandes problemas foi que a empresa coletava também os dados dos amigos desses usuários, conseguindo assim chegar a milhões de usuários.

De acordo com Sardeto (2004, p. 24) “alimentar, com dados, os milhares de computadores distribuídos pelo mundo é a grande prioridade do homem no momento, bem como transformar esses dados em informação diferenciada e consequentemente valiosa”. A autora ao citar Stair (1998) diz que:

> Todos os dias somos solicitados a divulgar dados sobre nós mesmos. Na maioria das vezes, o fazemos sem pensar duas vezes. Aceitamos a solicitação como necessária, e, mais importante, os dados serão usados apenas para a finalidade para a qual foram fornecidos. O que não conseguimos perceber é que, atualmente, mais do que nunca, nossos dados estão sendo processados e compartilhados, muitos deles sem a nossa permissão ou conhecimento. As empresas descobriram que a venda de dados é um negócio lucrativo. Infelizmente, os dados que elas vendem são nossos. Dados demográficos, sobre tendências de compras e preferências pessoais tornaram-se valiosos para as organizações que tentam vender seus produtos em um mercado altamente competitivo. Por esta razão, a indústria de dados é muito lucrativa. (STAIR, 1998, p. 112 apud SARDETO, 2004, p. 24).

O GDPR da União Europeia, implementada em meio ao escândalo do *Facebook,* trata principalmente sobre regras de como as empresas e órgãos públicos devem proteger os dados pessoais dos cidadãos dentro do bloco europeu (GOMES, 2018).

É direcionada às empresas de todos os setores não fazendo distinção ao porte, se pequena, média ou grande; e tampouco se pública ou privada. Obviamente, as empresas que utilizam o ambiente digital são as que mais terão que se adequar.

Outra grande questão é quanto às empresas com sede na União Europeia, mas sob a Lei de Proteção de Dados Pessoais em seus países de origem ou sem legislação específica. Havendo legislação esta deve ser nos mesmos moldes da Lei

europeia e não havendo, a União Europeia poderá vetar tratamento de dados fora do continente europeu. Por esse motivo, o GDPR influencia a criação de leis em todo o mundo com o intuito de não perder negócios com países da União Europeia. Assim como provavelmente ocorrerá com a implementação da Lei de Proteção de Dados Pessoais do Brasil (LPDP).

A lei brasileira foi sancionada em agosto de 2018 pelo Presidente Michel Temer e cria um marco legal de proteção de informações pessoais dos cidadãos brasileiros. Dentre os dados protegidos estão o nome, endereço, idade, estado civil, e-mail e situação patrimonial.

Entre seus principais objetivos está o de garantir maior transparência na forma de coleta, processamento, uso e compartilhamento dos dados dos cidadãos. Dados esses tanto encontrados na forma física como digital. Também visa prover o cidadão de maior controle sobre suas informações pessoais e a forma que terceiros as utilizam.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

A LPDP além de ser uma influência do GDPR (da União Europeia) também iniciou sua elaboração em 2012 através do Projeto de Lei nº 4060/2012 do Deputado Milton Monti do Partido Republicano de São Paulo. Todavia, a versão aprovada pela Câmara e, posteriormente, pelo Senado contou com a relatoria do deputado Orlando Silva do PCdoB de São Paulo. A LPDP entrará em vigor somente em 2020, prazo dado para as pessoas jurídicas públicas e privadas se adequarem (BRASIL, 2012).

O Art. 2º da LPDP sobre a disciplina da proteção de dados pessoais diz que seus fundamentos são:

> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;

> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Percebe-se nesses fundamentos uma relação com a Constituição e com as legislações já expostas: Lei de Acesso à Informação, Transparência e Marco Civil da Internet. Alguns termos são recorrentes: privacidade, liberdade de informação e de expressão, dignidade, intimidade, honra, imagem, dentre outros.

O tratamento de dados que for realizado por pessoa natural ou por pessoa jurídica de direito público ou privado não faz exclusão do local onde esse tratamento é realizado podendo ser na sede da empresa localizada em qualquer país e também não exclui o local onde os dados estejam localizados. Desde que, no país onde são tratados os dados haja uma lei análoga que preveja proteção adequada. Isto por que muitas vezes os dados são de pessoas que moram no Brasil e os dados são tratados em outro país, ou os dados de pessoas de outro país são tratados no Brasil, prevendo assim já adequar-se a normatizações como a da União Europeia. Também não exclui o meio utilizado para a coleta e tratamento desses dados. Os incisos do artigo 3º esclarecem sobre questões de localização de origem e tratamento dos dados que se enquadram na lei:

> I - a operação de tratamento seja realizada no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (BRASIL, 2018).

A exceção citada no § 2º faz referência a dados provenientes de fora do Brasil e que não sejam usados para comunicação, assim como em:

> [...] uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de

> proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2018).

Dessa forma, assim como a lei da União Europeia, a LPDP também exige que os países possuam lei de proteção de dados pessoais. Todavia, a LPDP não se aplica em vários casos que se encontram detalhados em seu Art. 4º, dentre eles, quando os dados forem gerados por pessoal natural para uso particular e não comercial/econômico, pois considera-se que a pessoa natural é a proprietária de seus dados e pode produzir e tratar para fins particulares.

O tratamento dos dados para fins exclusivamente jornalísticos e artísticos não se enquadram na LPDP, assim como as acadêmicas com a ressalva que nesse caso a lei recomenda que os dados pessoais sejam anonimizados, ou seja, que passem por um processo para que seja desvinculada a informação da pessoa a que se refere a informação.

A reversão do anonimato não deve ser possível de ser realizada, pois se for não será considerado como dado anonimizado. Somente o titular dos dados pode solicitar reversão de anonimização (BRASIL, 2018).

De acordo com o que consta no inciso III do Art. 4º estão excluídos também os dados para fins exclusivos de segurança nacional, defesa nacional ou atividades de investigação e repressão de infrações penais estão também excluídos da LPDP, mas no caso dessas situações a lei traz algumas ressalvas:

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
>
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
>
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
>
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado. (BRASIL, 2018).

As atividades de tratamento de dados pessoais da LPDP, além de terem que observar a boa-fé também são regidas por alguns princípios elencados no artigo 6º dispostos no quadro abaixo:

Quadro 3 - Princípios e atividade de tratamento de dados

PRINCÍPIOS	ATIVIDADE DE TRATAMENTO DE DADOS PESSOAIS
FINALIDADE	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
ADEQUAÇÃO	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
NECESSIDADE	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
LIVRE ACESSO	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
QUALIDADE DOS DADOS	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
TRANSPARÊNCIA	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
SEGURANÇA	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
PREVENÇÃO	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
NÃO DISCRIMINAÇÃO	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Fonte: Lei de Proteção de Dados Pessoais. Adaptada pela autora (2018).

O artigo 7º da Lei nº 13.709/2018 trata de assuntos de extrema importância sobre os requisitos para o tratamento de dados pessoais, em que somente poderá ser realizado nas hipóteses elencadas nesse artigo, como por exemplo o de que deverá

haver sempre o consentimento expresso da parte por escrito ou por qualquer outro meio.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (BRASIL, 2018).

No entanto, o poder público pode usar dados pessoais sem sequer solicitar ao cidadão pelo fato de que a utilização de dados pelo governo é realizada pelo interesse público. Além disso, o tratamento de dados pelas forças de segurança pública, fiscalização e investigações de crimes, também exclui o expresso consentimento. Quanto à revogação do consentimento, essa pode ser realizada a qualquer momento de forma gratuita e fácil através do consentimento expresso do titular.

A revogação também pode ser solicitada se houver alteração de informação pelo controlador que deverá de acordo ao § 6º do Art. 8º “informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração” (BRASIL, 2018).

A lei acarreta um caráter maior de transparência em relação ao uso dos dados, tratamento e destinação, em seu Art. 9º esclarece que “deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso” (BRASIL, 2018).

Esse direito de livre acesso tem a finalidade de o titular dos dados conhecerem de forma criteriosa as questões relativas ao tratamento de seus dados, dentre elas:

> I - finalidade específica do tratamento;

> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;
>
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL, 2018).

Os direitos citados no inciso VII que estão expressos no Art.18 são os de “confirmação da existência de tratamento” pois, até antes dessa lei, os dados além de serem capturados pelo controlador, com ou sem consentimento, os titulares não tinham conhecimento sobre a finalidade do uso de seus dados e tampouco como seriam tratados. Também consta como direito o livre acesso aos dados pelo titular e a possibilidade de correção de “dados incompletos, inexatos ou desatualizados” (BRASIL,2018).

