

**PROTEÇÃO
DE DADOS
PESSOAIS**
GLOSSÁRIO
TEMÁTICO

Proteção de dados pessoais [recurso eletrônico] : glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo : CEPI-FGV Direito SP, 2021.

38 p.

Inclui bibliografia e índice.

ISBN: 978-65-87355-26-9

1. Direito à privacidade. 2. Proteção de dados – Brasil. 3. Proteção de dados – Vocabulários, glossários, etc. 4. Brasil. [Lei de proteção de dados pessoais (2018)]. I. Escola de Direito de São Paulo. Centro de Ensino e Pesquisa em Inovação. II. Fundação Getúlio Vargas.

CDU 342.721(81)

SUMÁRIO

APRESENTAÇÃO.....	3
1. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018 – “LGPD”).....	4
1.1 DISPOSIÇÕES PRELIMINARES.....	4
1.2 PRINCÍPIOS.....	6
1.3 SUJEITOS.....	8
1.4 CONCEITOS JURÍDICOS BÁSICOS.....	10
1.5 CONCEITOS TÉCNICOS.....	14
1.6 BASES LEGAIS.....	17
1.7 DIREITOS DO(A)S TITULARES DE DADOS.....	21
1.8 ESTRUTURA REGULATÓRIA.....	23
1.9 RESPONSABILIDADE E SANÇÕES.....	25
1.10 GOVERNANÇA.....	27
2. DEFINIÇÕES TRAZIDAS PELA EUROPEAN DATA PROTECTION LAW.....	30
ÍNDICE.....	34
REFERÊNCIAS.....	36

APRESENTAÇÃO

A Lei nº 13.709/2018, mais conhecida como **Lei Geral de Proteção de Dados Pessoais** (LGPD) visa regular as atividades de tratamento de dados pessoais no Brasil e se aplica a quaisquer agentes que as realizam. Trata-se de uma lei transversal, aplicável aos mais diferentes setores econômicos do país.

Este Glossário Temático tem o propósito de oferecer definições fundamentais para a compreensão do escopo da LGPD, de maneira prática e objetiva, de modo a auxiliar profissionais que lidam com dados pessoais no dia a dia, bem como pessoas interessadas e que são afetadas pelo contexto da lei em seu cotidiano, disponibilizando um material de consulta rápida para conceitos-chave.

O presente Glossário foi elaborado com base na experiência acadêmica e profissional desenvolvida no âmbito do Centro de Ensino e Pesquisa em Inovação (CEPI FGV DIREITO SP), na linha de pesquisa Direito, Tecnologia e Sociedade.

O conteúdo foi organizado por tema, para tornar a pesquisa mais intuitiva. Dentro de cada tema, os termos foram dispostos em ordem alfabética.

Na primeira parte, são apresentadas definições relacionadas ao texto da LGPD, separadas em grupos referentes aos seguintes tópicos: (i) disposições preliminares; (ii) princípios; (iii) sujeitos; (iv) conceitos jurídicos básicos; (v) conceitos técnicos; (vi) bases legais; (vii) direitos do(a)s titulares de dados; (viii) estrutura regulatória; (ix) responsabilidade e sanções; e (x) governança. Além das disposições legais propriamente ditas, são abordados termos e expressões de relevância para o seu entendimento.

A segunda parte abrange conceitos da *European Data Protection Law*, considerando que o histórico e as regulações europeias na proteção de dados trouxeram importantes marcos para essa área — a exemplo da GDPR (*General Data Protection Regulation EU 2016/679*) — e influenciaram a estruturação da lei brasileira.



Jonas Liepe/Unplash

1. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018 – “LGPD”)

1.1 DISPOSIÇÕES PRELIMINARES

QUEM A LGPD SE APLICA?

As proteções e garantias trazidas pela LGPD aplicam-se somente às pessoas naturais, independentemente de sua nacionalidade ou de sua residência. Em outras palavras, o titular de dados pessoais (a quem se referem os dados que são objeto de tratamento), serão sempre pessoas físicas. Porém, vale notar que as pessoas jurídicas também são alvo da regulação, já que podem atuar como agentes de tratamento de dados pessoais (controladores ou operadores). Contudo, elas não são protegidas pelas garantias trazidas pela norma, pelo contrário, são garantidoras dos direitos das pessoas naturais (Art. 1º e Art. 5º, VI e VII, LGPD).

ESCOPO

A LGPD é aplicável 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 (Art. 3º, *caput* e incisos I a III, LGPD):

- 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; ou
- iii. os dados pessoais objetos do tratamento tenham sido coletados no território nacional.

FUNDAMENTOS

A disciplina da proteção de dados pessoais da LGPD tem como fundamentos (Art. 2º, *caput* e incisos I a VII, LGPD):

- 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.



MATÉRIA

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Art. 1º, LGPD). 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 da lei (Art. 17, LGPD).

OBJETIVOS

Dentre os seus objetivos, a LGPD visa à defesa dos(as) titulares de dados pessoais, por meio da proteção aos seus direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (Art. 1º, LGPD). Ao mesmo tempo, a Lei permite o uso de dados pessoais para finalidades diversas, equilibrando interesses e harmonizando a proteção da pessoa humana com o desenvolvimento tecnológico e econômico.

QUANDO A LGPD NÃO SE APLICA?

A LGPD não é aplicável nos seguintes casos de tratamento de dados pessoais (Art. 4º, incisos I a IV, LGPD):

- i. quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- ii. quando realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos (quando o estudo for realizado por órgão de pesquisa, garantida a anonimização de dados pessoais e dados pessoais sensíveis);
- iii. quando realizado para os fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou
- iv. quando os dados forem provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei.

1.2 PRINCÍPIOS

ADEQUAÇÃO: é a compatibilidade do tratamento com as finalidades informadas ao(à) titular, de acordo com o contexto do tratamento (Art. 6º, II, LGPD).

BOA-FÉ: significa a observância de um comportamento leal, correto e probó na realização das atividades de tratamento de dados pessoais. Esse princípio opera como norte a todos os demais e serve de baliza para a interpretação de conceitos abertos (Art. 6º, *caput*, LGPD).

FINALIDADE: é a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível ou desvirtuada (Art. 6º, I, LGPD).

LIMITAÇÃO TEMPORAL DO ARMAZENAMENTO: os dados pessoais devem ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades (Art. 16, *caput*, LGPD).

É autorizada, contudo, a **conservação dos dados pessoais** após o término de seu tratamento para as seguintes finalidades (Art. 16, *caput* e incisos I a IV, LGPD):

- i. cumprimento de obrigação legal ou regulatória pelo controlador;
- ii. estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- iii. transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou
- iv. uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

LIVRE ACESSO: é a garantia, aos(às) titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (Art. 6º, IV, LGPD).

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (Art. 6º, IX, LGPD).

NECESSIDADE: é a limitação ou redução 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 (Art. 6º, III, LGPD).



PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Art. 6º, VIII, LGPD).

QUALIDADE DOS DADOS: é a garantia, aos(às) titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (Art. 6º, V, LGPD).

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 (Art. 6º, X, LGPD).

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 (Art. 6º, VII, LGPD).

TRANSPARÊNCIA: é a garantia, aos(às) 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 (Art. 6º, VI, LGPD).



1.3 SUJEITOS

AGENTES DE TRATAMENTO: são o controlador e o operador (Art. 5º, IX, LGPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo território nacional (Art. 5º, XIX, LGPD). A ANPD foi instituída pela LGPD como órgão da administração pública federal com autonomia técnica, integrante da Presidência da República, definida sua natureza como transitória e passível de transformação pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (Art. 55-A e 55-B, LGPD).

CONTROLADOR: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI, LGPD). É quem determina como os dados são processados.

CONTROLE COMPARTILHADO (CO-CONTROLE): cenário em que dois ou mais agentes (pessoas naturais ou jurídicas) tomam decisões referentes ao tratamento de dados pessoais para uma mesma operação, projeto ou processo.

CONTROLE INTEGRAL: situação em que o controlador, para além de tomar decisões referentes ao tratamento de dados pessoais, também executa tecnicamente o tratamento dos dados pessoais.

ENCARREGADO(A) (DATA PROTECTION OFFICER — “DPO”): é a pessoa física ou jurídica indicada pelo agente de tratamento para atuar como canal de comunicação entre o controlador, os(as) titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O(a) encarregado(a) deve ser indicado pelos controladores e pelos operadores (Art. 5º, VIII e Art. 41, *caput*, LGPD) e a sua identidade e informações de contato do devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (Art. 41, § 1º, LGPD).

