HERBERT ALCÂNTARA FERREIRA

TAXONOMIAS CORPORATIVAS COMO SUPORTE AO *COMPLIANCE* EM LGPD

organização do conhecimento
em intituições hospitalares

EDITORA Unimontes

TAXONOMIAS CORPORATIVAS COMO SUPORTE AO COMPLIANCE EM LGPD

organização do conhecimento em instituições hospitalares

Herbert Alcântara Ferreira

TAXONOMIAS CORPORATIVAS COMO SUPORTE AO COMPLIANCE EM LGPD

organização do conhecimento em instituições hospitalares

EDITORA Unimontes
Montes Claros/2025

Laura Silveira Fahel
Capa

Maria Rodrigues Mendes
Diagramação

Ângela Heloisa Benedito
Ana Juliana da Silva Alcântara Ferreira
Revisão linguística

Maria Clara Maciel de Araújo Ribeiro
Editora-Chefe

Este livro foi selecionado por edital
e submetido a parecer duplo cego

Dados Internacionais de Catalogação-na-Pública(CIP) Associação Brasileira das Editoras Universitárias (ABEU)

F383t

Ferreira, Herbert Alcântara.
Taxonomias corporativas como suporte ao compliance em LGPD: organizaçãodo conhecimento em instituições hospitalares [recurso eletrônico] / Herbert Alcântara Ferreira. - Montes Claros, MG : Editora Unimontes, 2025.
143 p. ; E'book PDF.

Inclui bibliografia.
Modo de acesso: world wide web
http://www.editora.unimontes.br/index.php/ebook

ISBN: 978-65-86467-99-4. (E'book).

1. Direito a privacidade - Brasil. 2. Proteção de dados – Legislação - Brasil. 3. Saúde – Proteção de dados. I. Ferreira, Herbert Alcântara. II. Título. III. Título: Organização do conhecimento em instituições hospitalares.

CDD 342.81

Elaborado por Biblioteca Central Professor Antônio Jorge / Roseli Damaso – CRB-6/1892

Campus Universitário Professor Darcy Ribeiro
Montes Claros - Minas Gerais - Brasil
CEP 39401-089 - CAIXA POSTAL 126
www.editora.unimontes.br
editora@unimontes.br
Filiada à

Associação Brasileira
das Editoras Universitárias

A Deus, por todas as bênçãos que Ele me oferta, em especial, o dom da minha vida. À minha mãe, Ricarda, e ao meu pai, Clóvis, que dedicaram suas vidas aos seus filhos e cujo exemplo me serviu de “doutoramento” para a vida. Por fim, à minha esposa, Ana Juliana, por ter me apoiado durante esta jornada. Sem o apoio de vocês, nenhuma conquista valeria a pena.

Sumário

8 **Prefácio**

12 **1 Apresentação**

16 **2 Uma breve contextualização: a sociedade informacional**

20 **3 LGPD: uma visão teórico-legal da proteção de dados**

21 3.1 Uma análise prévia: os conceitos de dado e de informação
24 3.2 Violação de dados pessoais e a garantia da privacidade
28 3.3 Normas de proteção de dados pessoais pelo mundo
30 3.4 Proteção de dados no Brasil antes da LGPD
31 3.5 A elaboração da LGPD
33 3.6 Características, fundamentos e princípios da LGPD
35 3.6.1 Fundamentos e princípios
37 3.6.2 Aplicação da LGPD
38 3.6.3 Bases legais
40 3.6.4 Direitos do titular
41 3.6.5 Controlador, operador e encarregado
42 3.6.6 Autoridade Nacional de Proteção de Dados Pessoais
43 3.6.7 Sanções administrativas
44 3.6.8 Benefícios e desafios da adequação à LGPD

48 **4 *Compliance* em LGPD: uma visão pragmática da proteção de dados**

50 4.1 Definição de funções e conscientização da instituição
51 4.2 Análise de maturidade da organização em relação à proteção de dados pessoais
51 4.3 Registro de operações de tratamento de dados pessoais
52 4.4 Relatório de impacto de proteção de dados pessoais
Implantação de ações de privacidade e segurança de dados pessoais
53 4.5 Implantação de ações de privacidade e segurança de dados pessoais
55 4.6 Gestão de incidentes
56 4.7 Análise dos resultados

58 **5 Breve panorama dos sistemas de organização do conhecimento**
59 5.1 A organização do conhecimento e sua dimensão instrumental
60 5.2 O papel dos conceitos e das relações conceituais
61 5.3 Os sistemas de organização do conhecimento e os seus aspectos gerais
63 5.4 Principais sistemas de organização do conhecimento

68 **6 Taxonomias como suporte ao *compliance* em LGPD**
69 6.1 As taxonomias mais de perto
71 6.2 Taxonomias corporativas
73 6.3 Metodologia geral para construção de taxonomias
77 6.4 Taxonomias para mapeamento de dados pessoais

82 **7 Um modelo de taxonomia para *compliance* em LGPD**
83 7.1 A instituição-modelo: Hospital Universitário Clemente de Faria
85 7.2 O fluxo de dados pessoais na instituição-modelo
90 7.3 Executando as etapas de construção de taxonomias
120 7.4 Benefícios de uma taxonomia para mapeamento de dados na instituição-modelo

124 **8 Considerações Finais**

128 **Referências**

Prefácio

Adilson Luiz Pinto

Esta obra do Doutor Herbert Alcântara Ferreira sobre a Lei Geral de Proteção de Dados, com relação aos Sistemas de Organização do Conhecimento, tende a cumprir um papel relevante na estrutura taxonômica corporativa de instituições hospitalares. Especificamente, a obra traz um modelo para o Hospital Universitário Clemente de Faria, situado em Montes Claros - Minas Gerais, que pode ser seguido por outras instituições de características similares.

A proposta deste livro é fruto de um trabalho doutoral que o autor realizou na Universidade Federal de Santa Catarina (Programa de Pós-Graduação em Ciência da Informação, projeto DINTER) em parceria com a Universidade Estadual de Montes Claros, e está destinado a atender várias áreas do conhecimento, desde o Direito e a Ciência da Informação (áreas de formação do autor) até a Sociologia, Enfermagem, as Ciências Médicas e a Lógica.

O modelo estruturado da obra percorre a Lei Geral de Proteção de Dados, com seus fundamentos e princípios; a sua aplicação; as bases legais; o direito do titular; as competências dos envolvidos (controlador, operador e encarregados); as autoridades envolvidas; as sanções administrativas; e os desafios e benefícios de uma instituição ao adequar-se a esta lei. Em complemento, o autor dedica um apartado todo exclusivo para a *compliance* da lei, a fim de que as normas sejam adequadas ao ambiente corporativo.

Por outro lado, a proposta trata também de sistemas classificatórios (hierárquicos e facetados), lista de termos, taxonomias, tesauros, mapas conceituais, *folksonomias* e ontologias como estruturação lógica do cumprimento da LGPD. Em relação à preparação e à aplicação da taxonomia no Hospital Universitário Clemente de Faria, foi utilizada a taxonomia corporativa.

Em se tratando de aplicação, a obra trata de analisar a instituição e seu planejamento; coletar termos dentro de sua estrutura; analisar e controlar os termos recuperados; definir as categorias gerais e específicas; ordenar e padronizar gramaticalmente as categorias; definir as relações semânticas entre os termos; validar a taxonomia; definir a forma de apresentação da taxonomia e tecnologia de suporte; publicar; determinar ações de gerenciamento; e possíveis manutenções.

Contextualizada a obra, cabe-nos responder alguns questionamentos, como: (a) Por que esta obra? (b) Como utilizar esta obra? (c) Para quem serve esta obra? Em relação à primeira pergunta (a), acredito que seja voltada a todas as áreas de conhecimento que queiram estruturar um sistema de taxonomia. O ambiente proposto pelo Doutor Herbert Alcântara Ferreira sobrepassa a administração hospitalar e pode

ser replicado em qualquer ambiente que pretenda aplicar a Lei Geral de Proteção de Dados a partir de um ambiente taxonômico, como sistemas de vendas virtuais, sistemas físicos, estruturas acadêmicas e abordagem voltada ao cidadão.

Em resposta à utilização desta obra (b), a mesma pode ser aplicada em estruturas de dados pessoais e institucionais. Em um cenário de uso indevido de informações pessoais, como vendas de conteúdos por grandes corporações, faz-se necessário que cenários estruturais sejam responsabilizados pelo compartilhamento de dados de terceiros. Em sistemas hospitalares, o sigilo é fundamental, porém, em outras esferas também, e o modelo proposto é viável em muitas frentes, como no meio acadêmico, comércio eletrônico, serviços e sistemas de telecomunicação.

Quanto à última questão (c), esta obra deverá atender a todos os inquietos em se adequar à Lei Geral de Proteção de Dados na instituição que presta serviços e, ao mesmo tempo, aos inquietos em organizar o conhecimento de uma instituição. A taxonomia corporativa vem para dar um aporte em controlar grandes volumes de dados não estruturados. Por todas essas qualidades da obra, felicito o autor e recomendo a leitura aos curiosos dos sistemas de organização da informação e do conhecimento.

Prof. Dr. Adilson Luiz Pinto

Doutor em Documentação pela Universidad Carlos III de Madrid e Professor da Universidade Federal de Santa Catarina

Madrid, setembro de 2023

1

Apresentação

De acordo com o filósofo Karl Popper (2006), o universo pode ser dividido em três “mundos”, como “instâncias” da realidade que interagem entre si. O que ele se refere a “mundo um” compreende a perspectiva física da realidade, incluindo o conjunto universal de corpos materiais animados e inanimados, bem como de todos os eventos, movimentos, forças e tensões presentes no cosmos. O “mundo dois” é o terreno psicológico e subjetivo do humano e de outros seres (conscientes e inconscientes), ou seja, é tudo aquilo que se produz na mente. E, por fim, há o “mundo três”, o mundo dos produtos do espírito humano, cujos subsídios mentais são extraídos do segundo mundo.

Essa terceira instância da realidade reflete tanto no mundo um, na forma de produtos materiais do trabalho humano (como objetos utilitários, máquinas e registros do conhecimento), quanto nas ideias em trânsito no mundo dois (já que os produtos cognitivos do espírito humano são aproveitados no terreno psicológico subjetivo ou interpessoal). O que se produz no mundo três é, portanto, conhecimento, que se aproveita de informações depreendidas pela mente humana para criar novas entidades materiais e imateriais. Por isso, a informação, matéria-prima do mundo três, é elemento fundamental para as atividades humanas, desde as mais simples às mais complexas.

No mundo contemporâneo, em que as tecnologias de informação e comunicação (TICs) dominam as relações humanas, sejam econômicas, políticas ou privadas, a informação tem se materializado em dados. Incorporadas no mundo físico dos registros impressos ou computacionais, as informações neles contidas são subsídios para a geração de conhecimento, que pode ressoar na realidade material em forma de novos dados.

Considerando-se a importância desses registros informacionais para a atualidade, chamam a atenção o uso e os dilemas relacionados aos dados pessoais. Entendidos como dados que se referem à pessoa natural, eles tornaram-se importantes ativos econômicos na sociedade informacional contemporânea, consistindo-se em elementos estratégicos importantes para o desenvolvimento de bens e serviços, tanto no setor público quanto na iniciativa privada. Nesse contexto marcado por disputas em busca de vantagens econômicas, vêm acontecendo recorrentes casos de violação de dados de caráter privado, como números de identidades, cadastros de pessoas físicas, números de telefones e endereços de e-mail, assim como dados de caráter sensível (que envolvem saúde física e emocional dos indivíduos, por exemplo), o que dá contornos a um crescente cenário de violações generalizadas ao direito à privacidade. Por essa razão, cada vez mais, há a necessidade de regular o tratamento de dados dessa natureza, a fim de resguardar as pessoas a quem essas informações se referem.

Nesse sentido, muitas normas de proteção de dados pessoais têm sido publicadas pelo mundo. No Brasil, a Lei n° 13.709/2018, aprovada em agosto de 2018 e plenamente vigente desde agosto de 2021, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), é a legislação que regula as atividades de tratamento de dados pessoais em território nacional (e fora dele, em determinados casos). Em termos gerais, a LGPD "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado [...]" (Brasil, 2018a, art. 1°).

Influenciada pela norma vigente na União Europeia, a *General Data Protection Regulation* (GDPR), a LGPD tem como principais características: a) a definição de fundamentos e princípios acerca da proteção de dados pessoais; b) a explicação de conceitos básicos envolvendo a temática; c) a delimitação de regras de aplicação da lei dentro e fora do território brasileiro; d) a previsão de "bases legais" (justificativas) exigidas para que determinado tratamento de dados pessoais seja considerado legítimo (aceito pela lei); e) a determinação de direitos dos titulares dos dados e de competências de agentes de tratamento; f) a definição de autoridade pública responsável por tratar da matéria e; g) a previsão de sanções administrativas contra quem desobedecer às exigências legais.

Com a vigência da LGPD, entidades públicas e privadas que utilizam dados pessoais precisam adequar-se às regras da aludida lei, o que envolve mudanças e ajustes no tratamento de dados. Torna-se necessário o desenvolvimento de técnicas e instrumentos que auxiliem a implantação de suas previsões legais, a fim de não incorrerem em ilegalidades perante essa normativa. A esse processo de conformidade legal dá-se o nome de *compliance.*

Não obstante a proteção de dados pessoais seja uma preocupação fundamentalmente jurídica, há áreas científicas que podem nos auxiliar na promoção da privacidade informacional. Dentre elas, está a Ciência da Informação. Assim, a presente obra é resultado de tese de doutoramento produzida e defendida em âmbito do Programa de Pós Graduação em Ciência da Informação da Universidade Federal de Santa Catarina. Busca-se, com base em subsídios desse campo científico, contribuir para a preocupação jurídica de proteção de dados pessoais (sobre a qual se funda a LGPD). Mais especificamente, é na disciplina da organização do conhecimento (OC) – especialmente na sua dimensão instrumental – que chegamos ao objetivo daquele trabalho doutoral, ora transformado em livro.

A dimensão instrumental da OC encontra-se atualmente centrada no desenvolvimento e na sustentação dos chamados sistemas de organização do conhecimento (SOCs). Segundo Hodge (2000), o termo "sistemas de organização do conhecimento" foi proposto no âmbito do *Networked Knowledge Organization Systems Working Group*, em 1998, e se refere ao conjunto de instrumentos voltados à representação formal de domínios de conhecimento, tais como sistemas de classificação, listas de termos, vocabulários controlados, tesauros, mapas conceituais, taxonomias e ontologias, para citar os principais. Cada um desses instrumentos possui formas distintas de representar o conhecimento e contribuir para uma organização sistemática de conceitos/termos. Como consequência, tais ferramentas proporcionam eficientes meios de representar, tratar e recuperar a informação.

Dentre tantos sistemas de organização de conhecimento, escolhemos aquele chamado de taxonomia. Trata-se de modelo que organiza e representa itens de

informação, com especial vocação ao ambiente digital e à gestão informacional em instituições diversas, inclusive hospitalares. No capítulo oportuno, falaremos com mais detalhes sobre as causas da escolha desse sistema, além de como ele deve ser construído/aplicado em procedimentos de adequação à legislação de proteção de dados pessoais.

Como dito anteriormente, a demanda jurídica trazida pela LGPD deve ser observada por entidades públicas ou privadas, de pequeno, médio ou grande porte. No escopo desta obra, preferimos voltar-nos às instituições hospitalares, tendo em vista a diversidade e a sensibilidade de dados pessoais em fluxo nesse tipo de organização. Para demonstrar como taxonomias podem ser úteis para a adequação (*compliance*) em proteção de dados pessoais em instituições dessa natureza, tomamos como modelo o Hospital Universitário Clemente de Faria (HUCF), instituição hospitalar de natureza pública localizada em Montes Claros, norte de Minas Gerais.

Após a contextualização até aqui apresentada, as nossas inquietações podem ser sintetizadas na seguinte pergunta: como as taxonomias, enquanto sistemas de organização do conhecimento, podem contribuir para o compliance da Lei Geral de Proteção de Dados Pessoais? Durante a trajetória desta obra, encontraremos a resposta.

2

Uma breve contextualização: a sociedade informacional

Nas últimas décadas, o mundo tem presenciado uma acelerada evolução das tecnologias. Diversas inovações digitais, como os computadores, a *internet* e os telefones celulares têm sido determinantes para que o armazenamento e o gerenciamento de dados pessoais se tornem viáveis. Assim, indivíduos, órgãos públicos e instituições privadas passaram, em certa medida, a ter acesso a algum tipo de informação pessoal. Nesse contexto, a rede mundial de computadores é responsável por integrar indivíduos e instituições em prol do exercício de atividades que dependem do constante envio e recebimento de dados, num sistema que se retroalimenta e se enriquece a partir das informações compartilhadas.

Tudo isso faz parte de o que se chama "sociedade informacional". De acordo com o sociólogo espanhol Manuel Castells, a sociedade informacional se refere à presente era da humanidade, em "[...] que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais da produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico" (Castells, 1999, p. 64-65). Segundo Castells, são as novas tecnologias que promovem essa conjuntura social, colocando a informação, mais do que nunca, como a grande matéria-prima das atividades humanas.

Para a cientista da informação Emilia Currás (2014), a humanidade sempre viveu uma "era da informação", pois a informação é intrínseca às atividades humanas mais simples. Basta vermos, por exemplo, que mesmo um gesto ou uma simples palavra tem como objetivo transmitir alguma informação (mais à frente falaremos com mais detalhes sobre o conceito de informação). Para além disso, vivemos na "era da tecnologia da informação", em que os aparatos tecnológicos/digitais assumiram posição de protagonismo no trabalho e nas relações humanas – na mesma toada do que entende Castells.

Várias são as vantagens das tecnologias próprias da sociedade informacional. Algumas delas já citamos no início deste capítulo: itens utilitários como computadores e *smartphones*; a *internet* (invenção que certamente mudou os rumos da humanidade); e a consequente otimização da prestação de serviços públicos e privados. Vejam-se, como decorrência dessas inovações: as redes sociais, os aplicativos de mensagens, o sistema de *e-mails*, as plataformas de *streaming*, os buscadores on-line, os sistemas empresariais/institucionais de armazenamento e acesso de dados, dentre tantos outros espaços e ferramentas para finalidades variadas.

Porém, assim como reza o ditado popular, "nem tudo são flores". De fato, as contemporâneas tecnologias da sociedade informacional trouxeram vários avanços para a humanidade, mas também potencializaram antigos problemas e criaram outros. Um desses problemas é que a informação funciona como subsídio econômico e de conhecimento e, portanto, a falta de acesso a ela intensifica a desigualdade social

(Dziekaniak; Rover, 2011). Este é o dilema da "exclusão digital", que se refere à falta de acesso aos aparatos tecnológicos por grande parte da população. Dessa maneira, o excluído se vê desconectado e incapaz de utilizar os úteis recursos disponíveis pelas tecnologias, especialmente na *internet*. Conforme Silveira (2008), o motivo mais comum desse problema é a desigualdade socioeconômica entre classes sociais e entre nações, de modo que a exclusão digital expõe um dilema de raízes ainda mais profundas. Além disso, mesmo entre indivíduos que estão no mundo digital, há certas "assimetrias", a exemplo da falta de habilidades de algumas pessoas para utilizar computadores e celulares em oposição a outras que possuem mais facilidade em utilizá-los.

No Brasil, a exclusão digital pode ser demonstrada em números, através da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua) de 2019, a qual expõe que 12,6 milhões de domicílios no Brasil ainda não possuem acesso à *internet* (Instituto Brasileiro de Geografia e Estatística, 2021). Entre os motivos, destacam-se a falta de interesse no acesso à *internet* (32,9%), o alto valor de acesso a esses serviços (26,2%), além do desconhecimento de brasileiros sobre como utilizar essa tecnologia (25,7%). Nota-se que esses dois últimos empecilhos são consequências diretas da exclusão socioeconômica anteriormente mencionada.

Entretanto, se, por um lado, pessoas em situação de vulnerabilidade socioeconômica encontram dificuldades para acessar a *internet*, de outro lado, existe um cenário de notório exagero na utilização de tecnologias digitais por outra parte da população. As redes sociais, por exemplo, são ambientes em que se podem perceber situações de vício em relação à virtualidade, expondo as mentes e emoções humanas ao viciante excesso de informações e de estímulos. A adicção a esses ambientes digitais causa sérios danos, como "dependência, ansiedade, isolamento social, alucinação, inabilidade, dentre outros" (Scheneider; Santos; Santos, 2020, p. 53).

Além disso, há outros dilemas relacionados às TICs e às mídias atuais, tais como: as *fake news* (disseminações de informações falsas); a utilização de redes sociais para propagação de discursos de ódio (especialmente contra mulheres, pessoas negras, pessoas LGBTQIA+ e outros grupos sociais); e o uso da *internet* para a prática de crimes das mais variadas naturezas. Assim, percebe-se que as possibilidades de utilização das novas tecnologias na sociedade informacional são múltiplas, mas nem sempre benéficas.

Importante conhecer os "dois lados da moeda" no que concerne à sociedade informacional. É salutar afastar-se dos encantamentos com as novas tecnologias, mas também do exagerado pessimismo que as cerca. Melhor é adotar uma visão mais realista sobre essa conjuntura, posição que é imprescindível para compreender esta obra. Como conciliar a necessidade de utilização de dados pessoais, especialmente em ambientes digitais, com a obrigatoriedade legal de preservação da privacidade? A partir da contextualização aqui apresentada, temos os subsídios básicos para enfrentar as indagações que doravante nos esperam.

3

LGPD: uma visão teórico-legal da proteção de dados

3.1 Uma análise prévia: os conceitos de dado e de informação

Neste capítulo, apresentaremos uma visão teórica da proteção de dados pessoais (histórico, panorama global, fundamentos jurídicos etc.), além de trazer uma perspectiva legal sobre a matéria (mais especificamente uma análise sobre a LGPD, que é a norma geral brasileira sobre o tema). Contudo, antes de adentrarmos as discussões centrais deste capítulo, importa realizar uma análise prévia sobre os conceitos de dado e de informação. Esse é um trabalho necessário não apenas porque são terminologias constantemente citadas na disciplina legal de proteção de dados pessoais, mas também porque são muito importantes para a Ciência da Informação (campo científico em que se localiza a organização do conhecimento).

