Editora
Ibict

GUIA DE BOAS PRÁTICAS
PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

AUTORES

Rosilene Paiva Marinho de Sousa
Silvana Aparecida Borsetti Gregorio Vidotti
Milton Shintaku

2026

Ministério da Ciência, Tecnologia e Inovação
Instituto Brasileiro de Informação em Ciência e Tecnologia

GUIA DE BOAS PRÁTICAS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Editora Ibict

Brasília
2026

PRESIDÊNCIA DA REPÚBLICA

Luiz Inácio Lula da Silva
PRESIDENTE DA REPÚBLICA

Geraldo José Rodrigues Alckmin Filho
VICE-PRESIDENTE DA REPÚBLICA

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Luciana Santos
Ministra da Ciência, Tecnologia e Inovação

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA

Tiago Emmanuel Nunes Braga
Diretoria

Carlos André Amaral de Freitas
Coordenação de Administração - COADM

Ricardo Medeiros Pimenta
Coordenação de Ensino e Pesquisa em Informação para a Ciência e Tecnologia - COEPI

Henrique Denes Hilgenberg Fernandes
Coordenação de Planejamento, Acompanhamento e Avaliação - COPAV

Cecília Leite Oliveira
Coordenação-Geral de Informação Tecnológica e Informação para a Sociedade - CGIT

Washington Luís Ribeiro de Carvalho Segundo
Coordenação-Geral de Informação Científica e Técnica - CGIC

Alexandre Faria de Oliveira
Coordenação-Geral de Tecnologias de Informação e Informática - CGTI

Milton Shintaku
Coordenação de Tecnologias para Informação - COTEC

Ministério da Ciência, Tecnologia e Inovação
Instituto Brasileiro de Informação em Ciência e Tecnologia

GUIA DE BOAS PRÁTICAS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Autores
Rosilene Paiva Marinho de Sousa
Silvana Aparecida Borsetti Gregorio Vidotti
Milton Shintaku

Editora Ibict

Brasília - DF
2026

S725g Guia de boas práticas de privacidade e proteção de dados pessoais [recurso eletrônico] / Rosilene Paiva Marinho de Sousa, Silvana Aparecida Borsetti Gregorio Vidotti e Milton Shintaku. -- Brasília: Editora Ibict, 2026.

1 recurso online [57 p.] : il.

Modo de acesso: WWW
Publicação digital (e-book) no formato PDF. [980 KB]
ISBN: 978-85-7013-228-4
DOI: 10.22477/9788570132284

1. Lei Geral de Proteção de Dados (LGPD) - Brasil. 2. Governança de dados. 3. Privacidade e proteção de dados pessoais. 4. Segurança da informação. I. Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict). II. Título.

CDU 342.721(81):004.056

Ficha catalográfica elaborada por Bernardo Dionízio Vechi – CRB1/2775

Como referenciar este livro:

SOUSA, Rosilene Paiva Marinho de; VIDOTTI, Silvana Aparecida Borsetti Gregorio; SHINTAKU, Milton. **Guia de boas práticas de privacidade e proteção de dados pessoais**. Brasília, DF: Editora Ibict, 2026.

Endereço: Ibict - Instituto Brasileiro de Informação em Ciência e Tecnologia Setor de Autarquias Sul (SAUS), Quadra 05, Lote 06, Bloco H – 5o. andar CEP: 70.070-912 - Brasília.

SUMÁRIO

APRESENTAÇÃO

O presente trabalho é resultado dos estudos realizados no âmbito das atividades relacionadas ao atendimento do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) para cumprimento das premissas da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Apresenta a consolidação de informações relacionadas à implementação das diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD) em outras instituições, que a fizeram com sucesso.

Assim, representa o resultado do levantamento e análise de documentações oriundo de outras instituições que já implementam com sucesso as premissas da LGPD, de forma a apoiar outras instituições a fazê-lo. As informações aqui apresentadas foram validadas no Ibict, na promoção da proteção de dados pessoais nos sistemas de informação mantidos pela instituição. Entende-se aqui sistema de informação como um conjunto de atividades, processos, métodos, padrões e ferramentas informatizadas.

Nesse contexto, este guia está estruturado da seguinte forma:

Na introdução, evidencia-se a necessidade de observância à LGPD, e o diálogo necessário com outras normas que tratam de dados pessoais visando a harmonização e complementaridade entre elas, através do diálogo das fontes jurídicas. Descreve também o escopo do presente Guia de Boas Práticas - Privacidade e Proteção de Dados Pessoais e as bases que a orientam, indicando inclusive os canais de comunicação para o titular dos dados.

Na seção 2, direciona o entendimento sobre a importância da LGPD na Governança de Dados Pessoais em Órgão Público, no caso o Instituto Brasileiro de Informação em Ciência e Tecnologia - bict, e a conformidade legal. São apresentados os conceitos de governança e governança de dados pessoais como uma decorrência do primeiro e em conformidade com a governança de dados no setor público.

Na sequência, a seção 3, busca tornar simples a compreensão de conceitos relevantes, a saber, dados e informações, apresentou-se conceitos utilizados no campo da Ciência da Informação orientando as principais distinções, e apresentando o dado como registro, fato ou acontecimento que pode ser considerado matéria prima da informação.

Na seção 4, apresenta a relação entre privacidade e dados pessoais, inicialmente esta decorrente da primeira, porém, alinhando os conceitos ao considerar privacidade um conceito aberto e adaptável às circunstâncias específicas, enquanto dados pessoais relacionando-se ao objeto específico de existência de tratamento dos dados pessoais.

Aprofunda-se, na seção 5, uma discussão sobre o conceito de dado pessoal, dados pessoais sensíveis, dado anonimizado e pseudonimizado. Apresenta-se as principais diferenças e características dessas quatro categorias de dados. São apresentados também, os tipos de dados que não são objeto de proteção pela LGPD.

Para conhecimento dos leitores do presente Guia de Boas Práticas, na seção 6, apresenta-se os fundamentos e princípios constantes na LGPD, previstos nos artigos 2º e 6º, respectivamente, destacando que para o Ibict, fundamentos como privacidade, liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico e a inovação, são relevantes no desenvolvimento de suas atividades de pesquisa. Da mesma forma, em relação aos princípios, destacam-se a cultura da observância dos princípios, e em especial, em relação aos princípios da finalidade, necessidade, adequação, transparência, responsabilização e prestação de contas.

Na seção 7, discorre-se sobre o tratamento de dados pessoais, e considera as operações de tratamento distribuídas conforme o ciclo de vida dos dados pessoais, apresentados no Guia de Boas Práticas para implementação na Administração Pública Federal. As operações de tratamento de dados pessoais estão previstas no artigo 5º, inciso X, da LGPD.

São apresentadas na seção 8, as bases legais utilizadas como hipóteses de tratamento são apresentadas conforme artigo 7º, incisos I a X, artigo 11, incisos I e II, e artigo 23 da LGPD. Também ficam definidas as bases legais utilizadas como hipóteses de tratamento no âmbito do Ibict, considerando as relacionadas às atividades fins, sem desconsiderar o uso das demais, se necessário.

Propriedade, proteção e classificação de informações no ibict, são apresentados na seção 9, observando previsão legal de normativas que envolvem propriedade intelectual e acesso à informação, processo administrativo, dentre outras.

Na seção 10, apresenta-se um panorama sobre tratamento de dados pessoais para estudos e pesquisas, tendo como base o Guia Orientativo "Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas" da Agência Nacional de Proteção de Dados Pessoais.

Na seção 11, são apresentadas as boas práticas do dia-a-dia, abrangendo explicações sobre conceitos e definições, engenharia social, e boas práticas referentes à segurança da informação e em Privacidade e Proteção de Dados Pessoais nas Atividades de Pesquisa do Ibict. Em relação à segurança da informação, aspectos que envolvem correio eletrônico, instalação de *software*, Backup, proteção à *software* malicioso, navegação na internet, proteção de senhas, dispositivos móveis, e principais pontos em segurança da informação. Em relação à Privacidade e Proteção de Dados Pessoais, são detalhados aspectos relevantes no contexto da anonimização, identificação e alteração de projetos, princípios, políticas internas, incidente de segurança, dados sensíveis, de crianças e adolescentes, responsabilidades, auditoria e conformidade, propriedade intelectual.

São apresentadas as responsabilizações na seção 12, indicações de acesso a conceitos gerais na seção 13, orientações sobre acesso à central de dúvidas na seção 14 e possíveis atualizações nos casos de alterações legislativas ou orientações da ANPD.

Este guia proporciona ao leitor uma apreciação detalhada sobre as práticas institucionais voltadas à Privacidade e proteção de dados pessoais, e as influências recebidas de diversas fontes de informação oficiais. É um Guia que poderá servir de base a acadêmicos e estudiosos, titulares de dados, pesquisadores e outros órgãos que lidam direta ou indiretamente com o tema.

Os autores

PREFÁCIO

Proteger dados pessoais não é um capricho normativo ou uma simples burocracia da era digital, nem um obstáculo à inovação ou à transparência. É, antes de tudo, uma resposta jurídica e institucional a uma transformação profunda da sociedade contemporânea, marcada pela centralidade da informação — e, em especial, dos dados pessoais — como ativo econômico, político e social. Em um contexto no qual grande tratamentos de dados são capazes de gerar cada vez mais valor econômico, a ausência de regras claras e de práticas responsáveis desloca silenciosamente a balança de poder, fragilizando indivíduos e arriscando comprometer a própria democracia.

A transformação digital ampliou de forma inédita a capacidade de coleta, correlação e análise de dados. Não se trata apenas de volume ou velocidade, mas da possibilidade de inferir comportamentos, antecipar decisões e construir perfis detalhados, muitas vezes sem que o titular sequer perceba. Nesse cenário, já não existem "dados intrinsecamente inofensivos": o risco não está apenas na natureza isolada da informação, mas no contexto de uso, na agregação massiva e na opacidade dos processos decisórios que se constroem a partir dela.

É justamente por isso que a proteção de dados pessoais se afirma como um direito fundamental autônomo, distinto da privacidade, embora com ela dialogue. Enquanto a privacidade se relaciona ao espaço de liberdade individual necessário ao livre desenvolvimento da personalidade, a proteção de dados incide sobre a identificabilidade, sobre o controle, a transparência e a responsabilização nos processos de tratamento de informações que dizem respeito às pessoas naturais. Trata-se de assegurar que o indivíduo não seja reduzido a um objeto de análise, categorização ou predição, mas reconhecido como titular de direitos em uma economia movida a dados.