Dentre os direitos de o titular dos dados está o solicitar a qualquer momento a anonimização, bloqueio ou eliminação de dados desnecessários. Podendo também revogar consentimento aos considerados pelo titular como excessivos ou tratados em desconformidade com a lei.

A lei prevê como direito do titular “a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador” (BRASIL, 2018).

Os controladores muitas vezes compartilham os dados com entidades públicas ou privadas, por esse motivo a lei prevê como direito do titular saber do controlador como e para quem seus dados foram compartilhados. Por vezes existe a necessidade legal ou jurídica do fornecimento de dados por parte do titular e no caso da negativa de consentimento, o controlador deve informar ao titular as consequências de ele negar o consentimento.

Importante destacar o elencado nos parágrafos 1º, 2º e 3º do Art. 9º:

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham

> conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
>
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei. (BRASIL, 2018).

Quanto aos interesses legítimos do controlador, a lei impacta nas questões legais e do uso fundamentado e adequado de tratamento de dados.

Deve haver finalidades legítimas a partir de situações concretas, tais como para “apoio e promoção de atividades do controlador”. Essas necessidades legítimas do controlador muitas vezes dizem respeito ao próprio titular que precisa disponibilizar seus dados para exercer seus direitos ou na prestação de serviços que o beneficiem. Ou seja, se o titular não disponibilizar os dados não poderá exercer um direito. Assim, esse exercício do direito e essa prestação de serviços, que beneficiam o titular que se vê quase que na obrigação de dar seu consentimento, devem respeitar as “legítimas expectativas dele e os direitos e liberdades fundamentais” (BRASIL, 2018).

Quando “o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados” e o controlador deve em todos os casos “adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse” (BRASIL, 2018). No caso de o controlador alegar legítimo interesse, as autoridades nacionais poderão solicitar relatório de impacto à proteção de dados pessoais.

A LPDP dá especial atenção aos dados sensíveis que são os relacionados à religião; raça ou etnia; filiações sindicais; interesses e opiniões políticas e filosóficas; assim como dados referentes à saúde e a vida sexual, e a dados genéticos e/ou biométricos do titular.

Esses dados sensíveis geralmente são tratados pelo poder público, mas podem ser tratados por pessoas jurídicas de direito privado desde que sejam para finalidades bastante específicas, tais como prevenção de fraudes.

No caso de utilização de dados sensíveis o pedido de consentimento deve aparecer em destaque e com as explicações necessárias para que o titular entenda que serão usados seus dados sensíveis ao dar seu consentimento.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018).

Até o advento desta lei, as empresas comunicavam e compartilhavam dados sensíveis entre controladores e inclusive o faziam com o objetivo de obter vantagem econômica sem nenhuma regulamentação. Essa prática na LPDP poderá ser “objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências” (BRASIL, 2018).

A lei contempla vedação quanto à comunicação ou uso compartilhado entre controladores de dados sensíveis quanto aos dados referentes à saúde. Portanto é proibida a venda e o compartilhamento entre empresas de dados sensíveis sobre a saúde dos titulares. Entretanto, o próprio titular que se utiliza, por exemplo, de um

convênio médico poderá transferir através da portabilidade os dados sensíveis a outra empresa na qual terá novo convênio médico. A LPDP prevê também o uso de dados para estudos em saúde pública da seguinte maneira:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
>
> § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
>
> § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
>
> § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
>
> § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. (BRASIL, 2018).

Uma das características importantes da lei é a que se relaciona ao uso dos dados sensíveis para discriminação ou prática abusiva. A LPDP reforça a necessidade e o dever de que os direitos fundamentais previstos na Constituição sejam respeitados.

Esse respeito fica bastante claro em toda a lei e em destaque no Art. 17 que institui que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei” (BRASIL, 2018).

O uso da internet por crianças e adolescentes é comum e na maioria das vezes sem o controle dos pais e responsáveis. O tratamento dos dados até o momento não contemplava cuidados extremos quanto a identificação do titular dos dados se menor de idade e quanto ao consentimento dos pais ou responsáveis.

A LPDP contempla uma seção exclusiva sobre o tratamento de dados pessoais de crianças e adolescentes e que o seu uso seja realizado no interesse dos menores de idade respeitando legislações como o Estatuto da Criança e do Adolescente e ordenamento jurídico que trata sobre capacidade e incapacidade.

O tratamento de dados pessoais de menores de idade deverá ser realizado mediante consentimento específico e em destaque. Esse consentimento será “dado por pelo menos um dos pais ou pelo responsável legal” (BRASIL, 2018). Mas no caso de que os dados sejam usados para contatar os pais e responsáveis não é necessário o consentimento e somente poderá ser realizado por uma única vez e com a condição que esses dados não fiquem armazenados e em hipótese alguma sejam repassados a terceiros.

Os tipos de dados que serão coletados de crianças e adolescentes deverão ser mantidos públicos, assim como a forma de utilização e os procedimentos. Destaca-se também a vedação aos controladores de condicionar a participação das crianças e adolescentes em jogos, aplicativos de internet “ao fornecimento de informações pessoais além das estritamente necessárias à atividade” (BRASIL, 2018); prevendo também que os controladores devem realizar o máximo de esforço para conseguir o consentimento dos pais ou responsáveis e as informações sobre o tratamento de dados deverão:

> [...] ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (BRASIL, 2018).

O importante da LPDP é que esta contempla vários direitos aos titulares dos dados pessoais; o que antes era usado pelos controladores de forma indiscriminada, para fins comerciais, afetando inclusive os direitos fundamentais dos cidadãos, agora a partir da lei estão regrados e poderão ser passíveis de punições por violarem a lei.

O titular pode, de acordo com a LPDP, peticionar em relação “aos seus dados contra o controlador perante a autoridade nacional” (BRASIL, 2018) e se opor ao tratamento de dados nos casos em que o controlador alegue dispensa de consentimento com o objetivo de ludibriar o disposto em lei. Também é direito do titular consultar se algum controlador possui seus dados e ter acesso a esses dados mediante requisição em formato simplificado e resposta em 15 dias pelo controlador

por meio de declaração “clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento” (BRASIL, 2018).

No Art. 19 também consta que:

> § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
>
> § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
>
> I - por meio eletrônico, seguro e idôneo para esse fim; ou
>
> II - sob forma impressa.
>
> § 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
>
> § 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos. (BRASIL, 2018).

Os artigos 20 a 22 também descrevem direitos do titular em relação a solicitar revisão de decisões tomadas “unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses” também de decisões “destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade” (BRASIL. 2018). O controlador deve fornecer, sempre que lhe solicitarem, “informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada”, mas sempre devem ser observados os segredos comercial e industrial.

Se o controlador alegar que não pode fornecer as informações por se tratarem de segredo industrial ou comercial, a autoridade nacional poderá realizar auditoria para verificar se essa alegação procede e se não está ocorrendo por parte do controlador uso discriminatório no tratamento automatizado dos dados pessoais do titular.

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

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. (BRASIL, 2018).

Em relação à transferência internacional de dados a LPDP contempla um capítulo (dos artigos 33 a 36) que determina os casos de permissão e vedações. Essas determinações constam na Lei de Proteção de Dados Pessoais da União Europeia, a GDPR, por questões de relações tanto comerciais e econômicas como também para a proteção dos dados dos cidadãos brasileiros e o uso dos dados por controladores brasileiros e estrangeiros.

A LPDP permite a transferência internacional de dados pessoais “para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei” (BRASIL, 2018) e quando o controlador “oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei” (BRASIL, 2018). Dentre as garantias que devem ser oferecidas pelo controlador dispostas no artigo 33, inciso II estão:

> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos. (BRASIL, 2018).

Também é permitida a transferência de dados quando houver necessidade de “cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional”; quando se fizer necessária a transferência para a “proteção da vida ou da incolumidade física do titular ou de terceiro”; mediante solicitação e autorização da autoridade nacional e quando for necessária para o cumprimento de “compromisso assumido em acordo de cooperação internacional” (BRASIL, 2018).

A transferência internacional é autorizada também:

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

> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. º desta Lei. (BRASIL, 2018).

Neste capítulo sobre transferência internacional de dados a LPDP faz menção expressa ao artigo primeiro da LAI para arrolar as pessoas jurídicas de direito público que poderão realizar transferências para cooperação internacional e “no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional” (BRASIL, 2018).

As empresas arroladas na LAI são expostas em seu artigo 1º:

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
>
> Parágrafo único. Subordinam-se ao regime desta Lei:
>
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
>
> 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. (BRASIL, 2011).

A LPDP trata também de especificações sobre o nível de proteção de dados do país estrangeiro ou do organismo internacional, estabelecendo que o nível de proteção será avaliado pela autoridade nacional levando em consideração algumas características sobre “as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional” e a natureza dos dados e a adoção de “medidas de segurança previstas em regulamento” (BRASIL, 2018).