Dado e informação são termos cujos significados são objetos de preocupação da Ciência da Informação (CI) desde o seu nascimento. De caráter interdisciplinar, a CI é uma ciência que se consolidou enquanto disciplina moderna em meados do século XX (Barreto, 2002; 2007; Araújo, 2018; Gomes, 2017; Queiroz; Moura, 2015). Como o próprio nome denota, ela estuda as investigações teóricas sobre a informação e as atividades práticas que a envolvem (Saracevic, 2009). Nessa perspectiva, discussões de autores e de trabalhos no âmbito da CI servem como subsídios para conceituar aqueles termos, que são caros às investigações envolvendo a sociedade informacional e, também no escopo desta obra, os dados pessoais.

Araújo (2018), procurando analisar o conceito de "informação" sob uma perspectiva histórico-científica, expõe que houve três noções preponderantes do termo, desenvolvidas pelos estudiosos da Ciência da Informação no decorrer dos tempos. Em um primeiro momento, a informação era vista como um elemento material, como "algo mensurado, formalizado, universal e neutro" (p. 72), cuja noção fora muito influenciada pelo positivismo cientificista. A segunda ideia focou no campo cognitivo, de modo que seu estudo se ligava intimamente com o significado dos elementos de conhecimento. Ao analisar a informação sob a perspectiva da cognição e da comunicação, Yves-François Le Coadic prefere defini-la da seguinte maneira:

> É um significado transmitido a um ser consciente por meio de uma mensagem inscrita em um suporte espacial-temporal: impresso, sinal elétrico, onda sonora, etc. Essa inscrição é feita graças a um sistema de signos (a linguagem), signo este que é um elemento da linguagem que associa um significante a um significado: signo alfabético, palavra, sinal de pontuação (Le Coadic, 1996, p. 5).

A partir dessa lógica, estabelece-se a comunicação, que é o esquema cognitivo de troca de informações entre indivíduos. Dessa maneira, a informação se con-

cebe como o elemento cuja finalidade é perpassar saberes, a exemplo das notícias jornalísticas que se veiculam na televisão. Assim, para Le Coadic (1996), o objetivo da informação é "a apreensão de sentidos ou seres em sua significação" (p. 5). Por fim, atualmente, a definição de informação é mais estudada sob a ótica da ação humana, considerando "os contextos socioculturais concretos" (Araújo 2018, p. 78) em que a informação é veiculada.

Partindo para essa abordagem mais social da informação, são dignos de destaque os apontamentos de Barité (2001) sobre esse elemento. Para ele, a informação é uma realidade objetiva que pode estar tanto fora do indivíduo (nos espaços sociais) quanto dentro dele (em suas memórias). Ela é social, já que faz parte das relações humanas. Ao mesmo tempo, é elemento objetivo, de modo que pode ser mensurada (por exemplo, em *bits* que medem dados registradores de informação) e ser apresentada de formas diversas.

Araújo, preocupando-se com a repercussão social da informação, deixa claro que: "A informação é algo da ordem do coletivo, é de natureza intersubjetiva, da ordem das interações, é construída por meio da ação reciprocamente referenciada dos atores – assim como as demais ações e existências dos sujeitos" (Araújo, 2018, p. 85). Intrincada a um contexto social e real, a informação não se atém à comunicação entre emissor e receptor, mas ressoa pelo mundo, construindo a cultura e a memória coletivas. Assim, a sua transmissão é um processo de interação social fundamental.

Fato é que, devido à sua importância na comunicação e na atividade humana (que pressupõem conhecer elementos – informações – da realidade), as definições de informação encontradas no âmbito da CI tendem a se relacionar com a definição de conhecimento. Como aduzem Silva e Gomes (2015. p. 152), "a informação só tem sua plenitude consagrada quando permite efetivas condições intelectivas para construção do conhecimento".

Por mais que a conceituação de "conhecimento" não seja objeto de preocupação neste ponto da obra, é interessante apresentar uma breve noção sobre esse termo, até mesmo para podermos diferenciá-lo de "informação". Por ora, podemos ficar com a definição dada por Barité (2001). Para ele, o conhecimento forma-se do contato de informações que chegam à pessoa através do aprendizado ou da assimilação. Sob uma perspectiva individual, o conhecimento é subjetivo, sendo resultado dos processos mentais humanos que têm a informação como matéria-prima. Contudo, também é um produto coletivo, sendo considerado "[...] registro social de tudo o que o homem compreendeu sobre a natureza e de tudo o que acrescentou a ela" (p. 42, tradução nossa).

Com base nessas visões científicas, podemos buscar definições de "dado". Para Silva e Gomes, dado é o "[...] plano físico e histórico-social dos sujeitos da informação" (2015, p. 150), sendo, assim, um meio físico de transmissão da informação. A partir desse elemento material, a informação chega ao receptor e se estabelece uma relação de comunicação entre indivíduos. Barité (2001) entende dados como unidades formadoras da informação e que representam, autonomamente, um conhecimento registrado.

Sob o enfoque nas definições de "informação" e "dado" na Ciência da Informação, com base nos autores aqui trazidos, entende-se que há extensa tradição em busca de conceituações definitivas sobre esses termos. É possível inferir basicamen-

te que, para alguns autores, a informação tem relação direta com o âmbito da cognição, como um processo, ou mesmo um produto, da mente humana, enquanto o dado seria a própria estruturação material que viabiliza a informação.

Ainda vale observar que, para outros autores, a partir do contato do homem com a informação, forma-se o conhecimento, como abstração subjetiva do que foi vivido ou experienciado (Setzer, 2015). O conhecimento seria uma estrutura cognitiva ainda mais profunda que a informação, de maneira que não poderia ser descrita ou representada. Nesta lógica, são os dados que estruturam a informação e essa, por sua vez, contribui para a construção do conhecimento.

Diante disso, cabe concluir que dado, informação e conhecimento estabelecem relação helicoidal. A sua formação não é estritamente cronológica, em que o dado materializa a informação e essa gera o conhecimento, como poderia se pensar sob uma perspectiva cíclica. Ao contrário, influenciam-se, sustentam-se e formam-se mutuamente, em um processo dinâmico e que envolve a constante socialização dessas três categorias. Afinal, o dado não poderá ser criado, a informação não poderá ser transmitida e o conhecimento não poderá ser estabelecido senão por meio dos processos comunicacionais entre pessoas.

Transpassando a literatura em CI, entende-se razoável abordar definições de "informação" e "dado" – dois conceitos imprescindíveis para a compreensão desta obra interdisciplinar – também dentro do Direito. Na área jurídica, tende-se a discutir e abordar esses conceitos de maneira mais superficial – pelo óbvio motivo de que é a Ciência da Informação que lida com essas definições de maneira mais aprofundada. Na Ciência Jurídica, levando-se em especial consideração o Direito nacional, percebe-se que há uma confusão entre as duas palavras, amplamente citadas por uma extensa gama de instrumentos legais.

Ao investigar o conceito do termo "informação" em leis federais brasileiras, Santos (2021) aponta a existência de nove dimensões conceituais da referida terminologia nesses documentos jurídicos, quais sejam, da mais reincidente à menos comum: informação como objeto (documento); como objetivo (de publicizar um fato ou ato); como valor (bem ou interesse a ser protegido); como contexto (campo de atuação de sistema ou de órgão que gerencia informações); como conceito qualificado (associada a adjetivos, como "falsa" e "pessoal"); como tecnologia (referindo-se a *softwares*, portais digitais e outras tecnologias que manejam informações); como espaço profissional (associado a qualificações profissionais, como "analista de tecnologia da informação" e "assistente de informações"); como fundamento (enquanto noção de publicidade e transparência de atos ou normas); como fonte (associada ao local em que a informação é produzida ou expressa). Diante de tantas dimensões conceituais, percebe-se certa imprecisão da palavra em seus diversos usos em diplomas legais, confundindo-se informação com outras fontes e processos que a envolvem mas não a identificam.

Apesar de a definição desse elemento de análise da CI não ser o objetivo da ciência jurídica, Santos (2021) compreende que a informação é um instituto jurídico (objeto de estudo do Direito e que tem importância para essa área), ainda que careça de boa definição normativa. A análise de dois dos mais importantes diplomas legais que tratam do tema na história recente do Direito nacional, a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), revela que "informação" chega a ser confundida com "dado". Para efeitos de sua aplicação, a LAI define informação como "dados, processados ou não, que podem ser utilizados para

produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato" (Brasil, 2011a, art. 4°, inc. I). Uma associação semelhante, mas em sentido contrário, é feita pela LGPD, que conceitua dado pessoal como: "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2018a, art. 5°, inc. I).

Quando a análise conceitual de "informação" se defronta com a de "dado", observa-se que o Direito tende a não fazer distinção entre as duas nomenclaturas, de modo que, por vezes, as trata como palavras sinônimas. Diferentemente, a Ciência da Informação considera tais termos como elementos distintos, como se o dado fosse uma espécie de matéria-prima da informação, ou a informação uma consequência gerada a partir de dados.

Para uma melhor coesão terminológica desta obra, que tem "dado pessoal" como um de seus fundamentais objetos de análise, é justo convencionar uma definição de "informação" e "dado" respeitando as essenciais contribuições da CI, mas sem negligenciar entendimentos conceituais já existentes nas leis. Assim sendo, considera-se informação como elemento abstrato transmitido entre indivíduos através da comunicação e que se transforma em conhecimento quando interage (consciente ou inconscientemente) com outras informações na mente (como valores, ideias, saberes anteriores etc.). Apesar de sua presença na cognição humana, a informação é, antes de qualquer coisa, elemento intrinsecamente social, pois é transmitido e/ou registrado no seio da coletividade. Isso não significa dizer, porém, que a informação deve ser sempre publicizada, pois, como se verá mais à frente, existem informações de cunho pessoal que são entidades tuteladas pelo direito individual à privacidade. Por sua vez, os dados são os registros físicos da informação (em formato analógico ou digital), que podem ser interpretados por humanos ou por máquinas (tal como é possível graças às modernas tecnologias da *Web* Semântica e da Inteligência Artificial).

Considerando as definições aqui apresentadas, cabe dizer, de antemão, que a definição de "dado pessoal" de acordo com a LGPD é errônea, pois o define como "informação relacionada a pessoa [...]" (art. 5°, inc. I). Contudo, dado não é informação em si, mas a carrega em um registro físico impresso ou virtual. Logo, em respeito ao entendimento construído até aqui, referir-se-á aos registros sobre pessoas naturais (pessoas físicas) como dados pessoais, ao passo que os conteúdos neles contidos serão nominados como informações pessoais.

3.2 Violação de dados pessoais e a garantia da privacidade

Antes de adentrar na discussão sobre a violação de dados pessoais, é preciso evidenciar a importância terminológica dessa expressão. "Dado pessoal" é uma expressão que diz respeito aos registros físicos, impressos ou digitais, que carregam informações sobre pessoas naturais determinadas (identificadas, como o nome completo de alguém) ou passíveis de identificação (identificáveis, como a data de nascimento e o número de identidade, que podem levar à identificação de seu titular quando cruzados). Com a ressalva da confusão entre dado e informação, a LGPD é bem sucedida em sintetizar um conceito de dado pessoal: "informação relacionada a pessoa natural identificada ou identificável" (art. 5°, inc. I).

Nessa acepção, o adjetivo “pessoal” leva à ideia de uma tipologia que toma como critério o ente referenciado pela informação registrada (semelhante a “dado empresarial” ou “dado público”, por exemplo). Como é aprofundado mais à frente, é possível extrair outras tipologias dentro da categoria “dado pessoal”, desde que se cumpram os requisitos de sua definição legal. Ou seja, dados de contato, dados médicos, dados escolares, dados bancários, dentre outros, não deixam de ser pessoais, desde que seu conteúdo se refira a pessoa natural identificada ou identificável.

Quanto à prática de registrar informações pessoais, vale dizer que essa já existe há muito tempo. Antes das revoluções industriais, muitas relações privadas se davam verbalmente e quando necessária alguma informação referente a uma pessoa, era fácil conseguir, pois os grupos sociais eram menores. A partir da industrialização, emerge a necessidade de registros sistematicamente organizados, o que permitiu o desenvolvimento da prática da documentação. É a partir do processamento de dados em computadores (especialmente em âmbito corporativo e domiciliar), já no final do século XX, que os registros eletrônicos se tornam mais acessíveis (Ruaro; Rodríguez, 2010).

O uso de dados pessoais é, atualmente, imprescindível para a manutenção e o desenvolvimento de variados setores da economia e da sociedade. No comércio, diante da crescente virtualização do setor com o chamado *e-commerce*, o armazenamento de dados pessoais de clientes agiliza a comercialização, além de permitir que os algoritmos das lojas virtuais ofereçam produtos adequados ao perfil do consumidor. Na prestação de serviços públicos ou privados, a gravação de dados facilita o acesso às informações pessoais, de modo a aperfeiçoar a realização daqueles, além de torná-los personalizáveis às necessidades de cada usuário. De igual maneira, o registro e o salvamento de dados pessoais têm utilidade para bancos e instituições financeiras, a exemplo do “cadastro positivo de crédito” (Miragem, 2019). Em âmbito estatal, já há casos de cadastro único de dados pessoais, que integram as informações das pessoas físicas entre os órgãos públicos, de modo a dirimir a burocracia, em âmbito federal, estadual e, em certas localidades, até mesmo na esfera municipal[1].

Quanto às tendências tecnológicas da sociedade informacional, também a “*internet* das coisas” (IoT, do inglês “*Internet of Things*”) aproveita dados pessoais (Law, 2020). A IoT consiste em um tipo de sistema de dispositivos distintos que se integram a uma mesma rede. Como exemplo, há as chamadas “casas inteligentes”, nas quais os aparatos eletroeletrônicos se conectam a uma mesma rede, podendo, por vezes, ser controlados de qualquer cômodo do imóvel, inclusive por celular ou *tablet*, como a tecnologia *Google Home*. Dados pessoais são bastante utilizados na IoT, especialmente informações cadastradas em seus sistemas ou dados de experiência de usuários inferidos por Inteligência Artificial. A expansão dessa tecnologia no mercado, graças à sua capacidade de adaptação, facilidade de manuseio e integração entre dispositivos, eleva o número de dados pessoais em fluxo entre produtos dessa natureza.

Também o imenso volume de dados em acelerado fluxo nas redes, chamado de *Big Data*, carrega consigo imensurável conjunto de informações pessoais (Law, 2020). O gerenciador da *Big Data* tem, em suas mãos, uma estrutura sistêmica que abrange o armazenamento, o controle e a utilização de informações. Com adequados

[1] Vejam-se, por exemplo, os sites do Governo Federal (https://www.gov.br/pt-br) e da Prefeitura Municipal de Sete Lagoas (http://ecidadao.setelagoas.mg.gov.br/).

sistemas de gerenciamento, é possível aproveitar dados pessoais (de forma lícita e até ilícita) para diversas atividades sociais e econômicas.

Dada a conjuntura acima apresentada, tem se tornado comum a ocorrência de fatos que prejudicam o pleno desenvolvimento social e econômico de indivíduos que possuem suas informações em bancos de dados. A venda de informações de usuários sem o consentimento e o vazamento de registros por negligência de seus armazenadores, por exemplo, são ilícitos comuns nesta seara. A seguir, alguns casos marcantes que denotam a importância da eficaz tutela de dados pessoais.

Em 2017, monitoradores de vazamentos de dados encontraram um arquivo com mais de um bilhão de credenciais e senhas de usuários de diversos *websites*, entre eles, da empresa de *streaming* de filmes e séries *Netflix* (Mathews, 2017).

Em 2018, os tabloides *The Guardian*, *The Observer* e *The New York Times* tiveram conhecimento de que a empresa britânica de comunicação estratégica *Cambridge Analytica* teve acesso a dados pessoais de milhões de usuários da rede social *Facebook*. Segundo as fontes jornalísticas, as informações particulares seriam usadas para construir estratégias eleitorais nos Estados Unidos. A eclosão do escândalo levantou questionamento sobre a segurança dos registros de atividades do usuário dentro da plataforma e, segundo a *The New York Times*, fez com que muitas pessoas, inclusive famosas, excluíssem suas contas da rede por medo (Confessore, 2018).

A estadunidense *Mariott International*, que possui um conglomerado de hotéis de luxo, foi vítima de um ataque cibernético, iniciado em 2014, mas que só foi percebido em 2018. Estima-se que, nesse ínterim, mais de 300 milhões de dados dos seus hóspedes tenham sido roubados, incluindo nomes, endereços de *e-mail*, números de telefone, informações de passaporte e registros de viagens dos seus clientes. Dentre os prejudicados, estima-se que se encontravam sete milhões de hóspedes no Reino Unido. Diante da morosidade da empresa em detectar a ação dos *hackers*, autoridades britânicas multaram a *Mariott* em 18,4 milhões de euros, em 2020 (Tidy, 2020).

No Brasil, o *site* de *e-commerce Netshoes* foi invadido por *hackers* que conseguiram acessar dados de quase dois milhões de clientes, em 2018. A investigação do caso chegou à conclusão de que informações bancárias não foram violadas, mas que nomes, números de CPF (Cadastro de Pessoas Físicas), endereços de *e-mail* e registros de consumo chegaram ao conhecimento dos invasores. A *Netshoes* foi responsabilizada pelo Ministério Público do Distrito Federal pela insegurança digital que permitiu o ataque (Netshoes [...], 2019).

Em janeiro de 2021, descobriu-se que 223 milhões de dados de brasileiros vivos e falecidos foram vazados em fórum on-line, sendo que o conteúdo violado foi colocado à venda. As informações dividiam-se em duas remessas: uma disponível gratuitamente, que continha nomes, números de CPF e de CNPJ (Cadastro Nacional de Pessoas Jurídicas), e outro conjunto de dados que agregava informações sobre renda das vítimas, cadastro da Previdência Social e de outros programas sociais (Megavazamento [...], 2021). No mês seguinte, um novo vazamento, que expôs informações da mesma natureza que o último, foi detectado pela *startup* brasileira *PSafe*. A empresa alega ter entrado em contato com os invasores, para investigar a situação, e diz ter descoberto que os dados tinham origem nas contas telefônicas das vítimas (Bolzani, 2021).

Assim, os fatos demonstram que o gerenciamento de dados pessoais exige trabalho delicado e minucioso, a fim de proteger as pessoas a quem as informações se referem contra quaisquer violações que possam ocorrer, especialmente no ambiente cibernético. No entanto, a proteção de dados pessoais é precedida por outra necessidade jurídica: a garantia da privacidade (que é o principal valor nos movimentos recentes pela proteção de dados pessoais). Como exercício dessa prerrogativa, é conferido ao cidadão o direito de controlar os dados relativos a ele, em um grau maior ou menor de acordo com os limites legais[2].

Nesse sentido, faz-se necessário, mesmo que de maneira breve, abordar alguns aspectos atinentes à privacidade, para que a formação do movimento jurídico pela proteção de dados pessoais, verificado em diversos países, torne-se compreensível. É fundamental compreender a evolução histórica dessa ideia até a sua normatização (que se aplica a diversos contextos, não apenas à proteção de dados). O ponto de partida da ideia de privacidade está, pode-se dizer, na Antiguidade Clássica, especialmente entre os gregos, que distinguiam a esfera pública (vivenciada na política) da esfera privada (experienciada no lar). Na Idade Média, também ocorre uma progressiva separação entre a convivência em comunidade (experimentada nos espaços comuns) e o recolhimento (no lar). Ao longo dos séculos, essa demarcação é reforçada com a dissolução do feudalismo e o surgimento da burguesia (Cancelier, 2017).

Enquanto garantia jurídica, o direito à privacidade tem como marco inicial o artigo *The right of privacy*, escrito pelos juristas Louis Brandeis e Samuel D. Warren, nos Estados Unidos, em 1890. Essa discussão baseava-se nas mudanças sofridas pelos Estados Unidos naquela época, que experimentavam as inovações tecnológicas daquele tempo, como a fotografia e a popularização da imprensa. Nesse ponto, chega-se à discussão da privacidade violada pela circulação desautorizada de imagens e nomes de pessoas em meios de comunicação daquela época. Esses estudiosos remetem à privacidade o "direito de estar só" (*right to be let alone*), resguardando a intimidade e a vida privada. A partir dessa lógica, a privacidade passa a importar para o Direito e se desenvolve enquanto garantia para todo cidadão. A Declaração Universal dos Direitos Humanos traz a seguinte ordem:

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques (Organização das Nações Unidas, 1948, art. 12).

No Brasil, a Constituição Federal de 1988 afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]" (Brasil, 1988, art. 5°, inc. X). De maneira semelhante, o Código Civil brasileiro proclama: "A vida privada

[2] O grau de controle de um indivíduo sobre seus dados pessoais pode variar de acordo com as circunstâncias da utilização do dado e do sistema jurídico. Na LGPD, por exemplo, há exigência do consentimento pelo cidadão para que um dado pessoal seja coletado e tratado em determinadas situações, ao passo que a anuência do indivíduo não é obrigatória em outros casos (a exemplo do tratamento de dados pelo Poder Público). O cidadão, contudo, não deixa de ter controle sobre seus dados de maneiras distintas, como por meio do direito de solicitar, ao agente de tratamento, informações sobre como o dado está sendo tratado.

da pessoa natural é inviolável [...]" (Brasil, 2002, art. 21). Vale dizer que todas essas terminologias (intimidade, honra, direito de imagem, vida privada), ainda que possam ter suas nuances conceituais, são espécies de uma mesma grande garantia: a privacidade (Cancelier, 2017).