Cabe ao(à) encarregado(a), nos termos da LGPD, a realização das seguintes atividades (Art. 41, § 2º, LGPD):

- i. aceitar reclamações e comunicações dos(as) titulares, prestar esclarecimentos e adotar providências;



- ii. receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
- iii. orientar os(as) funcionários(as) e os(as) contratados(as) 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.

A autoridade Nacional de Proteção de Dados (ANPD) poderá estabelecer normas complementares sobre a definição e as atribuições do(a) encarregado(a), 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.

OPERADOR: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII, LGPD). É quem acata e executa as ordens de como os dados devem ser tratados.

SETOR ACADÊMICO: abrange organizações de Educação Profissional, Científica e Tecnológica, bem como as Instituições de Educação Superior (IES). As IES, de acordo com a sua organização e as suas prerrogativas acadêmicas, serão credenciadas para a oferta de cursos superiores de graduação, na qualidade de centros universitários, faculdades e universidades (Seção II, “Das organizações acadêmicas”, Art. 15, *caput*, Decreto nº 9.235/2017).

SETOR PÚBLICO: é o chamado setor público ou estatal e refere-se, tradicionalmente, ao “governo” (i.e., ao “primeiro setor”). O denominado setor público não estatal é composto pelas paraestatais, pelos entes de colaboração e serviços sociais autônomos.

TITULAR DE DADOS PESSOAIS: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Art. 5º, V, LGPD).

TERCEIRO SETOR: o setor público não estatal é também denominado terceiro setor e designa o conjunto de entidades da sociedade civil, sem fins lucrativos, que desenvolve atividades de relevância pública.



1.4 CONCEITOS JURÍDICOS BÁSICOS



BASES LEGAIS: base legal é o fundamento que autoriza o tratamento de dados pessoais e dados pessoais sensíveis por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na LGPD (em seus artigos 7º e 11). As bases legais só não serão necessárias nos casos em que a LGPD não se aplica, como nas hipóteses do Art. 4º ou em situações de tratamento que envolvam dados anonimizados.

BLOQUEIO: é a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (Art. 5º, XIII, LGPD).

CONSERVAÇÃO DE DADOS APÓS O TÉRMINO DO TRATAMENTO: os dados pessoais serão eliminados depois do término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada, entretanto, a sua conservação para as seguintes finalidades (Art. 16, *caput* e incisos I a IV, LGPD):

- i. o cumprimento de obrigação legal ou regulatória pelo controlador;
- ii. o estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- iii. a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- iv. o uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

DADO PESSOAL: é a informação relacionada a pessoa natural identificada ou identificável (Art. 5º, I, LGPD). Também são considerados dados pessoais, para os fins da Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (Art. 12, § 2º, LGPD).

DADO PESSOAL SENSÍVEL: é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º, II, LGPD).

DADOS COLETADOS NO TERRITÓRIO NACIONAL: são dados pessoais coletados dos(as) titulares que se encontram em território nacional no momento da coleta (Art. 3º, § 1º, LGPD).

ELIMINAÇÃO: é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (Art. 5º, XIV, LGPD).

ÓRGÃO DE PESQUISA: é o 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, em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Art. 5º, XVIII, da LGPD).



RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: é a 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 (Art. 5º, XVII, LGPD).

A Autoridade Nacional de Proteção de Dados (ANPD) 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 (Art. 38, *caput*, LGPD).

O relatório deverá conter, no mínimo (Art. 38, parágrafo único, LGPD):

- i. a descrição dos tipos de dados coletados;
- ii. a metodologia utilizada para a coleta e para a garantia da segurança das informações;
- iii. a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

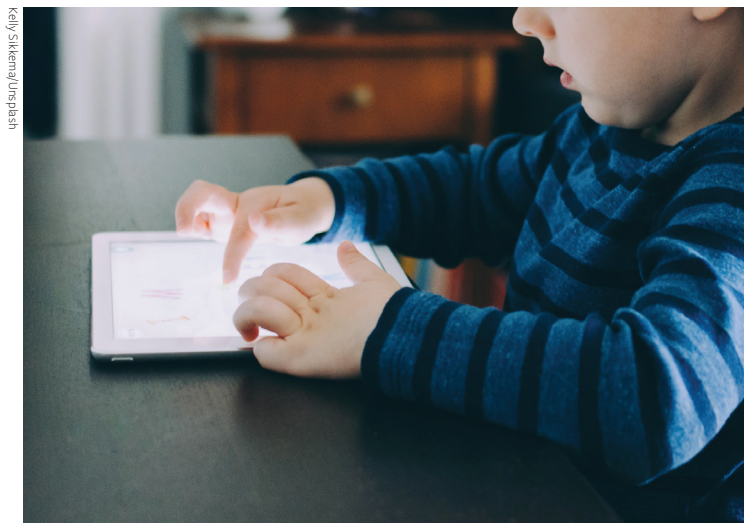
RETENÇÃO MÍNIMA: é a delimitação dos dados e do tratamento de dados apenas para finalidades específicas. Diante do alcance da finalidade determinada, ou da verificação de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade, é necessária a exclusão desses dados (Art. 15, I, LGPD).

TRATAMENTO: é 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 (Art. 5º, X, LGPD).

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES:

CENTES: é o tratamento que deve ser realizado no melhor interesse da criança e do adolescente, nos termos do Art. 14 da LGPD e da legislação pertinente (Art. 14, *caput*, LGPD). Além disso, as informações sobre o tratamento de dados desses(as) titulares precisam ser fornecidas de maneira simples, clara e acessível, consideradas as características do(a) usuário(a) (físico-motoras, perceptivas, sensoriais, intelectuais e mentais), com o uso de recursos audiovisuais quando adequado, proporcionando a informação necessária aos pais ou responsáveis legais e adequada ao entendimento da criança (Art. 14, § 6º, LGPD).

O § 1º do Art. 14 da LGPD estabelece que “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”.



TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO: é o tratamento efetuado pelas pessoas jurídicas de direito público, ou seja, órgãos integrantes da administração pública direta ou indireta, para o atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar competências legais ou cumprir atribuições legais do serviço público (Art. 23, *caput*, LGPD). Abrange o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (Art. 7º, III, LGPD).

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: o tratamento desses dados apenas poderá ocorrer quando o(a) titular ou sua/sua responsável legal **consentir**, de forma específica e destacada, para finalidades específicas (Art. 11, I, LGPD).

Sem fornecimento de consentimento do(a) titular ou sua/sua responsável legal, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas hipóteses em que for indispensável para (Art. 11, II, alíneas “a” a “g”, LGPD):

- i. o cumprimento de obrigação legal ou regulatória pelo controlador;
- ii. o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- iii. a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização;
- iv. o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (Lei nº 9.307/96);

- v. a proteção da vida ou da incolumidade física do(a) titular ou de terceiro;
- vi. a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- vii. a garantia da prevenção à fraude e à segurança do(a) titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do titular (Art. 9º, LGPD) e exceto no caso de prevalecerem direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais.

TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS: o término do tratamento de dados pessoais correrá quando houver (Art. 15, *caput* e I a IV, LGPD):

- i. a 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. o fim do período de tratamento;
- iii. a comunicação do(a) titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou
- iv. a determinação da ANPD, quando houver violação ao disposto na LGPD.

TRANSFERÊNCIA INTERNACIONAL DE DADOS: é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Art. 5º, XV, LGPD).

USO COMPARTILHADO DE DADOS (“COMPARTILHAMENTO”): é a 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 (Art. 5º, XVI, LGPD).



1.5 CONCEITOS TÉCNICOS

ANONIMIZAÇÃO: é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Art. 5º, XI, LGPD). Isto é, por meio da anonimização, as informações são modificadas ou removidas para que o titular não possa ser identificado, inclusive pelo controlador.

O dado anonimizado, nos termos da lei, deixa de ser considerado dado pessoal (Art. 12, *caput*, LGPD).

Trata-se de operação voltada a desvincular, na maior medida possível, o dado pessoal de seu(sua) titular. Envolve o emprego de técnicas consideradas razoáveis, observados os protocolos de segurança da informação, para afastar a possibilidade de ataques de inferência, diretos ou indiretos, acerca da titularidade do dado.