Leva em consideração também:

> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
>
> VI - outras circunstâncias específicas relativas à transferência. (BRASIL, 2018).

Nas questões de transferência internacional de dados será a autoridade nacional do Brasil que ficará responsável pela verificação e “definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta” (BRASIL, 2018).

Quando as transferências ocorrerem de outros países ou organismos para o Brasil a “análise de cláusulas contratuais, de documentos ou de normas corporativas globais serão submetidas a aprovação da autoridade nacional” e quando necessário “poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento” (BRASIL. 2018). A autoridade nacional poderá também “designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento” (BRASIL, 2018).

Para melhor divisão da lei e contextualização realiza-se a partir daqui uma divisão em subcapítulos para descrever o que a lei dispõe sobre tratamento de dados pessoais pelo poder público; agentes de tratamento de dados pessoais; e sobre segurança, boas práticas e fiscalização.

4.1. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

O capítulo IV da LPDP trata especificamente sobre o “Tratamento de dados Pessoais pelo Poder Público” dividindo-o em duas seções, a primeira sobre as regras e a segunda sobre as responsabilidades.

Da mesma forma que no capítulo sobre Transferência Internacional de Dados este capítulo também faz referência ao artigo 1º da Lei de Acesso à Informação para delimitar as instituições do Poder Público abarcadas pela Lei. Esclarece no caput do artigo 23 que o tratamento de dados pessoais pelas pessoas jurídicas de direito público listadas na Lei de Acesso à Informação “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o

objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]". (BRASIL, 2018). E estabelece algumas regras específicas:

> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> II - (VETADO); e
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.
>
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
>
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (**Lei de Acesso à Informação**) (grifo nosso).
>
> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
>
> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
>
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo. (BRASIL, 2018).

No Art. 24 (caput e parágrafo único) estabelece as regras e diferenças quando se tratar de empresas públicas e de sociedades de economia mista. Quando essas instituições estiverem atuando em regime de concorrência estarão sujeitas ao "tratamento dispensado às pessoas jurídicas de direito privado particulares", mas quando estiverem "operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público" (BRASIL, 2018).

As regras quanto aos dados dispostos no Art. 25 estabelece que esses dados

> [...] deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. (BRASIL, 2018).

O caput do Art. 25 dispõe sobre o uso compartilhado de dados pessoais pelo Poder Público que somente pode ser realizado para “atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei” (BRASIL, 2018).

A LPDP veda ao Poder Público a transferência a entidades privadas de dados pessoais de base de dados que tenha acesso, liberando somente em casos específicos de descentralização de atividade pública para empresas privadas e que exista a exigência de transferência de dados sempre observando o disposto na Lei de Acesso à Informação, conforme apresentado no Artigo 26 da LPDP.

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
>
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
>
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
>
> II - (VETADO);
>
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
>
> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.
>
> Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:
>
> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
>
> III - nas exceções constantes do § 1º do art. 26 desta Lei. (BRASIL, 2018).

A autoridade nacional poderá estabelecer normas complementares relacionadas à comunicação, uso e compartilhamento de dados pessoais, emitir e solicitar parecer técnico, dentre outras atribuições que de acordo com a LPDP estão sob seu encargo.

No que se refere às responsabilidades do Poder Público quando houver infração das instituições públicas em decorrência do tratamento de dados pessoais, a autoridade nacional poderá atuar através de “informe com medidas cabíveis para fazer cessar a violação” e poderá solicitar aos agentes do Poder Público que sejam publicados “relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público” (BRASIL, 2018).

4.2. AGENTES DE TRATAMENTO DE DADOS PESSOAIS

O capítulo VI da LPDP trata especificamente sobre os “Agentes de Tratamento de Dados Pessoais” dividindo o capítulo em três seções, a primeira sobre o controlador e o operador, a segunda sobre o encarregado pelo Tratamento de Dados Pessoais e a terceira sobre a responsabilidade e o ressarcimento de danos.

O Art. 37 diz que tanto controlador como operador “devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse” (BRASIL, 2018).

Já o Art. 39 se refere somente ao operador que deve realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Os artigos 38 e 40 descrevem sobre a relação entre a autoridade nacional com os controladores e operadores, e sobre sua função fiscalizadora.

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
>
> Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência. (BRASIL, 2018).

A Seção II trata sobre o encarregado pelo tratamento de dados pessoais em seu Art. 41 e esclarece que o controlador é quem deve indicar quem será esse encarregado. Sendo que “a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador” (BRASIL, 2018).

> § 2º As atividades do encarregado consistem em:
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018).

Dispõe também que a autoridade nacional poderá estabelecer “normas complementares sobre a definição e as atribuições do encarregado”. Também é a autoridade nacional que estabelecerá se poderá haver “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” (BRASIL, 2018).

A seção III que trata da responsabilidade e do ressarcimento de danos esclarece que tanto controlador como operador são obrigados a reparar danos patrimoniais, morais, individuais ou coletivos quando violarem a legislação de proteção e dados pessoais estando em exercício de atividade de tratamento de dados pessoais.

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (BRASIL, 2018).

Quando for provado que os agentes de tratamento “não realizaram o tratamento de dados pessoais que lhes é atribuído”; ou realizaram, mas não houve “violação de à legislação de proteção de dados; ou ainda que o “dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro”; esses agentes não serão responsabilizados (BRASIL, 2018).

A irregularidade no tratamento dos dados pessoais é considerada quando desrespeitar a legislação ou quando o tratamento não fornecer “a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes” levando-se em consideração “o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam” e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. (BRASIL, 2018).

Destaca-se o que diz o parágrafo único do Art. 44 que “responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador” pois ao deixarem de “adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano”.

Em relação as hipóteses de violação do direito do titular no que se refere às relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente como por exemplo o Código de Defesa do Consumidor.

4.3 DA SEGURANÇA E O SIGILO À FISCALIZAÇÃO E SANÇÕES

O capítulo VII da LPDP trata especificamente sobre “Segurança e Boas Práticas” dividindo o capítulo em duas seções, a primeira sobre a “Segurança e o Sigilo dos Dados” e a segunda sobre “Boas Práticas e Governança”.

Imprescindível a adoção de medidas tanto técnicas como administrativas de segurança que estejam “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” (BRASIL, 2018). Os padrões de segurança da informação devem ser garantidos e assegurados para seu cumprimento pelo agente de tratamento ou qualquer pessoa que venha a intervir em qualquer uma das fases do tratamento dos dados: desde a fase de concepção do produto ou do serviço até a sua execução. Os padrões de segurança poderão ser dispostos pela autoridade nacional em especial ao tratamento de dados pessoais sensíveis (BRASIL, 2018).

Em casos de ocorrência de incidente de segurança:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. (BRASIL, 2018).

Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança. Para isso os controladores e operadores poderão, segundo o caput do Art. 50:

> [...] formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018).

O estabelecimento dessas regras de boas práticas deverá levar em consideração: a natureza dos dados; “o escopo a finalidade, e a probabilidade e gravidade dos riscos e benefícios” (BRASIL, 2018) através da observância da estrutura, da escala e do volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados.

Quando da implementação de um programa de governança relacionado à privacidade deverá contemplar no mínimo políticas internas, normas de boas práticas para a proteção de dados pessoais, que seja aplicado ao “conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta” (BRASIL, 2018), observando também as questões já citadas em relação à estrutura, escala, volume de operações e a qualificação quanto a se os dados são ou não sensíveis (BRASIL, 2018).

De extrema importância que o programa e seus processos sofram avaliação periódica e sistemática para detectar impactos e riscos à privacidade dos titulares dos

dados, assim como o estabelecimento de relação de confiança com o titular dos dados através da transparência e de mecanismos que assegurem a participação do titular.

Jardim et al. (2009) traduz um conceito bastante interessante de política de informação de Daniel (2000):

> A política de informação é o conjunto de regras formais e informais que diretamente, restringindo, impulsionando ou de outra maneira, formam fluxos de informação [...] e inclui, entre outros, aspectos como: literacy, privatização e distribuição da informação governamental, liberdade de acesso à informação, proteção da privacidade individual, e direitos de propriedade intelectual. (DANIEL, 2000 apud JARDIM et al, 2009, p.7)

As alíneas “f, “g” e “h” do inciso I, o inciso II e o parágrafo 3º do Art. 50 dispõem mais regras sobre o programa de boas práticas e de governança:

> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
>
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
>
> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional. (BRASIL, 2018).