Na contemporaneidade, com a propagação das tecnologias de informação, a privacidade torna-se garantia ainda mais relevante, devido aos próprios aspectos do espaço virtual (especialmente na *internet*). No meio digital, os dados pessoais são um dos grandes alvos de atos contra a privacidade, os quais são realizados tanto por ações abusivas do Estado, quanto por interesses econômicos e políticos de corporações privadas (Ruaro; Rodríguez, 2010).

Já na década de 1990, os chamados *cypherpunks* já falavam sobre os desafios envolvendo dados pessoais na virtualidade. Eles entendiam a privacidade como garantia de que "[...] cada pessoa revelasse somente o possível, devendo ter sua identidade preservada na rede, e somente revelada quando e somente quando for de seu desejo [...]" (Ferreira; Marques; Natale, 2018, p. 3120). Em *A Cypherpunk's Manifesto*, Eric Hughes (1993) defende a criptografia como meio para garantir essa proteção nas redes, a fim de evitar a exposição desautorizada de informações privadas.

Com os avanços tecnológicos mais recentes (inclusive a consolidação da *internet* que se popularizou no fim do século passado), essa garantia se torna ainda mais cara aos cidadãos. Diante da proteção de dados pessoais, o direito à privacidade está centrado na "possibilidade de cada indivíduo controlar o uso de informações que lhe dizem respeito" (Ruaro; Rodríguez, 2010, p. 180). Assim, nesse contexto, tal garantia não se dá apenas pela via jurídica, mas pela associação de três abordagens. São elas: a normativa, ou seja, a necessidade de normas que efetivem esse direito, a tecnológica, que envolve a adoção de medidas de segurança computacional, e a comportamental, que abrange a formação técnica, política e ética de pessoas e instituições que trabalham com dados pessoais (Keinert; Corrizo, 2018).

Resguardar informações pessoais é, para além de um ato de justiça individual, também um ato de justiça social, na medida em que busca minimizar a vulnerabilidade e o assédio que as diversas possibilidades de violação de dados (vazamentos, perdas/furtos de dados, exposições indesejadas etc.) podem acarretar. Nesse sentido, parte-se para a compreensão de como o assunto de proteção de dados vem sendo trabalhado no contexto mundial.

3.3 Normas de proteção de dados pessoais pelo mundo

Segundo dados recentes, dezenas de países em todos os continentes do globo já possuem legislação sobre proteção de dados. Destacam-se as potências econômicas mundiais, como China, Japão, Canadá e Estados Unidos, além do bloco da União Europeia. Entretanto, países emergentes também possuem suas normas sobre o tema, a exemplo de Brasil, Indonésia, Chile, Argentina e África do Sul. Muitas dessas legislações, inclusive a brasileira, foram inspiradas na recente norma europeia, a *General Data Protection Regulation* - GDPR (*Consumers International*, 2018).

A título de observação, nem todos os países apresentam uma única legislação sobre o tema. Pode acontecer de várias normas atinentes à privacidade e ao

uso de dados coexistirem e se complementarem dentro de um mesmo ordenamento jurídico. É o caso, por exemplo, dos Estados Unidos, onde há sedes de importantes empresas na área da tecnologia, como *Google*, *Apple*, *Microsoft*, *Facebook* e *Amazon*. Há, dentro do sistema normativo estadunidense, normas diversas que abordam a proteção de dados em alguns pontos dos seus textos, como a Lei de Modernização Financeira (1999), a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (1996) e a Lei de Privacidade (1974), que regula registros em agências federais. Entretanto, não há, no ordenamento jurídico estadunidense, qualquer norma geral sobre a matéria, como a GDPR europeia (Law, 2020).

Diante disso, verifica-se que há uma preocupação mundial em regular o uso de dados pessoais, de modo a convergir tal prática com o direito à privacidade. Essa demanda social, que tende a ser satisfeita mediante instrumentos jurídicos, aponta para a necessária tutela de dados pessoais não apenas em registros físicos, mas também no meio digital, que ultrapassa fronteiras nacionais. Deste modo, não só estados nacionais, mas organismos internacionais têm discutido e se preocupado com esse importante assunto.

Nessa toada, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou uma atualização das suas Diretrizes, em 2013, a fim de adequar-se às necessidades acerca do tema (*Organisation for Economic Cooperation and Development*, 2013). O texto apresenta orientações para a proteção de dados, destinando-se tanto à iniciativa privada, quanto ao âmbito público, a nível nacional e internacional. É destacável a segunda parte do documento, que estabelece princípios básicos para entrega, armazenamento e acesso a dados pessoais, cujos teores são: coleta limitada, qualidade dos dados, especificação das finalidades do uso, utilização limitada dos dados (nunca arbitrária), garantias de segurança, liberdade e participação individual do usuário e prestação de contas (*accountability*) pelas atividades de tratamento. Apesar de o Estado brasileiro ainda não fazer parte dessa organização, entende-se que os posicionamentos tomados nas suas diretrizes podem influenciar governos que não são membros dela, mas querem tornar-se, como é o caso do Brasil (Leme, 2019).

Outro contexto geográfico, a região da América Latina, apresenta, segundo Thomas Law (2020), um processo peculiar diante da necessidade de proteção de dados. Tem havido um confronto teórico-jurídico entre os princípios da privacidade e da transparência em relação ao acesso a dados pessoais, especialmente no âmbito das relações públicas.

Esse embate entre valores é causado, em parte, por causa da cultura jurídica reinante na América Latina e da instabilidade política em seus países. Ao passo que a privacidade é um princípio consagrado no Direito de várias nações ibero-americanas, as emergentes legislações de acesso à informação têm privilegiado a transparência dos dados (como meio de combate à corrupção, por exemplo). Assim, os dois axiomas parecem se contradizer e inviabilizar um consenso sobre a proteção de dados. Para Law (2020), o ponto de equilíbrio deveria ser o mais adequado, para que as novas leis sobre o tema fossem mais identificáveis às necessidades contemporâneas e mundiais. Em nosso entender, a sugestão do autor se encontra correta, na medida em que as necessidades de transparência informacional (como para repressão de ilícitos ou publicidade das ações dos governantes) não podem ser afastadas pela garantia à proteção de dados pessoais. Em sentido contrário, nem toda informação pessoal pre-

cisa ser exposta em nome da transparência das relações públicas (especialmente as informações relativas à intimidade do indivíduo). Ainda que esse não seja ponto relevante do nosso estudo, entende-se que o primoroso critério de justiça, tão importante ao Direito, deve ser o grande referencial para estabelecer os limites da privacidade e da publicidade em cada caso concreto.

Aliás, observa-se que, apesar da tensão entre esses princípios jurídicos, os países latinos começaram a promulgar suas legislações sobre a proteção de dados em meados dos anos 2000, colocando o princípio da privacidade como demanda da sociedade informacional e buscando equilibrá-lo com o axioma da transparência. O Chile publicou sua legislação acerca da temática em 1999. No ano seguinte, a Argentina fez o mesmo, inspirada no modelo europeu anterior à GDPR que havia à época (Law, 2020). O México seguiu pelo mesmo caminho, aprovando uma lei federal sobre a proteção de dados em 2010. Nesse ínterim, outros países da região também passaram a desenvolver suas normas sobre o referido tópico (Valente, 2018b). Ante os fatos apresentados, é perceptível que o sistema legal brasileiro também necessitou adequar-se às novas demandas sobre o assunto.

3.4 Proteção de dados no Brasil antes da LGPD

Apesar de a proteção de dados ter ganhado legislações próprias em países vizinhos, como Chile (1999) e Argentina (2000), no Brasil, a norma específica sobre esse tema (a Lei Geral de Proteção de Dados Pessoais, ou LGPD) só veio a ser publicada em 2018. Antes disso, apenas a Constituição Federal e outras leis, que não eram suficientes, traziam pontos que remetiam à tutela de dados pessoais.

Conforme apontado anteriormente, a Constituição da República Federativa do Brasil de 1988 (CRFB/1988) assegura a inviolabilidade de direitos relativos à privacidade, no seu artigo 5°, inciso X. Entretanto, até a Emenda Constitucional n° 115/2022, que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais, a Carta Magna não abordava a temática de forma explícita. Antes da LGPD e, mais especificamente, da referida Emenda, o regramento constitucional sobre a proteção de dados se restringia à garantia da privacidade, que tem aquela demanda jurídica como uma de suas facetas contemporâneas. Para além da Constituição, que é a lei fundamental do ordenamento jurídico brasileiro, cabe indicar outras normas anteriores à LGPD que remetiam ao tema.

O Código de Defesa do Consumidor (CDC – Lei n° 8.078/1990) trouxe algumas regras relativas a bancos de dados referentes a consumidores, como o dever de fornecedores em manter essas informações claras e o direito do cliente de ter conhecimento desse cadastro. Entretanto, a garantia prevista no seu texto é própria para relações de consumo. A lei aduz:

> O consumidor [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas (Brasil, 1990, art. 43).

No ano seguinte, promulgou-se a Lei de Arquivos (Lei n° 8.159/1991), que discrimina direitos e deveres relacionados a arquivos privados que recaem no poder de agentes públicos. Quem detivesse esse tipo de documento deveria cumprir exigências formais previstas na lei, para resguardar o conteúdo de suas informações e a satisfação do interesse público (Brasil, 1991, art. 11-16). Em 2002, o atual Código Civil brasileiro também aludiu à inviolabilidade da vida privada (Brasil, 2002, art. 21), tal como já foi apresentado anteriormente.

A Lei de Acesso à Informação (LAI – Lei n° 12.527/2011), apesar de ser voltada à transparência de dados públicos, também faz alusão à segurança de informações pessoais em alguns pontos. Como diretriz, diz-se que órgãos e entidades do Poder Público são responsáveis por garantir a proteção de informações privadas (Brasil, 2011a, art. 6°, inc. III). Em decorrência disso, é proibido aos agentes públicos ou militares "[...] divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal" (Brasil, 2011a, art. 32, inc. IV).

Na toada de garantia à privacidade, destaca-se a Lei Carolina Dieckmann (Lei n° 12.737/2012). Ela alterou o Código Penal para criminalizar a invasão de computadores voltada à adulteração e/ou à destruição de dados pessoais, ou ainda vulnerabilizar o aparelho para tirar-lhe vantagem ilícita (Brasil, 2012b).

Por sua vez, diante do surgimento do *e-commerce* nas últimas décadas, foi publicado o Decreto de Comércio Eletrônico (Decreto n° 7.962/2013), que obriga fornecedores a "[...] utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor" (Brasil, 2013).

Por fim, destaca-se o Marco Civil da Internet (MCI – Lei n° 12.965/2014), que definiu diversos direitos relativos à proteção de dados no ambiente *on-line*, visto que a matéria foi um dos principais pontos de debate quando do desenvolvimento de seu anteprojeto e da sua tramitação no Legislativo (Zanatta, 2015). Dentre as principais menções e regras, estão: proteção de dados pessoais como princípio do uso da *internet* no Brasil (art. 3º, inc. III); atividades virtuais cujos objetos são dados pessoais "devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas" (art. 10); proibição dos agentes de *internet* de fornecer dados pessoais a terceiros quando não permitido pelo titular ou pela lei (art. 7°, inc. VII); exigência de consentimento para coleta de dados pessoais (art. 7°, inc. IX) (Brasil, 2014).

3.5 A elaboração da LGPD

Diante da conjuntura social e jurídica aqui narrada, o deputado federal Milton Monti, do Estado de São Paulo, apresentou um projeto de lei (PL) que dispunha sobre

o tratamento de dados pessoais, no ano de 2012. A proposta foi identificada sob o n° 4.060/2012. A partir daí, o Congresso Nacional passou a se movimentar em prol do desenvolvimento de uma norma sobre a temática, tendo a proposta do parlamentar paulista como base. Na justificativa para a apresentação do projeto, o deputado apresentou reflexão que sintetiza a necessidade social da referida lei:

> O tratamento de dados é hoje uma realidade cada vez mais presente em nosso cotidiano, especialmente quando experimentamos o avanço da tecnologia da informação, em especial a internet e suas aplicações nas mais diversas áreas de nossa vida em sociedade. Até pouco tempo era inimaginável pensar nas aplicações e a interação que a internet teria em nosso dia-a-dia, ao mesmo tempo em que podemos imaginar que isso continuará em ritmo acelerado e de incremento, tendo em vista a velocidade em que novas tecnologias são desenvolvidas para a comunicação com as pessoas (Brasil, 2012a, p. 7).

Enquanto o PL n° 4.060/2012 ainda tramitava no Congresso, o Ministério da Justiça abriu espaço virtual de sugestões públicas que contribuíssem para o desenvolvimento do anteprojeto de uma nova proposta sobre proteção de dados pessoais, no ano de 2015. Segundo informações jornalísticas da Agência Brasil, na época, houve mais de mil contribuições (Peduzzi, 2015). A versão apresentada pelo Executivo chegou ao Congresso no ano seguinte, sob a identificação de PL n° 5.276/2016. A minuta do anteprojeto, que fora apresentada pelo Ministério da Justiça, afirma:

> A consolidação de um regime integrado de proteção de dados no Brasil mostra-se, assim, fundamental no ordenamento jurídico pátrio, de modo a possibilitar uma regulação integral do tema e a coesão de diversas iniciativas na área. Somente uma regulação geral assegurará a instituição de princípios harmônicos sobre o tema, proporcionando o controle dos riscos envolvidos no processamento de dados e assegurando o controle do cidadão em relação às suas próprias informações pessoais e, assim, garantindo a necessária segurança jurídica para a atividade empresarial e para a administração pública no tratamento de dados pessoais (Brasil, 2016, p. 22).

Assim como outros projetos de lei, que também tratavam sobre o assunto, o texto entregue pelo Executivo foi apensado ao PL n° 4.060/2012. À época da apresentação do PL do Ministério da Justiça ao Congresso Nacional, os textos sobre a matéria encontravam-se sob a apreciação da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI).

Em outubro de 2016, a Mesa Diretora da Câmara decidiu pela criação de uma Comissão Especial para a apreciação do projeto de autoria do deputado Monti. Em maio de 2018, após várias audiências para discussão da matéria (algumas promovidas pela CCTCI e outras pela Comissão Especial), o relator da comissão especializada, deputado Orlando Silva, deu parecer favorável ao prosseguimento do PL. Dali em diante, a proposta tramitou na Câmara até ser aprovada pelos deputados federais em 29 de maio de 2018. Chegando ao Senado Federal, sob a identificação de Projeto de Lei da Câmara (PLC) n° 53/2018, o texto passou pelos trâmites legislativos, como de praxe, e foi discutido pela Comissão de Assuntos Econômicos (CAE). No dia 10 de julho de 2018, o projeto foi aprovado pelos senadores, com alguns ajustes, e partiu para a sanção presidencial.

A cerimônia em que o então Presidente da República, Michel Temer, assinou a sanção da Lei n° 13.709/2018 (ou Lei Geral de Proteção de Dados Pessoais – LGPD) ocorreu em 14 de agosto do mesmo ano (Valente, 2018c). Apesar de o Chefe de Governo ter anuído com a maior parte do texto, parte do seu teor foi vetada. Dentre os objetos dos vetos, estava a previsão da criação de autoridade controladora do tratamento de dados pessoais. As razões do veto apoiavam-se na prerrogativa constitucional de que apenas o Presidente da República pode tomar iniciativa sobre lei que disponha sobre "criação e extinção de Ministérios e órgãos da administração pública" (Brasil, 1988, art. 61, §1°, II, item 'e') (Brasil, 2018b). Na ocasião, Temer prometeu a propositura de projeto de lei ou medida provisória que criasse o referido órgão. Diante da publicação da lei, o seu prazo para vigência foi alvo de críticas. Segundo o texto original, a norma entraria em vigor em 18 meses após ser publicada.

Nos últimos dias no cargo de Presidente, Temer editou a Medida Provisória (MP) n° 869/2018, criando a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além de propor algumas alterações ao texto original da lei (Accioly, 2019). Após passar pelos trâmites regimentais e submeter-se à discussão numa comissão mista (formada por deputados e senadores), a MP n° 869/2018 sofreu alterações em alguns pontos, podendo, enfim, converter-se em lei. Jair Bolsonaro, que sucedeu o posto da Presidência da República, sancionou parcialmente a norma (vetando algumas partes) em 19 de dezembro de 2019 (Valente, 2019a). A norma identificada como Lei n° 13.853/2019 alterou a Lei n° 13.709/2018 em alguns pontos e, finalmente, incluiu a ANPD em seu texto (Brasil, 2019).

Nos primeiros anos após a publicação da LGPD, houve intensa discussão sobre a data de entrada da sua vigência, debate que não nos interessa no escopo desta obra. Basta saber que essa norma está, atualmente, em pleno vigor. Além das regras dispostas na própria LGPD e suas alterações posteriores, o Decreto n° 10.474, publicado pela Presidência da República em 26 de agosto de 2020, regulamentou a estrutura da ANPD (Brasil, 2020a). Assim, essas normas, junto com a remissão do mesmo tema em outras leis, formam o sistema normativo que regula a tutela de dados pessoais.

Ainda que sejam muitos os países com legislações próprias sobre a matéria, destaca-se a *General Data Protection Regulation* (GDPR) como a principal inspiração da lei brasileira, como anteriormente apontado. A publicação da norma europeia em 2016 ressoou na elaboração da LGPD. Segundo Pinheiro (2020), aquele regulamento obrigava países que comercializassem com a Europa a se adequar às suas regras de proteção de dados, o que motivou os parlamentares brasileiros a definir regras bastante próximas da GDPR.

Dentre as semelhanças entre os dois regramentos, é possível citar: princípios para proteção de dados, previsão de sanções, regulamentação de autoridades nacionais de proteção de dados pessoais e imposição de critérios de segurança para a transferência internacional de informações (Iramina, 2020).

3.6 Características, fundamentos e princípios da LGPD

A Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) é uma lei geral, ou seja, é uma norma que se aplica a todo o ordenamento jurídico, não apenas a uma determinada área. Em outros termos, ela será o fundamento e a diretriz de outras normas de proteção de dados que vierem a surgir. Distingue-se das

normas especiais, que só podem ser aplicadas a uma situação bastante específica (Gonçalves, 2021). Logo, o grande destaque da LGPD no sistema legal brasileiro é o seu poder de aplicação sobre múltiplas situações, seja no setor público ou na iniciativa privada, o que faz com que seu campo de incidência seja bastante amplo.

A LGPD possui 65 artigos distribuídos em dez grandes capítulos, cada um agrupando certa temática concernente à matéria da lei. De acordo com Pinheiro (2020), essa lei busca satisfazer a necessidade de resguardar informações pessoais dos cidadãos, que se tornaram fonte de poder para as instituições a partir da consolidação digital. Ainda assim, a LGPD não se aplica apenas ao tratamento de dados em meios digitais, mas também em ambientes físicos (como documentos impressos). Observa-se que tratamento se refere a

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018a, art. 5°, inc. X).

Aragão e Schiocchet apontam que o conteúdo da LGPD pode ser dividido em cinco eixos (depreendidos da análise da norma):

> i) unidade e generalidade da aplicação da Lei;
> ii) legitimação para o tratamento de dados [bases legais];
> iii) princípios e direitos do titular;
> iv) obrigações dos agentes de tratamento;
> v) responsabilização dos agentes (Aragão; Schiocchet, 2020, p. 697).

No sistema dessa lei, os registros de informações pessoais são divididos em dois grandes grupos: dados pessoais (em sentido geral) e dados pessoais sensíveis (ou apenas "dados sensíveis"). A primeira categoria refere-se à "informação relacionada à pessoa natural identificada ou identificável" (Brasil, 2018a, art. 5°, inc. I). A segunda diz respeito a dados pessoais que, em razão do seu conteúdo informacional, são potencialmente discriminatórios à pessoa a quem o registro se refere (Mulholland, 2018). A LGPD cita alguns desses dados sensíveis em uma lista exemplificativa:

> [...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018a, art. 5°, inc. II).

Se, de um lado, há a figura do titular, que é a pessoa a quem o dado se refere (Brasil, 2018a, art. 5°, inc. V), do outro, estão os agentes de tratamento. Eles são o controlador e o operador, responsáveis pelas operações que têm dados pessoais como objeto. A LGPD define essas figuras:

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

> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Brasil, 2018a, art. 5).

Nos processos de tratamento, vale destacar os dados anonimizados, que passam por um processo em que se torna impossível a sua identificação (anonimização). Esse procedimento consiste na "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Brasil, 2018a, art. 5°, inc. XI). De acordo com o artigo 12 da lei, os dados anonimizados não se referem a pessoa alguma quando não puderem ser revertidos (não são dados pessoais), o que afasta a observância das exigências da LGPD. Entretanto, é interessante observar que existe preocupação com essa determinação legal, pois há tecnologias que conseguem revelar as pessoas a quem os dados se referem, de modo a colocar em risco a privacidade dos titulares dessas informações. Assim, a anonimização de dados deve ser rigorosa, de modo que não seja possível revertê-los a dados pessoais, passíveis de identificação do titular (Pinheiro, 2020).

A partir dessas definições primárias e da estruturação da norma, os direitos e deveres nas relações entre titulares (pessoas a quem os dados se referem) e agentes de tratamento (responsáveis pelos dados) são apresentados na LGPD. Nessa perspectiva, analisaremos, nas páginas a seguir, as principais regras da aludida lei. Para melhor compreensão do conteúdo, a ordem da análise não coincidirá, necessariamente, com o arranjo estrutural da norma.

3.6.1 Fundamentos e princípios

O primeiro artigo da LGPD delimita a sua função geral:

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

Primeiramente, endossa-se que a LGPD protege dados pessoais de pessoas naturais (ou seja, referentes a elas). Por pessoa natural (ou física), entende-se o próprio indivíduo, o ser humano. Assim, não é preocupação desta lei a tutela de informações referentes a pessoas jurídicas, como entidades públicas, empresas e outras instituições privadas.

Por outro lado, a lei deve ser observada por qualquer pessoa, seja física ou jurídica, que realize tratamento de dados pessoais de acordo com as regras de aplicação dos artigos 3° e 4°. O objetivo central é, portanto, garantir direitos fundamentais da pessoa natural, como a liberdade, a privacidade e o seu livre desenvolvimento.