É importante ressaltar que, pelos ditames da LGPD, para ser considerado dado anonimizado, o processo de anonimização não pode ser revertido por meios próprios ou com esforços razoáveis (Art. 12, *caput*, LGPD). Caso isso ocorra, considera-se que o dado nunca foi anonimizado.

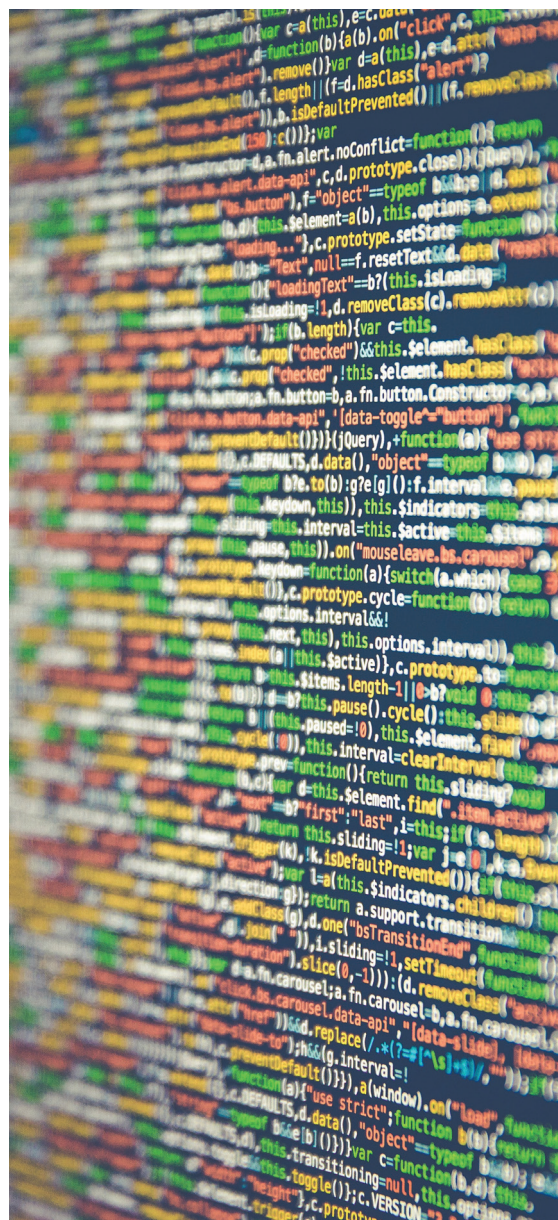
Para determinar o que é razoável, a LGPD leva em conta:

- i. fatores objetivos: tempo, custo e estado da arte para reversão do processo de anonimização;
- ii. fatores subjetivos: a própria capacidade do agente de tratamento de dados que, a partir de utilização exclusiva de meios próprios, poderia reidentificar uma base de dados.

BANCO DE DADOS: é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Art. 5º, IV, LGPD).

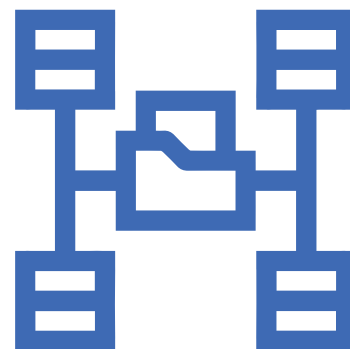
CICLO DE VIDA DOS DADOS: são as etapas que envolvem o trânsito interno e cronológico dos dados junto ao agente de tratamento, desde a sua obtenção até o seu descarte.

Os ciclos mais comuns englobam a coleta, o processamento, o uso, a divulgação, a retenção e a eliminação do dado. Relaciona-se ao fluxo de dados, embora geralmente o ciclo de vida dos dados implique uma definição cronológica mais apurada sobre o trânsito dos dados.



ENRIQUECIMENTO: é o processo de combinação dos dados pessoais entre uma base primária e uma base de terceiro. O enriquecimento envolve o incremento do volume de informações acerca de um(a) titular graças a fontes externas. É um processo que pode ser realizado em conjunto com a higienização.

Por exemplo, a empresa “A” possui apenas nome, CPF, endereço, e-mail e telefone de contato de um(a) cliente X. Após realizar parceria com a empresa B, ela passa a obter, ainda, dados sobre a renda, redes sociais e hábitos de consumo daquele(a) cliente.

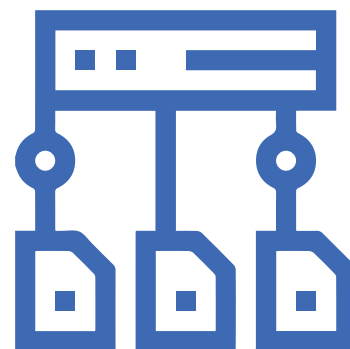


ESPELHAMENTO DE BASES DE DADOS ARMAZENADAS: técnica de criação de duas ou mais cópias redundantes da base de dados alocadas em diferentes espaços de servidores virtuais. O espelhamento minimiza a indisponibilidade da base de dados em situações nas quais haja dados corrompidos, mau funcionamento de uma rede ou ainda atualização de sistemas.

Por exemplo, durante uma atualização de seus sistemas virtuais, a empresa X foi surpreendida por um erro que corrompeu a sua base de dados principal. Nesse momento, devido à existência de uma base espelhada secundária, ela pode mudar o ponto focal para a base secundária e reestabelecer suas atividades de tratamento.

FLUXO DE DADOS: é a operação de correlação lógica acerca do trânsito dos dados em programas e *hardwares* presentes nos sistemas de um agente de tratamento. O processo de determinação do fluxo de dados geralmente engloba as transformações às quais os dados estão sujeitos, bem como a definição de quem tem acesso aos mesmos, onde estão armazenados e o que é feito. Relaciona-se ao ciclo de vida dos dados.

Assim, uma instituição, por exemplo, pode apresentar, por meio de um diagrama de fluxo de dados, como certo dado é coletado por um *software*, como o dado é tratado e refinado junto a outro *software* em conjunto com um *hardware* e como este dado é armazenado nas bases de servidores da instituição.



HIGIENIZAÇÃO: é o processo de certificação da confiabilidade de um dado pessoal contido na base do agente de tratamento. Envolve a atualização, a correção e a retirada de duplicações das informações já constantes na base e pode ser acompanhada por um processo de enriquecimento com o objetivo de tornar a base mais precisa.

É o caso de uma instituição que possui determinada base de cadastro antiga, integralmente constituída por fichas manualmente preenchidas. Ao submeter estes dados à higienização, ela, por meio de seus agentes de tratamento, poderá checar e atualizar informações de contato como telefone e e-mail, bem como padronizar os dados em um único formato e retirar duplicações.



PERFILAMENTO (PROFILING): implica o tratamento de dados pessoais com objetivo de traçar perfil dos(as) titulares de dados, envolvendo operações como cruzamento, agregação e enriquecimento de bases de dados.

Por exemplo, uma pesquisa de mercado que realiza cruzamento para identificar a faixa etária e gênero dos seus consumidores, obtendo perfis comportamentais. Outro exemplo é o armazenamento de informações de navegação por meio de *cookies* e sugestão de conteúdo a partir das preferências dos(as) usuários(as).

PSEUDONIMIZAÇÃO: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, a não ser que haja o uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (Art. 13, § 4º, LGPD).

Consiste em substituir um atributo (tipicamente um atributo único), em um registro, por outro, reduzindo a vinculação de um conjunto de dados com a identidade original de um dado. Não é um método de anonimização.

1.6 BASES LEGAIS

Conforme anteriormente mencionado, por base legal entende-se o fundamento que autoriza o tratamento de dados pessoais e dados pessoais sensíveis por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na LGPD (em seus artigos 7º e 11), indicadas abaixo.

As bases legais só não serão necessárias nos casos em que a LGPD não se aplica, como nas hipóteses do Art. 4º ou em situações de tratamento que envolvam dados anonimizados.

CONSENTIMENTO: é a manifestação livre, informada e inequívoca (Art. 7º, I, LGPD) pela qual o(a) titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Art. 5º, XII, LGPD). Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8º, *caput*, LGPD).