Segundo Rosenau (2000, p. 15), “governança não é o mesmo que governo”, para o autor a governança é bem mais ampla que governo pois abrange as instituições do governo, “[...] mas implica também mecanismos informais, de caráter não-governamental, que fazem com que as pessoas e as organizações dentro da sua área de atuação tenham uma conduta determinada, satisfaçam suas necessidades e respondam às suas demandas” (ROSENAU, 2000, p. 15-16).

O capítulo VIII da LPDP trata especificamente sobre Fiscalização contendo uma única seção denominada de Sanções Administrativas. O Art. 52 prevê os tipos de sanções que os agentes de tratamento de dados sofrerão em razão das infrações cometidas. As sanções serão aplicadas pela autoridade nacional:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração; [...]. (BRASIL, 2018)

Conforme o § 1º do artigo 52 as sanções somente serão aplicadas após ser realizado um processo administrativo “que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto” em que devem ser considerados alguns parâmetros e critérios: (I) a gravidade e a natureza das infrações e dos direitos pessoais afetados; (II) a boa-fé do infrator; (III) a vantagem auferida ou pretendida pelo infrator; (IV) a condição econômica do infrator; (V) a reincidência; (VI) o grau do dano; (VII) a cooperação do infrator; (VIII) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2o do art. 48 desta Lei; (IX) a adoção de política de boas práticas e governança; (X) a pronta adoção de medidas corretivas; e (XI) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

> § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.
>
> § 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
>
> § 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial

> em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea. (BRASIL, 2018).

A autoridade nacional criará regulamentos específicos sobre as sanções administrativas e a metodologia sobre essas sanções e a forma de cálculo do valor-base das multas, também que apresentem objetivamente formas e “dosimetrias e conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei” (BRASIL, 2018).

> § 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária. (BRASIL, 2018).

Ressalta-se que o valor da sanção deve obedecer a critérios de proporcionalidade e de razoabilidade, e que a intimação da sanção de multa diária deverá conter “no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento” (BRASIL, 2018).

5 IMPACTO NAS PESSOAS FÍSICAS E JURÍDICAS

A LPDP é um fato que deve ser absorvido por todos, no entanto as pessoas jurídicas são as que tem o prazo de 18 meses para se adaptarem até que a lei entre em vigor em 2020. E 18 meses pode ser considerado pouco tempo para que todas as mudanças e adaptações sejam realizadas.

A partir da vigência da LPDP o governo, na Administração direta e indireta terá que se adequar e esta mudança causará impacto em suas atividades e, inclusive, nas instituições privadas.

A nova Lei acarreta uma mudança no Marco Civil da Internet pois atribui uma maior responsabilidade às empresas que manuseiam dados pessoais no meio digital e atribui sanções e penalidades. A nova forma de coletar e tratar os dados dos clientes, usuários ou seguidores mudará significativamente com o propósito de proteger os direitos individuais como a liberdade de expressão, privacidade, direito de imagem, etc.

O Marco Civil da Internet estabelece várias garantias, direitos, deveres e princípios para o uso da Internet no Brasil e todos são afetados. Ele define, reconhece e regulamenta as relações jurídicas contratadas de forma on-line (virtual). Essas relações no Marco Civil focaram bastante nas questões da privacidade, mas deixaram lacunas que a LPDP veio para suprir.

A LPDP não deve ser considerada somente como a Lei que poderá punir pessoas jurídicas e deve ser vista como sendo de interesse de todos, desde os usuários e clientes, passando pelas empresas, fornecedores, provedores de serviços de internet, consumidores em geral até as pessoas comuns que usam as redes sociais no seu dia a dia.

Mesmo que haja a previsão constitucional do direito à privacidade a LPDP vem para detalhar essa privacidade e ao mesmo tempo abarcar os diversos nichos e espaços em que a privacidade pode ser violada como é o caso do espaço virtual.

Dentre essas lacunas está o tratamento dos dados pessoais, principalmente dos dados sensíveis. Seu uso, destinação, comercialização são a base da LPDP. Os escândalos sobre os vazamentos de dados já citados neste trabalho reforçaram a necessidade de regulamentar essas relações jurídicas virtuais.

A forma como são coletados os dados e tratados a partir de cadastros em aplicativos, compras e inclusive em relação às imagens publicadas, gerando consequências no universo on-line e off-line.

Nesse universo on-line, os usuários registram dados pessoais que são coletados, tratados e compartilhados diariamente, seja nas redes sociais - *Facebook, Google, Twitter, Instagram* - mas também em sítios eletrônicos de empresas privadas, que prestam serviços e comercializam produtos. No universo off-line, dentre eles o comércio, as lojas e os setores de identificações as entradas de residências ou prédios comerciais, serão incluídos na proteção de dados pessoais.

À medida que um Cadastro de Pessoa Física (CPF) é identificado, uma série de outras informações são elencadas e podem gerar outras informações acerca do indivíduo como endereço, cor, etnia, religião e outras. Como mencionado anteriormente, esses dados são denominados de dados sensíveis e direcionam a compreensão do perfil pessoal do portador de um CPF.

> A privacidade, porém, é seriamente ameaçada pela chamada “Sociedade da Vigilância”, baseada na mediação computacional constituída por mecanismos de extração, mercantilização e controle de dados que efetivamente retiram das pessoas o controle sobre suas próprias informações. O capitalismo de vigilância desafia as normas democráticas, pois cresce o interesse, tanto dos governos quanto da iniciativa privada, em relação ao acesso a informações pessoais, com reflexos evidentes na privacidade. (KEINERT; CORTIZO, 2018).

Portanto, estes tipos de dados demandarão maior tipo de cuidado para que não haja um vazamento de informações e que essas não sejam direcionadas a terceiros, conforme apresentado na LPDP como pressuposto de proteção à privacidade, imagem e honra.

Os dados pessoais podem se relacionar a uma série de informações que permitem identificar quase toda a vida de uma pessoa. Essa identificação pode levar ao uso indevido, comercialização, e até mesmo para atos criminosos previstos no Código Penal como estelionato, chantagem, entre outros.

Sem o consentimento formal do indivíduo, esses dados não poderão ser compartilhados e/ou disseminados de acordo com os interesses de terceiros.

As pessoas físicas e jurídicas deverão se adequar a todas as atividades desenvolvidas no país. Em caso de empresas privadas que prestam serviços para o

país, mas que não estejam localizadas fisicamente dentro do Brasil, estas deverão também se adequar à Lei vigente. Segundo o Art.3º, inciso II – “a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional”. A premissa é que os dados coletados são originalmente de brasileiros (dados nacionais) e que estão sob jurisdição brasileira; a normatização segue a da origem dos dados.

Toda pessoa física ou jurídica que solicitar dados pessoais de consumidores e usuários deverá nesse prazo de 18 meses adequar-se para não sofrer as sanções, multas e punições previstas na Lei.

A solicitação expressa de consentimento para coleta de dados é o ponto crucial da LPDP. Segundo a LPDP, Art. 5º, inciso XII – “consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. A cláusula de consentimento não pode ser genérica, deve ser específica, detalhada e de forma legível e de fácil compreensão.

Além do consentimento o titular dos dados deverá ser informado de forma detalhada qual o uso que será dado, a forma de compartilhamento, os direitos dos usuários, entre outras medidas protetivas a esse consumidor/usuário titular desses dados.

Os usuários também têm o direito de solicitar acesso, negar acesso, solicitar eliminação dos dados, dentre outros direitos. Qualquer infração cometida acarreta multas que podem chegar a 50 milhões de reais por infração (BRASIL, 2018).

A LPDP regulamenta os direitos dos usuários de mídias sociais, em relação a qualquer solicitação dos dados pessoais mantidos por uma plataforma digital. O usuário tem o direito de solicitar a qualquer tempo, os dados relacionados ao seu perfil e/ou também solicitar a alteração ou correção de algum dado que não corresponde ao seu perfil. A Lei especifica as garantias e direitos de crianças de até 12 anos; a coleta de dados de usuários até esta idade estará sujeita a restrições e a autorização estará condicionada a um dos pais (VALENTE, 2018).

Por esses motivos os empresários devem ficar atentos à LPDP e se agilizarem para se adequarem a ela para que não sofram prejuízos financeiros de grande impacto.

Além de ter que garantir a segurança dos dados, as empresas terão que determinar um encarregado para atuar na área de proteção de dados, o qual terá como atribuições receber as solicitações, reclamações do púbico externo e orientar demais funcionários da empresa referente as diretrizes da LPDP.

Todas as empresas deverão se adequar à LPDP, mas as empresas de grande porte e que atuam no mercado internacional possuem estratégias para demandar sobre o assunto. Inclusive, muitas já atuam com os pressupostos contidos na LPDP devido a se adequarem às exigências de outros países (GOMES, 2018).