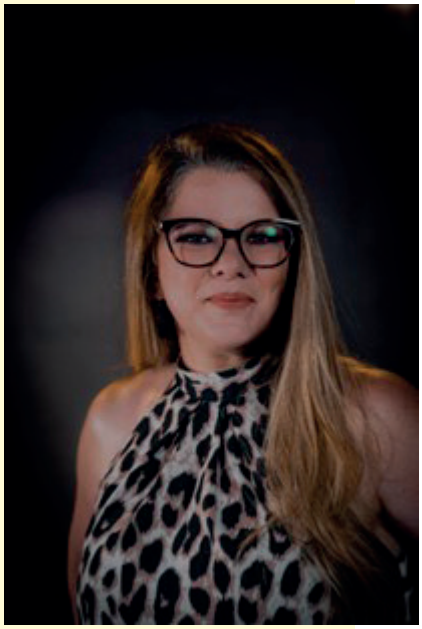
No setor público, essa discussão assume contornos ainda mais complexos. O Estado trata dados pessoais de forma intensa e legítima para formular políticas públicas, prestar serviços e garantir direitos fundamentais. Ao mesmo tempo, carrega um dever qualificado de proteção, decorrente da dimensão objetiva do direito fundamental à proteção de dados pessoais, que exige estruturas institucionais aptas a garantir efetivamente a concretização do direito fundamental, processos e procedimentos, critérios de proporcionalidade e mecanismos de accountability. Transparência e proteção de dados - ou, ainda, os direito fundamentais de acesso à informação e de proteção de dados pessoais - não são, nesse sentido, antagônicos: precisam ser harmonizados no caso concreto, à luz da Constituição.

É nesse ponto que este Guia de Boas Práticas de Privacidade e Proteção de Dados Pessoais, elaborado no âmbito do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), revela sua relevância. A obra vai além da exposição abstrata da Lei Geral de Proteção de Dados Pessoais e enfrenta o desafio prático de traduzir princípios em condutas institucionais, dialogando com o regime do acesso à infor-

mação, com a segurança da informação e com as rotinas reais da Administração Pública e da pesquisa científica. Ao fazê-lo, reconhece que a conformidade não se constrói apenas com normas, mas com cultura organizacional, capacitação contínua e escolhas responsáveis no cotidiano.

O Guia acerta ao destacar que proteger dados pessoais não significa paralisar a ação estatal, nem inviabilizar a produção e o compartilhamento de conhecimento. Significa, ao contrário, qualificar essas atividades, estabelecendo limites, finalidades claras, medidas de segurança e transparência suficiente para preservar a confiança social. Em tempos de decisões automatizadas, perfilização e intensificação da vigilância informacional, esse cuidado não é apenas jurídico: é ético, político e democrático.

Prefaciar esta obra é, portanto, reconhecer um esforço consistente de amadurecimento institucional e de compromisso com uma Administração Pública que compreende a proteção de dados como parte essencial da cidadania no século XXI. Que este Guia sirva não apenas como referência técnica, mas como convite permanente à reflexão crítica sobre o uso responsável da informação — sempre com a pessoa no centro da proteção.



Danielly Gontijo. Doutora em Direito Constitucional pela Faculdade de Direito da Universidade do Porto. Procuradora Federal. Corregedora da Procuradoria-Geral Federal. Professora IBMEC.

1 INTRODUÇÃO

A Lei Geral de Dados Pessoais surge da necessidade de proteger direitos fundamentais dos titulares de dados pessoais em face do uso crescente advindo pelos avanços das Tecnologias de Informação e Comunicação e pelo processo de globalização, que passam a exigir confiança no ambiente digital, ecossistema de economia de dados, Capacidade técnica e humana relativa ao uso e tratamento de volumes consideráveis de dados e Ambiente jurídico-regulatório que incentive o investimento e a inovação (Pinheiro, 2026; Vainzof, 2022).

Nesse contexto, a LGPD nasce como uma lei geral, de caráter principiológico que dialoga com outras leis setoriais que regulamentam aspectos específicos, podendo ser citadas, dentre elas:

- Código de Defesa do Consumidor (CDC - Lei nº 8.078/1990);
- Lei de Acesso à Informação (LAI - Lei nº 12.527/2011);
- Marco Civil da Internet (MCI - Lei nº 12.965, de 23 de abril de 2014);
- Lei do Cadastro Positivo (Lei nº 12.414, de 09 de junho de 2011);
- Lei do Prontuário Eletrônico (Lei nº 13.787/2018);
- Lei Orgânica da Saúde (Lei nº 8.080, de 19 de setembro de 1990);
- Resolução CNS nº 466/2012 e Resolução CNS nº 510/2016;
- Estatuto da Criança e do Adolescente (ECA - Lei nº 8.069/1990);
- Habeas Data (Lei nº 9.507, de 12 de novembro de 1997).

A multiplicidade de leis torna-se o desafio constante do operador do direito. O diálogo das fontes constitui uma abordagem fundamental para o estabelecimento da compatibilidade entre diferentes normas jurídicas, especialmente em contextos marcados pela complexidade regulatória e pela multiplicidade de regimes jurídicos.

A harmonização das leis que tratam do tema de proteção de dados considera-se essencial. Esta abordagem propõe uma leitura sistemática e cooperativa do ordenamento jurídico, buscando a harmonização e a complementaridade entre normas, como ocorre com a LGPD e a LAI no contexto do Poder Público.

O diálogo das fontes permite que diplomas legais distintos sejam aplicados de forma integrada, favorecendo soluções normativas mais adequadas à realidade social e institucional, ao reconhecer que diferentes normas podem coexistir e incidir simultaneamente sobre uma mesma situação jurídica.

Nesse contexto, esse Guia tem por objetivo definir boas práticas visando alinhar a atuação de todos os membros das unidades do Ibict aos padrões de adequação à proteção de dados pessoais considerando a LGPD - Lei nº 13.709, de 14 de agosto de 2018.

O Guia de Boas Práticas de Privacidade e Proteção de Dados Pessoais do Ibict tem como escopo cumprir a LGPD, que regulamenta o tratamento de dados pessoais, devendo ser observado por todos os servidores, terceirizados e colaboradores que atuem em nome do Ibict, que tenham acesso à dados pessoais. Também abrange parceiros e fornecedores que realizam o tratamento de dados pessoais em nome do Ibict, devendo seguir as diretrizes aqui estabelecidas. Além da LGPD, deve considerar a observância de outras normativas nacionais e internacionais que dialogam com a proteção de dados pessoais, tais como Constituição Federal, Nomas ISSO/IEC da família 27000, Regulamentações e Guias Orientativos da ANPD.

Este documento toma como base o Guia do *Framework* de Privacidade e Segurança da Informação, observando variadas publicações, orientações e documentos técnicos existentes, utilizados de forma abrangente por profissionais da área de privacidade e segurança da informação.

O Guia de Boas Práticas de Privacidade e Proteção de Dados Pessoais do Ibict auxilia na adoção de medidas vinculadas ao Controle 21 do *Framework*, contribuindo para a governança em privacidade e proteção de dados pessoais.

Como canais de comunicação, para esclarecer dúvidas, relatar incidentes ou obter informações sobre a proteção de dados pessoais no Ibict, estão disponíveis os seguintes canais de comunicação:

- E-mail da encarregada: silvanavidotti@ibict.br
- Link: https://www.gov.br/ibict/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-1
- Plataforma Fala.Br: https://www.gov.br/pt-br/servicos/abrir-requerimento-relacionado-a-lgpd

A Recomendação segue no sentido de que todas as interações relacionadas à privacidade e proteção de dados sejam formalizadas por meio dos canais oficiais indicados, para garantia de rastreabilidade e adequada resolução das solicitações. Inicialmente o pedido deve ser direcionado ao controlador por meio do encarregado de dados. Caso a solicitação não seja atendida ou atendida de forma insatisfatória, a comunicação deverá ser direcionada à ANPD por meio de uma Petição de Titular.

2 POR QUE COMPREENDER QUE A LGPD É ESSENCIAL PARA A GOVERNANÇA DE DADOS E CONFORMIDADE?

O termo Governança de dados surge de um contexto maior de governança corporativa e a partir do advento dos bancos de dados (1970), impõe maior controle formal desses ativos. Segundo Barbieri (2020, p. 33), objetivava a definição controlada de modelos integrados, regras de utilização, criação de dicionário de dados, em que cada elemento pudesse ter uma definição corporativa única, com maior riqueza nos metadados (definição dos dados), além de critérios para uso e aplicações de padrões de segurança. Ainda de acordo com o referido autor:

> [...] compreende-se por governança de dados um conceito em evolução, que envolve o cruzamento de diversas disciplinas, com foco central em qualidade de dados no sentido mais amplo deste conceito. Passa por busca de maturidade da empresa na gerência desses recursos, melhoria na valoração e produção dos dados, monitoração de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de compliance, associadas a eles. Para tal, as empresas deverão definir objetivos organizacionais e processos institucionalizados, que serão implementados dentro do equilíbrio fundamental entre TI e áreas de negócios, entendendo que os dados não são mais do domínio de tecnologia e sim um ativo organizacional (Barbieri, 2020, p. 33).

Da mesma forma, a governança de dados pessoais se trata de um conceito que deriva do campo mais amplo da governança de dados, entendida como um conjunto de diretrizes, processos, procedimentos e métricas que garantem que operações com dados pessoais ocorram com qualidade, integridade, legalidade, transparência, finalidade legítima, segurança e accountability, ao longo de seu ciclo de vida (coleta, retenção, processamento, compartilhamento e eliminação), alinhando-os aos objetivos estratégicos e de conformidade institucional.

Segundo o Grupo de Trabalho nº 04 (GT-4) do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), ao tratar de Governança de Dados no Setor Público, a "[...] governança de dados no Brasil é sustentada por um arcabouço legal robusto, incluindo a LGPD, que regula o tratamento de dados pessoais e promove a transparência e a privacidade" (Brasil, 2025a, p.7). Da mesma forma, menciona o Decreto nº 10.046/2019, que institui o Cadastro Base do Cidadão e estabelece diretrizes para o compartilhamento de dados no âmbito federal, e ainda menciona como arcabouço, outros instrumentos normativos, como a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011)

(Brasil, 2011) e a Lei do Governo Digital (Lei nº 14.129, de 29 de março de 2021) (Brasil, 2021) , que dispõe sobre o Governo Digital, de forma a criar os alicerces para uma governança que priorize a eficiência e a transparência, sempre com a observância dos preceitos de proteção fixados na LGPD.

A LGPD fornece a base normativa para o tratamento de dados pessoais, garantindo que as organizações atuem em conformidade com a lei e evitem sanções administrativas. Além disso, compreender a LGPD permite implementar estratégias eficazes de governança de dados, alinhando-se às exigências legais e favorecendo a gestão eficiente e segura das informações no ambiente organizacional.

O Governo Federal, por meio do Ministério da Gestão e Inovação em Serviços Públicos (MGI), instituiu o Programa de Privacidade e Segurança da Informação (PPSI), criado pela Portaria SGD/MGI Nº 852, de 28 de março de 2023, que regulamenta o Programa de Privacidade (PPSI) para implementação no âmbito dos órgãos e entidades do governo federal, e além disso, a Portaria institui o *Framework* de Privacidade e Segurança da Informação para apoio aos órgãos públicos, propondo "diretrizes para auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de privacidade e segurança da informação existentes" (Brasil, 2025a, p. 8-9).