Já no início do texto da lei, fica evidente o seu caráter principiológico, posto que ela é uma norma geral e serve como diretriz para outros regramentos que tratem de dados pessoais. O artigo 2° define fundamentos para a proteção de dados pes-

soais no Brasil, bastante inspirados pela GDPR (Pinheiro, 2020) e relacionados com o rol de direitos e garantias fundamentais previstos no artigo 5° da Constituição Federal (Brasil, 1988). Os fundamentos são os seguintes:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018a, art. 2°).

A listagem desses preceitos busca conceder equilíbrio às relações de tratamento de dados (entre titulares e agentes). Os incisos V e VI chamam atenção para a proteção econômica das instituições (especialmente empresas), ao mesmo tempo em que buscam garantir os direitos de privacidade aos cidadãos. Assim, a LGPD não quer prejudicar corporações, mas impõe que elas respeitem a segurança e a privacidade de informações pessoais. Esses fundamentos estão relacionados com o rol de direitos e garantias fundamentais previstos no artigo 5° da Constituição Federal (Brasil, 1988).

Tão importantes quanto os fundamentos, há os princípios para tratamento de dados pessoais, que possuem maior definição prática e também são estabelecidos com base nos direitos fundamentais constitucionais. No início do artigo 6°, que apresenta os princípios, cita-se a boa-fé, que não é conceituada, mas pode ser entendida como intenção honesta em relação ao tratamento de dados. O quadro seguinte apresenta as conceituações de outros princípios, conforme o artigo 6° da lei:

Quadro 1: Princípios das atividades de tratamento de dados pessoais

Princípio	**Definição**
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.

Princípio	Definição
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.
Responsabilidade 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, 2018a, art. 6°.

3.6.2 Aplicação da LGPD

Conforme já apresentado a partir da análise do artigo 1°, a LGPD regula direitos de pessoas naturais (na posição de titulares) e deveres de pessoas físicas ou jurídicas (enquanto agentes de tratamento) nas situações de tratamento de dados pessoais. Essa mesma separação está no *caput* do artigo 3°.

Para além da aplicação material da lei (isto é, em que tipo de situação ela é imposta – nesse caso, no tratamento de dados pessoais), há regras de aplicação territorial (onde a lei é aplicada). Quanto à territorialidade, segundo o artigo 3°, a LGPD será aplicada a operações:

i. realizadas no território nacional;
ii. cujos dados forem utilizados para o fornecimento de bens e serviços no Brasil ou se refiram a pessoas que estejam em território brasileiro;
iii. cujos dados sejam coletados no Brasil[3].

Assim, instituições estrangeiras podem ser obrigadas a respeitar a LGPD se o tratamento se enquadrar em alguma dessas hipóteses.

Logo, a regra geral do tratamento de dados deve se enquadrar em algumas das hipóteses previstas pelo artigo 3°, sendo que a pessoa natural é a figura a ser protegida e qualquer pessoa (física ou jurídica) que figure como agente de tratamento deve ser responsável por observar as regras da LGPD. Porém, mesmo que o tratamento satisfaça esses requisitos territoriais e materiais, há algumas exceções que afastam a aplicação da LGPD. De acordo com o artigo 4°, a lei não se aplica quando:

i. o tratamento for realizado por pessoa natural (pessoa física) para finalidades particulares e sem intenção econômica;
ii. os dados pessoais forem utilizados para fins exclusivamente jornalísticos, artísticos ou acadêmicos – neste último caso, exceto quanto à exigência de se enquadrar em algumas das bases legais dos artigos 7° ou 11;

[3] "Consideram-se coletados no território nacional [brasileiro] os dados pessoais cujo titular nele se encontre no momento da coleta" (Brasil, 2018b, art. 3°, §1°).

iii. dados forem utilizados para fins de grande interesse público, quais sejam, segurança pública e do Estado, defesa nacional, operações de investigação, atividades de repressão de infrações penais.

Outra hipótese de dispensa, prevista no inciso IV do mesmo artigo, está mais ligada à inaplicabilidade por questões territoriais:

> Esta Lei não se aplica ao tratamento de dados pessoais: [...] provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018a, art. 4°, inc. IV).

3.6.3 Bases legais

Além das regras para aplicação material e territorial da lei (conforme os artigos 1°, 3° e 4°), existem também as bases legais, que são hipóteses em que o tratamento de dados deve se enquadrar para ser legítimo (justificado, aceito pela lei). Elas estão previstas no artigo 7° (para dados pessoais, em geral) e no artigo 11 (em relação a dados sensíveis). Caso não incorra em pelo menos algumas dessas hipóteses (bases), o tratamento não poderá ocorrer (Mulholland, 2018).

Dentre as bases legais, uma das que mais se destaca e se discute é o consentimento do titular, que autoriza o agente a tratar os dados pessoais que lhes forem concedidos no momento da coleta. Ele está previsto tanto para informações pessoais em geral (art. 7°, inc. I) quanto para dados sensíveis (art. 11, inc. I). A LGPD define consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Brasil, 2018a, art. 5°, inc. XII). Assim, deve ser indubitável o conhecimento do cidadão sobre quais informações serão coletadas e qual será a finalidade do tratamento. Vícios de consentimento, como silêncio do titular ou erro (equívoco/engano) sobre o que seria feito com o dado, invalidam a sua anuência (Brasil, 2018a, art. 8°, §3°). Ademais, por ser uma base legal fundamentada na autonomia da vontade do titular, esse pode pedir a revogação do consentimento e, portanto, o encerramento do tratamento de seus dados (Brasil, 2018a, art. 8°, §5°).

A hipótese de coleta de dados por meio do consentimento possui regras especiais quando o titular das informações for criança ou adolescente. Nesse caso, segundo o artigo 14°, o consentimento deve ser dado por algum dos pais ou responsáveis pelo menor de idade (§1°). Dados de contato de seus responsáveis podem ser coletados sem o consentimento formal, desde que utilizados apenas uma vez e sem armazenamento desses dados (§3°). Alguns países europeus permitem que jovens consintam com coleta de seus dados a partir dos 16 anos. No Brasil, entretanto, ainda se entende que a regra deste artigo se destina a todos os menores de 18 anos (Pinheiro, 2020).

Além do consentimento, há outras bases legais. No artigo 7°, que trata das hipóteses de tratamento dos dados pessoais em geral, há dez justificativas de tratamento, dentre as quais é possível destacar:

a. quando for necessário para o cumprimento de alguma obrigação legal ou regulatória do controlador (inciso II);
b. para satisfação de políticas públicas em leis e regulamentos, por parte da Administração (inciso III);
c. para execução de contrato ou procedimentos contratuais, do qual o titular dos dados seja uma das partes (inciso V);
d. quando a coleta e o uso forem necessários para proteger a vida ou integridade física do titular ou de terceiros (inciso VII);
e. quando necessário para execução da tutela de saúde, mediante atividade de profissional da saúde ou de autoridade sanitária (inciso VII).

Quanto às hipóteses do artigo 11 (sobre dados sensíveis), percebe-se que há algumas bases semelhantes às do art. 7°, como a própria possibilidade de coleta por consentimento (art. 11, inc. I), para execução de políticas públicas (art. 11, inc. II, 'b') ou para tutela de saúde (art. 11, inc. II, item 'f'). Porém, devido ao seu potencial discriminatório e à necessidade de maior proteção, algumas hipóteses previstas no artigo 7° não constam nas bases legais dos dados sensíveis, como o tratamento para execução de procedimento previsto em contrato.

Outro destaque é a base legal do legítimo interesse (Brasil, 2018a, art. 7°, inc. IX), que não pode ser adotado para tratamento de dados pessoais sensíveis. Ele é um conceito aberto, que pode ser reputado como apropriado ou não de acordo com cada caso concreto (Pinheiro, 2020). De acordo com a LGPD:

> O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei (Brasil, 2018a, art. 10).

Assim, apenas dados estritamente relacionados com a legítima finalidade do controlador podem ser tratados sob essa hipótese. Um exemplo possível é a utilização dos dados pessoais de clientes para promoção de *marketing* do próprio negócio (Ferreira; Lima, 2021).

Ademais, o tratamento de dados sob alguma das bases legais não ocorre para sempre, mas deve ser encerrado quando verificada ao menos uma das hipóteses de término previstas no artigo 15 da lei:

i. quando a finalidade do tratamento for alcançada ou o dado não for mais necessário;
ii. fim do período pré-determinado de tratamento (se houver estipulação cronológica para tratamento);
iii. sob pedido de revogação do consentimento, quando o tratamento se deu com base nessa hipótese;
iv. quando determinado pela Autoridade Nacional de Proteção de Dados Pessoais por motivo de violação à lei.

3.6.4 Direitos do titular

Além das bases legais, que preveem a legitimidade para tratamento de dados pessoais (através do consentimento ou de outras hipóteses), existem direitos próprios do titular. Eles estão fundamentados na ideia de titularidade do cidadão sobre seus dados pessoais (Brasil, 2018a, art. 17), ou seja, cada pessoa é "dona" das informações que se referem a ela.

Os direitos do titular regulados pelo Capítulo III da lei são exercidos por meio de requerimento expresso (por exemplo, por escrito) do titular ou de seu representante legal (por exemplo, pai ou mãe), entregue ao agente de tratamento (Brasil, 2018a, art. 18, §3°). O retorno do agente acerca do pedido pode ser feito tanto por meio eletrônico, quanto por documentação impressa (Brasil, 2018a, art. 19, §1°).

O quadro a seguir apresenta os principais direitos dos titulares, junto com a remissão das passagens do texto legal que os regulamentam:

Quadro 2: Exemplos de direitos dos titulares

Direito	Previsão na lei
Confirmação da existência de seus dados pessoais em tratamento, por meio de resposta simplificada imediata ou certificação detalhada sob entrega em até 15 dias a partir do pedido do titular.	Art. 18, inc. I; art. 19.
Acesso aos dados, também por meio de resposta simplificada entregue imediatamente ou por certificação detalhada em até 15 dias.	Art. 18, inc. II; art. 19.
Correção de dados que estejam incompletos, desatualizados ou inexatos.	Art. 18, inc. III.
Dados desnecessários, excessivos ou tratados de forma contrária às exigências da lei podem ser anonimizados, bloqueados (suspensão temporária de tratamento) ou eliminados (encerramento definitivo do tratamento). O processo deve ser repetido por todos os agentes de tratamento com quem o primeiro controlador compartilhou os dados.	Art. 18, inc. IV, §6°; art. 5°, incs. XI, XIII, XIV.
Eliminação de dados que foram coletados sob a base legal do consentimento.	Art. 18, inc. VI.
Revogação de consentimento dado anteriormente, que não anula os tratamentos realizados antes desse pedido.	Art. 18, inc. IX; art. 8°, §5°.

Fonte: adaptado a partir de Brasil, 2018a.

Apesar da sua existência e importância, esses direitos possuem certas limitações. Uma das mais notáveis restrições a esses direitos é a permissão de conservação de dados pessoais, mesmo que verificada alguma das hipóteses para término de tratamento (previstas no artigo 15 da lei). De acordo com a LGPD, "os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades [...]" (Brasil, 2018a, art. 16). Porém, segundo o mesmo artigo, é permitido ao controlador conservar os referidos dados pessoais para satisfação dos seguintes fins:

> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (Brasil, 2018a, art. 16).

Portanto, ao passo que o descarte é um direito do titular, a conservação dos dados (em alguma das condições anteriormente citadas) é um direito do controlador. Porém, independentemente da hipótese para conservação, recomenda-se a anonimização dos dados sempre que possível, para fins de segurança (Pinheiro, 2020).

3.6.5 Controlador, operador e encarregado

Como já apresentado, os agentes de tratamento são aqueles responsáveis pelas operações cujos objetos são dados pessoais. São eles o controlador (pessoa física ou jurídica competente para decidir sobre as questões fundamentais do tratamento – como finalidade e quais dados serão tratados) e o operador (pessoa física ou jurídica que realiza o tratamento em nome do controlador e pode decidir sobre aspectos secundários do tratamento – como o *software* a ser utilizado no banco de dados).

De acordo com orientações da ANPD, o controlador é a pessoa física (natural) a quem interessa o tratamento ou uma pessoa jurídica, como empresa, instituição privada ou entidade pública. O operador pode ser uma pessoa contratada, uma empresa terceirizada ou até mesmo um comitê de especialistas que realizam o tratamento (Brasil, 2021b). Ele deve possuir certa autonomia em relação ao controlador, a qual é limitada pelas ordens fornecidas por esse. Por essa razão, de acordo com a ANPD:

> não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento (Brasil, 2021b, p. 7).

Os agentes de tratamento são responsabilizados pelos danos causados aos cidadãos em razão do descumprimento da lei. Esses danos podem ser de ordem patrimonial ou moral, contra um indivíduo ou um grupo de pessoas, o que implica no direito de indenização aos lesados (Brasil, 2018a, art. 42, *caput*). O operador responde junto com o controlador pelos danos, quando ele também descumprir as exigências legais ou não seguir as orientações lícitas dadas pelo segundo (Brasil, 2018a, art. 42, §1°).

Na averiguação de irregularidades, considera-se que o tratamento é irregular quando o agente de tratamento deixa de observar a lei ou não adota medidas de segurança que sejam esperadas pelo titular. Assim, critérios como o modo de execução das operações, resultados e riscos esperados, bem como técnicas de tratamento utilizadas, devem ser explicitados (Brasil, 2018a, art. 44). Nessa perspectiva, os agentes de tratamento não serão responsabilizados por danos quando não houver qualquer desrespeito à legislação de proteção de dados (incluindo LGPD e outras normas cor-

relatas) ou quando provado que o prejuízo foi causado por ação do próprio titular (Brasil, 2018a, art. 43).

Além do controlador e do operador, existe também a figura do encarregado (que, na GDPR, é chamado de *Data Protection Officer* ou DPO). De acordo com a lei, o encarregado trabalha como um canal de comunicação entre o controlador, a ANPD e os titulares dos dados (Brasil, 2018a, art. 5°, inc. VIII). Ele é indicado pelo controlador e deve ter suas informações de contato divulgadas, preferencialmente, no *website* do controlador (Brasil, 2018a, art. 41, *caput* e §1°).

O encarregado pode ser uma pessoa física ou jurídica, um funcionário ou comitê interno da instituição responsável pelo tratamento, terceirizados ou até mesmo robôs – pois não há definição quanto a isso na lei. Deve ter conhecimento multidisciplinar, dentre eles, da legislação de proteção de dados, de segurança da informação e de relações interpessoais. Seu trabalho inclui as seguintes quatro grandes áreas: atendimento de titulares de dados; relacionamento com autoridades legais (como a ANPD); apoio na adequação do tratamento à lei; intermediação de comunicação em caso de incidentes (Pinheiro, 2020).

3.6.6 Autoridade Nacional de Proteção de Dados Pessoais

A LGPD também prevê a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que, originariamente, era órgão federal ligado à Presidência da República e com autonomia técnica. Com a promulgação da Lei n° 14.460/2022, a ANPD foi transformada em autarquia de natureza especial. Na prática, as principais implicações com a mudança da natureza jurídico-administrativa da Autoridade são a conquista de autonomia administrativa e a garantia de patrimônio próprio (Brasil, 2022d). No que tange à sua atuação técnica, permanecem as mesmas funções institucionais previstas no texto anterior à Lei n° 14.460/2022, tais como: zelar pela proteção de dados no país, elaborar diretrizes, dar orientações, receber denúncias, fiscalizar agentes de tratamento, aplicar sanções, dentre outras competências (Brasil, 2018a, art. 55-J).

No âmbito da ANPD, encontra-se o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, composto por 23 representantes do Poder Público e da sociedade civil. Esse Conselho é responsável por auxiliar a ANPD a conhecer a realidade da proteção de dados pessoais no país, bem como propor as ações necessárias para a melhoria do setor, além de outras competências (Brasil, 2018a, art. 58-B).

A ANPD é inspirada nos modelos de autoridades estrangeiras de controle de dados, como há na Europa, em que cada Estado-membro possui sua autoridade nacional. Esse tipo de agente regulador já existe em centenas de países e pode ter atuação mais punitiva (voltada à repressão de violações de sanções) ou orientativa/fiscalizadora (que prioriza a educação e promoção da cultura da privacidade, colocando as sanções em segundo plano). Esse segundo é o modelo mais próximo da Autoridade brasileira (Pinheiro, 2020).

De acordo com Pinheiro (2020), a existência de uma Autoridade Nacional (com funções orientativa, fiscalizadora e sancionadora) implica na mudança de alguns pontos da cultura informacional nas organizações, a saber:

. As instituições passam a verificar se os dados pessoais em seus bancos internos estão em conformidade e em volume estritamente necessário para satisfação de suas necessidades; se os titulares estão cientes da coleta e das finalidades; se o uso de informações está adequado às finalidades do tratamento.

. Exclusão de dados pessoais cujas circunstâncias de coleta e tratamento não estejam de acordo com a norma (coleta sem devido consentimento ou fora de alguma base legal, tratamento fora das finalidades informadas, etc.).

. Identificação e análise de seus próprios bancos de dados, para conhecer seu conteúdo, seus usos e suas finalidades.

. O titular passa a ser a figura de protagonismo no tratamento de seus dados pessoais, devendo o controlador prestar contas do que faz com eles (sempre que a lei o exigir ou permitir).

3.6.7 Sanções administrativas

Apesar da sua postura mais orientativa/pedagógica, a LGPD atribui à ANPD o poder de aplicar sanções administrativas pelo descumprimento às regras de proteção de dados pessoais. São chamadas de "sanções administrativas" pois são penalidades aplicadas em processo administrativo conduzido pela ANPD, em que se verifica a existência da ilicitude, sua gravidade, além de outras circunstâncias do caso concreto, como condição econômica do controlador, verificação de má-fé, reincidência etc. (Brasil, 2018a, art. 52). Assim, a sanção deve ser proporcional ao ato ilícito verificado e às suas circunstâncias. As possíveis sanções, desde a menos grave até a mais dura são as seguintes (Brasil, 2018a, art. 52, inc. I-XII):

. Advertência, com estipulação de prazo para correções na conduta do processado.

. Multa simples (aplicada em uma taxa única), com valor de até 2% do faturamento anual da instituição (controladora) responsável, limitadas ao valor de R$50.000.000,00 (cinquenta milhões de reais) por cada infração.

. Multas diárias, no mesmo limite financeiro das multas simples.

. Publicização da infração.

. Bloqueio (temporário) dos dados pessoais até que a situação se regularize.

. Eliminação dos dados pessoais a que a infração se refere.

. Suspensão (parcial ou não) do banco de dados envolvido, por até seis meses, até a regularização das atividades de tratamento. Pode ser prorrogada pelo mesmo período da primeira suspensão.

. Proibição parcial ou total do tratamento de dados.

Como as entidades públicas também são obrigadas a se adequarem à norma, a ANPD deve informar violações da lei à instituição do Poder Público que as cometer. O comunicado deve apresentar as medidas cabíveis para fazer cessar os ilícitos. Por outro lado, às entidades públicas não serão aplicadas penalidades de multa (Brasil, 2018a, art. 31; art. 52). O impedimento das chamadas sanções pecuniárias (multas) às entidades públicas não impede, porém, que elas sejam judicialmente responsabilizadas e obrigadas a pagar indenização a titulares ou terceiros por danos materiais ou morais decorrentes do tratamento irregular de dados pessoais.

3.6.8 Benefícios e desafios da adequação à LGPD

Diante da promulgação da Lei Geral de Proteção de Dados, o sistema jurídico nacional encontra sustentação em uma norma que dispõe sobre os direitos e deveres dos titulares de dados e os agentes de tratamento. Quanto à ANPD, destaca-se que ela já está em funcionamento, tratando principalmente da elaboração de diversas orientações (especialmente em forma de guias) para que os destinatários da respectiva lei consigam proteger dados pessoais em diferentes circunstâncias.

Como dito anteriormente, outra inovação recente no ordenamento jurídico em relação ao assunto foi a constitucionalização da proteção de dados, isto é, o tema passou a ser tratado como direito fundamental no artigo 5° da Constituição Federal, através da Emenda Constitucional n° 115/2022. Ademais, a Emenda define que é competência privativa da União a organização e a fiscalização da proteção de dados, cabendo apenas a ela legislar sobre esse tema (Brasil, 2022d). A intenção dessa mudança é criar um sistema de proteção de dados pessoais coerente em todo o território nacional, para que agentes de tratamento não tenham que despender recursos para se adequar a regras específicas em cada região do Brasil.

Dessa maneira, espera-se que a LGPD cause impacto positivo às relações previstas no seu texto. São numerosos os benefícios que podem ser promovidos quando da aplicação dessa legislação às relações jurídicas que envolvam tratamento de dados pessoais. A positivação do direito de consentir com o tratamento de dados, por exemplo, é uma das regras que visam o respeito à privacidade e à liberdade individual. A necessidade de anuência para que o usuário tenha seus dados coletados, de maneira esclarecida sobre quais informações seriam acessadas e a finalidade do seu tratamento, exigida em determinados casos, é uma das regras que consagra o direito à privacidade, o qual é prerrogativa constitucional.

Os benefícios para o consumidor também são diversos, visto que a problemática de proteção de dados vinha se tornando crescente, diante da propagação dos cadastros de consumidores em lojas e o crescimento do *e-commerce*. Assim, os consumidores podem gozar das garantias abordadas pela norma. O mesmo vale para usuários de serviços públicos, nos limites das numerosas disposições apresentadas pela lei quanto ao tratamento de dados pelo Poder Público (Brasil, 2018a, art. 22-32).