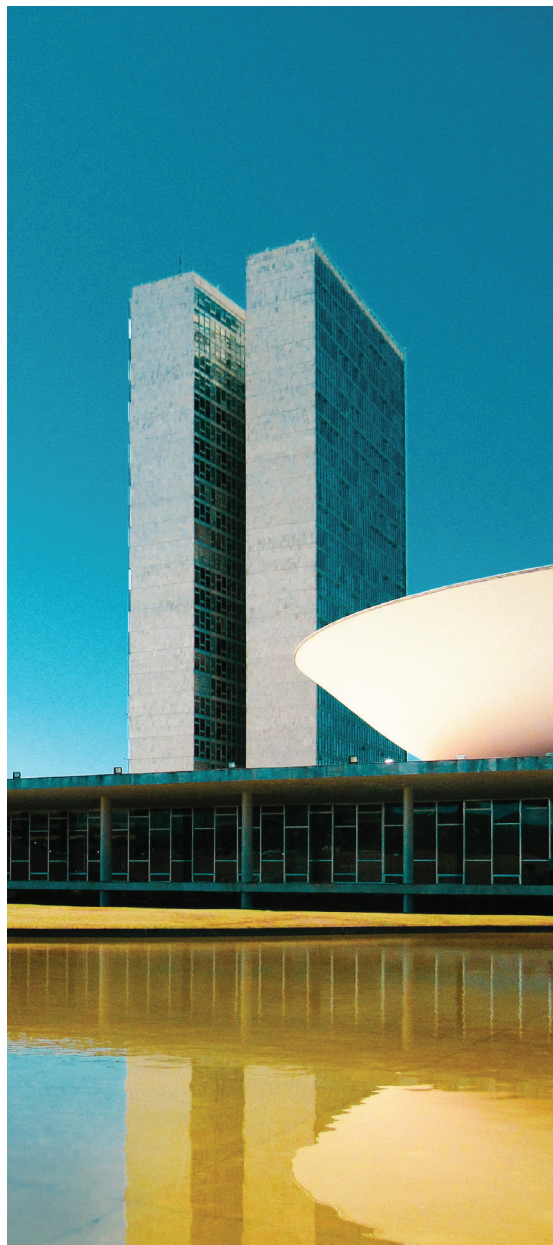
O consentimento deve ser **expresso** sobre a coleta, uso, armazenamento e qualquer outro tratamento de dados pessoais, de forma destacada das demais cláusulas contratuais (Art. 7º, IX, da Lei nº 12.965/2014 — Marco Civil da Internet). Ele deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do(a) titular dos dados pessoais.

O termo **livre** remete à ação espontânea, desinibida de pressão, que possibilite a tomada de escolha. Trata-se das situações em que não existe qualquer coação para que o(a) titular expresse a sua anuência para com o tratamento dos seus dados pessoais.

O adjetivo **informado** reflete o direito-dever de fornecer informações claras, precisas, em linguagem acessível e de fácil compreensão sobre o tratamento. É elementar certificar que informações essenciais sobre a operação de tratamento, seus modos, os agentes envolvidos e os eventuais riscos não tenham sido omitidas do(a) titular. Nesse sentido, ele(a) terá mais controle com relação aos seus dados.

Além disso, deve figurar como uma declaração de vontade **inequívoca** por parte do(a) titular. Dessa forma, abrange-se o modo de manifestação, firme e claro, acerca da concordância do(a) titular para o tratamento de seus dados.

É imprescindível garantir que a pessoa natural concordou com as operações que serão realizadas com as suas informações, de modo que o destaque das cláusulas de tratamento de dados pessoais deve ser



Ramon Braga/Inphash

sempre garantido ao titular de dados, seja em meio eletrônico ou impresso. Ou seja, não se admite o consentimento presumido para o tratamento de dados pessoais.

Quanto ao adjetivo **específico**, trata-se de uma decisão pontual, diferente do consentimento trivial. Aparece de forma taxativa quando se tratar de envolvimento de controladores terceiros à relação direta com o titular para o tratamento de seus dados (Art. 7º, § 5º, LGPD); de dados pessoais sensíveis (Art. 11, I, LGPD); de uma condição de vulnerabilidade do(a) titular, como crianças e adolescentes (Art. 14, § 1º, LGPD); ou de uma das hipóteses de transferência internacional para um país sem o mesmo nível de proteção de dados que o Brasil (Art. 33, VIII, LGPD).

Por fim, reitera-se que para que o consentimento só será considerado livre, informado e inequívoco, se levada em conta a **finalidade** da operação de tratamento de dados pessoais. O consentimento deve se dirigir a uma finalidade determinada, isto é, para propósito específico e explícito.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO

CONTROLADOR: é a hipótese na qual o controlador realiza o tratamento de dados para demonstrar conformidade com normas às quais está submetido, como por exemplo, para atender interesse público (Art. 7º, II, LGPD).

EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO:

é a possibilidade de tratamento de dados pessoais quando necessário para a execução e cumprimento de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o(a) titular, neste último caso, desde que a requerimento deste(a) (Art. 7º, V, LGPD).

EXECUÇÃO DE POLÍTICAS PÚBLICAS:

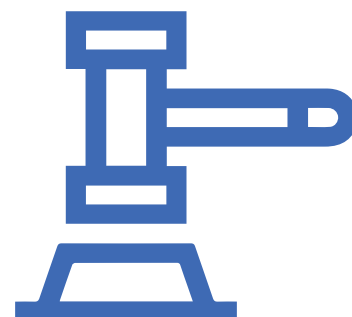
são as operações realizadas pela administração pública, para o tratamento e uso compartilhado de dados, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (Art. 7º, III), observadas as disposições do Capítulo IV da LGPD (*“Do tratamento de dados pessoais pelo poder público”*).

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL:

é a possibilidade de tratamento de dados pessoais para fins de andamento de processos judiciais, administrativos e arbitrais, como no caso da utilização de dados para a produção de provas (Art. 7º, VI, LGPD).

INTERESSE LEGÍTIMO DO CONTROLADOR OU DE TERCEIRO:

quando o tratamento é necessário para atender aos interesses legítimos do controlador ou de terceiro (Art. 7º, IX, LGPD). Esta base legal não pode ser utilizada em detrimento dos direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais.



O legítimo interesse somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: apoio e promoção de atividades do controlador; proteção, em relação ao(à) 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 da LGPD (Art. 10, LGPD).



Na hipótese de o tratamento se basear no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (Art. 10, § 1º, LGPD).

Além disso, deverá o controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse (Art. 10, § 2º, LGPD). A Autoridade Nacional de Proteção de Dados (ANPD) 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 (Art. 10, § 3º, LGPD).

Nota-se que apesar de se tratar de uma base legal mais abrangente, ela tem requisitos para a sua aplicabilidade. É recomendável que seja feito o chamado teste de proporcionalidade ou avaliação de legítimo interesse, previamente à operação de tratamento, mantendo-se o registro do respectivo teste.

O teste leva em conta:

- i. se o tratamento de dados pessoais possui uma finalidade legítima;
- ii. se não existem outras estratégias que utilizem uma menor quantidade ou que independam de dados pessoais;
- iii. um balanço de riscos avaliando a natureza da relação;
- iv. as expectativas razoáveis do(a) titular; e
- v. os efetivos resultados diante de suas garantias fundamentais e liberdades civis.

PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO(A) TITULAR OU DE TERCEIRO:

é a possibilidade de tratamento de dados pessoais para a tutela e proteção de aspectos da vida e da saúde física do(a) titular de dados (Art. 7º, VII, LGPD).

PROTEÇÃO DO CRÉDITO:

é a hipótese de tratamento de dados pessoais voltada a viabilizar e proteger as operações do mercado financeiro de crédito, permitindo, por exemplo, a inscrição de consumidores nos cadastros positivos de crédito e análises de risco com base no histórico de inadimplemento (Art. 7º, X). É mais um caso em que a LGPD deve dialogar com outras leis setoriais (e.g. Código de Defesa do Consumidor e Lei do Cadastro Positivo).

REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISA: possibilidade de tratamento de dados para fins de pesquisa, devendo garantir, sempre que possível, a anonimização dos dados pessoais (Art. 7º, IV, LGPD).

Quando se tratar de realização de estudos por órgãos de pesquisa em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, desde que eles sejam tratados exclusivamente dentro do órgão, e estritamente para a finalidade de estudos e pesquisa em saúde pública.

Ainda, os dados devem ser mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização, considerando os devidos padrões éticos relacionados a estudos e pesquisas (Art. 13, caput, LGPD).

TUTELA DA SAÚDE: é a possibilidade de tratamento de dados pessoais quando necessário em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (Art. 7º, VIII, LGPD).