Para conformidade e governança de dados pessoais do Ibict, devemos observar um conjunto de normativas para subsidiar as atividades desenvolvidas no âmbito do Instituto, considerando a Constituição Federal de 1988, a Lei Geral de Proteção de Dados Pessoais, a Lei de Acesso à Informação, Marco Civil da Internet, a Lei de Governo Digital, as Resoluções e Guias Orientativos da ANPD, além de normas internacionais sobre dados pessoais e Segurança da Informação.

3 O QUE SE COMPREENDE POR DADOS E INFORMAÇÃO

O Dado se diferencia da informação de forma que dado constitui fatos registrados, e que têm um significado implícito, sobre os acontecimentos. O Quadro 1 apresenta as principais diferenças entre dados e informações.

Quadro 1 - principais diferenças entre dados e informações

Dados	Informação
Registro	Significado atribuído ao dado
Representados por sinais não processados	Dados interpretado
Fatos ou descrições de coisas, eventos e atividades	Diferentes contextos
Não apresenta sentido isoladamente	Necessidade do usuário
Matéria-prima (fonte) de informação	Mutabilidade e flexibilidade

Fonte: Le Coadic (1996), Turban; Rainer Júnior; Potter (2003) e Belkin e Robertson (1976).

Segundo Setzer, (2015, on-line), o dado se trata de uma:

> [...] seqüência de símbolos quantificados ou quantificáveis. Quantificável significa que algo pode ser quantificado e depois reproduzido sem que se perceba a diferença para com o original. Portanto, um texto é um dado. [...] Também são dados fotos, figuras, sons gravados e animação, pois todos podem ser quantificados ao serem introduzidos em um computador, a ponto de se ter eventualmente dificuldade de distinguir a sua reprodução com o original (Setzer, 2015, on-line).

Segundo exposto por Oliveira e Sousa (2020), os conceitos que envolvem dados e informações apresentam caráter polissêmico exigindo-se uma compreensão sobre suas particularidades. As referidas autoras apresentam uma discussão sobre essas distinções, a partir de uma revisão de literatura com autores utilizados na Ciência da informação, compreendendo essa área como o estudo das propriedades e comportamento da informação, a partir de Borko.

Le Coadic (1996), compreende o dado como uma forma de representação composta de informação codificada, que permite dispô-las sobre o processamento eletrônico. Para Turban; Rainer Júnior; Pot-

ter (2003), os dados constituem descrições de coisas, eventos e atividades que, isoladamente, não se articulam nem são capazes de produzir significado. Davenport (1998), apresenta o dado como matéria prima da informação, pois o dado fornece subsídios para seu tratamento, transmissão e uso.

Já a informação, trata-se de um significado associado ou deduzido de um conjunto de dados e de associações entre eles. O mesmo dado pode fornecer informações diferentes para objetivos distintos.

Segundo Capurro (2003), não existe uma definição única sobre informação, contudo, o autor destaca elementos essenciais para sua compreensão, tais como a centralidade da interpretação, a necessidade de contextualização para que essa interpretação seja possível e a adoção de uma abordagem interdisciplinar para o entendimento do conceito.

A noção fundamental de informação, comum às diferentes perspectivas, relaciona-se à capacidade de promover uma mudança intencional na estrutura cognitiva do indivíduo. Nessa linha, Machlup e Mansfield (1983) compreendem a informação como um fenômeno que envolve sujeitos que transmitem e recebem mensagens no contexto de suas ações e possibilidades de atuação.

Ao revisarem o conceito de informação, Capurro e Hjørland (2007) enfatizam que informação pode ser considerada como aquilo que se mostra informativo para um determinado indivíduo, sendo essa condição dependente de suas necessidades interpretativas e de suas competências cognitivas. Em convergência, Belkin e Robertson (1976, p. 198) definem a informação como algo capaz de modificar uma estrutura, ressaltando que sua transferência somente se concretiza quando há efetiva comunicação.

Buckland (1991, p. 352), por sua vez, propõe uma tipologia que distingue a informação em três dimensões: informação como processo, relacionada às transformações decorrentes do ato de informar; informação como conhecimento, associada ao conteúdo cognitivo comunicado; e informação como coisa, que abrange tudo aquilo que pode ser considerado informativo — como dados, documentos e objetos — constituindo a materialização da informação para fins de compreensão e uso.

4 O QUE DIFERENCIA A PRIVACIDADE DE DADOS PESSOAIS?

A origem da **privacidade** está ligada ao final do século XIX, a vida privada representava uma projeção do direito de propriedade "[..] proteger a propriedade em primeiro plano, significava, também, preservar as relações privadas nelas construídas, ainda que indiretamente" (Marineli, 2019, p. 85).

Segundo Doneda (2019, p. 30), o direito à privacidade tornou-se evidente justamente num período de mudança de percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos de sua vida.

A moderna doutrina do direito à privacidade originou-se a partir do ensaio elaborado pelos norte-americanos Samuel Warren e Louis Dembitz Brandeis, intitulado *The right to privacy*, publicado na *Harvard Law Review*, como "direito a ser deixado em paz". Segundo Marinelli (2019, p. 90), esse ensaio surgiu como referência jurídica doutrinária sobre o tema da privacidade, seja pelo pioneirismo no tratamento acadêmico da matéria ou pela influência exercida sobre sistemas jurídicos.

Segundo Rodotà (2008, p. 92), as discussões teóricas e as intrincadas experiências dos últimos anos demonstram que a privacidade se apresenta como noção fortemente dinâmica com uma estreita e constante relação entre as transformações determinadas pelas tecnologias da informação e as mudanças em seu conceito. A partir de então, embora as raízes de seu reconhecimento se mantenham, a privacidade assume diversos significados, dependendo, desta forma, do objetivo almejado pela coleta de informações.

Não há unanimidade quanto ao conceito de privacidade. Segundo Marineli (2019, p. 121), em uma visão civil-constitucional do direito à privacidade, o ordenamento jurídico reconhece a existência de dois direitos distintos: o direito à vida privada e o direito à intimidade.

Moraes (2003, p. 224) defende a existência de dois direitos, quais sejam, a vida privada e a intimidade. Estes estão interligados, porém o segundo apresenta menor amplitude e se encontra no âmbito de incidência do primeiro. Para o referido autor, a intimidade compreende as relações subjetivas e de trato íntimo da pessoa humana, suas relações familiares e de amizade. Já a vida privada envolve os relacionamentos da pessoa, tais como relações comerciais, de trabalho, dentre outras.

Segundo Rodotà (2008, p. 92), na atualidade, "[...] tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo de informações a ele relacionadas". Para o referido autor, a definição

de privacidade, em uma primeira aproximação, pode ser definida como o direito de manter o controle sobre as próprias informações.

Para Rodotà (2008), a nova perspectiva de privacidade, permite uma mudança de paradigma que segundo Rodotà (2008), parte de uma visão sobre "**cidadão-informação-sigilo**", para uma visão que atribui relevância cada vez mais ampla e clara sobre o poder de controle, envolvendo "**cidadão-informação-circulação-controle**"**.** Segundo o referido autor, delineia-se duas tendências:

> **1ª)** a redefinição do conceito de privacidade que atribui relevância cada vez mais ampla e clara ao poder de controle;
>
> **2ª)** a ampliação do direito à privacidade decorrente da valorização da noção técnica da esfera privada, a qual compreende um número sempre crescente de situações juridicamente relevantes.

No que se refere aos **dados pessoais**, embora decorra do direito à privacidade, que possui raízes remotas[1], normalmente utiliza-se os termos "proteção de dados" e "privacidade" como sinônimos, que segundo Maldonado (2022, p. 12), "do ponto de vista técnico, representa imprecisão terminológica, haja vista que se referem a bens jurídicos distintos". Corroborando com Rodotà (2008), entende o conceito de privacidade como um conceito aberto e subjetivo que pode variar em função de uma multiplicidade de situações juridicamente relevantes.

Enquanto a proteção de dados pessoais, segundo Maldonado (2022, p. 12), está relacionada a um evento concreto e específico, a saber, **a existência do tratamento de dados pessoais**, conforme definido no artigo 5º, inciso X da LGPD, compreendida como toda operação realizada com dados pessoais, como as relacionadas ao ciclo de vida dos referidos dados.

A Emenda Constitucional nº 115, de 10 de fevereiro de 2022 (Brasil, 2022), veio fortalecer o entendimento, com o reconhecimento da proteção de dados pessoais como direito fundamental, previsto no artigo 5º, inciso LXXIX, ao assegurar, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

1 Retrocedendo-se ao período da Grécia antiga, chega-se à concepção de privacidade idealizada por Aristóteles (384-322 AC), que formulou a distinção entre a esfera pública e a esfera doméstica, assim denominadas, respectivamente, polis e oikos, essa última atribuível ao que se pode chamar de reino da vida privada (Maldonado, 2022b, p. 13-14).

5 O QUE SÃO DADOS PESSOAIS?

No Brasil adotou-se o conceito expansionista de dado pessoal, pelo qual informações relativas à pessoa diretamente identificada estão protegidas pela lei, assim como, informações que tenha o potencial de tornar a pessoa identificável (Maldonado; Opice Blum, 2022, p. 94; Machado, 2023).

O componente da identidade de uma pessoa natural torna-se imprescindível para característica fundamental do dado pessoal. Isso significa resguardar a própria personalidade do ser humano, pois esta constitui conjunto de características que distinguem uma pessoa (Maldonado; Opice Blum, 2022, p. 95).

De acordo com a LGPD, artigo 5º, I, considera-se dados pessoais toda informação relacionada a pessoa natural identificada ou identificável (*nome completo, CPF, RG, número de celular, título de eleitor, carteira de trabalho, carteira de motorista*). O Quadro 2 elenca exemplos de dados pessoais identificados e dados pessoais identificáveis:

Quadro 2 - Tipos de dados pessoais identificados e identificáveis

Dados que tornam a pessoa Identificada	Nome, telefone, endereço, e-mail, idade, endereço residencial ou eletrônico
Dados que tornam a pessoa Identificável	Dados que, em conjunto, podem identificar alguém, com exemplos: Dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, avaliações, notas, etc.

Fonte: Elaborado pelos autores (2026).

Dado sensível, refere-se à dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico.