Entretanto, o regime de normas constituídas pela LGPD não é prejudicial ao controlador de dados. Na verdade, diante dos recorrentes casos de escândalo por vazamento de informações de usuários (como em *websites* e até nos chamados serviços "presenciais"), as empresas e instituições que se adequarem às normas de proteção de dados podem vir a gozar de credibilidade perante a sociedade (Vasconcelos, 2020). Além disso, há regras da lei que também podem ser benéficas aos agentes de tratamento de dados, a exemplo da possibilidade de utilizar informações com base em legítimo interesse. Assim, ainda que os controladores de dados precisem se adequar às novas regras sobre a matéria, vale destacar que a LGPD não foi criada para prejudicar qualquer das partes, mas para assegurar uma relação jurídica justa e que seja vantajosa para ambos os lados.

Apesar disso, faz-se importante uma observação crítica de possíveis entraves da LGPD frente aos monopólios (ou oligopólios) de informações. Ainda que essa norma institua mecanismos que procurem extinguir (ou, ao menos, mitigar) os riscos

envolvendo o tratamento de dados pessoais em diversos ambientes possíveis, é importante tecer uma crítica quanto à concentração de informações pessoais por parte de certas instituições, fenômeno constituído por ocasião do poder econômico de organizações tanto públicas quanto privadas.

Um dos clássicos exemplos de concentração de dados referentes a cidadãos é o caso de um censo alemão ocorrido na década de 1980, no apogeu do Estado Social, em que o governo germânico buscou levantar informações demasiado íntimas sobre as pessoas (como suas opiniões políticas ou religiosas). Aliás, naquela circunstância, o Tribunal Constitucional Alemão suspendeu a realização do censo e decidiu sobre a existência da autodeterminação informativa enquanto prerrogativa do poder do cidadão sobre seus próprios dados (Ruaro; Rodríguez, 2010).

Entretanto, contemporaneamente, tal discussão volta à tona com o advento e a consolidação das grandes corporações (especialmente as *big techs*, como *Google* e *Facebook*), que, ao trabalharem com TICs, coletam e produzem dados referentes aos seus consumidores e, até mesmo, a terceiros. As informações auferidas permitem que essas corporações entendam os interesses e demandas de seus clientes.

Esse fenômeno econômico gera monopólios (ou oligopólios), que, diferente do contexto estatal alemão do século passado, são pautados, principalmente, em poder de concentração informacional por instituições privadas, isto é, empresas. Na lógica econômica dos fluxos informacionais em *big techs*, por exemplo, os monopólios/oligopólios se formam pela concessão dos dados pessoais do cliente à empresa. Para o usuário, fornecer seus dados pessoais a apenas uma corporação de tecnologia (ou poucas delas), para a utilização de cada serviço, facilita a sua vida e diminui custos (não apenas financeiros, mas também de tempo) com a portabilidade desses dados. Para as empresas, as informações contidas nos dados coletados servem como subsídio para que algoritmos desenvolvam estratégias para aumentar o faturamento do negócio, como por meio de venda de anúncios direcionados em motores de pesquisa e em redes sociais (Santos; Schimitt, 2021). Assim, utilizam-se das potencialidades de suas TICs para extrair o máximo de valor dos dados.

O problema se assenta na concentração exagerada de informações pessoais, que gera uma relação assimétrica em que a empresa monopoliza dados, ao passo que o titular não detém poder sobre eles, ainda que o consentimento formalize tal finalidade. Estabelecer uma relação extremamente vantajosa para si é de interesse desse tipo de corporação:

> A assimetria informacional é fundamental para a lucratividade desse negócio, pois é necessário retirar do usuário/titular o poder de processar dados de forma complexa, restringindo assim seus domínios ao aceite dos termos de serviço (consentimento), o qual, quando livre e devidamente informado, não sana a questão estrutural de estratificação, caracterizada, de um lado, pela capacidade de gerir inteligências artificiais complexas e em tempo real, além do contingente humano empregado [...] (Fornasier; Knebel, 2021, p. 1022).

São vários os casos em que o poderio das empresas que concentram grandes volumes de dados pessoais fica evidente. Um deles, anteriormente mencionado, é o da *Cambridge Analytica* e do *Facebook*, em que aquela empresa de *marketing* político se aproveitou de dados de usuários dessa rede social para compreender e

direcionar opiniões que influenciassem o público em relação às eleições estadunidenses de 2016 (Confessore, 2018). Nessa perspectiva, questiona-se até onde as regras de leis de proteção de dados, como a LGPD, são efetivas para afastar os riscos à concentração de informações pessoais. É possível traçar dois grandes pontos de vulnerabilidade da norma, além de outros, no que tange a essa problemática, quais sejam: a fragilidade do consentimento de titulares e a limitação de sanções administrativas frente à capacidade econômica dessas corporações.

Tal como enfatizado anteriormente, o consentimento trata-se da base legal (talvez) mais discutida e celebrada, funcionando como instrumento formal para que o titular concorde com o tratamento de dados propostos para as finalidades pleiteadas pelo controlador. Assim, é uma manifestação "livre, informada e inequívoca" (Brasil, 2018a, art. 5°, inc. XII) que se pauta na autonomia da vontade do titular e pode, inclusive, ser revogada por ele.

No entanto, ainda que seja importante a existência do consentimento, base legal bastante utilizada nas relações de consumo, ele pode ser levantado como argumento para que os monopólios/oligopólios informacionais sejam formados (Santos; Schimitt, 2021), já que a vontade do titular se mostra respeitada, ao menos sob uma perspectiva jurídico-formal. Porém, o que ocorre é que o próprio monopólio (ou oligopólio) econômico de grandes empresas (especialmente *big techs*) condiciona a escolha dos consumidores aos mesmos serviços, o que também gera o monopólio/oligopólio informacional, como indicam Fornasier e Knebel:

> O consentimento como afirmação dos direitos relativos aos dados digitais possui uma natureza controversa, justamente porque intenta consagrar liberdade e autonomia privada em um cenário de profunda desigualdade na gestão de dados — tendo em vista a assimetria de infraestrutura e conhecimento acerca da ciência de dados e da interpretação de dados massivos na era do big data — principalmente no que se refere ao mais recente aprendizado de máquinas e inteligência artificial (Fornasier; Knebel, 2021, p. 1018).

Na toada da discussão acerca dos limites fáticos (metajurídicos) do consentimento, ainda há o problema relativo à legitimidade das finalidades apresentadas pelo controlador. Devido às tecnologias avançadas (como algoritmos e computadores superpotentes) e os grandes volumes de dados pessoais à disposição dessas corporações, há risco de que as informações coletadas sejam utilizadas para fins escusos, que não podem ser detectados pelo usuário. Ainda que o usuário exerça seu direito de requerer informações sobre o andamento do tratamento nos termos do artigo 9° da LGPD, não se pode assegurar que o controlador concederá o registro verídico e completo das atividades, de modo a ocultar a existência de operações que ofendam a autodeterminação informativa dos titulares (como ocorreu no caso entre a *Cambridge Analytica* e o *Facebook*).

Outra limitação da LGPD quanto à proteção de dados na concentração de informações deve-se às possíveis sanções previstas pela lei. A multa, enquanto penalidade mais discutida, possui a quantificação pecuniária no limite de cinquenta milhões de reais, o que é um valor nada impactante para grandes empresas que faturam bilhões ao ano (como *Amazon*, *Apple* e *Microsoft*). Nesse sentido, a violação às regras da LGPD (como a utilização de dados para fins ocultos) pode envolver práticas que

incorrem em riscos financeiros que não têm impacto profundo sobre o comportamento desses controladores, de modo que a ilicitude acaba se tornando rentável (mesmo que tenha que se pagar um "preço" por isso, a título de multas). Outras penalidades mais graves, como bloqueio do tratamento até a regularização ou a definitiva eliminação dos dados violados (Brasil, 2018a, art. 52, inc. V-VI), podem ser arguidas como prejudiciais a empresas que possuem a informação pessoal como um de seus ativos mais importantes.

Nesse sentido, sob uma perspectiva mais crítica, pontua-se que o consentimento, apesar da sua importância, não é um exercício de liberdade plena na realidade (ainda que o seja juridicamente), visto que há condicionamentos econômicos, sociais e informacionais que instigam uma grande massa de consumidores a concederem seus dados a uma mesma empresa, gerando monopólios de informação. Ademais, outra limitação da LGPD se assenta no limitado valor de multas previstas, o qual não coíbe a prática de ilícitos que tenham retorno financeiro a grandes corporações e, assim, não se mostra como penalidade efetiva. Apesar de o tratamento de dados pessoais em âmbito das *big techs* não ser objeto deste estudo, fato é que o seu exemplo evidencia certas fragilidades da LGPD frente às configurações econômicas, jurídicas e institucionais que permeiam a sociedade informacional, tal como aqui discutido.

4

Compliance em LGPD: uma visão pragmática da proteção de dados

A adequação às regras da LGPD pelas organizações que tratam dados constitui-se como um dos grandes desafios (ou, talvez, o maior) para efetivação da aludida lei, visto os encargos materiais, intelectuais, de tempo e de energia que envolvem mover toda uma instituição em prol da implantação daquelas exigências normativas. Entretanto, não há alternativa que exima agentes de tratamentos de observar a lei e aplicar as necessárias medidas técnicas e administrativas para a sua implantação[1]. Como já apresentado, as pessoas físicas ou jurídicas (de direito público ou privado) que operam dados pessoais nos termos do artigo 3° da LGPD, salvo aquelas exceções apontadas no artigo 4°, devem se adequar à lei.

Nesse sentido, surge a ideia de *compliance* em LGPD (também chamado *compliance* de dados pessoais ou *compliance* em proteção de dados). Do verbo inglês *comply* (adequar-se, cumprir, observar norma), o substantivo *compliance* diz respeito a um "conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade" (Frazão, 2007 *apud* Frazão; Oliva; Abílio, 2019, p. 683-684). Assim, o *compliance* compreende um corpo de mecanismos, preferencialmente organizados em etapas, do qual dispõe uma organização (seja pública ou privada) para adequar-se a uma demanda regulatória.

Os programas de *compliance* surgem da ideia de que apenas o poder punitivo estatal não é suficiente para coibir tais ilicitudes perpetradas por corporações, de modo que é necessário que essas adotem práticas para complementar a regulação do Estado. Por isso, fala-se de uma "autorregulação regulada", isto é, autoadequação a exigências normativas a partir do que o agente normatizador (geralmente o Estado) orienta. Trazendo para o campo da LGPD, a título de ilustração: a Lei dá as diretrizes sobre como dados pessoais devem ser protegidos e a ANPD orienta/normatiza sobre questões mais específicas, enquanto os agentes de tratamento formulam e executam medidas necessárias para cumprimento daquele regramento.

Nessa toada, o presente capítulo explora propostas de ações e ferramentas para *compliance* de dados pessoais, de acordo com estudos na literatura especializa-

[1] Apesar de a LGPD não fazer distinção entre as medidas técnicas e as administrativas, a nosso entender, as primeiras estão mais voltadas a ações de segurança computacional (como antivírus e senhas de segurança) e as segundas à garantia da privacidade por meio de ações gerenciais (como limitação do número de funcionários a ter acesso a determinado dado pessoal). Em última instância, não há como separar medidas técnicas e administrativas (assim como também não é possível fazê-lo entre ações de segurança e privacidade). São instâncias interdependentes, que chegam a se confundir em muitas situações no processo de *compliance*. Por isso, o caminho aqui escolhido é citá-las em conjunto, como se fossem uma só.

da e nos Guias Orientativos da Autoridade Nacional de Proteção de Dados Pessoais. Diante da literatura analisada acerca da temática, entende-se que essas ações podem ser divididas nos seguintes passos.

4.1 Definição de funções e conscientização da instituição

O primeiro passo para adequação de uma organização à LGPD é a conscientização da sua alta gerência sobre as mudanças que precisam ser feitas e dos investimentos (material, de pessoal e de tempo) que precisam ser tomados, dentro de suas possibilidades financeiras (Pohlmann, 2019). Deve-se conhecer o impacto do programa de *compliance* para a legalidade do tratamento de dados pessoais na instituição, além de tomar consciência de que é necessária a continuidade de medidas para observância da lei mesmo após a execução inicial das ações de segurança e privacidade de dados. Afinal, adequar-se à LGPD é uma demanda constante de qualquer operação de tratamento de dados pessoais (Maroso, 2020).

Igualmente, é importante que, desde o primeiro momento de planejamento e execução de *compliance* em proteção de dados, os colaboradores de todos os setores da instituição (especialmente aqueles que tratam diretamente com dados pessoais, como setores de recursos humanos, de contratos, atendimento ao público etc.) tenham conhecimento da lei e do programa que será executado, ainda que, por ora, de maneira superficial. À medida que o programa de *compliance* for executado, essas pessoas podem ser convocadas pela equipe de implantação da LGPD a colaborar com o diagnóstico do fluxo de dados na organização e a implantação de medidas técnicas e administrativas de segurança e privacidade, conforme será detalhado mais à frente. Ainda nesta etapa, é fundamental a definição de funções no programa de implementação da lei (Maroso, 2020). Deve-se definir quem é o controlador e quem é (ou quem são) o(s) operador(es) de dados no âmbito da organização, à luz do que define a LGPD e do que orienta a ANPD.

Por força da lei, deve-se nomear (ou contratar) um encarregado de dados (DPO). O Guia de Elaboração de Programa de Governança em Privacidade da ANPD traz alguns apontamentos sobre o papel do encarregado no início do processo de *compliance* de dados[2]. Esse deve se enquadrar na definição de DPO prevista na LGPD, devendo ser um profissional multidisciplinar, com a devida competência para exercer as funções que lhes são atribuídas e que goze de independência técnica para a execução dessas. O encarregado precisa ter o apoio das unidades administrativas da instituição, ter acesso aos processos da organização e instruir os responsáveis pelo tratamento de dados sobre riscos que possam ser corrigidos (Brasil, 2020a). Autores como Kohls, Dutra e Welter (2021) sugerem, além disso, a nomeação de equipe de apoio ao DPO, para que ele possa exercer melhor a sua função precípua de ser canal de comunicação entre as várias partes no tratamento de dados pessoais (controlador, operadores, titulares, ANPD etc.).

[2] Apesar de esse Guia Orientativo (não vinculante) publicado pela Autoridade em 2020 destinar-se especialmente a órgãos da Administração Pública Federal, a nosso entender, também pode ser aplicado a entidades privadas (como empresas) e entidades públicas municipais, estaduais e distritais, com os devidos ajustes à sua realidade. O mesmo se aplica a outros Guias da ANPD também utilizados neste estudo, como o Guia de Elaboração de Inventário de Dados Pessoais (Brasil, 2021a) e o Guia Orientativo para Definições dos Agentes de Tratamento de Dados e do Encarregado (2021b; 2022a).

4.2 Análise de maturidade da organização em relação à proteção de dados pessoais

De acordo com Pohlmann (2019), é preciso conhecer o contexto da instituição, sua estrutura e seus processos para entender quais seus reflexos no fluxo de dados pessoais. De forma ampla, o que Pohlmann (2019) essencialmente propõe é estabelecer um panorama geral dos processos da organização para, assim, conhecê-la e analisar a sua maturidade em relação à proteção de dados pessoais. Para tanto, sugere-se a análise de elementos que compõem o fluxo de dados da instituição e as medidas de segurança informacional a ele relacionados. Dentre esses elementos, o autor cita: páginas *Web* (ou *intranet*), *e-mails* internos e externos, colaboradores, rede *wi-fi*, serviços de nuvens, operadores de tecnologia de informação envolvidos, procedimentos de segurança de informação, procedimentos bancários e financeiros, contratos e convênios, clientes, fornecedores e terceirizados. De acordo com o Guia de Elaboração de Programa em Governança de Privacidade da ANPD (2020), a análise de maturidade envolve a verificação da existência de medidas com finalidade de segurança e privacidade de dados, como rastreabilidade de dados, canal de comunicação com o cidadão, política de privacidade, termos de uso de serviços, dentre outros. Aqui, também se pode citar a sugestão de Maroso (2020) de criar um inventário de ativos informacionais (computadores, impressoras, redes e demais máquinas e sistemas que produzam informações), assim como verificar o modo que a rede de computadores de uma instituição está organizada. Ainda nesta fase, pode-se registrar o planejamento (*roadmap*), ainda que provisório, de quais serão os passos seguintes no processo de *compliance*.

4.3 Registro de operações de tratamento de dados pessoais

Esta fase consiste no registro de operações de dados pessoais, que é um dos deveres dos agentes de tratamento, de acordo com o texto da LGPD: “O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse” (Brasil, 2018a, art. 37). Entende-se que essa atribuição pode ser delegada à equipe de *compliance* da instituição, ainda que formada por funcionários ou colaboradores que estejam sob poder diretivo da pessoa jurídica controladora dos dados. Juridicamente, nesse caso, por instruir seus colaboradores e/ou a equipe de *compliance* a registrar as operações de tratamento, o agente de tratamento não deixa de estar cumprindo com tal dever. Mais do que uma obrigação legal, o registro das operações de tratamento é uma maneira efetiva de conhecer os processos informacionais na organização para aplicar as medidas mais adequadas à privacidade e segurança de dados.

Para Furtado (2020), o dever de registro das operações com dados pode ser executado por meio destes processos possíveis: mapeamento de dados (*data mapping*) e/ou descobrimento de dados (*data recovery*), sendo a primeira a mais conhecida e realizada nas ações de *compliance* de dados pessoais. Assim, o registro torna-se “[...] a compilação estruturada de informações relacionadas às operações de tratamento de dados pessoais [...]” (Furtado, 2020, p. 87). O autor apresenta as seguintes definições para cada um desses processos:

> [...] o *data mapping* pode ser definido como uma atividade de catalogação de todo o fluxo de dados pessoais que são objeto de qualquer operação de tratamento (coleta, uso, armazenamento, compartilhamento e eliminação) por uma organização, bem como os seus principais elementos (quais são os tipos de dados, formato, finalidade, base legal, localização, etc.). O *data mapping* é realizado mediante entrevistas ou preenchimento direto de formulários (*self-assessment*) (Furtado, 2020, p. 87-88).
>
> [...] o *Data Discovery* pode ser definido como um processo realizado a partir da combinação de ferramentas e processos de *software*, com objetivo de identificar quais são os dados objeto de tratamento pela organização, seja aqueles armazenados em suas instalações, ou na nuvem, em redes de parceiros e repositórios externos, ou nos dispositivos pessoais de sua equipe. Essas ferramentas podem identificar quaisquer dados mantidos em qualquer formato, como documentos, apresentações e *e-mails* (Furtado, 2020, p. 88).

Apesar das duas possibilidades, a literatura especializada dedica seus estudos mais ao mapeamento de dados do que ao outro procedimento. Para Pohlmann (2019), o mapeamento de dados é uma das primeiras etapas para implementação da LGPD. Organizam-se as informações pessoais em fluxo na instituição de acordo com categorias representativas de diferentes aspectos do tratamento de dados. A despeito de sua importância para conhecer os processos informacionais na instituição e implantar adequadas medidas técnicas e administrativas de proteção de dados, realizar o mapeamento não é tarefa fácil. Ao contrário, exige maior esforço da equipe de implementação da LGPD (Maroso, 2020).

Enquanto outros autores entendem que o mapa é produto (não mero processo), Furtado (2020) considera que o mapeamento de dados (ou descobrimento de dados) é o procedimento instrumental para se chegar ao registro de tratamentos em formato de inventário de dados pessoais. O Guia de Elaboração de Inventário de Dados Pessoais da ANPD segue raciocínio semelhante, ao compreender o inventário de dados como o resultado do processo de mapeamento das operações de tratamento de dados (Brasil, 2021).

4.4 Relatório de impacto de proteção de dados pessoais

Depois de criado o mapa de dados, é interessante a conseguinte elaboração de um relatório de impacto de proteção de dados pessoais (RIPD), que é um instrumento de avaliação dos riscos que envolvem o tratamento de dados pessoais para implementar adequadas medidas de segurança e privacidade informacional. Eventualmente (ou em determinadas hipóteses de acordo com possível futura regulamentação dessa temática pela ANPD), a Autoridade pode exigir que o controlador lhe apresente RIPD, especialmente quando o tratamento envolve questões mais caras à privacidade de titulares, como dados sensíveis e base legal de legítimo interesse (Brasil, 2018a, art. 10, §3°; art. 32; art. 38). A LGPD o define como

> documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Brasil, 2018a, art. 5°, inc. XVII).

Não se pode, porém, confundir o registro de operações de tratamento de dados com o RIPD:

> Enquanto o registro das atividades de tratamento de dados pessoais se presta a meramente documentar os processos relacionados ao tratamento de dados pessoais, o relatório de impacto à proteção de dados pessoais apresenta um foco específico no mapeamento dos riscos decorrentes da atividade de tratamento de dados pessoais objeto do relatório. Nesse sentido, a finalidade principal do relatório de impacto à proteção de dados pessoais é de apontar qualquer risco que possa advir daquela operação de tratamento de dados pessoais, e direcionar o controlador e/ou operador à mitigação daqueles riscos mapeados (Bruno, 2019).

O RIPD, assim como o mapa de dados, também é um documento de complexa elaboração, visto que envolve não apenas a identificação das operações de tratamento de dados (que podem ser depreendidas do próprio mapeamento ou inventário de dados), mas também cálculos matemáticos para levantamento estatístico de riscos e de medidas de segurança, o que exige acompanhamento de profissionais especializados.

4.5 Implantação de ações de privacidade e segurança de dados pessoais

As fases anteriores preparam a equipe responsável pela implantação da LGPD para conhecer melhor as operações de tratamento de dados pessoais, seu fluxo informacional, riscos envolvidos e as medidas de segurança mais adequadas. Após esse "reconhecimento do campo" em que se deve adequar às normas da lei, será possível adotar as ações mais adequadas para proteção de dados, de acordo com a realidade da instituição e do seu fluxo informacional. Esta etapa também possui fundamento na LGPD, que determina:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018a, art. 46).

As medidas técnicas e administrativas evocadas por esse artigo da lei referem-se, respectivamente, a implantação de instrumentos computacionais de segurança informacional e promoção de uma cultura de proteção de dados. Ou seja, não basta implementar serviços tecnológicos de proteção de dados (como antivírus*, firewall*, sistemas de organização informacional etc.) – abordagem tecnológica da proteção de dados, mas, também, é preciso preparar os diversos setores de uma corporação para respeitar as regras da lei e a privacidade dos titulares – abordagem comportamental da proteção de dados.