O impacto mais relevante será sentido nas pequenas e médias empresas para se adequarem às novas demandas e à revisão de processos de trabalho. Como mencionado, independentemente do tamanho da empresa, deverá ter um encarregado para desempenhar as funções referentes à segurança de dados. Neste caso, toda a conjuntura objetivada pela LPDP demandará esforços das empresas para investir em capital financeiro, tecnológico, material e humano para desenvolver práticas efetivas da manutenção das operações e segurança de dados.

A partir da LPDP, as instituições não poderão coletar dados sem especificar a finalidade para a qual estão realizando esta atividade. Segundo a LPDP, as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio de finalidade, “Art. 6º, inciso I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018).

As coletas deverão ser autorizadas pelo titular; a partir da adaptação dos serviços já prestados, o usuário deverá ser perguntado sobre a sua posição referente ao consentimento com o uso dos dados. Ou seja, a autorização para a identificação dos dados estará condicionada a finalidade da atividade que a empresa atua.

Para a sociedade atual a informação tornou-se mercadoria de alto valor agregado tanto para o governo como para as empresas privadas. Ao pensar nos diversos segmentos econômicos pode-se analisar o impacto do uso dessas informações e dados a partir da LPDP em alguns deles.

Os bancos, por exemplo, que costumam utilizar-se dos dados dos clientes terão que se adequar ao realizarem operações com os dados referentes principalmente a cadastro de crédito. Eles possuem em sua base de dados o que chamam de Cadastro

Positivo com dados de pessoas que livremente decidiram em determinando momento fazer parte desse cadastro (PINHEIRO, 2012).

O Cadastro Positivo serve para analisar estatisticamente os consumidores, mas o uso que deverá ser feito desses dados a partir da LPDP deve ser detalhadamente explicado ao titular desses dados.

De acordo com o Jornal Folha de São Paulo (2018) mais de 13 milhões de pessoas estão neste Cadastro Positivo e os bancos pensavam em incluir dados de outras bases de dados sem o consentimento dos titulares. Mas com a LPDP isso não será mais possível.

As empresas de *marketing,* pessoas físicas que prestam serviços de *marketing* ou os setores de *marketing* das empresas em geral são também algumas das quais mais terão que se adequar à LPDP.

Terão que usar métodos, instrumentos e aplicativos mais transparentes e de fácil uso para que possam alcançar o público-alvo sem ferir a LPDP. O uso de estratégias de *marketing* deverá ser repensado para que gere valor ao cliente, pensando em suas preferências e de forma que as interações se tornem mais transparentes.

Ao tratar-se de *marketing* empresarial ou mais especificamente em empresas especialistas em *marketing* se deve discorrer sobre *Inbound Marketing*. De acordo com o sítio eletrônico “Marketing de Conteúdo” o termo “*Inbound Marketing”* significa “qualquer estratégia de marketing que visa atrair o interesse das pessoas. Também é chamado de marketing de atração e possui três grandes pilares: SEO, Marketing de Conteúdo e Estratégia em Redes Sociais” (MARKETING DE CONTEÚDO, 2018).

A ideia principal do *Inbound Marketing* é a obtenção e análise de dados e informações; e na criação e compartilhamento de conteúdo direcionado a determinado público alvo para conquistar uma comunicação e um relacionamento mais direto com esse público (MARKETING DE CONTEÚDO, 2018).

Com a LPDP a forma de aproximação e comunicação com esse cliente deverá ser mais transparente e com seu consentimento expresso. As estratégias utilizadas com o cliente para conhecê-lo e posteriormente oferecer-lhe conteúdo através de *marketing* também deve ser repensada.

Entender os interesses do consumidor, com a LPDP, não poderá mais ser realizado de forma transversal a partir de dados e informações adquiridas de terceiros

ou de forma invasiva. Esse entendimento deverá ocorrer de forma natural e espontânea e com o consentimento expresso.

Poder-se-ia aqui, a título de exemplo e analogia, utilizar os termos transparência ativa e passiva. A transparência ativa ocorre quando as instituições públicas espontaneamente publicizam as informações de interesse público e a passiva quando se faz necessário que o cidadão solicite as informações.

Seguindo a analogia proposta, mas sob o viés do *marketing*, a ativa seria quando o consumidor libera suas informações espontaneamente de forma consentida e a passiva quando as empresas “forçam” o consumidor a liberar suas informações, mas não de forma espontânea e muitas vezes de forma pouco ortodoxa.

A LPDP obriga que as empresas somente utilizem as informações que o consumidor liberou de forma ativa (explícita) e consentida. As empresas ao se utilizarem *Marketing* de Conteúdo com publicações relevantes e originais poderão atrair o público-alvo e potenciais clientes que participem de forma natural e ativa. O engajamento de forma transparente levará ao consentimento.

A partir de uma análise da LPDP (2018) pode-se inferir mais algumas questões sobre sua influência no *marketing*, pois a descoberta e geração de clientes potenciais deverá ser realizada com maior atenção e cuidado pelas empresas e profissionais de *marketing*, dentre elas:

- **Obtenção do consentimento**: O consentimento deve ser explícito e não genérico. A LPDP é clara quanto à nulidade de autorizações genéricas para uso e tratamento de dados pessoais.

  Com a LPDP tornam-se ilegais o uso de caixas de seleção automáticas e pré-marcadas ou as autorizações automáticas existentes em muitos sítios de internet em que aparece a mensagem dizendo que se usuário continuar conectado está autorizando automaticamente o uso de suas informações.

  As empresas deverão realizar uma análise minuciosa de suas plataformas on-line, verificar o que está indo de encontro à lei e elaborar estratégias para adequação. Essas mudanças irão gerar custos de investimento em tecnologia, profissionais de informática, dentre outros.

- **Princípio da finalidade:** A LPDP tem como um dos seus pilares, além do consentimento, o princípio da finalidade. O uso, processamento e tratamento

de dados pessoais devem atender às necessidades e finalidades específicas das empresas. Portanto não podem ser coletados de forma indiscriminada.

As empresas terão que, além de limitar a coleta, essa deve ser a necessária para suprir suas necessidades comerciais.

Portanto os e-mails *marketing* tão utilizados pelas empresas deverão ser revistos. Hoje é muito comum que as empresas disparem milhares de e-mails a partir de um banco de dados que foi alimentado de diversas maneiras inclusive com dados pessoais sem autorização expressa do titular e/ou os que chegaram no banco de dados através de terceiros.

A base de dados deverá ser analisada para identificar quais titulares dos dados deram consentimento, para os demais as empresas deverão criar estratégias para conseguir o consentimento de forma que atenda aos requisitos da LPDP.

As listas de e-mails comprados e “frias” é oficialmente ilegal de acordo com a LPDP, por isso o cuidado deve ser redobrado para que no novo banco de dados não conste nenhum e-mail adquirido dessa forma.

- **Anúncios e publicidades indesejadas:** As campanhas de *marketing* são o maior desafio das empresas a partir das regras impostas pela LPDP.

  O consentimento acarreta personalização e estratégias de anúncios e publicidades relevantes para cada consumidor.

  O *Facebook*, por exemplo, atualmente coleta e usa os dados de sua rede e de outros sítios de internet afilados a ele para “melhorar a experiência do usuário”.

  Os usuários são segmentados por comportamento na rede, localização, “amigos”, “conhecidos”, etc.

  Os usuários o *Facebook* e redes sociais em geral, a partir da LPDP, terão o direito de saber quais as informações sobre eles estão sendo armazenadas e se estas foram devidamente autorizadas.

  Também prevê o direito dos usuários em recusar a utilização de seus dados.

Essas imposições às redes sociais e direitos aos seus usuários acarretam além da transparência, a mudança de papel assumido frente aos usuários. Ou seja, o *Facebook* e a empresa podem ser tantos controladores de dados como operadores de dados de acordo com a circunstância.