Importante elucidar que a LGPD não apresenta como objeto de proteção outros tipos de dados que não estejam relacionados à pessoa natural. Numa visão sistematizada, o Quadro 3 apresenta os tipos de dados **não** protegidos pela LGPD:

Quadro 3 - Tipos de dados não protegidos pela LGPD

Tipo de dado / situação	Descrição	Fundamento Legal (LGPD)	Observações
Dados Anonimizados	Perde a característica de ser pessoal. O processo de anonimização não pode ser revertido por utilização de meios próprios e razoáveis	Arts. 5º, III, e 12	Se houver possibilidade de reversão, a LGPD voltará a incidir
Dados de Pessoas Jurídicas	Dados corporativos ou entes coletivos	Arts. 1º e 5º, I	Pode haver proteção indireta se envolver dados de sócios ou representantes
Uso Pessoal e Não Econômico	Dados tratados em contexto estritamente privado, isto é, fins exclusivamente particulares e não econômicos	Art. 4º, I	Não se aplica a atividades com finalidade econômica ou institucional
Finalidade Jornalística e Artística	Produção e Disseminação de informações e criação e expressão cultural	Art. 4º, II, "a" e Art. 4º, II, "b"	Respeitar direitos fundamentais, a exemplo, acesso à informação.
Acadêmica (aplicando-se os arts. 7º e 11 desta Lei)	Ensino, pesquisa e produção científica como atividade fim.	Art. 4º, II, "c"	Atividades meio que utilizam dados pessoais devem ser objeto de proteção da LGPD. Exemplo: dados de matrícula dos alunos, estágios, processos seletivos, registros de presença e notas de avaliação ou, ainda, do tratamento de dados pessoais de funcionários e de docentes pelo setor de recursos humanos dessas instituições (Brasil, 2023).
Segurança Pública e Defesa Nacional	Atividade de segurança, defesa e atividades de investigação e repressão de infrações penais	Art. 4º, III	Regulado por legislação específica.
Dados de Pessoas Falecidas	Informações relativas a pessoas naturais já falecidas	Interpretação do art. 5º, I	Nota Técnica nº 3/2023/ CGF/ANPD incidência se dá no âmbito do tratamento de dados pessoais de pessoas naturais, ou seja, vivas, já que, de acordo com o art. 6º do Código Civil, a existência da pessoa natural termina com a morte.

Fonte: Elaborado pelos autores (2026).

Diante disso, de acordo com a LGPD, pode-se afirmar que os dados pessoais podem ser classificados como dados pessoais diretos (identifica de forma direta o titular de dados), dados pessoais indiretos (necessita de informação adicional para identificação do titular), dados pseudonimizados (perde a possibilidade de associação direta ou indireta ao titular, senão pelo uso de informação adicional mantida separada pelo controlador) e anonimizada (após anonimização não se considera dados pessoais). Para pseudonimização torna-se necessário o uso de algumas técnicas, a exemplo da criptografia com chave secreta, função hash e codificada com chave armazenada e tokenização.

6 QUAIS OS FUNDAMENTOS E PRINCÍPIOS DA LGPD?

Pinheiro (2026, p. 113), os **fundamentos da LGPD** se relacionam ao texto constitucional brasileiro no que se refere ao conteúdo, haja vista que a Constituição Federal pauta-se na proteção aos direitos fundamentais. A referida autora destaca os seguintes artigos da Constituição Federal:

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:
>
> I - construir uma sociedade livre, justa e solidária;
>
> II - garantir o desenvolvimento nacional;
>
> Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:
>
> [...]
>
> II - prevalência dos direitos humanos;
>
> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> [...]
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
>
> [...]

> Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social:
>
> [...]
>
> XXVII - proteção em face da automação, na forma da lei;
>
> [...]
>
> Art. 219. O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e sócio-econômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal (Brasil, 1988, on-line).

Conforme a previsão do artigo 2º da LGPD, a disciplina da proteção de dados pessoais tem como fundamentos:

Respeito à Privacidade: visto como um direito do indivíduo e sua proteção pode ser vista como elemento indissociável da pessoa humana. As discussões sobre privacidade já foram mencionadas na seção 5.

A Autodeterminação Informativa: trata-se do direito do titular de dados de decidir de forma livre e consciente sobre o que terceiros podem fazer com o fluxo e uso de seus dados pessoais. Esse fundamento tem sua origem na Corte Alemã ao julgar parcialmente constitucional uma lei sobre censo demográfico, em face da coleta excessiva de dados, reconhecendo que o titular pode ter sua liberdade restringida.

Liberdade de Expressão, de informação, de comunicação e opinião: a LGPD deve coexistir harmonicamente com as liberdades fundamentais dialogando com a privacidade, assim como internacionalmente, com os direitos humanos, visando garantir que a inobservância desses direitos, em face do tratamento dos dados pessoais, possa ser considerado ilícito (Maldonado; Opice Blum 2022, p. 34), promovendo um equilíbrio entre a tutela da privacidade e a garantia do livre fluxo informacional em uma sociedade democrática.

A Inviolabilidade da intimidade, da honra e imagem: reafirma a proteção da dignidade da pessoa humana em face do uso abusivo de dados pessoais. A apropriação sistemática de dados pessoais para fins de previsão, modulação e monetização das condutas humanas, centra a LGPD como resposta jurídica buscando reequilibrar assimetrias de poder informacional frente à exploração econômica da vida privada.

O desenvolvimento econômico e tecnológico e a inovação: a lei busca criar um ambiente de segurança jurídica que incentive a inovação, a competitividade e o uso ético de tecnologias emergentes. As ações governamentais devem focar na proteção à privacidade e proteção de dados pessoais e defesa

do ambiente digital, visando melhores práticas como Estratégia Nacional de Segurança Cibernética, garantia de atuação independente da ANPD, dentre outras. O uso responsável de dados pessoais se trata de elemento estratégico para o progresso econômico e científico.

A livre iniciativa, livre concorrência e defesa do consumidor: estabelece regras claras e uniformes para o tratamento de dados pessoais no mercado, e ao mesmo tempo, reforça a defesa do consumidor, evitando práticas abusivas, assimetrias informacionais e uso indevido de dados como vantagem competitiva ilícita, contribuindo para relações econômicas mais justas e transparentes.

Os Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais: esse fundamento confere à proteção de dados uma dimensão ética e social, vinculando-a à construção de uma sociedade democrática, inclusiva e orientada à valorização da pessoa humana.

Quanto aos **princípios**, a LGPD trata-se de uma norma principiológica, de forma que, segundo Pinheiro (2026, p. 123), "A garantia da proteção dos direitos dos titulares dos dados pessoais é pautada na indicação de princípios relativos ao tratamento de dados pessoais, cuja ação deve respeitar os limites dos direitos fundamentais".

Conhecer os **princípios** que regem uma norma significa conhecer sua essência. Os princípios são os valores que devem reger a interpretação e aplicação da lei. A LGPD em seu artigo 6º, determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios, conforme apresentados no Quadro 4:

Quadro 4 - Princípios da LGPD

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: Brasil (2018, on-line).

A LGPD trata-se de uma norma principiológica, de forma que os princípios devem ser considerados em toda operação de tratamento que envolva dados pessoais.

7 O QUE PODE SER COMPREENDIDO POR TRATAMENTO DE DADOS PESSOAIS?

O conceito de tratamento de dados está previsto no artigo 5º, X da LGPD. A LGPD considera como tratamento de dados "**toda operação realizada com dados pessoais**" (Brasil, 2018), 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.

A LGPD estabelece o chamado *ciclo de vida do dado pessoal*, ou seja, *toda operação* realizada desde a coleta até a exclusão do dado é considerada como tratamento de dados.

Conforme exposto no Guia de Boas Práticas para Implementação na Administração Pública Federal (Brasil, 2020, p. 45), a Figura 1 sintetiza as fases do ciclo de vida dos dados pessoais:

Figura 1 – Ciclo de Vida do Tratamento dos Dados Pessoais

Fonte: Brasil (2020, p. 45).

Segundo exposto em Brasil (2020, p. 45), a Tabela 2 estabelece as fases do ciclo de vida dos dados e a relação existente entre as operações de tratamento de dados pessoais previstos no artigo 5º, inciso X, da LGPD:

Tabela 2 – Fases do Ciclo de Vida e a Relação com operações de dados pessoais

Coleta	Coleta, produção, recepção.
Retenção	Arquivamento e armazenamento.
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.

Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação.

Fonte: Adaptado de Brasil (2020, p. 45).

Ainda segundo exposto em Brasil (2020, p. 45), "[...] A operação de tratamento "acesso" (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação".

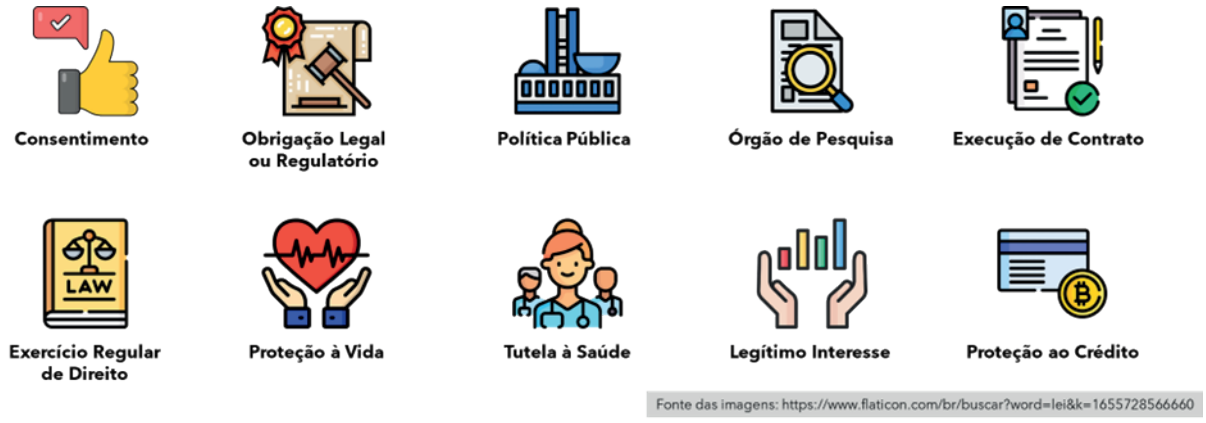
Essa definição torna-se relevante para entender até onde a proteção da LGPD se estende e em quais momentos deve-se proteger os dados pessoais. Assim, a operação de *acessar* dados pessoais passa a ser considerada tratamento pela lei.

8 QUAIS AS BASES LEGAIS UTILIZADAS NO TRATAMENTO DE DADOS NO IBICT?

A LGPD surgiu para regular o uso indiscriminado dos dados pessoais visando evitar transtornos ao titular. Portanto, para estabelecer conformidade ao uso dos dados e responsabilizar aqueles que não zelam pelos dados de seus parceiros, servidores, co-participantes, dentre outros,a Lei apresentou *bases legais* para o tratamento dos dados, ou seja, determinou em quais casos os dados podem ser tratados.

A LGPD apresenta em seu artigo 7°, incisos I a X, as hipóteses de tratamento de dados pessoais. Trata-se de um rol taxativo, em que as operações de tratamento deve observar. Na Figura 2, apresenta-se as hipóteses legais de tratamento da LGPD:

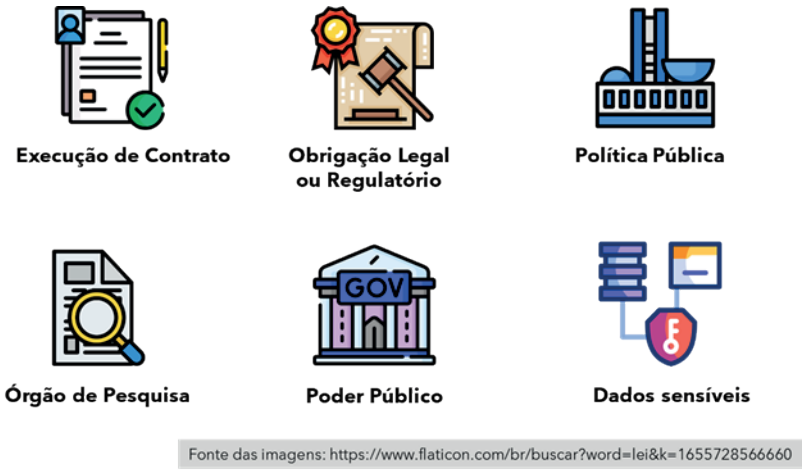
Figura 2 - Hipóteses Legais de Tratamento (artigo 7°, incisos I a X da LGPD)



Fonte: Elaborado pelos autores (2026).