Dentre as principais medidas a serem adotadas, é imprescindível a formulação de Política de Segurança da Informação, que estabelece critérios e diretrizes para a justa proteção das informações em fluxo na instituição, considerando os recursos (materiais, financeiros, de pessoal, de tempo, etc.) que podem ser investidos pela alta gerência da organização. Igualmente, deve ser elaborada uma Política de Privacida-

de, que é "um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário" (Brasil, 2020, p. 20). Diversas questões devem ser abordadas pela Política de Privacidade, conforme a ANPD, por exemplo: "Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos" (Brasil, 2020, p. 20).

A adequação de cláusulas contratuais às regras e aos princípios da LGPD também é uma ação importante. Nesses documentos, destaca-se a observância ao princípio da transparência, que orienta a inclusão das seguintes informações que devem ser descritas no registro contratual que contenha informações pessoais:

> . Delimitações claras e objetivas das responsabilidades do controlador e operador;
> . A forma que é realizada a coleta e o tratamento de dados;
> . A existência da possibilidade de o titular acessar os seus dados coletados;
> . A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
> . A existência da possibilidade de revogação do consentimento dado pelo titular;
> . O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
> . As medidas de proteção e segurança dos dados coletados e armazenados pela contratada (Brasil, 2020, p. 24).

No que tange à publicidade de tratamento, recomenda-se que as categorias de dados coletados e tratados sejam informadas no sítio eletrônico do órgão público, em seção especial – além de outras informações sobre as operações de tratamento. Dados de contato do encarregado (nome, cargo, localização, horário de atendimento, telefone e e-mail) também devem ser apresentados. Ademais, versões resumidas do RIPD também devem estar disponíveis ao cidadão (Brasil, 2021).

De posse do mapa, a equipe de *compliance* pode, por exemplo, verificar quais dados pessoais deveriam ser tratados sob a base legal do consentimento, mas cuja anuência não foi dada de acordo com as exigências da LGPD. Com especial apoio do setor de Tecnologia da Informação e de profissionais da organização administrativa da instituição, a equipe responsável pelo *compliance* pode definir como esses consentimentos podem ser obtidos (Pohlmann, 2019).

Ainda de acordo com Pohlmann (2019), a instituição também deve criar formulários para facilitar o exercício de direitos de titulares, que são exercidos mediante requerimento. Eles podem ser disponibilizados em formato físico, mas também digital (no *website* da organização, em aba destinada à LGPD).

Como medida de segurança de dados, é imprescindível que haja controle sobre quem pode acessar informações, sendo recomendável a criação de *checklist* para verificar o controle de acesso a sistemas de informação, como no exemplo a seguir:

> . Identificar todas as contas ativas e os serviços, privilégios, aplicações e demais características;
> . Validar a necessidade de manter os mesmos privilégios e acessos;

. Validar roteiro de aprovação dos acessos autorizados e negados;
. Remover contas inativas;
. Submeter todas as contas e as políticas de senhas;
. Processo definido de exclusão das contas;
. Notificar aos responsáveis sobre qualquer mudança da conta (Maroso, 2020).

Aliás, tomando-se o mapeamento de dados e o RIPD como apoios para verificação de seus itens, *checklists* podem ser instrumentos valiosos para verificação de medidas técnicas e administrativas de segurança e privacidade de dados suficientes para proteger os dados pessoais (ainda que alguns riscos possam persistir, como se destaca mais à frente) (Brasil, 2020).

4.6 Gestão de incidentes

Merecedora de especial atenção, a elaboração de programa de gestão de incidentes (de violação de dados pessoais) também é uma das ações que devem ser implantadas. A gestão de incidentes consiste no registro dos seguintes fatos:

> [...] a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências (Brasil, 2020, p. 26).

Essa etapa do *compliance* inclui implementação de ações para detecção e resposta a incidentes, com vistas à diminuição de riscos. Por força da lei, deve-se manter plano de comunicação a interessados em caso de incidentes:

> O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente (Brasil, 2018a, art. 48).

Um plano de ações para comunicação de incidentes e mitigação de seus danos deve ser adotado ainda que a instituição já tenha passado pelo processo de ade-

quação à LGPD, visto que os riscos que envolvem o tratamento de dados pessoais persistem ainda que minorados. Em seu guia de implementação da LGPD, Pohlmann esclarece ao seu interlocutor:

> Mesmo tendo toda a preocupação do mundo em proteger seus dados, e estando em absoluta compliance com a LGPD, você seguirá tendo riscos de que possa haver um vazamento de dados, ou um incidente específico com algum dado de titular. Se isto acontecer, você deve estar preparado para conter o vazamento, reagir de forma a tratar de solucionar as causas, e comunicar aos titulares de dados e à Autoridade Nacional de Proteção de Dados, sobre o ocorrido (*sic*) (Pohlman, 2019, não paginado).

Além da previsão de medidas para gestão de incidentes, é recomendável a criação de Comitê de Crise que execute tais ações. De acordo com Kohls, Dutra e Welter (2021), esse comitê deve ter o DPO, representante dos setores de Tecnologia da Informação e *marketing*, bem como membros da diretoria institucional, dentre seus membros. Dentre as atividades desse grupo, destacam-se:

> . Definir o problema para ter clareza sobre o que exatamente está acontecendo. Qual é o grupo de titulares foi afetado, a extensão do problema e quais os tipos de dados foram afetados.
> . Levantar informações relevantes para identificar os fatos, descartar boatos, conversar com quem for diretamente responsável pelo problema e entender o que realmente aconteceu a fim de definir o que poderá ser feito.
> . Centralizar a comunicação para que todas as comunicações acerca do incidente partam desse comitê. Tal medida se faz indispensável para minimizar informações desencontradas.
> . Comunicar, o mais breve possível e com frequência, ao público interno e externo informações relevantes, a fim de demonstrar transparência nas ações e mantê-los seguros de que o problema está sendo tratado com todo o cuidado e responsabilidade.
> . Definir as estratégias de mídia mais adequadas para que a comunicação chegue aos titulares atingidos pelo incidente (Kohls; Dutra; Welter, 2021, p. 148-149).

4.7 Análise dos resultados

A periódica análise dos resultados obtidos com a implantação das medidas de segurança e privacidade de dados, bem como do ajuste do tratamento às exigências da LGPD, também deve ser observada nesse processo. Os resultados levantados devem ser reportados à alta gerência da instituição. Uma das principais medidas para avaliar resultados é monitorar históricos de incidentes de violação de dados, incluindo o registro de como a instituição tem reagido a esse tipo de acontecimento (Brasil, 2020b). Também, podem ser levantados indicadores de *performance*, dentre os quais são recomendáveis:

> . Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados dividido pelo número de serviços com dados pessoais do órgão e multiplicado por 100;

> . Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado dividida pela quantidade de serviços do órgão e multiplicado por 100;
> . Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado dividida pela quantidade de serviços do órgão e multiplicado por 100;
> Índice de conscientização em segurança: quantidade de treinamentos realizados dividida pela quantidade de treinamentos previstos e multiplicado por 100;
> . Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço dividida pela quantidade total de controles de segurança e privacidade identificados para o serviço e multiplicado por 100 (Brasil, 2020b, p. 26).

A análise de resultados é um importante procedimento para que os agentes de tratamento reconheçam lacunas de segurança e privacidade. Com isso, podem melhorar, cada vez mais, os procedimentos de proteção de dados pessoais, reduzindo paulatinamente os riscos que envolvem seu tratamento.

Passados os apontamentos sobre as principais fases de *compliance* em proteção de dados pessoais, prossigamos no nosso "caminho" de diálogo (não apenas teórico, mas também pragmático) entre a Ciência da Informação (mais especificamente, os sistemas de organização do conhecimento) e as demandas de proteção de dados pessoais.

5

Breve panorama dos sistemas de organização do conhecimento

5.1 A organização do conhecimento e sua dimensão instrumental

A informação é elemento imprescindível para a execução de atividades humanas (Currás, 2014), tornando-se conhecimento na mente, o qual pode ser registrado, voltando a ser transferido em forma de informação pelo processo de comunicação (Barité, 2001). Em outras palavras, a informação é fonte do conhecimento organizado e socializado através de itens informacionais. Assim, devem existir métodos estruturados para recuperar o conhecimento em registros físicos e, mais recentemente, digitais, a fim de que o indivíduo possa assimilar informações que lhe interessam. Contudo, a recuperação de conhecimento e de informação pressupõe a sua organização em sistemas especializados.

Atrelada aos estudos teóricos e à prática da CI, existe a organização do conhecimento (OC), disciplina focada em fornecer subsídios científicos e pragmáticos para que o conhecimento seja eficientemente organizado e recuperado, bem como em refletir sobre dilemas organizacionais e sociais que envolvem esses processos. Considerando o que fora dito nesta obra sobre as acepções dessas duas terminologias, reitera-se que informação é elemento abstrato para compreensão da realidade, extraível de registros físicos. Já o conhecimento é aquilo que o indivíduo desenvolve a partir do recebimento de informações (conhecimento individual) e acaba por ressoar entre determinado grupo social ou toda uma sociedade (conhecimento socializado). O conhecimento, ao ser socializado, é comunicado na forma de informação, de modo que essa é a fonte do conhecimento (Barité, 2001). Logo, é no escopo do conhecimento socializado, voltado ao uso coletivo (em instituições ou disciplinas científicas, por exemplo), que se funda a OC, que considera contextos e domínios. Porém, não se pode olvidar que o conhecimento pressupõe a informação, de modo que entendemos que a OC, como prática mais ampla de organização, visa a recuperação também da informação.

Diante da complexidade de conceitos, relações, sujeitos, contextos e outros aspectos envolvendo o conhecimento, a OC pode ser dividida em três dimensões, conforme proposta do capítulo brasileiro da *International Society for Knowledge Organization* (ISKO-Brasil) (Pinho, 2017). A dimensão epistemológica compreende os estudos sobre os fundamentos conceituais, históricos e metodológicos da OC, servindo como base teórica para a dimensão aplicada. Por sua vez, a dimensão social e política (ou cultural) se ocupa dos dilemas de ordem sociopolítica e ética no campo da OC, como formação e prática profissional em OC, cultura e identidade. Por fim, há a dimensão instrumental (ou aplicada), que se ocupa das estruturas, produtos, modelos, formatos e todos os outros instrumentos voltados à prática de organizar o conhecimento (Araújo; Ferneda; Guimarães, 2016).

No entanto, um ponto de encontro notório nas mais diversas visões que se têm a respeito da organização do conhecimento é o papel central que ocupam os chamados sistemas de organização do conhecimento (SOCs), que consistem em sistemas que formalizam maneiras de se representar e organizar o conhecimento, ora classificando, ora controlando terminologias e ora modelizando domínios de conhecimento. Localizados na dimensão instrumental da OC, os SOCs não têm sua pertinência verificada somente em atividades bibliográficas, científicas e acadêmicas. Pelo contrário, é possível perceber seu importante apoio, por exemplo, em atividades corporativas, na medida em que seus instrumentos fornecem recursos teóricos e metodológicos para a prática da organização informacional. Entende-se, nesse sentido, que esses recursos instrumentais da OC são eficientes para a propositura de práticas de organização do conhecimento corporativo, que é socializado, comunicado através da coletividade.

Diante disso, o presente capítulo se volta à compreensão dos principais sistemas que organizam o conhecimento, a fim de que o leitor melhor compreenda o porquê de as taxonomias serem (em nosso entender) os sistemas que melhor satisfazem eventuais demandas no processo de *compliance* de dados pessoais, de modo a contemplar princípios e regras da LGPD, especialmente em ambientes digitais.

5.2 O papel dos conceitos e das relações conceituais

Não há como adentrar na dimensão instrumental da organização do conhecimento sem antes apresentar a noção de conceito. Conforme Barité (2001), o conhecimento organiza-se por sistemas de conceitos (estruturados entre si) e é expresso por conceitos. Logo, para organizar o conhecimento, através das ferramentas dispostas pela OC, é preciso, antes de tudo, organizar conceitos (Maculan *et al.*, 2009). Afinal, sob uma perspectiva ontológica, "os SOCs referem-se a sistemas conceituais que representam determinado domínio por meio de sistematização dos conceitos e das relações semânticas que se estabelecem entre eles" (Suenaga *et al.*, 2013, p. 503). Os conceitos e as relações que eles formam entre si (relações semânticas/conceituais) são elementos cognitivos, linguísticos e, portanto, informacionais, que assumem posição de protagonistas no propósito instrumental e social da OC.

A organização de conceitos na mente é parte imprescindível para a produção cognitiva do conhecimento, conforme Pinto (2020, p. 7) afirma: "[...] a partir da definição de conceitos que a mente produz mecanismos que levam a compreensão de uma informação e ao conhecimento de determinado assunto" (*sic*). No universo do conhecimento (individual ou socializado), nenhum conceito subsiste sozinho, mas depende do estabelecimento de relações com outros conceitos (Barité, 2001), conforme esmiuçado mais à frente.

Ainda sobre seus aspectos ontológicos, de acordo com a norma ANSI/NISO Z39.19-2005, "os conceitos existem na mente como entidades abstratas independentes dos termos usados para expressá-los" (2010, p. 4, tradução nossa). Assim, um conceito pode ser o mesmo, independentemente da quantidade de termos que o expressam. Por exemplo, ainda que uma pessoa utilize o termo "cão" ou "cachorro", o conceito a que ambas as terminologias remetem continua o mesmo. Smiraglia enfatiza a importância da ideia de conceito para a OC:

> [...] o conceito - uma ideia nomeada e definida - é a entidade atomista para a organização do conhecimento. Ou seja, tanto a ciência da organização do conhecimento quanto a atividade de desenvolvimento de sistemas para a organização do conhecimento dependem do conceito em sua essência (Smiraglia, 2014, p. 85, tradução nossa).

Quando conceitos se relacionam entre si, formam-se as relações semânticas (ou relacionamentos semânticos). Dentre essas relações, citam-se:

- Relações hierárquicas: Também chamadas de relação de gênero e espécie, são aquelas em que "[...] dois conceitos diferentes possuem características idênticas e um deles possui uma característica a mais do que o outro [...]" (Dahlberg, 1978, p. 104). Algumas ideias mais comuns são as relações entre conceitos mais amplos ou mais restritos e, ainda, entre conceitos superiores e inferiores. As relações hierárquicas podem acontecer a níveis de subordinação-superordenação, ou ainda em nível de coordenação (*relations in array*), quando os conceitos estão sob um mesmo nível hierárquico.
- Relações partitivas: relação de um conceito que representa um todo e outro conceito que representa as suas partes, ou ainda entre um produto e seus elementos constitutivos. É o que ocorre na relação do conceito "árvore" como todo e outros conceitos como partes ("raízes", "tronco", "galhos", "folhas", "flores", "frutos").[1]
- Relações de equivalência: Ocorre quando dois ou mais conceitos possuem características semânticas (de significado) definitivamente iguais ou iguais em determinado contexto. Em sentido mais amplo, referem-se às formas de sinônimos existentes, em que se incluem quase-sinônimos, sinônimos absolutos, acrônimos, reduções e siglas (Maia; Lima; Maculan, 2017).
- Relações associativas: Maia, Lima e Maculan (2017) as definem como as relações em que dois termos estão associados entre si, mas não são equivalentes nem hierárquicos. São as mais diversas, compreendendo relacionamentos como antônimos (termos opostos entre si), opostos (contrários, mas não no mesmo nível de oposição dos antônimos), causais (um termo é causa de outro) etc.

Todo sistema de organização do conhecimento, tenha ele a função de classificar assuntos, controlar terminologias ou modelizar domínios de conhecimento, tem como fio condutor de seu desenvolvimento a definição de conceitos e o estabelecimento de suas relações possíveis.

5.3 Os sistemas de organização do conhecimento e os seus aspectos gerais

Os sistemas de organização do conhecimento (SOCs) são, segundo Bräscher e Café (2008), instrumentos que representam dado domínio de conhecimento por meio da formalização sistemática de relações semânticas entre conceitos. É um termo proposto no âmbito do *Networked Knowledge Organization Systems Working Group,* em 1998 (Hodge, 2000). Eles podem ser definidos sob um sentido amplo, referindo-se

[1] De acordo com Maia, Lima e Maculan (2017), as relações partitivas são subtipos de relacionamentos hierárquicos, assim como as relações de gênero-espécie (também denominadas hipônimo-hiperônimo).

a enciclopédias, bibliotecas, bancos de dados bibliográficos, teorias, disciplinas, culturas e a divisão social do trabalho. Já em sentido estrito, aquele que nos interessa, compreendem as diversas ferramentas voltadas à organização e representação do conhecimento com finalidade de recuperação da informação (Mazzochi, 2017). Cada um desses sistemas, em sentido estrito, possui formas distintas de representar o conhecimento, conforme veremos mais à frente. De acordo com Hodge (2000):

> O termo *sistemas de organização do conhecimento* pretende abranger todos os tipos de esquemas de organização da informação e promoção da gestão do conhecimento. Os sistemas de organização do conhecimento incluem esquemas de classificação e categorização que organizam materiais em um nível geral, cabeçalhos de assuntos que fornecem acesso mais detalhado e arquivos de autoridade que controlam versões variantes de informações importantes, como nomes geográficos e nomes pessoais. Os sistemas de organização do conhecimento também incluem vocabulários altamente estruturados, como tesauros, e esquemas menos tradicionais, como redes semânticas e ontologias (itálicos da autora) (Hodge, 2000, p. 1, tradução nossa).

Maculan *et al.* (2009) afirmam que os variados sistemas possuem, cada qual, suas peculiaridades e utilidades mais comuns. Podem se utilizar da linguagem natural (comum da fala e escrita humanas) ou de linguagens artificiais. Ainda, a usabilidade de cada sistema vai depender das necessidades de seu usuário. Há múltiplas possibilidades de uso dentre os SOCs, possuindo mais ou menos funcionalidades a depender da complexidade de cada sistema. Dentre as funções encontradas nos diversos tipos de SOCs, pode-se destacar:

> [...] eliminação de ambiguidades, controle de sinônimos ou equivalentes, estabelecimento de relacionamentos semânticos explícitos, como relacionamentos hierárquicos e associativos, e apresentação de relacionamentos e propriedades de conceitos nos modelos de conhecimento (Zeng, 2008, p. 160, tradução nossa).

Segundo Serejo Neto (2014), os SOCs devem ser escolhidos e/ou construídos de acordo com as necessidades dos usuários da informação, as quais Souza, Tudhope e Almeida (2012) entendem como "características extrínsecas" desses sistemas (ou seja, fazem parte do contexto em que o SOC se encontra, ainda que não sejam aspectos do seu funcionamento). Os SOCs devem, portanto, ser estruturados a fim de que satisfaçam necessidades informacionais.

Ainda na apresentação de apontamentos acerca da construção e da utilização de SOCs de acordo com a literatura em OC, importa destacar o papel de garantias na organização do conhecimento. Como visto, organizar o conhecimento pressupõe organizar conceitos, sendo esses explicitados por termos. Na construção de SOCs que organizam conceitos adequados para a representação do conhecimento desejado, garantia é entendida como "princípio de autoridade que legitima a inclusão ou exclusão de termos dentro de um sistema de organização do conhecimento, bem como as relações que se estabelecem entre esses termos" (Barité *et al.*, 2015, p. 77, tradução nossa). São diversos os tipos de garantias que contribuem para que o construtor de um SOC possa balizar a escolha e a organização de conceitos afeitos à temática trabalhada e ao público-alvo do sistema.

A garantia literária, uma das mais tradicionais, consiste no princípio afirmativo de que a literatura predominante sobre a temática do SOC deve determinar a escolha dos termos a serem organizados (vocabulário). Inicialmente utilizada em sistemas classificatórios bibliotecários no início do século XX, a garantia literária é comumente utilizada em tesauros. O problema dessa garantia reside no fato de que, nem sempre, as terminologias recorrentes na literatura científica de uma área são conhecidas pelo usuário do SOC. Para a resolução dessa problemática, surge a garantia do usuário, que foca no maior aproveitamento de termos que sejam provavelmente conhecidos pelo público-alvo do sistema. Esse princípio não busca excluir as contribuições da garantia literária, mas complementar-se a ela (Moreira; Moura, 2006).

Diante do escopo desta obra, é valioso o reconhecimento da garantia organizacional, que associa as garantias literárias e de usuário, voltando-se a satisfazer as demandas informacionais de uma organização a partir da justa consideração do vocabulário em voga nela. Como uma corporação pode conter uma "linguagem" particular, com conceitos e termos específicos ao seu contexto, um SOC que seja utilizado nesse ambiente deve considerar essas especificidades (Barité *et al.*, 2015).

Uma última garantia que deve ser enfatizada é a cultural. De acordo com Guimarães (2017), todo SOC representa uma visão de mundo própria de quem o construiu, condicionada às circunstâncias sociais de tempo e espaço. Em outros termos, todo sistema de organização do conhecimento é enviesado. Por exemplo, pode-se dizer que um esquema de classificação construído por um bibliotecário europeu no século XX não refletirá a visão de mundo de um bibliotecário brasileiro no século XXI. Da mesma forma, vieses se tornam necessários em sistemas que se fundam na garantia organizacional, pois valorizam a definição de conceitos específicos recorrentes na cultura linguística daquela instituição. O problema surge quando um SOC demasiadamente enviesado, que reflete peculiaridades linguísticas e até mesmo preconceitos do seu construtor, dificulta o acesso à informação por pessoas de outras culturas. Logo, os estudos sobre garantia cultural partem do pressuposto de que essa problemática precisa ser dirimida (porque vieses não podem ser completamente excluídos) dentro de um sistema que se proponha a ser utilizado em âmbito intercultural.