Será controlador quando lida, usa e toma decisões diretas em relação aos dados pessoais de determinado titular, e será operador quando processa os dados pessoais para outros controladores. Pode-se resumir essas relações da seguinte forma:

a) Empresa como controlador: O *remarketing* é uma técnica que trabalha com publicidade direcionada aos usuários que alguma vez acessaram a página de uma empresa (CONVERTTE, 2013). O *remarketing* nas redes sociais é muito comum, mas utilizado com mais frequência no *Facebook*. Esse processo ocorre a partir da interação do usuário no sítio da internet de uma empresa que salva os *cookies* e depois envia informações no *Facebook*. O usuário sem ter solicitado começa a receber propaganda em seu *Facebook* sobre o produto e a empresa que ele acessou o sítio da internet. A responsabilidade da empresa a partir da LPDP inicia no acesso do usuário em seu sítio de internet. A empresa exerce nesse caso o papel de controladora dos dados e deverá informar de forma expressa o uso de *cookies* e o que fará com os dados coletados. Também deverá solicitar o consentimento para coletar e usar essas informações no *Facebook*. A responsabilidade é da empresa ao ser controladora de dados (que extraiu através dos *cookies*) quando cria campanhas no *Facebook*.

b) *Facebook* e empresas como controladores: Quando as campanhas publicitárias, como por exemplo os mais diversos tipos de testes que aparecem para os usuários preencherem, tiverem como objetivo a coleta de dados para geração de cadastro tanto empresa como *Facebook* são controladores de dados, pois o cadastro será utilizado e processado por ambos.

c) Empresa controlador e *Facebook* operador: O denominado *Pixel* do *Facebook* é acionado quando um usuário do Facebook acessa o sitio da internet de uma empresa. Ou seja, o *Facebook* rastreia os seus usuários. Com a LPDP as empresas devem obter consentimento do usuário alertando que o *Facebook* foi autorizado a coletar dados. As empresas em seus termos de uso e de privacidade deverão expor expressamente o que o *Facebook* faz e deve

> pedir consentimento ao usuário. Pode-se pensar que quem deveria solicitar o consentimento seria o *Facebook*, mas não é assim que ocorre, pois quem autorizou o *Facebook* a acessar e coletar dados do seu sítio eletrônico foi a empresa. Nesse caso a responsabilidade é solidária. Tanto as empresas (controladores) como o *Facebook* (operadores) serão responsabilizadas pelos danos causados aos usuários. Mas a maior atenção e maior impacto recai sobre a empresa que toma as decisões sobre os dados que extrai dos clientes que acessam sua página na internet e sobre o tratamento que será realizado nesses dados e principalmente por que foi a empresa que autorizou o *Facebook* a coletar os dados.

O impacto referido às pessoas físicas e jurídicas é uma análise do que se exigirá de modificações e fiscalização do tratamento de dados. A LPDP tem a finalidade de proteger os dados pessoais e, a fundamentação deste tratamento com previsão em Lei permite ao Brasil se alinhar à União Europeia no que tange a prerrogativa de operação de dados pessoais, de quem trata estes dados.

O Marco Civil da Internet estabeleceu regras sobre o uso de dados pessoais por parte das empresas que administram informações, mas neste dispositivo ainda se encontrava uma limitação legal. A ausência de um instrumento legal direcionado a esta matéria poderia criar divergências jurídicas para àqueles que realizam tratamento dos dados europeus.

A desburocratização foi um dos principais fatores para a criação da Lei de Proteção de Dados Pessoais (LPDP) no Brasil e alcança uma estratégia de estimular os negócios com o continente europeu, devido a demanda bem fundamentada pela *General Data Protection Regulation* (GDPR) que impacta os usuários da rede e as empresas de tecnologia que guardam dados pessoais europeus e brasileiros.

No texto original da Lei constava a criação de uma entidade denominada “Autoridade Nacional de Proteção de Dados (ANPD), na forma de agência reguladora que deveria “emitir opiniões técnicas ou recomendações previstas” e “solicitar aos responsáveis relatórios do impacto à proteção de dados pessoais” (BRASIL. 2018).

Mas a criação deste órgão foi vetada e a LPDP foi sancionada sem a autorização de criação de uma autoridade competente para zelar, implementar e fiscalizar o cumprimento desta Lei. As adequações indicadas poderão ser realizadas

pelas instituições públicas e privadas, mas a autoridade que exercerá as demandas de fiscalização e aplicação de sanções referente ao não cumprimento das orientações apresentadas, não é especificada no instrumento legal.

Não se poderia encerrar este trabalho sem relacionar a LPDP com a Arquivologia e com o papel do Arquivista nessas novas demandas geradas pela Lei.

Com as novas demandas de proteção de dados pessoais que surgiram na União Europeia e no Brasil, em 2018, a área da Arquivologia e o arquivista como profissional da informação podem vislumbrar novas perspectivas de atuação em instituições públicas e privadas.

A LPDP versa também sobre segurança da informação e a atuação de agentes de tratamento de dados. Estas podem ser consideradas atribuições relacionadas à prática arquivística durante o processo de gestão documental. No artigo 5º, inciso X é apresentado o conceito de tratamento:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018).

Esta conceituação indica que o tratamento de dados necessita de preceitos relacionados à Arquivologia como a coleta, classificação, arquivamento, eliminação, avaliação ou controle da informação, transferência, difusão. Estas etapas que foram relacionadas ao processo de tratamento de dados compreendem um conjunto de requisitos relacionados à gestão documental e gestão da informação.

Segundo o Artigo 3º da Lei nº 8.159/1991, que dispõe sobre a política nacional de arquivos e privados, as práticas associadas às atribuições dos arquivistas são bem fundamentadas desde a década de 90, conforme Lei difundida e que ainda vem sendo implantada nas instituições públicas e privadas.

> Art. 3º - Considera-se gestão de documentos o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. (BRASIL, 1991).

Faz-se necessário ressaltar que não é indicado na Lei ou mesmo não é realizada nenhuma referência às atribuições desenvolvida pelos arquivistas ou à área da Arquivologia. Somente ao realizar a análise encima da letra da Lei é que se pode identificar uma possível atuação do arquivista nesta nova demanda que foi criada em 2018.

Ao relacionar o conteúdo do texto na íntegra, suas relações com demais legislações como a Lei de Acesso à Informação e com todo o contexto apresentado no trabalho se desprende a importância da inserção do Arquivista. Como profissional da Informação e por seus conhecimentos em informação arquivística, mesmo que não citado de forma direta e nominativa na Lei, a atuação do Arquivista é fundamental.

A tarefa, de acordo com a LPDP, pode ser executada por um profissional de qualquer área que efetue o controle e a fiscalização, assim como manter o registro das operações de tratamento (BRASIL, 2018).

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
>
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
>
> Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência (BRASIL, 2018).

Cabe a esses profissionais da Informação começarem a entender as legislações que circundam suas atividades e neste caso em especial a LPDP para poderem atuar nas empresas como colaboradores nesta etapa de adequação à Lei e, posteriormente, para a manutenção e controle assegurando que as empresas continuem atuando de forma a não ferir os preceitos e regras instituídos pela LPDP.

Mesmo após a publicação da LPDP, ainda não existe nenhuma política arquivística que contemple orientações e adequação às novas demandas em alinhamento às atividades preconizadas na Lei.

Tendo em vista, a capacidade de abrir novos campos de trabalho a partir da regulamentação das atribuições os agentes de tratamento de dados pessoais, compreendeu-se que os arquivistas podem desempenhar tais funções devido aos conhecimentos contemplados pela Arquivologia serem pertinentes às operações e às funções apresentadas na LPDP. Mas, ainda não foi encontrado nada que indicasse um posicionamento das autoridades da área da Arquivologia.

A LPDP é sem dúvida alguma mais um campo de atuação a ser explorado pelo arquivista. Estes poderiam desempenhar a função de monitoramento e controle do fluxo das informações e dados que circulam nas empresas.

Esta Lei preconiza que os indivíduos podem solicitar o conhecimento de seus dados nos arquivos e/ou bases de dados ou ainda solicitar a eliminação de seus dados. Tais prerrogativas previstas na LPDP aumentarão a demanda no que se refere aos dados e registros pessoais em instituições públicas e privadas.

Houve um crescimento da difusão da área da Arquivologia, dos conhecimentos arquivísticos e do nicho de mercado aos arquivistas, a partir da divulgação e publicidade da Lei de Acesso à Informação (LAI), em 2011. Nesta Lei também são apresentados conceitos que contemplam as práticas arquivísticas, conforme Art. 4º, inciso V sobre de tratamento da informação:

> V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (BRASIL, 2011).

A diferença conceitual é que na LPDP, o conceito de tratamento da informação é apresentado com outras ações a serem realizadas como coleta, processamento, modificação, comunicação, transferência, difusão ou extração. E ampliam o desenvolvimento de ações difundidas na LAI e que necessitam de mais conhecimentos e qualificação dos profissionais que desempenharão o tratamento de dados pessoais.

A ampla divulgação da LAI que foi realizada pelas autoridades arquivísticas no país poderia ser considerada também para a implantação da Lei de Proteção de

Dados Pessoais. A partir da comparação de conceitos apresentados nas duas leis, o conceito de tratamento de dados se aproxima e conecta-se às atividades arquivísticas.