Torna-se relevante entender que a LGPD não veio proibir o uso e o tratamento de dados, mas estabelecer o fluxo correto para a proteção dos titulares de dados pessoais. Nesse sentido, as bases legais utilizadas no tratamento de dados pessoais no âmbito do Ibict, a depender da finalidade, são apresentadas conforme a Figura 3:

Figura 3 - Hipóteses Legais de Tratamento que podem ser adotadas pelo Ibict



Fonte: Elaborado pelos autores (2026).

Execução ou preparação contratual: refere-se à hipótese em que o tratamento dos dados pessoais torna-se indispensável ao procedimento que antecede a formalização de instrumento jurídico contratual, assim como à própria execução das obrigações acordadas contratualmente entre o Ibict e operadores de dados pessoais.

Cumprimento de obrigação legal ou regulatória Conforme o art. 7º, II, da LGPD, o tratamento de dados pessoais pelo Poder Público poderá ser realizado "para o cumprimento de obrigação legal ou regulatória pelo controlador". A mesma hipótese está prevista no art. 11, II, a, que rege o tratamento de dados sensíveis.

Segundo a ANPD, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, quais sejam, das normas de conduta (regra que disciplina um comportamento, em geral estabelecendo um fato ou uma hipótese legal) e das normas de organização (o tratamento constitui parte essencial do exercício de prerrogativas estatais típicas). Nesse caso, a base legal pode ser utilizada visando atender a uma regra específica (uma determinação legal expressa ou uma obrigação de natureza regulatória estabelecida por um órgão regulador) (Brasil, 2023, p. 15).

Execução de Políticas Públicas: Previsto no inciso III, do artigo 7º, e em relação aos dados sensíveis, o art. 11, II, b, segundo a ANPD (2023, p. 18-19), a "[...] aplicação dessa base legal por entidades e órgãos públicos pressupõe a adequada compreensão sobre os principais termos utilizados", quais sejam, Administração Pública (órgãos e entidades do Poder Executivo dos Poderes Legislativo e Judiciário, inclusive das Cortes de Contas e do Ministério Público, desde que a respectiva atuação ocorra no exercício de funções administrativas) e Políticas Públicas (deve-se observar dois requisitos, a saber: primeiro, a existência de ato formal que institui a política pública (pode ocorrer por meio de ato normativo – lei ou regulamento – ou por ajustes contratuais - contratos, convênios e instrumentos congêneres) (ANPD, 2023, p. 19).

Nesse sentido, a ANPD recomenda que a Política pública seja interpretada de forma ampla, com abrangência de programas ou ações governamentais; que tenha sido definido em instrumento formal (lei, regulamento ou ajuste contratual), e cujo conteúdo possa incluir, em regra, objetivos, metas, prazos e meios de execução.

Realização de Estudos por Órgãos de Pesquisa: conforme exposto no artigo 5º, inciso XVIII, conceitua "como instituição que inclui em sua missão institucional ou em seu objeto social ou estatutário a pesquisa básica aplicada de caráter histórico científico tecnológico ou estatístico" (Brasil, 2018). Nesse sentido, o Ibict poderá realizar pesquisas com dados pessoais utilizando-se como base legal o artigo 7º, inciso IV da LGPD, realizando preferencialmente anonimização dos dados pessoais. Assim como, poderá utilizar como base legal o artigo 11, inciso II, alínea "c", quando se tratar de dados sensíveis.

Tratamento de dados pelo Poder Público: Deve-se observar também, o artigo 23 da LGPD, em especial a exigência de que o tratamento seja realizado para o "atendimento da 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).

Dados sensíveis: Observando-se o artigo 5º, inciso II e artigo 11, incisos I e II, definido as hipóteses em que podem ser utilizadas hipóteses de tratamento, quando necessário.

9 PROPRIEDADE, PROTEÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

As informações produzidas pelo Ibict ou por ele adquiridas, são consideradas de sua propriedade, sendo parte de seu patrimônio, independente da sua forma de representação ou armazenamento. Com a ressalva do que o próprio órgão define como informações de acesso aberto, considerando sigilo e restrições legais.

As informações institucionais devem ser utilizadas exclusivamente para fins relacionados diretamente às atividades fins e meio do Ibict.

Quanto à classificação da informação, como controle, *segundo a ISO/IEC 27001* (2023), a informação deve ser classificada considerando seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

- **Pública** - informação que pode ser divulgada a qualquer pessoa, seja externa ou internamente. Nesse caso, o acesso é aberto, salvo restrições previsto em lei ou contrato. Preferencial para dados e documentos públicos;

- **Restrita** - informações que podem ser divulgadas apenas a um grupo restrito de pessoas, sujeitas a controle de acesso. Nesse caso, acesso permitido apenas a grupos autorizados. O acesso ao objeto digital é limitado e/ou controlado a um grupo de pessoas. Ex: membros da instituição, pesquisadores.

- **Pessoais -** informações privadas relativas a pessoas físicas identificadas;

- **Sigilosas -** informações críticas para os processos da organização, onde perda ou dano pode causar impactos que demandam necessidade de mitigação dos riscos. Sem qualquer acesso digital permitido, geralmente por restrição legal de sigilo ou contratual.

O usuário tem a responsabilidade de garantir a segurança da informação sob sua responsabilidade. Não é permitido divulgar informações de acesso restrito, interna ou externamente, seja através de conversas formais, e-mails ou qualquer outro meio de comunicação, sem a prévia autorização do responsável.

10 TRATAMENTO DE DADOS PESSOAIS PARA REALIZAÇÃO DE ESTUDOS E PESQUISAS

A LGPD definiu regras específicas para o tratamento de dados pessoais para fins acadêmicos e realização de estudos e pesquisas. Essas regras têm por objetivo garantir que o tratamento dos dados pessoais seja realizado com segurança jurídica e respeito aos direitos dos titulares, sempre que associadas à produção e à disseminação do conhecimento.

A LGPD procurou estabelecer relações de equilíbrio, entre proteção de dados pessoais *versus* liberdade acadêmica; garantia de privacidade e autodeterminação informativa *versus* livre fluxo de informações, necessárias à realização de estudos e pesquisas nas mais diversas áreas do saber.

No artigo 5º, inciso XVIII da LGPD, conceitua-se órgãos de pesquisa "como instituição que inclui em sua missão institucional ou em seu objeto social ou estatutário a pesquisa básica aplicada de caráter histórico científico tecnológico ou estatístico" (Brasil, 2018).

Segundo exposto no Guia Orientativo sobre Tratamento de Dados Pessoais para Realização de Estudos e Pesquisas (ANPD, 2023), no caso de órgãos de pesquisa, apresenta regime jurídico especial e mais flexível com pontos de regime jurídico fixados em seis disposições na LGPD:

- Apresenta como fundamentos a Liberdade de expressão, de informação, de comunicação e de opinião (art. 2º, III) e desenvolvimento econômico, tecnológico e inovação (art. 2º, V). Observa-se também os artigos 206 e 218 da Constituição Federal (Brasil, 1988);

- A LGPD tem aplicação parcialmente afastada, para tratamento realizado para fins acadêmicos visando proteger a liberdade acadêmica e adequar-se às suas dinâmicas próprias. Essa exceção está prevista no artigo 4º, inciso II, alínea "b", sendo aplicáveis, ainda assim, as bases legais previstas nos artigos 7º e 11 da lei;

- A LGPD estabelece hipóteses específicas para o tratamento de dados para a realização de estudos por órgãos de pesquisa. Nesse caso, os agentes de tratamento **deverão garantir a anonimização** dos dados pessoais sempre que possível. O artigo 7º, inciso IV, estabelece que o tratamento de dados pessoais somente poderá ser realizado em estudos por órgãos de pesquisa e com a adoção de medidas de anonimização, sempre que viável (Brasil, 2018).

Em se tratando de dados sensíveis, o artigo 11, II, também estabelece que o tratamento de dados pessoais sensíveis somente poderá ocorrer sem o consentimento do titular quando esse tratamento for indispensável para a realização de estudos por órgãos de pesquisa, devendo também buscar, sempre que possível a anonimização dos dados pessoais sensíveis (Brasil, 2018).

Segundo exposto no Estudo Técnico sobre Anonimização de Dados na LGPD, emitido pela ANPD, a abordagem da anonimização deve ser compreendida como um processo contínuo baseado em risco. Cabe ao controlador definir, conforme o seu contexto, "[...] o compromisso entre ao grau de utilidade e o grau de anonimização que contemple a finalidade definida no tratamento e minimize o risco de reidentificação do titular" (ANPD, 2023).

A LGPD também reconhece a legitimidade do tratamento posterior de dados pessoais quando realizado para fins de investigação científica, histórica ou estatística, desde que esse novo tratamento seja compatível com a finalidade que justifica o tratamento original. Essa presunção não autoriza o uso irrestrito desses dados, sendo necessário avaliar o caso concreto, considerando aspectos como a natureza dos dados pessoais, expectativas legítimas dos titulares e seus impactos, os princípios da LGPD, medidas de prevenção e segurança, além de padrões éticos aplicáveis à hipótese.

- Identificada a necessidade de guarda dos dados pessoais para a realização de estudos e pesquisas, os órgão poderão conservar esses dados de forma legítima, considerando as normas arquivísticas aplicáveis, regras de classificação de documentos e tabela de temporalidade.

O pedido de eliminação dos dados por parte dos titulares pode ser negado pelo órgão de pesquisa se houver interesse público que justifique a manutenção dessas informações. Nesse caso, a negativa deve ser devidamente fundamentada, demonstrando a necessidade da guarda dos dados e que está diretamente relacionada à finalidade específica do estudo ou da pesquisa, conforme os artigos 15, inciso II, e 16, inciso II, da LGPD;

- A LGPD também trata da realização de estudos em saúde pública previstos no artigo 13 da LGPD. Este artigo autoriza o uso de dados pessoais para fins de realização de estudos específicos. Assim, esses estudos podem ser realizados desde que o tratamento ocorra exclusivamente dentro do próprio órgão responsável e apenas para atender à finalidade da pesquisa, sendo proibida a transferência desses dados a terceiros. Deve-se observar medidas de segurança e prevenção, conforme previsão do artigo 6º, incisos VII e VIII, como o uso de ambientes controlados e seguros, além da anonimização ou pseudonimização sempre que possível. Também devem ser observados os padrões éticos aplicáveis, sendo vedada a divulgação de informações pessoais nos resultados publicados das pesquisas (ANPD, 2023).