1.7 DIREITOS DO(A)S TITULARES DE DADOS

ACESSO AOS DADOS: é o interesse resguardado do(a) titular de dados de receber uma cópia dos dados pessoais detidos pela empresa, se assim o requisitar (Art. 18, II, LGPD). Conforme a LGPD, tal direito será objeto de regulamentação por parte da ANPD e das autoridades da área de saúde e sanitárias, no âmbito de suas competências (Art. 13, § 3º, LGPD).

Sublinha-se que os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as suas finalidades (Art. 23, § 5º, LGPD).

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO: é o direito que o(a) titular de dados tem de solicitar que seus dados sejam anonimizados, bloqueados ou que haja a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei (Art. 18, IV, LGPD).

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO: é o direito de obter do controlador a informação, a qualquer momento e mediante requisição, de que os dados pessoais do(a) próprio(a) titular estão sendo tratados (Art. 18, I, LGPD).

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS: é direito do(a) titular requerer a retificação dos seus dados, caso estejam incorretos, insuficientes, imprecisos, não expressem a completude das informações armazenadas ou careçam de atualização (Art. 18, III, LGPD).

DIREITO DE PETICIONAR: é o direito do(a) titular de dados de fazer qualquer requerimento com relação aos seus dados contra o controlador, perante a Autoridade Nacional de Proteção de Dados (Art. 18, § 1º, LGPD).

ELIMINAÇÃO DOS DADOS PESSOAIS: o(a) titular de dados pode requerer que seus dados sejam excluídos, de forma que o agente de tratamento deverá eliminar todos os dados coletados com relação a esse(a) titular, a não ser que exista base legal que autorize a sua manutenção (Art. 18, VI, LGPD). Por exemplo, as hipóteses previstas no Art. 16 da LGPD, que dispõe sobre os casos em que é possível conservar dados pessoais após o término do tratamento.



INFORMAÇÃO DAS ENTIDADES PÚBLICAS E PRIVADAS: é possibilitado ao(à) titular de dados a solicitação de informações das entidades públicas e privadas com as quais o controlador realiza o uso compartilhado de dados (Art. 18, VII, LGPD).

INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO: é direito do(a) titular de dados solicitar informações sobre a possibilidade e hipóteses de não fornecimento do consentimento, além de entender sobre as consequências da negativa (Art. 18, VIII, LGPD).

INFORMAÇÕES CLARAS E ADEQUADAS: são informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, que podem ser solicitadas pelo(a) titular de dados. Tais informações, a serem oferecidas pelo controlador, deverão apresentar clareza e adequação com o que foi solicitado (Art. 20, *caput* e § 1º, LGPD).

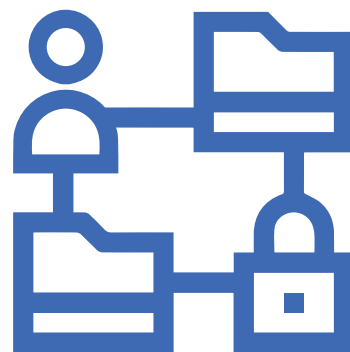
OPOSIÇÃO AO TRATAMENTO DE DADOS PESSOAIS: é a possibilidade de oposição do(a) titular ao contexto do tratamento de dados e/ou às suas respectivas finalidades, incluindo tratamento realizado com base em uma das hipóteses de dispensa do consentimento (Art. 18, § 2º, LGPD).

PORTABILIDADE DOS DADOS: é a disponibilização dos dados do titular a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação da Autoridade Nacional de Proteção de Dados, observados os segredos comercial e industrial (Art. 18, V, LGPD).

REVISÃO: é o pedido que o(a) titular de dados pode realizar com pretensão de revisar as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (Art. 20, *caput*, LGPD).

REVOGAÇÃO DO CONSENTIMENTO: é manifestação expressa do(a) titular, por procedimento gratuito e facilitado, de revogar o consentimento (Art. 18, IX, LGPD), sendo ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação (Art. 8º, § 5º, LGPD).

TITULARIDADE DOS DADOS PESSOAIS: é direito de toda pessoa natural, sendo assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (Art. 17, LGPD). O(a) titular é, portanto, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Art. 5º, V, LGPD).



1.8 ESTRUTURA REGULATÓRIA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): conforme definição apresentada na seção “Sujeitos”.

CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE: é o órgão criado no âmbito da ANPD, composto por 23 (vinte e três) representantes, titulares e suplentes, designados por ato do Presidente da República, permitida a delegação (Art. 58-A, LGPD).

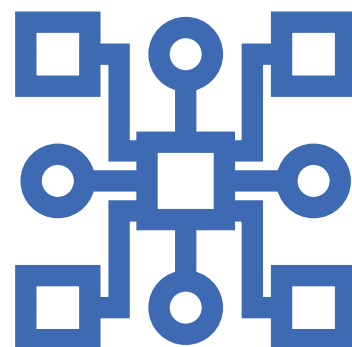
Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 58-B, LGPD):

- i. propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
- ii. elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- iii. sugerir ações a serem realizadas pela ANPD;
- iv. elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e
- v. disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (“MPDFT”): é uma instituição que possui autonomia funcional e administrativa, responsável por defender a ordem jurídica, o regime democrático e os interesses sociais e individuais indisponíveis (Art. 127, caput e § 1º, CF). No caso específico do MPDFT, tem-se que este possui uma Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec), instituída pela Portaria Normativa nº 539, de 12 de abril de 2018, e que atua de forma ativa em questões opinativas, informativas, investigativas, de notificação e de sanção que se referem às normas de proteção de dados pessoais no Brasil.

PROCON: é órgão estadual ou municipal que atua em âmbito local no que se refere a matérias de proteção e defesa do consumidor. Também é responsável pelo monitoramento do mercado de consumo local. Os Procons fazem parte do Sistema Nacional de Defesa do Consumidor.

REGULAÇÃO ESTATAL: refere-se ao condicionamento, coordenação e disciplina da atividade privada, abrangendo a edição de normas e a sua implementação concreta, bem como a fiscalização do seu cumprimento e a punição de infrações.





Christina wocniachat.com/unsplash

REGULAÇÃO DE RISCO: envolve ações que promovam a melhoria da gestão de risco (i.e., a cognição, avaliação e gerenciamento, que possui como viés a implementação da política de gestão de riscos). Exige o implemento de medidas apropriadas para assegurar e demonstrar conformidade, levando em consideração, entre outros, os riscos de probabilidade e gravidade em certas circunstâncias, apresentando-se em um contexto de obrigação geral de gerir adequadamente os riscos.

SECRETARIA NACIONAL DO CONSUMIDOR (“SENACON”): foi instituída pelo Decreto nº 7.738, de 28 de maio de 2012, e integra a estrutura do Ministério da Justiça. Atua com o acompanhamento (planejamento, elaboração, coordenação e execução) da Política Nacional das Relações de Consumo. Dentre os objetivos da SENACON, destacam-se a garantia dos direitos dos consumidores, a harmonização das relações de consumo e a atuação integrada dos órgãos que compõem o Sistema Nacional de Defesa do Consumidor.

1.9 RESPONSABILIDADE E SANÇÕES

ADVERTÊNCIA: reprimenda ao agente de tratamento que possui indicação de prazo para adoção de medidas corretivas (Art. 52, I, LGPD).

BLOQUEIO DOS DADOS PESSOAIS: é a suspensão temporária das operações de tratamento envolvendo os dados pessoais a que se refere a infração, até que a situação seja regularizada (Art. 52, V, LGPD).

CRITÉRIOS PARA APLICAÇÃO DAS SANÇÕES: as sanções serão aplicadas após procedimento administrativo que garanta a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, conforme com as peculiaridades do caso concreto (Art. 52, § 1º, LGPD).

Serão considerados os seguintes parâmetros e critérios (Art. 52, § 1º, incisos I a XI, LGPD):

- i. a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- ii. a boa-fé do infrator;
- iii. 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;
- 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.

ELIMINAÇÃO DOS DADOS PESSOAIS: é a exclusão dos dados pessoais a que se refere a infração (Art. 52, VI, LGPD).

MULTA DIÁRIA: é limitada a R\$ 50.000.000,00 — cinquenta milhões de reais — (Art. 52, III, LGPD).

MULTA SIMPLES: é valorada em até 2% 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 (Art. 52, II, LGPD).