5.4 Principais sistemas de organização do conhecimento

São muitos os sistemas de organização do conhecimento e ainda mais múltiplos todos os aspectos que os circundam. Como a nossa pretensão não é explicá-los com detalhes, mas, sim, dar um panorama geral sobre o universo dos SOCs, segue quadro demonstrativo que sintetiza as definições e os principais usos de cada sistema:

Quadro 3: Comparação entre os sistemas de organização do conhecimento (SOCs)

SOC	Síntese da definição	Principais usos
Classificações hierárquicas tradicionais	Sistemas que organizam assuntos ou ações institucionais de acordo com classes e subclasses temáticas.	Voltados para a organização temática de documentos bibliográficos ou representação arquivística em domínios institucionais.
Classificações facetadas	Sistemas que classificam, mas, também, instruem a análise e a síntese de assuntos e conceitos por meio de categorias fundamentais e facetas que as manifestam, permitindo que o mesmo conceito seja observado sob diversas dimensões.	Além da sua aplicação em bibliotecas convencionais (que é reduzida), tratam-se não somente de um instrumento, mas de uma abordagem que vem sendo empregada para a construção de SOCs em domínios específicos e é hoje fortemente recomendada para ambientes virtuais.
Listas de termos	Organizam termos em listas para fins de indexação e catalogação de assuntos, podendo explicá-los (como glossários e dicionários).	Listar termos e, em alguns casos, apresentar definições. Voltam-se predominantemente ao controle terminológico.
Tesauros	Vocabulários controlados que visam ao controle terminológico em domínios específicos. Organizam termos por meio de relações hierárquicas, de equivalência e associativas.	Controlar terminologias em domínios específicos para fins de indexação e compreensão temática.
Mapas conceituais	Representam graficamente os termos e as relações entre eles para fins especialmente de ensino e aprendizagem.	Normalmente utilizados para fins didáticos; servem para uma compreensão visual de assuntos e textos e operam também como SOCs.
Taxonomias	Sistemas que organizam informações (nomes, temas, produtos, serviços, processos, etc.) em estruturas hierárquicas, podendo indicar outras relações semânticas entre os termos, a fim de proporcionar uma navegação em um espaço classificado.	Organizar informações em meio digital em domínios diversos. Auxiliar sistemas de recuperação da informação, proporcionando uma navegação classificada, intuitiva e precisa.
Folksonomias	Permitem a indexação livre de termos on-line pelos próprios usuários, em um processo de classificação colaborativa e descentralizada.	Utilização em plataformas *Web* para relacionamentos livres entre recursos e termos (etiquetas).
Ontologias	Artefato computacional que concede uma estrutura conceitual formal e explícita sobre dado domínio de conhecimento ou atividade.	Uso exclusivo em ambiente digital. Pode servir tanto para modelizar domínios de conhecimento quanto para permitir que máquinas deduzam expressões em linguagem natural.

Fonte: elaboração própria.

Posto que o objetivo final deste livro seja apresentar um sistema de organização do conhecimento capaz de dar suporte ao processo de *compliance* em LGPD, é interessante explicar o motivo de termos escolhido a taxonomia como elemento mais apropriado a essa missão.

As classificações facetadas, graças à sua possibilidade de abarcar diversas óticas epistemológicas e organizacionais por meio da distribuição de entidades em categorias e facetas, podem ser úteis para observar as diferentes espécies de dados pessoais. Com o método analítico-sintético, é possível separar dados (enquanto

entidades) como sensíveis ou não sensíveis, de um ou de outros formatos, tratados sob uma ou outra base legal, e assim por diante. Entretanto, não há que se falar em utilização desse SOC em ambiente bibliotecário para a consecução do objetivo pragmático desta obra – como é próprio dos esquemas de classificação tradicionais. Melhor seria aproveitar a abordagem classificacional facetada em outra tipologia de SOC, preferencialmente em ambiente computacional.

Por sua vez, as listas de termos podem até ser úteis para indexação de informações, mas seus recursos são simples e escassos. Para além da própria listagem alfabética, a acessória explicação das expressões indexadas não poderia fornecer grande benefício ao penoso processo de adequação institucional à LGPD, senão uma debilitada e remota utilidade para compreensão temática ou conjuntural. Na primeira possibilidade, a mera compreensão temática acerca dos mecanismos de proteção de dados poderia ser mais bem fornecida por meio de outras formas, como manuais de estudo ou, até mesmo, mapas conceituais. Ademais, a ausência de hierarquias explícitas dificultaria a possibilidade de analisar bem a situação das informações pessoais em uma instituição, já que devem ser devidamente classificadas para ser mais bem compreendidas.

Os tesauros também são utilizados para indexação informacional, apresentando relacionamentos hierárquicos, associativos e de equivalência entre termos. Neste escopo, a espécie de SOC é pouco rentável para fins de *compliance*, já que apresentam as mesmas dificuldades de representação do conhecimento das listas de termos, exceto quanto à presença de hierarquias. Por fim, a sua destacável função como controle de vocabulário pode até ser útil para buscar coesão linguística sobre a temática dentro da instituição, mas nada para além disso.

Folksonomias, desde a primeira análise, mostram-se como os sistemas mais inviáveis para a proposta desta obra. O processo de indexação desses sistemas é aberto e descentralizado, contrariando a necessidade de que a aplicação aos princípios legais na OC pressuponha privacidade e controle de processos de segurança.

Sobre os mapas conceituais, eles podem ser benéficos para representar o conteúdo de estudo da LGPD ou o fluxo de dados pessoais em uma instituição, mas não são muito úteis para a recuperação de informações. É válido reconhecer essa possibilidade destinada ao estudo da instituição e da lei, que também se levanta diante da hipótese de listas de termos ou tesauros para o objetivo pragmático desta obra. Entretanto, melhor do que compreender a aplicação da lei nessa instituição por meio de meras representações gráficas de conceitos ou indexações, vale a pena procurar outro tipo de SOC que melhor organize itens de informação para que o entendimento do fluxo de dados em uma instituição seja ainda mais efetivo.

Quanto às ontologias, é louvável o seu uso computacional e dedutivo para a finalidade de modelizar domínios de conhecimento. Porém, devido à delicadeza do conteúdo veiculado em dados pessoais, entende-se não ser seguro automatizar toda ou a maior parte de uma organização do conhecimento. Entende-se que, devido à tutela jurídica recebida pelos dados pessoais (especialmente aqueles de teor sensível), melhor seria que profissionais capacitados pudessem organizar pessoalmente as informações sobre o fluxo de dados pessoais, ainda que em suporte digital e por meio de ferramentas digitais.

Neste ponto, já é possível deduzir que o melhor caminho é o das taxonomias, visto que são sistemas que organizam itens de informação (em um contexto de *compliance* em LGPD, dados pessoais) em classes/categorias (tipos de dados pessoais) para que se tenha um panorama completo do universo de dados pessoais em fluxo em uma instituição. As taxonomias, por serem predominantemente adotadas em ambientes institucionais, corporativos e de *e-commerce,* normalmente lidam com categorizações, classificações e ordenações de "processos", "atividades" e "serviços", fato que converge com a tônica da LGPD, cujo foco está direcionado para o "como" (processo) proteger dados pessoais.

Nesse sentido, identificar categorias e facetas de dados pessoais em fluxo numa instituição é algo que pode servir como suporte para a equipe de *compliance* entender o que precisa ser melhorado nas operações de tratamento de dados, a fim de melhor adequá-la à LGPD. A organização do mapa de dados em formato taxonômico em um sistema digital é igualmente viável, pois facilitaria a observação das peculiaridades de cada tipo de dados sob diferentes aspectos. Assim sendo, uma taxonomia pode ser especificamente útil para representar o mapeamento de dados pessoais da instituição, separando os tipos de dados tratados de acordo com categorias diversas, tornando-se importante para diagnosticar medidas de segurança e privacidade mais adequadas. Uma vez decidido pela taxonomia e indicada sua finalidade no longo processo de *compliance* em LGPD, cabe, agora, compreender com mais detalhes como ela pode organizar dados pessoais.

6

Taxonomias como suporte ao *compliance* em LGPD

6.1 As taxonomias mais de perto

Após conhecermos a dimensão conceitual da organização do conhecimento, bem como evidenciar as razões para eleger as taxonomias como SOC mais adequado ao *compliance* institucional em LGPD, passemos a uma análise mais detida sobre esse tipo de sistema. A taxonomia possui diversas definições existentes na literatura, ainda que se sobreponha a sua função básica de classificar termos, especialmente através de relações hierárquicas. Segundo Aganette e Teixeira (2017, p. 5), a taxonomia "[...] é um termo genérico cobrindo uma miríade de técnicas e aplicações". Para Camargo (2016), a taxonomia é um modelo de representação da informação "[...] que facilita a recuperação e a organização da informação, sendo utilizadas em SOC como suporte de navegação" (*sic*) (Camargo, 2016, p. 27). Já Terra *et al.* (2004, p. 1) definem taxonomia como "vocabulário controlado de uma determinada área do conhecimento, e acima de tudo um instrumento ou elemento de estrutura que permite alocar, recuperar e comunicar informações dentro de um sistema, de maneira lógica" (*sic*).

Em síntese, todos esses autores concordam que as taxonomias trabalham com conceitos correlacionados, visando, precipuamente, a navegação pela informação para sua recuperação. Além dessa finalidade básica, existem outros recursos comumente encontrados em taxonomias: controle (diferenciação) de sinônimos, estabelecimento de referências entre os termos, representação visual da informação (Aganette, 2010).

As suas utilidades organizacionais são amplamente aproveitadas em ambiente digital, onde a taxonomia se configura como "[...] classificação sistemática de um espaço conceitual" (Aganette; Teixeira, 2017, p. 9). Observa-se, com base nos autores citados até aqui, que as taxonomias cumprem o papel de controle terminológico, assim como os tesauros, mas, notadamente, operam com finalidades organizacionais mais específicas, ligadas às atividades operacionais das instituições. Ao habitar especialmente o meio digital, ajudam a reduzir o tempo pela procura de conteúdos, dinamizando, assim, o processo de recuperação da informação. Diferentemente dos tesauros, que fornecem listas de termos mais precisos para se indexar e buscar uma informação, as taxonomias já conduzem os usuários, por meio de uma navegação previamente organizada, ao destino (produto, serviço, documento etc.) desejado.

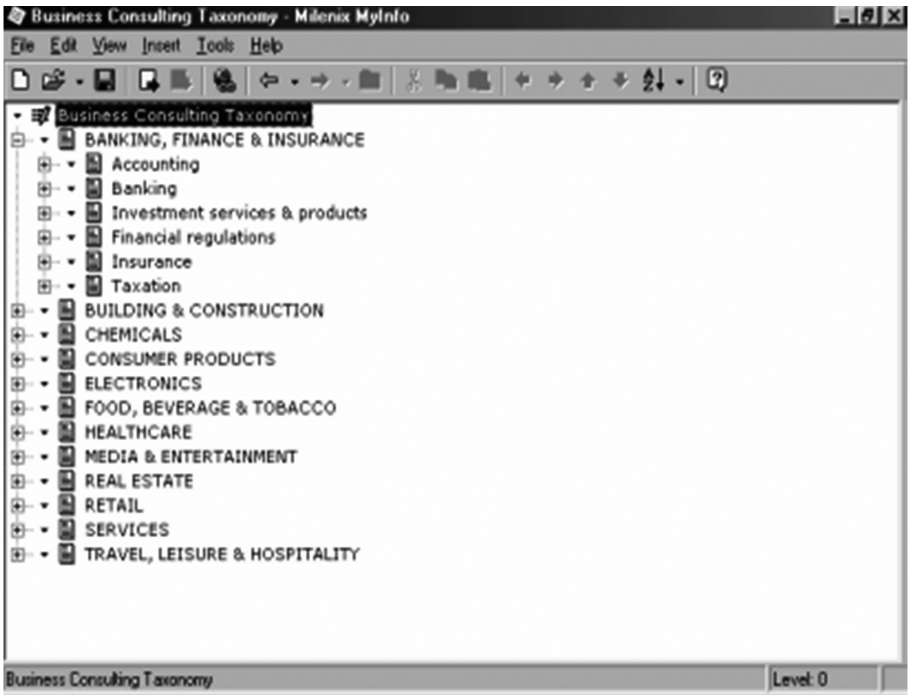
Do ponto de vista das relações conceituais, os termos em uma taxonomia podem ser ligados entre si de diversas maneiras, desde que seja obedecida uma estrutura hierárquica e/ou associativa. O tipo mais marcante de relacionamentos entre termos (não somente nas taxonomias, mas na grande maioria dos SOCs) é o hierárquico, que ordena termos em distintos níveis em relações gênero-espécie e partitivas

(parte-todo), por exemplo. Nas classificações, também há relações de coordenação (renques), em que os conceitos se encontram em um mesmo nível de especificidade (Serejo Neto, 2014).

Como prática e produto da classificação, a taxonomia se utiliza de categorias para ordenar seus termos. Com a necessidade de adequação e de atualização da sua estrutura, suas categorias também precisam estar de acordo com as intenções classificatórias e devem ser periodicamente atualizadas. Em uma taxonomia, a possibilidade de analisar a informação sob diversas categorias permite que a sua manipulação seja arbitrária, isto é, estruturada de acordo com as necessidades de seu proprietário, quer seja a empresa, instituição pública ou pessoa que o mantém (Aganette; Teixeira, 2017). Logo, é a própria estrutura classificatória da taxonomia, composta por categorias e classes, que torna mais fácil e intuitiva a recuperação de informações.

Ponto destacado pela literatura é o aspecto navegacional da taxonomia, que permite o usuário percorrer categorias e termos para recuperação da informação, em uma lógica de níveis e subníveis taxonômicos. Para Blackburn e Small-wood (2014), em uma taxonomia digital, a navegação é resultado da organização hierárquica de termos (que funcionam como "pastas") e leva aos objetos de conteúdo indexados. A figura a seguir apresenta parte da lista de opções (identificadas como categorias e termos) de uma taxonomia digital construída para uma empresa:

Figura 1: Modelo de taxonomia digital



Fonte: Chaudry e Ling (2005, p. 34).

Em geral, as taxonomias trabalham com termos sem defini-los. Ainda assim, permitem que um usuário infira conceitos quando ele observa termos relacionados à palavra pesquisada. Ou seja, a estrutura da taxonomia permite que a pesquisa ocorra de maneira mais intuitiva (Lopes; Aganette; Maculan, 2018).

Aganette (2010) indica, ainda, que a taxonomia pode ser utilizada de forma associativa com outros sistemas (como os tesauros), para que possa refletir, de maneira mais fidedigna, a linguagem e a ordem da área com que se trabalha. Por esse motivo, a sua construção exige o trabalho de profissionais especializados, mas também de *softwares* específicos em que eles se assentam. Ainda, segundo a autora, é possível agregar várias mídias à taxonomia, desde dados e documentos em texto até arquivos audiovisuais e páginas da *Web*. Em suma, a diversidade e a hospitalidade da estrutura taxonômica contribuem não só para a busca de termos e informações através da navegação, mas também para facilitar a análise deles.

6.2 Taxonomias corporativas

Atualmente, considerável parcela das instituições tem trabalhado com grandes volumes de dados, que, quando não organizados adequadamente, podem colocar em risco a produtividade das corporações quanto ao aproveitamento de recursos informacionais. Soma-se a isso o chamado analfabetismo informacional nas instituições, que é a dificuldade de seus membros em utilizar mecanismos adequados para gerir informações (Argudo; Centelles, 2005). Esses dois fatores levam à atual conjuntura, em que as instituições precisam recorrer a SOCs para organizar, representar, disponibilizar e recuperar a informação em ambientes digitais, de maneira ágil e eficiente. Dentre os SOCs mais promissores para o uso nesses ambientes, está a estrutura de taxonomia de uso corporativo (ou taxonomia corporativa), geralmente aplicada em portais internos das instituições.

É possível apontar alguns fatores que implicam na crescente utilização de taxonomias em portais corporativos, segundo Gilchrist (2003): a) maior capacidade das taxonomias (com adequados mecanismos de filtro e pesquisa) em lidar com grandes volumes de dados, se comparadas com motores de busca convencionais; b) maior facilidade de usuários inexperientes em buscar informações; c) o vocabulário de uma taxonomia pode compreender a linguagem de uma instituição específica, ao passo que tesauros e sistemas classificatórios de uso público não conseguem fazê-lo totalmente; d) uma taxonomia própria para uma instituição evita problemas culturais, já que seus vocabulários podem ser particularizados. Por essas razões, a taxonomia também tem se verificado como um importante recurso da organização do conhecimento nas instituições corporativas. Segundo Argudo e Centelles (2005, p. 1, tradução nossa):

> A taxonomia corporativa é definida como um tipo de vocabulário controlado que reflete o contexto, o público e os conteúdos de uma organização específica e que permite a representação de todos os seus objetos informativos para desenvolver diferentes funções dos sites corporativos: a organização do conteúdo, pesquisa, navegação, pesquisa competitiva etc.

Sua finalidade é facilitar e agilizar a organização e recuperação da informação através da padronização da linguagem institucional – como bem apontado por Gilchrist (2003) – reduzindo custos indiretos, auxiliando na tomada de decisões (cotidianas ou de planejamento) e mapeando processos organizacionais (Aganette, 2010). Em síntese, as taxonomias corporativas são utilizadas para representar conceitos próprios da organização (chamados de descritores), suportando estruturas interoperáveis (integração com outros sistemas e tecnologias) e sendo suporte para a navegação, busca de dados e documentos, além de permitir o mapeamento de atividades institucionais (Aganette, 2010).

A seguir, algumas das principais vantagens das taxonomias corporativas levantadas na literatura:

a) Organização de imenso volume de informações: A taxonomia no ambiente digital já é, em si, capaz de organizar e representar um volume imenso de informações. Essa capacidade dá-se através da sua estrutura hierárquica e da sua ordenação em categorias, conforme já argumentado. No âmbito corporativo, isso é ainda mais vantajoso, visto o valor econômico atribuído à informação, o que exige que seja organizada de maneira mais segura e intuitiva possível (Camargo, 2016; Terra *et al.,* 2004). No setor público, por exemplo, a adequada organização da informação também é fundamental para a boa prestação de serviços, aprimoramento de processos comunicacionais e realização de atividades que exijam o conhecimento do fluxo informacional (como é o caso do *compliance* em LGPD).

b) Agilidade no acesso e na recuperação de informações: Devido à sua estrutura propícia à navegação entre categorias, além de ser suporte para outros mecanismos tecnológicos (como mecanismos de busca), a taxonomia facilita o acesso e a recuperação de dados. De acordo com Jacintho e González:

> A taxonomia permite classificar os termos e conceitos obtidos, facilitando a organização do conhecimento alcançado. Isto se deve ao fato de que, uma vez padronizadas, organizadas, estas informações deverão ser acessadas pelos usuários, de forma clara e sem problemas e que estes acessos deverão ter um alto índice de aproveitamento (Jacintho; González, 2017, p. 5).

a) Facilidade para recuperar registros informacionais: Devido a todas as suas vantagens para acesso à informação, registros informacionais presentes em sistemas organizados taxonomicamente podem ser facilmente encontrados, muito por causa da atribuição de categorias e da estruturação hierárquica. Segundo Terra *et. al.* (2004), por exemplo, a taxonomia é vantajosa na procura por documentos porque seus critérios de organização e sua estrutura podem ser personalizados, de acordo com as necessidades de cada instituição.

b) Controle semântico: O controle de vocabulário (isto é, organizar vocabulário para mantê-lo padronizado e coeso) já é algo comum nas várias definições de taxonomia, como visto nas seções anteriores. Terra *et al.* (2004) também apontam que o controle semântico (controle de significado de termos) é uma vantagem desse sistema. Tal utilidade também é fator que aprimora a comunicação adequada entre membros da corporação, pois facilita o alcance do consenso sobre terminologias antes ambíguas e contraditórias.

c) Representação do domínio: Conforme Serejo Neto (2014), uma das vantagens da taxonomia corporativa é conseguir representar um domínio (universo de termos trabalhados). A sua estruturação figura como uma espécie de mapa conceitual, em que a informação pode ser graficamente representada.

d) Tomada de decisões: Essa é uma atividade essencial nos ambientes organizacionais (tanto em relação às decisões a serem enfrentadas cotidianamente quanto àquelas de planejamento). Toda decisão tomada impacta, em alguma medida, a corporação. Por esse motivo, ter acesso à informação correta e de maneira ágil é um fator de apoio ao processo decisório (de rotina e de planejamento) nas organizações (Camargo, 2016).

e) Mapeamento de processos e atividades institucionais: Autores como Aganette e Teixeira (2017) e Terra *et al.* (2004) apontam a possibilidade de mapear processos e atividades da instituição através da estrutura navegacional da taxonomia. Campos e Gomes (2007, p. 3) pontuam que o uso das taxonomias nas corporações permite "[...] reconhecer e relacionar atividades agregadoras de valor, diminuindo esforços na produção e utilização do conhecimento". Por isso, ter a taxonomia como suporte para esse mapeamento é bastante útil. Lopes, Aganette e Maculan (2018) afirmam que a tomada de decisão, muitas vezes, dá-se pelo mapeamento de informações sobre a realidade institucional na estrutura desse SOC.

f) Comunicação entre usuários: Quando unifica a organização do conhecimento na corporação (ou em alguns de seus setores, se for o caso), ela permite que haja uma maior comunicação de informações corporativas entre os usuários (gerentes, funcionários e demais colaboradores) (Terra *et al.*, 2004).

Na seção seguinte, passemos à apresentação de uma metodologia para construção de taxonomias corporativas, especialmente em ambientes digitais (que é o *locus* onde esses sistemas podem ser melhor aproveitados).

6.3 Metodologia geral para construção de taxonomias

Antes de demonstrar como uma taxonomia pode ser construída para o objetivo proposto, é interessante delimitar uma metodologia para a construção desse sistema em corporações. Para tanto, decidimos desenvolver um método autoral de elaboração de taxonomias, com base em mais de dez trabalhos científicos sobre o tema. Como apoio científico-bibliográfico, também recorremos à norma americana ANSI/NISO Z39.19-2005 (R2010), que fornece diretrizes para construção de diversos tipos de SOCs (inclusive as taxonomias). De posse dessas fontes, definimos onze etapas para a construção de uma taxonomia corporativa em ambiente digital, bem como as ações próprias de cada uma das fases. Chegamos ao resultado exposto nas linhas a seguir.