- Princípios de prevenção e segurança, são princípios básicos da LGPD aplicáveis a qualquer operação com dados pessoais. Para fins de estudos e pesquisas, independentemente da área do conhecimento, os agentes de tratamentos devem adotar medidas protetivas adequadas para

redução de risco, proteção da privacidade dos titulares, a confidencialidade das informações, sempre observados os padrões éticos aplicáveis. Deve-se observar o artigo 6º. inciso VII e VIII, bem como os artigos 46, §2º e artigo 47 da LGPD (ANPD, 2023).

11 BOAS PRÁTICAS DIÁRIAS EM SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Serão apresentadas as boas práticas em segurança da informação, seguida das boas práticas em privacidade e proteção de dados adotadas pelo Instituto Brasileiro de Informação em Ciência e Tecnologia.

11.1 Conceitos e Definições (ISO/IEC 27001 e 27002)

Alguns conceitos e definições são considerados relevantes ao considerar as Normas ISO/IEC 27001 (2023) e 27002 (2022):

Integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental (Resolução CD/ANPD nº 15, de 24 de abril de 2024) (ANPD, 2024). Está relacionada com a informação ter sido criada ou alterada apenas por quem tem dever e acesso a fazer essa operação.

Confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizadas (Resolução CD/ANPD nº 15, de 24 de abril de 2024). Refere-se a informação que deve estar disponível apenas para pessoas autorizadas a acessá-la.

Disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados (Resolução CD/ANPD nº 15, de 24 de abril de 2024). Trata-se do grau em que as informações estão disponíveis para quando a pessoa que tem o direito de acesso ou alteração poder realizar a operação.

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade (Resolução CD/ANPD nº 15, de 24 de abril de 2024).

Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização (ISO/IEC 27000:2020). São agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impactos aos negócios de uma organização.

Ataque: tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de, um ativo (ISO/IEC 27000:2020).

Risco: frequentemente expresso em termos de uma combinação das consequências de um evento (incluindo mudanças nas circunstâncias) e da "probabilidade" associada de ocorrência (ISO/IEC 27000:2020).

Risco ou dano relevante: quando afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios: dados pessoais sensíveis; dados de crianças, de adolescentes ou de idosos; dados financeiros; dados de autenticação em sistemas; dados protegidos por sigilo legal, judicial ou profissional; ou dados em larga escala (Resolução CD/ANPD nº 15, de 24 de abril de 2024). Combinação da probabilidade de um evento e sua consequência. Um efeito é um desvio do que é esperado, o qual pode ser positivo e/ou negativo.

Vulnerabilidades: fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças (ISO/IEC 27000:2020). Fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais pilares (confidencialidade, integridade, disponibilidade e autenticidade) da segurança da informação.

Incidente de segurança: Qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais (Resolução CD/ANPD nº 15, de 24 de abril de 2024).

Impacto: abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.

Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização (ISO/IEC 27000:2020).

Ameaças humanas: as ameaças humanas podem ser definidas como intencional, por exemplo um ataque hacker, um colaborador insatisfeito que deletar uma informação sigilosa do sistema. Temos também as ameaças humanas não intencionais, exemplo um colaborador deletar ou alterar uma informação no sistema por falta de conhecimento, inserir um pen drive contaminado em sua máquina, deletar um arquivo armazenado em uma pasta pública de rede e entre outros.

Ameaças não humanas: casos fortuitos (evento imprevisível ou inevitável, de ordem interna, ligada à própria atividade ou ao comportamento humano) ou força maior (evento imprevisível ou inevitável, de ordem externa alheio à vontade e controle humano). São ameaças como raios, incêndios, inundações, tempestades ou até mesmo terremotos. Grande parte dos dados dependerá da localização dos equipamentos nas instalações da organização.

11.2 Engenharia Social

A engenharia social, segundo Fontes (2006, p. 119), trata-se de "[...] conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade". Para Aramuni e Maia (2020, p. 31), o termo ficou conhecido em 1990, e "[...] designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las". Segundo os referidos autores, com a evolução do comércio eletrônico e sistemas rotineiros automatizados, a forma mais comum de ataque da engenharia social acontece na modalidade online, aumentando a preocupação quanto à privacidade. Ainda segundo Aramuni e Maia (2020, p. 32):

> A Engenharia Social é uma técnica antiga e muito popular, que poderia ser traduzida, grosso modo, como 'enganar pessoas'. A ideia é que o engenheiro social, como são conhecidos aqueles que praticam essa arte, possa manipular pessoas para que elas revelem informações importantes ou, então, para que elas façam algo que facilite o seu trabalho.

Trata-se de uma forma de obtenção de informações importantes por meio de conversa informal, aproveitando-se do desconhecimento das pessoas sobre boas práticas de proteção a dados, e explorando a sua confiança ou boa-fé.

A engenharia social pressupõe ações que podem ocorrer em contexto pessoal, para obter informações pessoais, ou em contexto profissional, para conseguir informações sobre sua instituição. Os tipos mais comuns de engenharia social são:

- *Phishing* direcionado a servidores (*spear-phishing*): e-mail aparentemente legítimo direcionado a um servidor/servidora pública pedindo atualização de cadastro ou abertura de link/arquivo:
  - » Normalmente visando acesso a credenciais de acesso, CPF, dados de usuários com atividades vinculadas à instituição;
  - » Deve-se observar: linguagem fora do padrão institucional, links com URLs estranhas, pedido urgente e fora de procedimento;

» Formas de Mitigação: autenticação multifator, filtragem de e-mail, treinamento contínuo e procedimentos formais para solicitações sensíveis, dentre outros implementados pelo setor específico de tecnologia.

- Golpe por telefone, fingindo ser chefe/fornecedor/órgão superior. Efetua ligação com tom de urgência pedindo "verificar documentos" ou "enviar lista de beneficiários".

» Normalmente visando dados cadastrais, listas de beneficiários, informações financeiras;

» Deve-se observar: pressão para agir sem checagem, pedido por canais não oficiais;

» Mitigação: políticas que proíbam atender solicitações sensíveis por telefone sem confirmação por canal autenticado; *scripts* de verificação.

- *Pretexting* com identidade falsa (ex.: auditor, controle interno, Tecnologia da Informação). O solicitante finge ser auditor/técnico e solicita acesso a sistemas ou arquivos "para auditoria/checagem":

» Normalmente visando: bases de dados, relatórios com dados pessoais;

» Deve-se observar: ausência de ordem formal, falta de comunicação prévia, pedidos de credenciais;

» Mitigação: exigir ordem de serviço/autorização formal, verificação prévia junto ao setor responsável.

- *Spear-phishing* a cidadãos para obter documentos e depois usar para comunicações com a instituição. O invasor convence um cidadão a enviar documentos (RG, CPF) e depois usa esses dados para solicitar serviços ou alterações à instituição:

» Normalmente visando acesso à documentos de identificação, comprovantes de residência;

» Deve-se observar: cidadão reporta contato estranho; documentos enviados de conta de e-mail não institucional;

» Mitigação: exigir autenticação forte para atendimento remoto; validar documentos presencialmente.

- Uso de redes sociais para coleta de informação prévia (reconhecimento) e depois abordagem personalizada. O atacante reúne informações públicas de servidores/gestores para construir pretexto convincentes (nomes de familiares, cargos):

» Normalmente visando dados pessoais relacionados a funcionários e cidadãos que facilitam fraudes;

» Deve-se observar: mensagens que citam informações pessoais que não deveriam ser públicas;

» Mitigação: políticas de privacidade e conscientização sobre exposição nas redes; limitar divulgação desnecessária.

- Solicitação por canais oficiais falsificados (sites ou portais clonados). Formulário online que imita portal público solicita *upload* de documentos:

» Normalmente visando documentos pessoais, senhas, números de processos;

» Deve-se observar: URL diferente, certificado ausente, formulário pede dados não usuais;

» Mitigação: certificação, comunicação pública sobre URLs oficiais, campanhas informativas.

- Comprometimento de conta de colaborador e uso dela para pedir dados a outros setores. Invasão de conta de e-mail interna, usada para solicitar dados a terceiros dentro da instituição:

» Normalmente visando listas de cidadãos, relatórios, dados sensíveis já armazenados;

» Dever de Observar: mensagens internas fora do padrão, pedidos incomuns vindos de colegas;

» Mitigação: detecção de sessão anômala, processos para confirmar pedidos sensíveis via múltiplos canais.

- Exploração de procedimentos burocráticos mal definidos (ex.: "atualização cadastral por telefone"). Falhas nos procedimentos permitem que um atacante, fingindo ser agente/servidor público, altere dados sem validação:

» Normalmente visando alteração de endereço, conta bancária para pagamento de benefícios;

» Dever de observar: falta de comprovação documental, mudança por canal frágil;

» Mitigação: revisão de processos, exigir documentos e autenticação presencial/eletrônica segura.

- Solicitação de confirmação de dados via SMS ou WhatsApp. Mensagem pedindo “confirmar CPF/telefone” via link ou texto que leva a formulário fraudulento:

  - Normalmente visando dados pessoais para fraude ou engenharia posterior;

  - Dever de observar: links curtos, número desconhecido, mensagens com erro de português;

  - Mitigação: usar envio de SMS/WhatsApp apenas com *templates* oficiais, educar usuários e canais de denúncia.

11.3 Boas Práticas em Segurança da Informação

As boas práticas diárias consistem em compilados de orientações recomendadas por profissionais em segurança da informação e normativas que envolvem privacidade de proteção de dados pessoais.

Proteção de dados pessoais

- Nunca fornecer informações sensíveis em sites sem que se tenha solicitado o serviço que o exige, e o faça somente se houver confiança no *site* e se ele estiver utilizando métodos criptográficos (*procurar pelo cadeado na barra do navegador e um informativo de certificado digital*);

- Nunca compartilhar dados pessoais de parceiros, fornecedores, colaboradores com o público externo sem ter o real conhecimento da necessidade;

- Manter sigilo ou anonimização sobre os dados pessoais tratados no decorrer das atividades, devendo sempre zelar pelos princípios dispostos no artigo 6º da LGPD;

- Nunca utilizar os dados pessoais para finalidades que não sejam objeto do escopo de trabalho. Exemplo: não utilizar os dados dos titulares para finalidades distintas para os quais foram coletados.

- Ao realizar o descarte de documentos, certificar-se de rasgar ou riscar os dados pessoais neles contidos, de forma a torná-los ilegíveis. Ou utilizar triturador antes de eliminar papéis que contenham dados pessoais;

- Não deixar documentos com dados pessoais em cima das mesas, uma vez que o simples acesso por pessoa não autorizada, já pode ser considerado incidente de segurança.

Correio eletrônico

- Não instalar jamais arquivos recebidos via e-mail, mensagens instantâneas, nem clicar neles, sem ter a certeza do que se está fazendo;

- Deve-se verificar sempre a procedência de e-mails com anexos duvidosos, observando o cabeçalho completo da mensagem.

- Jamais clicar em links de acesso à internet que estejam no corpo do e-mail, sem que se tenha certeza de sua integridade e qualquer dúvida entre em contato com o setor de Tecnologia da Informação;

- Apenas responder, abrir e encaminhar e-mails de remetentes conhecidos e com conteúdo esperado. E-mail suspeitos devem ser comunicados ao departamento de Tecnologia da Informação.