5 CONSIDERAÇÕES FINAIS

Através da análise da Lei nº 13.709, conhecida como Lei de Proteção de Dados Pessoais (LPDP), sancionada em 14 de agosto de 2018, foi possível compreender questões referentes ao tratamento de dados pessoais, inclusive em meios digitais para proteger os direitos fundamentais de liberdade, privacidade e do desenvolvimento da pessoa natural.

Essa lei tão recente, preconiza um tempo de 18 meses a partir de sua publicação para a adequação das instituições públicas e privadas, em relação ao tratamento de dados pessoais e como serão efetivadas as demandas concernentes à prerrogativa do direito do cidadão da privacidade e da eliminação de dados. Uma temática complexa que traz mudanças na forma de coletar e tratar os dados em todas instituições fazendo parte de uma evolução de dispositivos normativos legais que advém desde a Constituição Federal de 1988.

A análise da LPDP propiciou a compreensão de contextos na qual está envolvida e realiza interferências ou mudanças, tais como o político, econômico, social, cultural e todos aqueles que demandavam a constituição de um instrumento relevante que normatizasse os direitos e deveres de pessoas físicas e jurídicas. Essa normatização e regramento incidirão no tratamento de dados pessoais, em prol de questões invioláveis como a privacidade e a intimidade da pessoa humana.

O advento de leis que proporcionam o acesso à informação são direitos elencados pela CF/88, pela Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI), que criou mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem apresentação de motivo, o recebimento de informações públicas dos órgãos e entidades, ou seja, a LAI se constitui de um conjunto de dispositivos legais referentes ao acesso à informação e de criação de mecanismos que sejam condicionados a prática bem fundamentadas de produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (BRASIL, 2011).

A importância da LAI é fundamental para a efetividade da transparência pública e a acesso às informações aos cidadãos, contextualizada dentro da perspectiva de

práticas arquivísticas de gestão documental, com o avanço de novas tecnologias e os paradigmas de múltiplas interfaces entre usuário e governo.

Em 2014, com a publicação da Lei nº 12.965, a Lei do Marco Civil da Internet possibilitou a regulação de princípios, garantias, direitos e deveres dos usuários da rede e da atuação do Estado, com as diretrizes preconizadas no instrumento legal. Já com esta lei constavam normas que deviam ser seguidas por usuários e instituições públicas e privadas, com referência aos direitos fundamentais, à privacidade e a intimidade.

No ano de 2018, a União Europeia iniciou o regramento sobre a proteção de dados pessoais, com referência a impulsionar um conjunto de estratégias de proteção com vistas à segurança da informação e da privacidade. Conforme a lei europeia, o potencial do regulamento impacta os usuários da rede e as empresas de tecnologias que estão espalhadas pelo mundo. Toda empresa que guarda ou trata informações deve se adequar à lei europeia sob pena de sanção e multas.

Para alinhar-se as demandas europeias, o governo brasileiro sancionou a Lei de Proteção de Dados Pessoais (LPDP), para evitar qualquer forma de barreira e/ou sanção política e econômica que pudesse intervir nos negócios entre instituições brasileiras e europeias.

Então, as instituições públicas e privadas deverão adequar-se às prerrogativas potencializadas pela LPDP e definir formas de conseguir atender ao tratamento de dados pessoais. Toda pessoa que solicitar informações sobre seus dados tem o direito à privacidade e a eliminação de dados, conforme previsão legal.

A adaptação a este novo paradigma pode levar a necessitar dos conhecimentos do arquivista. Ainda não existe nenhuma política ou orientação referente à LPDP e poucos ainda conhecem a lei e as potencialidades que ela pode proporcionar ao campo arquivístico.

Segundo Silva e Ribeiro (2011, p. 58) “no meio de tantas oportunidades e de não menos desafios, está a emergir um novo paradigma entre os profissionais da documentação/informação, um paradigma que afecta e afectará cada vez mais a sua formação [...]”. A inserção de novas demandas às atribuições dos arquivistas também pode suscitar da mudança na formação e no desenvolvimento de práticas que envolva novas formas de perceber o arquivista que atue em políticas de informação com ênfase a aumentar a possibilidade de estratégias no mercado de trabalho.

A Lei de Proteção de Dados Pessoais é uma nova prática de tratamento de dados, que suscita a inserção de um profissional habilitado que tenha conhecimentos sobre coleta, acesso, processamento, classificação, avaliação, arquivamento, eliminação, difusão. Portanto, o arquivista tem este perfil para integrar-se a uma nova oportunidade, devido às práticas tecnológicas atuais que convergem a um perfil diferenciado no mercado de trabalho, não mais custodiador de papeis em um arquivo fechado, mas um profissional da informação que proporciona o tratamento, o acesso, a difusão e eliminação de dados, assim como a demanda para atuação em novos serviços de informação.

REFERÊNCIAS

ARNAUDO, Daniel. O Brasil e o Marco Civil da Internet: o estado da governança digital brasileira. **Instituto Agarapé**, abr. 2017. Disponível em: < https://igarape.org.br/marcocivil/assets/downloads/igarape_o-brasil-e-o-marco-civil-da-internet.pdf>. Acesso em: 01 nov. 2018.

BERNADES, Camila. O direito fundamental de acesso à informação: uma análise sob a ótica do princípio da transparência. 2015. 175 f. Dissertação (Mestrado em Direito)- Programa de Pós-Graduação em Direito, Universidade Federal de Uberlândia, Uberlândia, 2015. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/13238/3/DireitoFundamentalAcesso.pdf>. Acesso em: 01 out. 2018.

BRAGA, Marcus Vinicius de Azevedo. A auditoria governamental como instrumento de promoção da transparência. **Revista Jus Navigandi**, Teresina, ano 16, n. 2900, 10 jun. 2011. Disponível em: <https://jus.com.br/artigos/19318>. Acesso em: 10 set. 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 set. 2018.

BRASIL. Lei 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm>. Acesso em: 20 set. 2018.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 20 set. 2018.

BRASIL. Lei Complementar n° 101, de 04 de maio de 2000. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp101.htm>. Acesso em: 16 set. 2018.

BRASIL**.** Lei Complementar nº 131, de 27 de maio de 2009. Acrescenta dispositivos à Lei Complementar nº 101, de 4 de maio de 2000, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências, a fim de determinar a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp131.htm>. Acesso em: 22 set. 2018.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 22 set. 2018.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 17 out. 2018.

BRASIL. Lei no 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso: 01 set. 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 05 out. 2018.

BRITISH BROADCASTING CORPORATION NEWS BRASIL. **O escândalo que fez o Facebook perder US$ 35 bilhões em horas.** 20 mar. 2018. Disponível em: < https://www.bbc.com/portuguese/internacional-43466255>. Acesso em: 01 out. 2018.

CONVERTTE. **Você sabe o que é remarketing.** Disponível em: < https://www.convertte.com.br/voce-sabe-o-que-e-remarketing/> . Acesso em: 05 out. 2018.

DICIONÁRIO JURÍDICO ONLINE. Disponível em: < https://dicionariodireito.com.br/>. Acesso em: 10 out. 2018.

DICIONÁRIO MICHAELIS. Disponível em: <https://michaelis.uol.com.br/>. Acesso em: 10 out. 2018.

JARDIM, José Maria et al. Análise de políticas públicas: uma abordagem em direção às políticas públicas de informação. **Perspectivas em Ciência da Informação**, Minas Gerais, v. 14, n. 1, p. 2- 22, jan./abr. 2009

GALLO, Amynthas. Gestão Estratégica da Informação no Ambiente do Governo Digital. **Revista Brasileira de Biblioteconomia e Documentação**, São Paulo, v. 6, n. 2, p. 3-19, jul./dez. 2010. Disponível em: <https://rbbd.febab.org.br/rbbd/article/viewFile/126/174>. Acesso em: 23 out. 2018.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.

GOLDENBERG, Mirian. **A arte de pesquisar.** Rio de Janeiro: Record, 1997.

GOMES, Helton. Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo. **G1.com**, 25 maio 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>. Acesso em: 01 out. 2018.

GRINOVER, Ada. **As nulidades no processo penal**. São Paulo: Malheiros, 1994.

KEINERT, Tania; CORTIZO, Carlos. Dimensões da privacidade das informações em saúde. **Caderno de Saúde Pública**, Rio de Janeiro, v. 34, n. 7, 2018. Disponível em: <http://www.scielo.br/pdf/csp/v34n7/1678-4464-csp-34-07-e00039417.pdf>. Acesso em: 20 out. 2018.

MACHADO, Joana. A expansão do conceito de privacidade e a evolução da tecnologia da informação com o surgimento dos bancos de dados. **Revista da AJURIS**, Porto Alegre, v. 41, n. 134, jun. 2014. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/206-263-1-sm.pdf>. Acesso em: 20 out. 2018.