PUBLICIZAÇÃO DA DECISÃO: é o ato de tornar a infração pública após ter sua ocorrência devidamente apurada e confirmada (Art. 52, IV, LGPD).

RESPONSABILIDADE: é a obrigação de reparação de danos patrimoniais, morais, individuais ou coletivos causados em razão de exercício de atividade de tratamento de dados pessoais, violando a legislação de proteção de dados pessoais (Art. 42, *caput*, LGPD).

A responsabilidade que vige sob a LGPD é, principalmente, a solidária. Nesse sentido, a LGPD estabelece que o operador responde solidariamente pelos danos causados pelo tratamento de dados quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.

Além disso, os controladores diretamente envolvidos no tratamento que causou danos aos(às) titulares de dados também respondem solidariamente pelo dano (Art. 42, § 1º, I e II, LGPD).

SANÇÕES ADMINISTRATIVAS: são as penalidades aplicáveis aos agentes de tratamento de dados em razão das infrações cometidas às disposições da Lei (Art. 52, *caput*, LGPD).

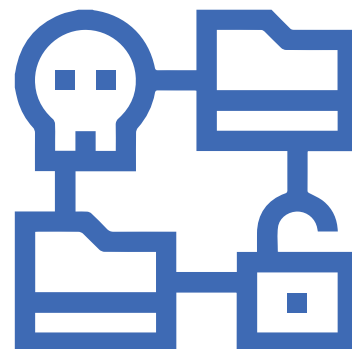


1.10 GOVERNANÇA

GOVERNANÇA DE DADOS: pode ser definida como os processos, estruturas, normas, regras, políticas, decisões e responsabilidades na maneira como os agentes de tratamento utilizam e processam os dados e informações, de forma a garantir que esse uso seja realizado de maneira correta e apropriada.

INCIDENTES DE SEGURANÇA: apesar de fazer menção a incidentes de segurança em diversas disposições (principalmente em seu Art. 48), a LGPD não traz uma definição clara do termo.

A GDPR (*General Data Protection Regulation EU 2016/679*), por outro lado, traz a definição de “*data breach*” (violação de dados pessoais). Um incidente de segurança, conforme o Art. 4(12) da GDPR, caracteriza-se como uma violação da segurança dos sistemas e redes que leva a situações acidentais ou ilícitas de destruição, perda, alteração ou divulgação não autorizada de dados pessoais transmitidos, armazenados, ou de qualquer outra forma tratados.



PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: é a forma de endereçamento e comunicação de determinadas informações quando da ocorrência de um incidente de segurança da informação. A LGPD apresenta algumas dessas informações e outros requisitos para o Plano de Resposta a Incidentes de Segurança da Informação em seu Art. 48, *caput* e § 1º.

O controlador deverá comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos(às) titulares dos dados quando da ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos(às) titulares. Tal comunicação deve ser feita em prazo razoável (conforme definido pela ANPD) e conter (Art. 48, § 1º, incisos I a VI):

- i. a descrição da natureza dos dados afetados;
- ii. as informações sobre o(a)s 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 da comunicação, caso não tenha sido imediata; e
- vi. as medidas que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Informações que também podem constar da resposta, de forma a deixá-la mais completa e transparente são:

- i. a natureza do incidente de segurança;
- ii. a categoria dos dados (e.g. que tipo de dados estão envolvidos, se há dados sensíveis, de crianças e adolescentes etc.);
- iii. a quantidade de titulares de dados afetados;
- iv. as áreas da empresa, órgão, entidade ou instituição afetadas; e
- v. a execução do plano de notificação.

POLÍTICA DE PRIVACIDADE: é o documento que dispõe aos(as) titulares de dados a forma como o(a)s agentes vão realizar o tratamento dos dados pessoais que estão em seu poder e explicita os direitos do(a)s titulares nessa relação.

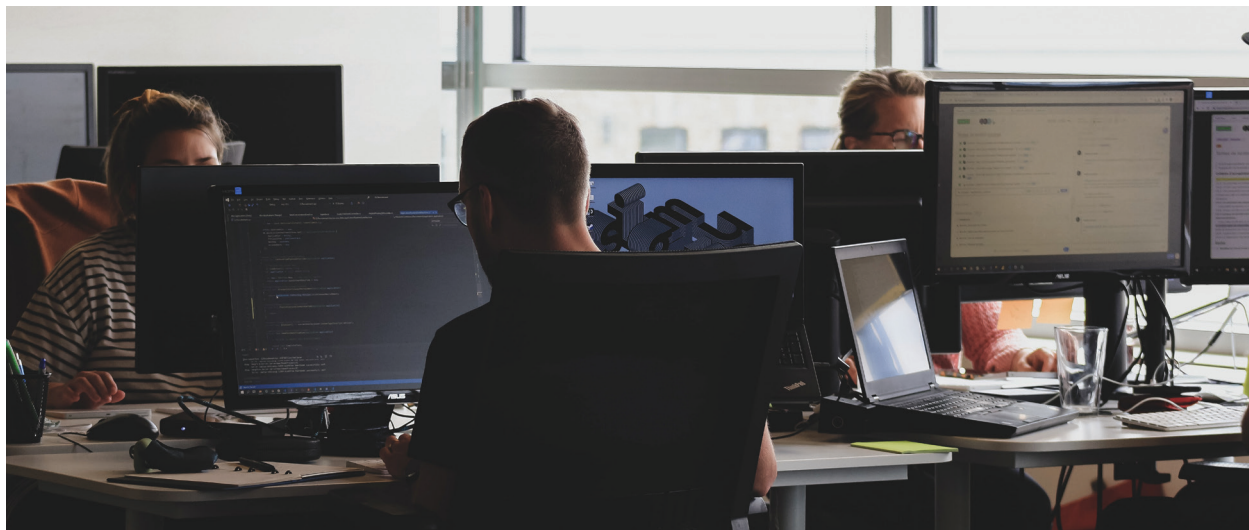
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: é o documento que dispõe sobre as diretrizes de proteção às informações que estão sob guarda do agente de tratamento (padrões e medidas técnicas), de forma a garantir a segurança dessas informações. A Política de Segurança da Informação é geralmente aplicada a todos os(as) funcionários(as) e outras pessoas que tenham acesso às informações, dados e sistemas.



PROGRAMA DE GOVERNANÇA EM PRIVACIDADE: sobre o denominado programa de governança em privacidade, a LGPD determina que ele deve conter, no mínimo (Art. 50, § 2º, I, LGPD):

- i. a demonstração do 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;
- ii. a aplicação a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- iii. adaptação à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- iv. o estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- v. o objetivo de estabelecer relação de confiança com o(a) titular, por meio de atuação transparente e que assegure mecanismos para sua participação;
- vi. a integração à sua estrutura geral de governança e estabelecimento e aplicação de mecanismos de supervisão internos e externos;
- vii. os planos de resposta a incidentes e remediação; e
- viii. a atualização constante com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

REGRAS DE BOAS PRÁTICAS E DE GOVERNANÇA: são 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 (Art. 5º, *caput*, LGPD).



2.

DEFINIÇÕES TRAZIDAS PELA *EUROPEAN DATA PROTECTION LAW*

ACCOUNTABILITY: definido pelo Art. 5(2), da GDPR (*General Data Protection Regulation EU 2016/679*), tal princípio é compreendido como a responsabilidade e a demonstração, pelo controlador, de que este está em conformidade com as normas e demais princípios de proteção de dados.

ARTICLE 29 DATA PROTECTION WORKING PARTY (“WP29”): o Grupo de Trabalho do Artigo 29 era um órgão formado pelas 28 autoridades de proteção de dados da União Europeia, que formulava opiniões e orientações para a aplicação das normas sobre proteção de dados vigentes. O WP29 foi substituído pelo *European Data Protection Board* (EDPB) quando da entrada em vigor da *General Data Protection Regulation* (GDPR).

CONVENÇÃO 108/CONVENÇÃO 108+: é a Convenção para a Proteção dos Indivíduos relativamente ao Processamento Automático de Dados Pessoais. Trata-se de uma convenção internacional elaborada no âmbito do *Council of Europe*, e que entrou em vigor em outubro de 1985.

Foi um dos primeiros documentos internacionais que buscou proteger as pessoas naturais de possíveis consequências negativas do tratamento automatizado de dados pessoais e regular outros aspectos desse tratamento, como a proibição do tratamento de dados sensíveis, o direito dos indivíduos sobre os próprios dados e a transferência internacional de dados.