- Tomar cuidado ao enviar um e-mail, certificando-se se o destinatário está correto para que informações sigilosas não caiam em destinatários incorretos.

Instalação de software

- Nunca solicitar ou realizar a instalação de softwares piratas em máquina corporativa;

- Baixar *software* apenas com autorização da superior imediato, mesmo que seja conhecido, registrar via canal de atendimento ao departamento de Tecnologia da Informação e informar o endereço do site onde o executável se encontra;

- Somente é permitida a instalação de software homologado e/ou licenciado, salvo indicado pela instituição, quando se tratar de *software* livre;

- Toda e qualquer instalação, atualização ou configuração de software deve ser realizado pelas Coordenações que lidam com Tecnologia da Informação e registrado através de chamado.

Realização de backup

- Informações mantidas na máquina são de responsabilidade de quem à utiliza, portanto deve-se manter cópias redundantes e jamais confiar em apenas uma mídia para armazenar dados mais valiosos;

- Pensar sempre no impacto da perda de dados e cuidar para que isso não ocorra. Criar uma rotina de cópias (*backup*) de todos os dados importantes que possam estar armazenados localmente em sua máquina;

- Verificar se a instituição dispõe de *Datacenter* para armazenamento de *backup*. Recomendada em ISO/IEC 27040 requisitos técnicos detalhados e orientações sobre como as organizações po-

dem atingir um nível adequado de mitigação de riscos, utilizando uma abordagem comprovada e consistente para o planejamento, projeto, documentação e implementação da segurança do armazenamento de dados.

Proteção contra software malicioso

- Realizar uma varredura completa em sua máquina através do antivírus ao menos uma vez por semana.

- Realizar *download* de arquivos apenas de sites conhecidos e confiáveis.

Navegação na internet

- Lembrar-se sempre de averiguar se a conexão é segura e de analisar o certificado digital ao acessar contas bancárias, webmail, ou outros sites nos quais há troca de informações de dados sensíveis;

- Em conexões seguras, o ícone do cadeado fechado deve se encontrar na barra do navegador (*e não na página*) e a *URL* (*endereço do site*) deve iniciar com https: (*note sempre o "s"*);

- Não navegar em sites duvidosos pode gerar risco, tais como sites de músicas, jogos, fotos e redes sociais;

- Evitar utilizar recursos de "lembrar senha" e "continuar conectado", existentes em diversos navegadores e aplicativos;

- É recomendável uma limpeza dos *cookies* do navegador ao menos uma vez por semana;

- Não realizar *download* de quaisquer documentos que contenham informações pessoais dos parceiros e dos colegas de trabalho em dispositivo pessoal, salvo se houver expressa autorização do gestor;

- Caso precisar se ausentar do computador de trabalho, mesmo que por poucos minutos, sempre bloqueie a tela.

Administração segura de suas senhas

- Nunca escrever senha em local público ou de fácil acesso como, por exemplo, sem agenda, um pedaço de papel colado no monitor ou guardado em uma gaveta;

- Alterar senhas regularmente ou sempre que suspeitar de quebra de sigilo, sendo sugerido realizar a troca da senha a cada 6 meses, observando sempre as disposições da Política de Uso de senhas;

- Não compartilhar sua senha com outros colaboradores.

- Ao criar uma nova senha misturar caracteres especiais (*ex: @#$% ¨&*()+=.;*) e combinações entre números e letras maiúsculas e minúsculas.

- Não utilizar números fáceis de serem descobertos, tais como número da carteira de identidade, data de nascimento, CPF ou qualquer outro documento identificável.

- Não deixar senha visível ao digitá-la, muito menos na presença de desconhecidos.

Utilização de dispositivos móveis

- Evitar usar redes sem fio públicas para acesso de contas institucionais;

- Utilizar mecanismos de segurança, como antivírus, antispam, *antispyware* e *antimalware*;

- Manter o dispositivo atualizado com as versões mais recentes de todos os aplicativos instalados;

- Configurar uma senha para o dispositivo e se possível configurar o bloqueio de tela inicial, para ser ativado quando o aparelho não está em uso;

- Ao se desfazer do dispositivo, realizar uma formatação, ou seja, apagar os dados e restaurar as configurações de fábrica.

Dez pontos da segurança da informação

Trata-se de uma lista de cuidados básicos, mas que podem evitar incidentes de segurança que possam comprometer o andamento correto do ciclo de vida dos dados dentro da instituição.

- Utilizar senhas difíceis de serem descobertas;

- Alterar senha periodicamente;

- Ter atenção com *downloads*;

- Ter atenção com e-mails de remetentes desconhecidos;

- Evitar acessar sites com conteúdo duvidosos;

- Não abrir ou executar anexos de e-mails desconhecidos;
- Ficar atento com as compras via internet;
- Ficar atento ao acessar sites de instituições bancárias;
- Não revelar informações confidenciais sobre você na internet;
- Ao informar dados em sites, verifique se a página é segura (*com prefixo "https"*).

As boas práticas em privacidade e proteção de dados pessoais serão apresentadas na sequência.

11.4 Boas Práticas em Privacidade e Proteção de Dados Pessoais nas Atividades de Pesquisa do Ibict

Constituem boas práticas na pesquisa, para proteção da privacidade e de dados pessoais:

Anonimização de dados pessoais:

- Normalmente não se identifica necessidade de manutenção dos dados para a finalidade científica;
- Dever de observar: atender os artigos 5º, incisos III e XI, artigo 7º, inciso IV e artigo 11, II, c;
- Mitigação: transformar dados pessoais utilizando meios técnicos razoáveis disponíveis para que não haja associação de forma direta ou indireta ao titular de dados pessoais.

Identificação em projetos:

- Normalmente os projetos de pesquisa desenvolvidos pelo Ibict ou realizados com co-participação devem conter informações claras e documentadas na forma escrita;
- Dever de observar: identificação dos responsáveis (responsável técnico, equipe de tratamento de dados pessoais, executores e co-participantes)
- Mitigação: manter instrumentos jurídicos formais tais como convênios, contratos, pareceres do Comitê de Ética, termos de compromisso de uso de dados e quando necessário, termo de consentimento livre e esclarecido.

Observância aos Princípios da LGPD:

- Deve-se observar os princípios da LGPD em especial os princípios da finalidade, necessidade, adequação, transparência, responsabilização e prestação de contas;

- Dever de observar: o artigo 6º, incisos I a X da LGPD;

- Mitigação: visando reduzir eventuais riscos, utilizar os dados conforme as finalidades definidas de forma expressa e legítimas, defeso a utilização para fins incompatíveis com as finalidades definidas sendo necessário, em caso de alterações, a realização de reavaliação da base legal e comunicação aos titulares.

Observância das políticas internas:

- As políticas internas do Ibict, tais como de proteção de dados pessoais, segurança da informação, ética em pesquisa e uso de inteligência artificial e gestão de documentos, devem ser observadas;

- Dever de observar: Resoluções, guias e orientações internas sobre segurança da informação, privacidade e proteção de dados pessoais;

- Mitigação: responsabilização administrativa sem prejuízos para responsabilidade civil e penal, incluindo sanções previstas na LGPD.

Incidente de Segurança:

- Os procedimentos previstos sobre comunicação de incidente de segurança tem como escopo definir orientações às unidades do Ibict para viabilizar estratégias de comunicação para prevenção e ações efetivas que possam responder às situações de emergência e exceção, de forma documentada e padronizada;

- Dever de observar: o artigo 48 da LGPD, bem como a Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o regulamento de comunicação de incidente de segurança;

- Mitigação: o órgão deve conter um Plano de Incidente de Segurança que atenda a lei e as normas e orientações da ANPD.

Tratamento de Dados Sensíveis:

- Os dados sensíveis envolvem tratamento de dados como saúde, biométricos, de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político;

- Dever de observar: justificativa da coleta, utilizar hipóteses de tratamento adequados, previstos no artigo 11, em especial o inciso II, “c”;

- Mitigação:realização de Relatório de Impactos, se for o caso, e estrita observância às regras de segurança da informação, assim como, acesso restrito à equipe autorizada e registro automatizado de acesso e descrição de finalidade.

Tratamento de Dados de Criança e Adolescente:

- O tratamento de dados de criança e adolescentes na pesquisa deve ser realizado considerando o melhor interesse do menor, com o consentimento específico e em destaque por pelo menos um dos pais ou responsável legal;

- Dever de observar: artigo 14 da LGPD e Guias Orientativos da ANPD;

- Mitigação: aprovação em Comitê de ética, obtenção de consentimento específico, atendimento ao melhor interesse e realizar a anonimização dos dados.

Responsabilidades dos envolvidos nas pesquisas:

- Os envolvidos na pesquisa envolvem servidores, tecnologistas e bolsistas, a depender do projeto co-participantes;

- Dever de observar: expertise em proteção de dados pessoais, termos de compromisso e normativas internas da instituição;

- Mitigação: participar de capacitação sobre temas relacionados à proteção de dados pessoais no contexto de desenvolvimento de pesquisa.

Alterações nos projetos e Instrumentos contratuais:

- Atenção voltada para alterações em projetos e instrumentos contratuais;

- Dever de observar: instrumentos jurídicos que envolvam co-participantes, observa-se obrigações que envolvam segurança e compartilhamento de dados;

- Mitigação: definir responsabilidades e atribuições relacionadas aos desenvolvimento da pesquisa e utilização de dados pessoais, assim como inclusão de cláusulas de proteção de dados pessoais e alterações de finalidade, conhecimento do titular sobre alterações para tratamento de dados pessoais, ou novo consentimento, se for o caso.

Auditoria e Conformidade:

- Visa assegurar a adequação e integridade das informações quanto a governança dos dados pessoais no desenvolvimento dos projetos do ibict;

- Dever de observar: cumprimento das etapas do processo de conformidade à LGPD;

- Mitigação: procedimentos de monitoramento periódicos que garantam o cumprimento da LGPD, instrumentos legais e políticas institucionais internas inclusive planos, guias e orientações internas e da ANPD.

Propriedade intelectual:

- O tratamento de dados pessoais também deve estabelecer diálogo das fontes com os direitos autorais e propriedade industrial;

- Dever de observar: Lei de Direitos Autorais (Lei nº 9.610, de 19 de fevereiro de 1998) e Lei de Propriedade Industrial (Lei nº 9.279, de 14 de maio de 1996);

- Mitigação: observância no compartilhamento de banco e bases de dados, na proteção à inovação e novas criações, assim como nas publicações oriundas de pesquisas, na proteção de dados de participantes.

12 APURAÇÃO DE RESPONSABILIDADES

Em caso de inobservância às orientações do órgão sobre a observância à LGPD, devidamente apurada pelo responsável pela privacidade e proteção de dados pessoais, representada pelo Diretor do Órgão**,** a depender da gravidade e severidade da infração cometida, poderão ser aplicadas sanções disciplinares, conforme prevista no Estatuto do Servidor Público e na LGPD. A depender da natureza da infração cometida, o Ibict poderá notificar as Autoridades competentes, sem prejuízo de responsabilidade no contexto cível e penal.