MARCONI, Marina; LAKATOS, Eva. **Metodologia do trabalho científico:** procedimentos básicos, pesquisa bibliográfica, projeto e relatório; publicações e trabalhos científicos. São Paulo: Atlas, 2003.

MARKETING DE CONTEÚDO. **O que é Inbound Marketing?** Disponível em: <https://marketingdeconteudo.com/o-que-e-inbound-marketing/>. Acesso em: 20 out. 2018.

MARTINS, Paula; VIVARTA, Veet. **Acesso à Informação e Controle Social das Políticas Públicas.** Brasília, DF: ANDI, 2009. Disponível em: < http://www.acessoainformacao.gov.br/central-de-conteudo/publicacoes/arquivos/acesso-a-informacao-e-controle-social-das-politicas-publicas.pdf/view>. Acesso em: 19 out. 2018.

NEVES, José Luís. Pesquisa qualitativa: características, usos e possibilidades. **Cadernos de Pesquisas em Administração**, v. 1, n. 3, 1996. Disponível em: < http://www.hugoribeiro.com.br/biblioteca-digital/NEVES-Pesquisa_Qualitativa.pdf>. Acesso em: 15 out. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: <http://www.dudh.org.br/declaracao/>. Acesso em: 05 out. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção das Nações Unidas contra a corrupção**. Mérida, México: ONU, 2007. Disponível em: <https://www.unodc.org/documents/lpobrazil//Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf>. Acesso: 05 out. 2018.

PEZZI, Ana Paula. A necessidade de proteção de dados pessoais nos arquivos de consumo: em busca da concretização do direito à privacidade. 2007. 216 f. Dissertação (Mestrado em Direito) – Programa de Pós-graduação em Direito, Universidade do Vale do Rio dos Sinos, 2007. Disponível em: < http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf>. Acesso em: 01 out. 2018.

PINHEIRO, Caroline. **Cadastro Positivo:** a possibilidade de acesso ao crédito como um dos caminhos para o desenvolvimento social. 2012. 108 f. Dissertação (Mestrado Profissional em Poder Judiciário) – Fundação Getúlio Vargas, Rio de Janeiro, 2012. Disponível em: < https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/9792/Caroline%20da%20Rosa%20Pinheiro.pdf>. Acesso em: 01 out. 2018.

PORTINARI, Natália. Entenda o cadastro positivo, que pode mudar suas condições de crédito. **Folha de São Paulo**, São Paulo, 16 maio de 2018. Disponível em: < https://www1.folha.uol.com.br/mercado/2018/05/entenda-o-cadastro-positivo-que-pode-mudar-suas-condicoes-de-credito.shtml>. Acesso em: 05 nov. 2018.

ROSENAU, James. Governança, ordem e transformação na Política Mundial. In: ROSENAU, James; CZEMPIEL, Ernst-Otto. **Governança sem governo:** ordem e transformação na política mundial. Brasília: Ed. Unb, 2000, p. 11-46.

SARDETO, Patrícia Eliane. **Tratamento informatizado de dados pessoais e direito à privacidade.** 2004. 103 f. Dissertação (Mestrado em Direito) - Pós-graduação em Direito, Universidade Federal de Santa Catarina Florianópolis, 2004. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/87824/209091.pdf?sequence=1>. Acesso em: 03 nov. 2018.

SEABRA, Sérgio; CAPANEMA, Renato; FIGUEIREDO, Renata. **Lei de Acesso à Informação: uma análise dos fatores de sucesso da experiência do Poder Executivo Federal.** Controladoria Geral da União, Brasília, 2013. Disponível em: <http://www.cgu.gov.br/sobre/institucional/ministro/artigos/artigos-de-outros-dirigentes/artigo_201307_seabra-capanema-figueiredo_revistaadministracaomunicipal.pdf>. Acesso em: 03 nov. 2018.

SILVA, Armando; RIBEIRO, Fernanda. **Paradigmas, serviços e mediações em Ciência da Informação.** Recife: Néctar, 2011.

SILVA, Camila. Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos. **Revista Jus Navigandi**, Teresina, 2014. Disponível em: < https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos>. Acesso em: 01 out. 2018.

SIRAQUE, Vanderlei. **O controle social da função administrativa do Estado:** possibilidades e limites na Constituição de 1988. 2004. 212 f. Tese (Doutorado em

Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2004. Disponível em: <http://www.siraque.com.br/monografia2004.pdf>.
Acesso em: 24 out. 2018.

SANTOS, Vinicius. **Neutralidade da rede e o Marco Civil da Internet no Brasil:** atores, políticas e controvérsias. 2016. 269 f. Tese (Doutorado em Política Científica e Tecnológica)-Instituto de Geociências, Universidade Estadual de Campinas, 2016. Disponível em: < http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf>. Acesso em: 01 out. 2018.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, São Paulo, v. 30, n. 86, jan./apr. 2016. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269>. Acesso em: 20 out. 2018.

VALENTE, Jonas. Lei de Proteção de Dados trará impactos a pessoas, empresas e governos. **Agência Brasil**, Brasília, 18 ago. 2018. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-08/lei-de-protecao-de-dados-trara-impactos-pessoas-empresas-e-governos>. Acesso em: 20 out. 2018.

WOLOSZYN, André. A inconstitucionalidade da Lei nº 12.965/2014 quanto a quebra do sigilo das comunicações na internet. **Semana de Extensão, Pesquisa e Pós-graduação**, Centro Universitário Ritter dos Reis, 10., 2014. Disponível em: <https://www.uniritter.edu.br/uploads/eventos/sepesq/x_sepesq/arquivos_trabalhos/2968/132/378.pdf>. Acesso em: 25 out. 2018.

ANEXOS - TEXTOS LEGAIS

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Vigência

Regulamento

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

(Vide Lei nº 13.709, de 2018) (Vigência)

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

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

I - o reconhecimento da escala mundial da rede;

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

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

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

VI - a finalidade social da rede.

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

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

II - proteção da privacidade;

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

IV - preservação e garantia da neutralidade de rede;

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

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

VII - preservação da natureza participativa da rede;

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

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

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

I - do direito de acesso à internet a todos;

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

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

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

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

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

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

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

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

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

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

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

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5ºda Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

Mensagem de veto

Vigência

Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

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

I - o respeito à privacidade;

II - a autodeterminação informativa;

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

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

V - o desenvolvimento econômico e tecnológico e a inovação;

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

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

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

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

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

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

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

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

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

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

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

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

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

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

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

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.

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

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

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado

referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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

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

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

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

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

VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

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

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

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

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

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

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

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

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

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

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

XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

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

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

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

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

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

§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional.

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

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

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

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

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

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

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

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

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

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

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

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

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

III - identificação do controlador;

IV - informações de contato do controlador;

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

VI - responsabilidades dos agentes que realizarão o tratamento; e

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

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

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

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

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

I - apoio e promoção de atividades do controlador; e

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

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

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

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

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

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

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

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

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

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

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

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

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

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

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

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

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

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

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

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

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

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

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

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

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

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

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

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

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

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

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

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

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

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

CAPÍTULO III
DOS DIREITOS DO TITULAR

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

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

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

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

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

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

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

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

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

§ 6º O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento.

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

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

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

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

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

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

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

II - sob forma impressa.

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

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

Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

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

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

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

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

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

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

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

II - (VETADO); e

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

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

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

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

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

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

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

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

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

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

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

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO);

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

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

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

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

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

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

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

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

Seção II
Da Responsabilidade

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

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

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

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

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

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

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

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

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

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

V - quando a autoridade nacional autorizar a transferência;

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

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

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

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

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

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

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

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

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

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

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

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

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

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

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

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

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

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

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

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

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

§ 2º As atividades do encarregado consistem em:

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

II - receber comunicações da autoridade nacional e adotar providências;

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

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

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

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

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

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

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

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

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

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

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

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

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

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

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

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

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

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

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

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

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

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

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

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

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

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

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

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

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

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

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

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

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

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

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

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

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

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

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

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

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

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

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

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

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

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

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

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

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

X - a pronta adoção de medidas corretivas; e

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

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

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

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

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

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

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

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

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

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

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

Art. 55. (VETADO).

Art. 56. (VETADO).

Art. 57. (VETADO).

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

Art. 58. (VETADO).

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

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

....." (NR)

"Art. 16. .....

.....

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

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

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

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

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial.

Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim
Aloysio Nunes Ferreira Filho
Eduardo Refinetti Guardia
Esteves Pedro Colnago Junior
Gilberto Magalhães Occhi
Gilberto Kassab
Wagner de Campos Rosário
Gustavo do Vale Rocha
Ilan Goldfajn
Raul Jungmann
Eliseu Padilha