Importante notar que a Convenção passou por uma atualização recentemente, sendo que o seu resultado — a Convenção Modernizada para a Proteção dos Indivíduos relativamente ao Processamento de Dados Pessoais, adotada em 18 de maio de 2018 — passou a ser conhecido como Convenção 108+.

Christian Lue/Umsplash



COUNCIL OF EUROPE (“CoE”): é a instituição europeia que trabalha a temática de direitos humanos, proteção às minorias, igualdade, liberdade de expressão e reunião. Também lida com combate à corrupção e terrorismo. Note-se que não se trata de uma instituição pertencente à estrutura da UE. Possui 47 Estados-membros.

COUNCIL OF THE EUROPEAN UNION (“COUNCIL”): é um dos órgãos de decisão da União Europeia composto pelos(as) ministros(as) de governo dos Estados-membros do bloco. Possui as atribuições de negociação e adoção das normas propostas da *European Commission*, coordenação das políticas internas e externas do bloco, celebração de acordos internacionais e aprovação do orçamento da União Europeia (juntamente com o *European Parliament*).

DATA BREACH (VIOLAÇÃO DE DADOS PESSOAIS): definido pelo Art. 5(12) da GDPR *General Data Protection Regulation EU 2016/679*) como uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

DATA PROTECTION IMPACT ASSESSMENT (“DPIA”): a Avaliação de Impacto na Proteção de Dados (DPIA) é um processo para criar e demonstrar conformidade, pensado nas diretrizes da GDPR *General Data Protection Regulation EU 2016/679*), considerado obrigatório para todas as operações de tratamento que resultem em um alto risco aos direitos e liberdade das pessoas naturais. Trata-se de uma maneira útil para os controladores de dados implementarem sistemas de tratamento de dados que estejam em conformidade com a GDPR.

DATA PROTECTION AUTHORITY (“DPA”)/SUPERVISORY AUTHORITY: a *Supervisory Authority* é definida pela GDPR (*General Data Protection Regulation EU 2016/679*) em seus artigos 4(21) e 51(1) como: autoridade pública independente que é estabelecida por um Estado Membro, responsável pelo monitoramento e aplicação da GDPR, com o objetivo de proteção dos direitos e liberdades fundamentais das pessoas naturais com relação ao tratamento de dados e para facilitação do fluxo livre de dados pessoais na União Europeia. Tal autoridade também tem a função de aplicar a GDPR de maneira consistente, conforme artigo 51(2), da GDPR.

DIRETIVA 95/46/CE: é antiga norma de proteção de dados pessoais que estava em vigor na União Europeia. A Diretiva 95/46/CE era relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi aprovada pelo *European Parliament* e pelo *Council of the European Union* e entrou em vigor em



dezembro de 1995. Foi revogada em 24 de maio de 2018, sendo substituída pela GDPR (*General Data Protection Regulation EU 2016/679*).

EUROPEAN COMMISSION (“EC”): é o órgão executivo da União Europeia que realiza as decisões políticas e estratégicas em seu âmbito, elabora propostas legislativas, trata de questões do orçamento (gestão, distribuição e controle de despesas) do bloco, executa as decisões do *European Parliament* e do Council, garante o cumprimento das normas da União e representa o bloco nas questões internacionais. É composta por 28 comissários(as) (um(a) representante de cada país que compõe a União).

EUROPEAN DATA PROTECTION BOARD (“EDPB”): é um órgão independente, composto pelas autoridades de proteção de dados da Europa e pelo *European Data Protection Supervisor*. O EDPB possui a missão de contribuir com a correta aplicação das normas envolvendo proteção de dados e para a promoção de cooperação entre as autoridades de proteção de dados.

EUROPEAN DATA PROTECTION SUPERVISOR (“EDPS”): é a autoridade independente de proteção de dados da União Europeia (UE) que possui as seguintes atribuições:

- i. garantir a proteção de dados pessoais e a privacidade no tratamento de dados realizados por instituições da EU;
- ii. como auxiliar tais órgãos nas questões relativas a esse tipo de tratamento; monitorar as tecnologias que podem afetar a proteção de dados pessoais;
- iii. assistir a Corte de Justiça da União Europeia na interpretação das normas de proteção de dados; e
- iv. cooperar com outras autoridades de proteção de dados no que se refere à proteção de dados.

EUROPEAN PARLIAMENT (“EP”): é órgão legislativo da União Europeia (UE), que possui poderes legislativos (sugere propostas legislativas à *European Commission* e adota as normas por estas propostas, decide sobre legislações e acordos internacionais); tem poderes de supervisão (com o controle das instituições do bloco, aprovação do orçamento da União, realização de inquéritos, entre outras atribuições); e poderes orçamentais (estabelecendo o orçamento do bloco em conjunto com o Conselho Europeu e aprovando o quadro financeiro plurianual da União). Os membros que compõem o Parlamento Europeu são eleitos pelos(as) cidadãos(ãs) a cada cinco anos.



GENERAL DATA PROTECTION REGULATION EU 2016/679 (“GDPR”):

Regulação Geral de Proteção de Dados UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Trata-se de regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Revogou a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados).

A GDPR foi um importante marco para a proteção de dados pessoais, por propor uma regulação que contempla os novos aspectos e avanços da era digital. Dessa forma, atualizou no direito europeu os princípios e regras de tratamento aos dados pessoais, os quais foram parâmetros para a elaboração e proposição da lei brasileira.

PERSONAL DATA BREACH:

de acordo com o Art. 4(12), da GDPR, trata-se de uma violação da segurança que conduz, de forma acidental ou ilícita, à destruição, perda, alteração, divulgação não autorizada ou acesso não autorizado a dados pessoais transmitidos, armazenados ou tratados de outra maneira.

PROCESSING:

é trazido pelo artigo 4(1), da GDPR *General Data Protection Regulation EU 2016/679*, que estabelece que o processamento é qualquer operação ou conjunto de operações efetuadas em dados pessoais ou em conjuntos de dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou qualquer outra forma de tornar o dado disponível, alinhamento ou combinação, restrição, eliminação ou destruição.

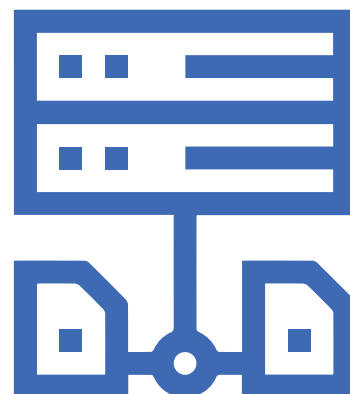
É o equivalente ao tratamento de dados pessoais na legislação brasileira.

PROFILING:

é definido pelo artigo 4(4), da GDPR (*General Data Protection Regulation EU 2016/679*), como qualquer tratamento automatizado de dados pessoais que os utilize para analisar ou fazer previsões sobre determinados aspectos de um(a) titular de dados, em especial com relação ao seu desempenho no trabalho, sua situação econômica, saúde pessoal, preferências, interesses, credibilidade, comportamento, localização ou movimentos.

UNIÃO EUROPEIA (“UE”):

é um bloco econômico composto por 27 países da Europa, sendo eles: Alemanha, Áustria, Bélgica, Bulgária, Chipre, Croácia, Dinamarca, Eslováquia, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Holanda, Hungria, Irlanda, Itália, Letônia, Lituânia, Luxemburgo, Malta, Polônia, Portugal, República Tcheca, Romênia, Suécia.