13 CONCEITOS GERAIS

Além dos conceitos e definições apresentados nesse Guia de Boas Práticas, a orientação consiste na observância do Glossário de Proteção de Dados Pessoais e Privacidade, elaborado pela Autoridade Nacional de Proteção de Dados (Brasil, 2025b). Sua finalidade consiste em "[...] sistematizar os principais conceitos referentes a termos e expressões amplamente utilizados na legislação de proteção de dados pessoais, bem como nos documentos e demais comunicações publicadas pela ANPD" (ANPD, 2025). Para sua elaboração, foram consultadas, além da Lei nº 13.709/2018 – LGPD, toda a gama de documentos técnicos e doutrinários expedidos pela ANPD. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/glossario-anpd.

CANAL DE DÚVIDAS

Em caso de dúvidas ou sugestões acerca das disposições deste Guia, os destinatários deverão pedir esclarecimentos ao seu gestor imediato, ou formalmente por meio do canal de proteção à privacidade de dados encontrados no link: https://www.gov.br/ibict/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-1.

14 ATUALIZAÇÕES

O Guia de boas práticas poderá ser atualizado sempre que necessário, mediante aprovação prévia do Comitê de Proteção de Dados Pessoais, e se tornará válida a partir da data de publicação e da disponibilização nos canais oficiais do Ibict para todos os interessados.

O Guia de Boas Práticas deve ser obrigatoriamente revisado no período de 1 ano, ou quando necessário, considerando as orientações e normativas publicadas no contexto da ANPD, e eventuais atualizações na legislação pátria, com validade de um ano a partir da publicação.

SOBRE OS AUTORES

ROSILENE PAIVA MARINHO DE SOUSA

Professora do Departamento de Ciência da Informação da Universidade Federal da Paraíba – UFPB e do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação – PROFNIT/UFOB. Pesquisadora junto ao Instituto Brasileiro de Informação em Ciência e Tecnologia – Ibict. Doutorado e Mestrado em Ciência da Informação pela Universidade Federal da Paraíba (UFPB). Mestrado em Direito pelo Centro Universitário de João Pessoa (UNIPÊ). Graduação em Direito e História pela Universidade Federal de Campina Grande – UFCG e Graduação em Biblioteconomia pelo Centro Universitário Claretiano. Realiza estudos e pesquisas nas áreas de Propriedade Intelectual, Aspectos Jurídicos da Informação, Privacidade e Proteção de Dados, Direito Administrativo e Direito Empresarial.

https://orcid.org/0000-0002-4699-8692

http://lattes.cnpq.br/4465533418771961

rosilenesousa@ibict.br

SILVANA APARECIDA BORSETTI GREGORIO VIDOTTI

Doutora em Educação, na área de concentração em Educação Brasileira, pela Unesp, e Mestre em Ciências, com ênfase em Ciência da Computação e Matemática Computacional, pela USP. Possui especialização em Ciência da Computação pela USP e licenciatura em Matemática pela Unesp. Atualmente, é docente da Unesp e do Programa de Pós-Graduação em Ciência da Informação da mesma instituição, além de Coordenadora da Coordenadoria de Tecnologias Aplicadas (COTEA) do Instituto Brasileiro de Informação em Ciência e Tecnologia.

(Ibict).https://orcid.org/0000-0002-4216-0374

http://lattes.cnpq.br/7390573927636069

silvana.vidotti@unesp.br

MILTON SHINTAKU

Doutor em Ciência da Informação pela Universidade de Brasília. Coordenador de Tecnologia para Informação (Cotec) do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict). Professor do Programa de Pós-graduação em Gestão da Informação na Universidade Federal do Paraná (PPGGI/UFPR).

.https://orcid.org/0000-0002-6476-4953

http://lattes.cnpq.br/8605833104600600

shintaku@ibict.br

REFERÊNCIAS

ABNT NBR ISO/IEC 27000:2020 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Visão geral e vocabulário. Rio de Janeiro: ABNT, 2020.

ABNT NBR ISO/IEC 27001:2023 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2023.

ABNT NBR ISO/IEC 27002:2022 – Tecnologia da informação — Técnicas de segurança — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ANPD. Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília: 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 23 set. 2025.

ANPD. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 20 out. 2025.

ARAMUNI, João Paulo Carneiro; MAIA, Luiz Cláudio. O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. **AtoZ: novas práticas em informação e conhecimento**, *[S. l.]*, v. 7, n. 1, p. 31–37, 2020. DOI: 10.5380/atoz.v7i2.64640. Disponível em: https://revistas.ufpr.br/atoz/article/view/64640. Acesso em: 13 jan. 2026.

BARBIERI,Carlos. **Governança de Dados - Práticas, Conceitos e Novos Caminhos**. Rio de Janeiro: Alta Books, 2020.

BELKIN, Nicholas J.; ROBERTSON, Stephen E. Information Science and the phenomenon of information. **Journal of the American Society of Information Science**, p. 197 - 204, july/aug. 1976.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988, 292 p.

BRASIL. **Guia de Boas Práticas para Implementação na Administração Pública Federal**. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 15 jan. 2026.

BRASIL. **Glossário ANPD**. 2025b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/glossario-anpd. Acesso em: 15 jan. 2026.

BRASIL. **Lei Geral de Proteção de Dados** (LGPD): Guia de Boas Práticas para Implementação na Administração Pública Federal. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 13 jan. 2026.

BRASIL. **Emenda à Constituição nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 13 jan. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 23 set. 2024.

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: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 jan. 2026.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 15 jan. 2026.

BRASIL. **Relatório Final - GT nº 4 Governança de Dados (Setor Público)**. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. 2025a. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/relatorios-gts-2a-formacao/relatorio-final-gt4-do-cnpd.pdf. Acesso em: 10 jan. 2026.

BRASIL. **Tratamento de dados pessoais pelo Poder Público**. Guia Orientativo. 2023. Disponível em: https://portal.uern.br/acessoainformacao/wp-content/uploads/sites/23/2024/08/Guia-Tratamento-de-Dados-Pessoais-pelo-Poder-Publico-ANPD.pdf. Acesso em: 15 jan. 2026.

Buckland, M. (1991). Informação como coisa. ***Journal of the Association for Information Science and Technology*** , 42(5), 351-360. Disponível em: https://escholarship.org/uc/item/4x2561mb. Acesso em: 10 jan 2026.

CAPURRO, Rafael. Epistemologia e Ciência da Informação. In: Encontro Nacional de Pesquisa em Ciência da Informação – Enancib, 5., 2003, Belo Horizonte. **Anais...**Belo Horizonte: ECI/UFMG, 2003.

CAPURRO, Rafael; HJØRLAND, Birger. O conceito de informação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 12, n. 1, p. 148 - 207, jan./abr. 2007.

DAVENPORT, Thomas H; PRUSAK, Laurence. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DONEDA. Danilo. **Da Privacidade à Proteção de Dados Pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FONTES, Eduardo. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

LE COADIC, Yves - François. **A ciência da informação**. Brasília, DF: Briquet de Lemos/Livros, 1996.

MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. **Civilistica.com**, Rio de Janeiro, v. 12, n. 1, p. 1–34, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/843. Acesso em: 22 dez. 2025.

MACHLUP, Fritz; MANSFIELD, Una. (Ed.). **The study of information**: Interdisciplinary messages. New York, NY: Wiley, 1983.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coords.). **LGPD – Lei Geral de Proteção de Dados**: comentada. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

MALDONADO, Viviane Nóbrega (Coord.). **Manual do DPO Data Protection Officer**. Revista dos Tribunais. 2022. (Edição do Kindle).

MARINELI, M. R. **Privacidade e Redes Sociais Virtuais**: sob a égide da Lei 12.965/2014 – Marco Civil da internet e da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MORAES, A. Constituição do Brasil Interpretada e Legislação Constitucional. São Paulo: Atlas, 2003.

OLIVEIRA, Flávia de Paiva Medeiros de; SOUSA, Rosilene Paiva Marinho de. O DESENVOLVIMENTO SOCIOECONÔMICO E O VALOR DA INFORMAÇÃO NOS PADRÕES DE PRODUÇÃO E CONSUMO RESPONSÁVEL. **Revista Jurídica da FA7**, [*S. l.*], v. 17, n. 2, p. 87–98, 2020. DOI: 10.24067/rjfa7;17.2:1158. Disponível em: https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1158. Acesso em: 9 jan. 2026.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 5. ed. Rio de Janeiro: Saraiva Jur, 2026.

RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**: A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SETZER, V. W. **Dado, Informação, Conhecimento e Competência.** Universidade de São Paulo, São Paulo, 2015. Disponível em: https://www.ime.usp.br/%7Evwsetzer/dado-info.html. Acesso em: 15 jan. 2026.

TURBAN, Efraim; RANIER JÚNIOR, R. Kelly; POTTER, Richard E. **Introdução a Sistemas de Informação**: uma abordagem gerencial. Tradução Daniel Vieira. Rio de Janeiro: Elsevier, 2003.

VAINZOF, Rony. Lei nº 13.709, de 14 de agosto de 2018. In. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coords.). **LGPD – Lei Geral de Proteção de Dados**: comentada. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

No cenário atual, em que a informação ocupa papel estratégico e o tratamento de dados pessoais integra a rotina de instituições públicas e privadas, o Guia de Boas Práticas de Privacidade e Proteção de Dados Pessoais, do Ibict, apresenta abordagem objetiva e juridicamente consistente, alinhada à atuação de um órgão público de pesquisa. A obra articula fundamentos normativos, orientações práticas e princípios de governança da informação, superando a lógica de adequação meramente formal à legislação. Ao considerar as especificidades da pesquisa científica e seu regime jurídico próprio, estrutura diretrizes voltadas à capacitação de servidores e parceiros, fortalecendo a cultura institucional de proteção de dados e a atuação responsável no contexto da LGPD.

Fábio Lucas de Albuquerque Lima
Doutorando em Direito e Políticas Púbicas pelo UNICEUB. Editor-Chefe da Revista RASS em Brasília. Editor Científico certificado pela ABEC Brasil. Mestre em Administração Pública pela FGV (RJ).

Em um contexto no qual a informação se consolidou como eixo estratégico da gestão pública e da produção científica, o Ibict apresenta o Guia de Boas Práticas de Privacidade e Proteção de Dados Pessoais como referência em governança de dados. A obra supera o formato de manual operacional e se estabelece como instrumento de alinhamento normativo e organizacional. Com base técnica consistente, articula LGPD, Lei de Acesso à Informação e regime jurídico da pesquisa, abordando ciclo de vida dos dados, gestão de riscos, prevenção de incidentes e anonimização. O guia orienta gestores e pesquisadores na construção de práticas éticas, seguras e juridicamente fundamentadas.

César medeiros Cupertino
Perito Criminal Federal
Secretário-Adjunto no Ministério Público Militar
Doutor em Administração

ISBN: 978-85-7013-228-4
CBL
9 788570 132284

ibict
Instituto Brasileiro de Informação em Ciência e Tecnologia

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Ibict | **BRASÍLIA/DF**