ÍNDICE

- Accountability, 30
- Acesso aos dados, 21
- Adequação, 6
- Advertência, 25
- Agentes de tratamento, 8
- Anonimização, 14
- Anonimização, bloqueio ou eliminação, 21
- Article 29 Data Protection Working Party (“WP29”), 30
- Autoridade Nacional de Proteção de Dados (ANPD), 8, 23
- Banco de dados, 14
- Bases legais, 10
- Bloqueio dos dados pessoais, 25
- Bloqueio, 10
- Boa-fé, 6
- Ciclo de vida dos dados, 14
- Confirmação da existência de tratamento, 21
- Conselho nacional de proteção de dados pessoais e da privacidade, 23
- Consentimento, 17
- Conservação de dados após o término do tratamento, 10
- Controlador, 8
- Controle compartilhado (co-controle), 8
- Controle integral, 8
- Convenção 108/Convenção 108+, 30
- Correção de dados incompletos, inexatos ou desatualizados, 21
- Council of europe (“coe”), 31
- Council of the european union (“council”), 31
- Crítérios para aplicação das sanções, 25
- Cumprimento de obrigação legal ou regulatória pelo controlador, 18
- Dado pessoal, 10
- Dado pessoal sensível, 10
- Dados coletados no território nacional, 10
- Data breach (violação de dados pessoais), 31
- Data Protection Authority (“DPA”)/Supervisory Authority, 31
- Data Protection Impact Assessment (“DPIA”), 31
- Direito de petição, 21
- Diretiva 95/46/ce, 31
- Eliminação, 11
- Eliminação dos dados pessoais, 21, 25
- Encarregado(a) (Data Protection Officer — “DPO”), 8
- Enriquecimento, 15
- Espelhamento de bases de dados armazenadas, 15
- European Commission (“EC”), 32
- European Data Protection Board (“EDPB”), 32
- European Data Protection Supervisor (“EDPS”), 32
- European Parliament (“EP”), 32
- Execução de contrato ou de procedimentos preliminares relacionados a contrato, 18
- Execução de políticas públicas, 18
- Exercício regular de direitos em processo judicial, administrativo ou arbitral, 18
- Finalidade, 6
- Fluxo de dados, 15
- General Data Protection Regulation EU 2016/679 (“GDPR”), 33
- Governança de dados, 27
- Higienização, 15
- Incidentes de segurança, 27
- Informação das entidades públicas e privadas, 22
- Informação sobre a possibilidade de não fornecer consentimento, 22

- Informações claras e adequadas, 22
- Interesse legítimo do controlador ou de terceiro, 18
- Limitação temporal do armazenamento, 6
- Livre acesso, 6
- Ministério Público do Distrito Federal e Territórios (“MPDFT”), 23
- Multa diária, 25
- Multa simples, 25
- Não discriminação, 6
- Necessidade, 6
- Operador, 9
- Oposição ao tratamento de dados pessoais, 22
- Órgão de pesquisa, 11
- Perfilamento (profiling), 16
- Personal data breach, 33
- Plano de resposta a incidentes de segurança da informação, 27
- Política de privacidade, 28
- Política de segurança da informação, 28
- Portabilidade dos dados, 22
- Prevenção, 7
- Processing, 33
- Procon, 23
- Profiling, 33
- Programa de governança em privacidade, 28
- Proteção da vida ou da incolumidade física do(a) titular ou de terceiro, 19
- Proteção do crédito, 19
- Pseudonimização, 16
- Publicização da decisão, 26
- Qualidade dos dados, 7
- Realização de estudos por órgãos de pesquisa, 20
- Regras de boas práticas e de governança, 29
- Regulação de risco, 24
- Regulação estatal, 23
- Relatório de impacto à proteção de dados pessoais, 11
- Responsabilidade, 26
- Responsabilização e prestação de contas, 7
- Retenção mínima, 11
- Revisão, 22
- Revogação do consentimento, 22
- Sanções administrativas, 26
- Secretaria Nacional do Consumidor (“SENACON”), 24
- Segurança, 7
- Setor acadêmico, 9
- Setor público, 9
- Terceiro setor, 9
- Término do tratamento de dados pessoais, 13
- Titular de dados pessoais, 9
- Titularidade dos dados pessoais, 22
- Transferência internacional de dados, 13
- Transparência, 7
- Tratamento de dados pessoais de crianças e adolescentes, 12
- Tratamento de dados pessoais pelo poder público, 12
- Tratamento de dados pessoais sensíveis, 12
- Tratamento, 11
- Tutela da saúde, 20
- União Europeia (“UE”), 33
- Uso compartilhado de dados (“compartilhamento”), 13

REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679**. Adotado em 4 abr. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Acesso em: 16 jun. 2019. p. 6

_____. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. Adotado em 3 de outubro de 2017. Disponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=47742. Acesso em: 11 set. 2019.

_____. **Statement on the role of a risk-based approach in data protection legal frameworks**. Adotado em 30 mai. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf. Acesso em: 17 jun. 2019.

BINNS, R. Data protection impact assessments: a meta-regulatory approach. **International Data Privacy Law** (2017) 7 (1), p. 22-35. Disponível em: <https://academic.oup.com/idpl/article/7/1/22/3782692>.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 190-200.

BRASIL. **Decreto nº 7.738, de 28 de maio de 2012**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Conselho Administrativo de Defesa Econômica – CADE [...]. Diário Oficial da União, 29 de maio de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7738.htm. Acesso em: 02 ago. 2021.

BRASIL. **Lei nº 9.307 de 23 de setembro de 1996**. Dispõe sobre a arbitragem (Lei de Arbitragem). Diário Oficial da União, 24 de setembro de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9307.htm. Acesso em: 20 ago. 2021.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 ago. 2021.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 ago. 2021.

CHEONG, L. K.; CHANG, V. **The Need for Data Governance: a Case Study.** 18th Australasian Conference on Information System. Toowoomba, 2007. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1110&context=acis2007>. Acesso em: 12 jun. 2019. p. 1001.

IAPP. **Glossary of Privacy Terms. International Association of Privacy Professionals, 2019.** Disponível em: <https://iapp.org/resources/glossary/#information-life-cycle-management-2>. Acesso em: 06 set. 2019.

NOHARA, I. P. **Direito administrativo.** 7. ed. rev., atual. e ampl. São Paulo: Atlas, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597011104/cfi/6/10!/4/2/4/2/2@0:o>. Acesso em: 17 jun. 2019. p. 66 e 661-662.

OLIVEIRA, R. R. **Novo Perfil da Regulação Estatal — Administração Pública de Resultados e Análise de Impacto Regulatório.** Rio de Janeiro: Forense, 2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/978-85-309-6746-8/>. Acesso em: 17 mai. 2019. s/p. Item 3.1.

PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. **General Data Protection Regulation – EU 2016/679.** Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>. Acesso em: 12 jun. 2020.

REINO UNIDO. INFORMATION COMMISSIONER'S OFFICE. **Guide to the General Data Protection Regulation (GDPR).** Publicado em 2 de agosto de 2018. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-o.pdf>. Acesso em: 25 mar. 2020.

SEATTLE. **City of Seattle Open Data Risk Assessment.** January 2018-Final Report. Future of Privacy Forum: Seattle, 2018. Disponível em: <https://www.seattle.gov/Documents/Departments/SeattleIT/DigitalEngagement/OpenData/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>. Acesso em: 06 mai. 2019.

STUMPF, Ricardo Dantas. O porquê de governança de dados em organizações de controle. **Revista do TCU**, n 137, p. 106-115, set./dez. 2016. Disponível em: <https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1383/1529>. Acesso em: 12 jun. 2019. p. 108-110.

O presente Glossário consiste em material meramente informativo e não substitui a necessidade de aconselhamento jurídico para a avaliação do caso concreto.

As manifestações expressas por integrantes dos quadros da Fundação Getulio Vargas representam, exclusivamente, as opiniões do(a)s seus/suas autores(as) e não, necessariamente, a posição institucional da FGV.



Este trabalho está licenciado sob uma licença Creative Commons CC BY-NC-ND 4.0. Essa licença permite que outros façam download do material e o compartilhem desde que atribuam crédito ao autor corretamente, mas sem alterar o material de nenhuma forma ou utilizá-lo para fins comerciais. Veja o [texto da licença](#).



[Nosso site](#) | [Medium](#)

EQUIPE DO CEPI

Coordenação Técnica

Alexandre Pacheco da Silva

Coordenação Executiva

Victor Nóbrega Luccas

Equipe de Pesquisadores(as)

Fábio Ferraz de Almeida

Fabício Vasconcelos Gomes

Fernando Issao Ninomiya

Laurianne-Marie Schippers

Livia Pazianotto Torres

Marcelo de Castro Cunha Filho

Maria Cecília Oliveira Gomes

Marília Papaléo Gagliardi

Jordan Vinícius de Oliveira

Ramon Silva Costa

Thaís Duarte Zappellini

Responsáveis pela organização e revisão deste material

Laurianne-Marie Schippers

Thaís Duarte Zappellini

Responsável pelo layout

Laurianne-Marie Schippers

Projeto gráfico e diagramação

Gustavo Abumrad

Ícones: [flaticon.com](#)

Imagem de capa: [LuckyTD/iStockphoto.com](#)