1) Análise da instituição e planejamento

Esta é a etapa em que se fará o diagnóstico da realidade da instituição e o planejamento da implantação da taxonomia. As fontes para esse diagnóstico podem

ser os próprios membros da instituição (através de entrevistas), documentos institucionais, bancos de dados, bem como sistemas de informação e SOCs já existentes. As atividades próprias desta fase são as seguintes:

. Verificação da área institucional para a qual a taxonomia será implantada, abrangência do pretenso sistema, sua utilidade e finalidade corporativa.

. Análise da instituição como um todo: áreas e modo de atuação, valores, objetivos institucionais, nível de complexidade.

. Análise dos processos da área na corporação que será beneficiada pela taxonomia.

. Verificação de taxonomias já existentes (que possam servir como modelo), inclusive em *websites* institucionais.

. Identificar os futuros usuários da taxonomia.

. Indicar as necessidades dos futuros usuários do sistema.

. Fazer planejamento prévio sobre: responsáveis pela taxonomia, recursos para a criação e manutenção, definição do público-alvo, recursos voltados à acessibilidade (como para deficientes visuais ou pessoas com baixa visão, por exemplo), idioma, questões legais relacionadas às informações tratadas.

2) Coleta de termos

Fase em que serão coletados e listados os termos que comporão a taxonomia. Cada termo deve ser condizente com o futuro uso e a finalidade do sistema. Deve-se proceder com as seguintes ações durante a coleta de termos:

. Identificar informações relacionadas a documentos, produtos e serviços referentes à área da corporação que se beneficiará da taxonomia.

. Coleta de termos nas fontes informacionais da instituição (sistemas de informação e SOCs pré-existentes, documentos, bancos de dados, informações externas), de acordo com a temática da taxonomia a ser criada.

. Definir o uso das garantias de usuário, de literatura e/ou cultural, de acordo com as necessidades informacionais da instituição.

. Na listagem de termos, é possível incluir termos deduzidos a partir das terminologias já presentes no vocabulário da instituição.

3) Análise e controle dos termos coletados

Os termos coletados, segundo os critérios postos e observados na fase anterior, serão analisados e submetidos a controle terminológico (incluindo padronização gramatical). Lembra-se de que os termos serão mais específicos quanto mais especializada for a área em que a taxonomia se instalar (Aganette, 2010). Dentre as ações propostas e orientações levantadas na revisão de literatura para esse momento, encontram-se:

. Os termos utilizados devem ser específicos à ideia que se quer passar, evitando-se polissemias e expressões genéricas.

. Definição de idioma em português do Brasil para termos e categorias, podendo-se utilizar terminologias derivadas de outros idiomas em casos excepcionais (quando as garantias de usuário, literária e/ou cultural o exigirem).

. Evitar ou, quando não for possível, esclarecer quaisquer ambiguidades.

. Para palavras com várias grafias, usa-se aquela mais recorrente em dicionários oficiais.

. Termos devem ser colocados, sempre que possível, em substantivos masculinos no singular ou em verbos no gerúndio. No que couber, ações (quando expressas na forma verbal) também devem ser substantivadas.

. Números no meio ou no fim dos descritores devem estar em algarismos arábicos.

. Quando for recorrente o uso de um termo composto por substantivo e seu adjetivo, assim deve ser colocado como descritor.

. São permitidas locuções substantivas, prepositivas ou adjetivas (como "Agente responsável"), mas nunca locuções verbais e adverbiais (como "Agente que se responsabiliza").

. Abreviaturas e termos estrangeiros podem ser utilizados apenas se forem comuns à área beneficiada pela taxonomia.

. Gírias e jargões podem ser utilizados, se forem comuns na linguagem daquela área em que se instala a taxonomia.

. Podem ser utilizados parênteses para indicar breve observação junto ao descritor do termo.

4) Definição de categorias gerais e específicas

Após a coleta e a escolha dos termos, devem ser escolhidas as categorias gerais e específicas que ordenam esses conceitos. Como diretrizes para a definição das categorias, têm-se:

. Sejam evitadas descrições polissêmicas ou vagas para nominar categorias.

. As categorias e seus diversos níveis classificatórios devem ser organizados de forma lógica, estando relacionados uns com os outros.

5) Ordenação e padronização gramatical das categorias

Depois de definidas as categorias, é preciso ordená-las de acordo com as seguintes orientações:

. Os nomes de cada categoria devem ser padronizados conforme as regras de controle terminológico utilizadas na etapa 3 (análise e controle dos termos coletados). Devem ser ordenadas hierarquicamente, da categoria mais ampla à mais restrita.

. Observar o critério da sequência relevante, segundo o qual a ordem de citação das categorias deve possuir relação lógica com a natureza da taxonomia.

. Escolher algum dos critérios para a ordem de citação das categorias: temporalidade, progressão, noção espacial, medidas quantitativas, complexidade, sequência tradicional, pertinência de cada categoria na literatura, ordem alfabética. Esses critérios atentam aos princípios para ordenação de categorias (Campos; Gomes, 2007).

6) Definição de relacionamentos semânticos entre os termos

Além das hierarquias (relacionamentos de superordenação, subordinação e coordenação), existem outros relacionamentos semânticos entre os termos. O termo relacionado com outro deve ser indicado por uma notação em sequência dele. Esses também devem ser indicados após a organização das ideias nas categorias.

. Relações hierárquicas de gênero-espécie: o termo superordenado de outro deve ser indicado por TG (termo genérico), enquanto o termo subordinado deve ser indicado por TE (termo específico).

. Relações hierárquicas partitivas (todo-parte): o "todo" deve ser indicado por TGP (termo genérico partitivo) e a sua parte deve ser indicada por TEP (termo específico partitivo).

. Relações associativas (causa-efeito, ação-resultado, ação-paciente etc.): o termo relacionado ao outro é indicado por TR.

. Relações de equivalência: para termos equivalentes (sinônimos), indica-se por USE, o termo que deve ser sempre usado, e por UP (usado para), o termo que não deve ser utilizado.

7) Validação

Como amplamente abordado pela literatura, a validação é o processo em que se verifica se a taxonomia está de acordo com as expectativas e as necessidades dos usuários. A validação pode ser feita através de reuniões, testes e questionários. Se o próprio construtor da taxonomia for uma das pessoas do público-alvo, ele mesmo pode analisar o grau de maturidade do sistema.

8) Definição da forma de apresentação da taxonomia e tecnologia de suporte

Após a estruturação da taxonomia e as validações, define-se como esse sistema deve ser apresentado, incluindo aspectos como *layout*, *design* das categorias e modo de navegação na taxonomia. Também deve ser definida a tecnologia que servirá como suporte desse sistema, sendo que seus recursos também serão critérios para definir o modo de apresentação do SOC. Ainda, definem-se quais recursos adicionais podem ser acrescidos à taxonomia (por exemplo, mecanismos de busca por palavras-chave).

9) Publicação

Momento em que a taxonomia passará a estar disponível para utilização. Frisa-se que isso só será possível quando todas as etapas anteriores forem devidamente executadas.

10) Determinação de ações de gerenciamento

Junto com a publicação da taxonomia, também é necessário definir ações de gerenciamento (conforme estipuladas na fase de planejamento do sistema). É nesse momento que elas serão determinadas. Incluem indicação de responsáveis pela gestão e pela manutenção da taxonomia, obrigações dos usuários ao trabalhar com dados e documentos hospedados na estrutura taxonômica, determinação de periodicidade de manutenções, planejamento de reuniões periódicas para discussão sobre o uso da taxonomia na área institucional beneficiada etc.

11) Manutenção

Manutenções periódicas constituem uma atividade constante na implantação da taxonomia corporativa. Por isso, ela nunca é um produto, mas sempre um processo, como dito por Vogel (2005). Sempre precisará de ajustes para manter as informações organizadas e, de atualizações, para aumentar sua utilidade.

6.4 Taxonomias para mapeamento de dados pessoais

A proposta central desta obra é apresentar uma abordagem metodológica de organização do conhecimento que seja adequada para a implantação das regras da LGPD em instituições que necessitem se adequar às exigências dessa lei, mais especificamente os hospitais. Diante de tal necessidade, que emerge com a vigência da aludida norma, entende-se que a organização do conhecimento corporativo acerca de dados pessoais pode se dar a partir da atividade de mapeamento, que é parte do processo de *compliance* em LGPD e que estabelece categorias de dados pessoais.

Anteriormente, demonstramos através da comparação entre os principais sistemas de organização do conhecimento constantes da literatura que a taxonomia é um sistema apropriado para o propósito de organizar informações mapeadas (quais sejam, dados pessoais) a fim de verificar a sua adequação às emergentes exigências normativas. Neste ponto da obra, aprofunda-se na ideia de mapa/mapeamento de dados pessoais para, posteriormente, aplicar a metodologia autoral a uma instituição-modelo, que servirá como exemplo de como as taxonomias podem ser utilizadas para o *compliance* em LGPD.

Quando realizado através de estrutura taxonômica em que se atribui diferentes tipos de dados pessoais, o mapeamento permite navegar pelas informações pessoais em fluxo (no formato de termos), de modo a facilitar a observação do contexto de tratamento de dados na instituição e as possíveis necessidades para garantia da

privacidade e segurança informacional. Portanto, com o fito de desenvolver a aludida proposta, apresentamos os principais aspectos dos mapas de dados e algumas propostas de categorização relativas a esse processo de *compliance*.

Reitera-se que o mapeamento de dados faz parte da fase de registro de operações de tratamento no processo de *compliance* e "existe para nortear, facilitar e permitir que o controlador e o operador de dados, por meio e/ou com apoio do encarregado, consigam criar e gerir um programa de governança aderente com a sua realidade e ao seu modelo de negócio" (Furtado, 2020, p. 88). De acordo com Furtado (2020), o registro de operações é um processo necessário para a satisfação das seguintes finalidades:

a) aderência ao princípio de responsabilização e prestação de contas (pois é necessário que o controlador conheça sobre o fluxo de dados para prestar esclarecimentos);

b) fiscalização da ANPD (na mesma lógica do item anterior);

c) aderência ao princípio da transparência;

d) atendimento ao direito de confirmação de existência e ao direito de acesso;

e) atribuição da adequada base legal a cada operação de tratamento;

f) adoção de medidas adequadas de proteção;

g) identificação de tipos de dados que estejam envolvidos em cada operação de tratamento de dados;

h) criação de plano de ação orientado a riscos.

Retornando o foco ao mapeamento (ou mapa) de dados, reiteram-se as diferentes maneiras de defini-lo, ora como processo, ora como procedimento, associando-o com o dever de registro de operações. Para Komnenic (2022), por exemplo, o mapeamento de dados é resultado da combinação do inventário de dados (em planilhas) e do fluxo de dados (fluxograma do movimento desses dados em sistemas internos e externos). A autora define:

> O mapeamento de dados é um sistema de catalogação de quais dados você coleta, como são usados, onde são armazenados e como percorrem toda a organização e além. Existem várias maneiras de atingir esse objetivo – seja por meio de uma simples planilha ou de um programa de mapeamento de dados apropriado – e a extensão ou limite de seu mapeamento de dados dependerá de seu negócio (Komnenic, 2022, tradução nossa).

O Guia de Elaboração de Inventário de Proteção de Dados da ANPD, por outro lado, posiciona-se sobre o entendimento de que o mapeamento é um processo, sendo que o inventário de dados é o resultado do registro de operações previsto no texto da LGPD. Define-se o seguinte: "O IDP [Inventário de Dados Pessoais] consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição. Ele proporciona uma espécie de 'fotografia' do atual cenário do tratamento de dados pessoais do serviço/processo de negócio" (Brasil, 2021a, p. 26). Fato é que o inventário se trata de um registro mais amplo que o mapa de dados. Enquanto aquele prevê a descrição de todas as informações envolvendo o tratamento dos dados,

incluindo nomes e contatos de responsáveis (Bruno, 2019), o mapeamento se atém à separação dos dados pessoais em categorias para facilitar a visualização dos processos que lhes envolvem.

Logo, para fins de coesão terminológica nesta obra, entende-se ser mais adequado dizer que o mapeamento é o processo de vislumbrar e categorizar dados, enquanto o mapa é o seu resultado visualmente representado, seja por planilha, diagrama, mapa conceitual ou, até mesmo, como é nossa proposta, por uma taxonomia. Reitera-se que não se confunde com o inventário de dados, que compreende registros mais amplos de tudo o que ocorre no tratamento. Assim, não há que se falar em IDP como objeto da nossa proposta pragmática, mas no reconhecimento do fluxo informacional (mapeamento) como processo e na organização categorial de dados pessoais (mapa) como resultado, tomando-se a taxonomia corporativa como referencial na construção e na estruturação dessa ação de *compliance*.

Frente à lógica de divisão dos itens de informação (termos) de uma taxonomia em múltiplas facetas/categorias (possível na estrutura taxonômica), os dados pessoais podem ser classificados de acordo com diversas perspectivas, por exemplo: por dado sensível ou não, por setor da instituição, por dado de menor ou maior de idade, dentre outras possibilidades que possam auxiliar a equipe de *compliance* de uma organização a compreender o fluxo de dados e aplicar medidas de segurança e privacidade mais adequadas.

A categorização de dados pessoais sob diversas perspectivas não é novidade desta obra, mas já é uma proposta amplamente utilizada pela literatura para apoiar o *compliance* em dados pessoais, especialmente na fase de mapeamento. Komnenic (2022), por exemplo, entende que os mapas de dados pessoais devem conter as seguintes informações: dados coletados; existência de dados sensíveis; bases legais; finalidade do tratamento; local de armazenamento; período de armazenamento; medidas de proteção e segurança adotadas; existência de dados transferidos; destino de transferência e local de armazenamento de dados transferidos; protocolos para proteção de dados durante transferência.

Tomando como referência uma instrução da autoridade de proteção de dados pessoais da Bélgica, o Guia de Elaboração de Inventário de Proteção de Dados da ANPD sugere o seguinte padrão de categorização de dados pessoais (*apud* Brasil, 2021a): dados de identificação pessoal (como nome, endereço e telefone); dados financeiros (como informações bancárias e salariais); características pessoais (como idade, sexo e descrição fisionômica); hábitos pessoais (como informações sobre estilo de vida, viagens, contatos sociais e posses); características psicológicas (como personalidade e caráter); composição familiar (como histórico conjugal e nomes de familiares); interesses de lazer (como *hobbies*); associações (informações de relações do titular com associações diversas); processo judicial/administrativo/criminal (nos quais o titular esteja envolvido); hábitos de consumo; dados residenciais (informações sobre residência do titular); educação e treinamento (como dados acadêmicos, escolares e profissionais); registros/gravações de vídeo, imagem e voz.

Sobre essa última proposta de categorização de dados pessoais, é nítido o seu enfoque na organização de acordo com o conteúdo da informação registrada no dado (sendo todas referentes a um titular identificado ou identificável), com exceção da última categoria, que se preocupa mais com o formato do dado. Além disso, a sua

cobertura é bastante ampla, compreendendo uma longa série de informações de caráter privado. Contudo, nem todas as categorias de dados sugeridas estão presentes em qualquer instituição. Isso porque cada organização pública ou privada tem seus objetivos institucionais próprios, bem como diferem no que se refere a produtos/serviços fornecidos, tipo de público que fornece dados etc. Por isso, como relatado anteriormente, cada taxonomia deve conter uma linguagem (termos e categorias) distinta, de acordo com a sua instituição.

Quanto à forma de registro das operações de tratamento para implementação da LGPD, fase na qual se inclui o mapeamento de dados, Furtado (2020) entende por bem que seja por escrito e em meio eletrônico, sendo preferencialmente redigido em língua portuguesa (ou que, ao menos, possua versão em português, periodicamente, atualizada).

De acordo com Komnenic (2022), o mapeamento deve ser um processo tão seguro quanto qualquer outra atividade. Devem ser adotadas medidas de segurança técnico-computacionais e administrativas para evitar violações dos dados analisados. Por exemplo, sugere-se que apenas indivíduos autorizados possam acessar e atualizar o mapa.

Por fim, o mapeamento não é uma atividade que se encerra definitivamente, mas que necessita de atualizações periódicas. Ainda assim, a nosso entender, um mapa de dados que compreenda todas as atividades de tratamento e os principais atributos das informações pessoais em fluxo na instituição já é útil para que se entenda quais medidas devem ser adotadas para privacidade e segurança dos dados. Para a devida atualização, é necessário definir quem serão os responsáveis pela manutenção do mapa, delimitando bem a sua função. Ainda, a atualização do registro não deve compreender apenas a inclusão de novos tipos de dados que surgem no fluxo informacional da organização, mas também a exclusão de tipo de dados que já não são mais tratados pela instituição (Komnenic, 2022).

7

Um modelo de taxonomia para *compliance* em LGPD

7.1 A instituição-modelo: Hospital Universitário Clemente de Faria

Durante a produção desta obra, foi-se desenvolvendo o entendimento de que não poderia demonstrar, com clareza, os usos e os benefícios de uma taxonomia para *compliance* em LGPD, sem que, para tanto, se criasse um modelo inspirado na realidade de alguma instituição. Afinal, como já dissemos, uma taxonomia deve ser construída de acordo com as necessidades da instituição onde será aplicada. Para tanto, elegemos o Hospital Universitário Clemente de Faria (HUCF) como instituição-modelo, servindo como demonstração de como uma taxonomia de mapeamento de dados deve ser desenvolvida.

As informações referentes ao HUCF, brevemente descritas nas páginas a seguir, foram extraídas de trabalhos científicos sobre o hospital, bem como de dados públicos fornecidos pela própria instituição mediante solicitação deste autor por ofício.[1]

O HUCF está vinculado à Universidade Estadual de Montes Claros (Unimontes) e atende à população do norte do Estado de Minas Gerais e áreas circunvizinhas. Porquanto, a alta demanda de processos que envolvem pessoas (como pacientes, doadores de órgãos, acompanhantes e colaboradores) implica em grande fluxo de dados pessoais.

Para se ter uma noção quantitativa da atuação do HUCF, em suas unidades (Unidade Hospitalar, Centro de Especialidades Tancredo Neves e Centro de Referência e Assistência à Saúde do Idoso) foram realizados 415.154 procedimentos hospitalares no ano de 2020, incluindo atendimento a servidores da Unimontes, consulta básica, consulta especializada, consulta de urgência, atendimento de emergência, apoio diagnóstico, cirurgias e exames. No ano de 2019, foram realizados 572.901 procedimentos nas unidades do hospital.

Até maio de 2021, o HUCF contava com 141 leitos hospitalares distribuídos nos seguintes setores:

[1] Neste capítulo, considera-se que as informações qualitativas ou quantitativas do hospital, quando desacompanhadas da indicação de referências bibliográficas, foram extraídas de dados e relatórios fornecidos pela própria instituição. Por outro lado, informações extraídas de trabalhos científicos serão acompanhadas da respectiva indicação de referência.

Tabela 1: Número de leitos no HUCF

Especialidade	N° de leitos
Clínica Cirúrgica Geral	24
Clínica Médica	23
Clínica Pediátrica	13
UTI COVID	20
Enfermaria COVID	06
Maternidade	24
Neonatologia/Intermediário	14
UTI Adulto	07
UTI Neonatal e Pediátrico	10
Total	141

Fonte: informações cedidas pelo HUCF, 24 jun. 2021.

No que se refere a recursos humanos, o HUCF contava, até maio de 2021, com 909 servidores efetivos (médicos universitários, analistas universitários da saúde, enfermeiros, nutricionistas, psicólogos, fisioterapeutas, farmacêuticos, técnicos universitários, técnicos de laboratório, técnicos em radiologia, técnicos de enfermagem, etc.); 211 profissionais de empresa terceirizada (recepcionistas, eletricistas, bombeiros hidráulicos, pintores, porteiros, vigias, almoxarifes etc.); 241 médicos credenciados.

O corpo administrativo do hospital é dividido em Superintendência, Diretoria Clínica, Diretoria Administrativa (serviços administrativos) e Diretoria Assistencial (atividades-fim do hospital, ou seja, serviços médico-hospitalares). Dentro dessas Diretorias, também se encontram as Gerências, as Comissões e outros setores. Nota-se que essa organização hospitalar é bastante complexa, pois exige a realização de diversas atividades especializadas para a execução dos serviços de saúde (Botelho, 2006). Observa-se que cada setor é responsável pelo seu próprio gerenciamento cotidiano, ainda que as Gerências e as Diretorias também exerçam função de gestão dessas unidades. Por isso, é comum que, além dos profissionais destinados às principais atribuições do setor, também existam técnicos e/ou auxiliares administrativos para executar serviços gerenciais.

Dentre as diversas unidades administrativas do HUCF, podemos citar (Carvalho, 2008): Gerência de Engenharia e Infraestrutura Hospitalar; Gerência de Materiais e Suprimentos; Gerência de Pessoas; Gerência de Tecnologia da Informação (GTI); Faturamento; Gerência de Governança e Hotelaria; Ambulatórios; Gerência de Apoio Diagnóstico; Gerência de Atendimento Multidisciplinar; Gerência de Desenvolvimento Acadêmico, Multiprofissional e Interdisciplinar; Gerência de Clínicas; Gerência de Urgência e Emergência; Blocos Cirúrgicos; Gerência de Enfermagem; Nutrição Enteral; Gerência de Farmácia; Serviço Social.

7.2 O fluxo de dados pessoais na instituição-modelo

Apresentados os aspectos administrativos e operacionais dessa instituição, fica agora evidente que as ações realizadas no âmbito do hospital envolvem coleta, produção e transferência de dados pessoais (interna ou externamente ao HUCF). Realizar operações de tratamento com dados, inclusive os de caráter privado, exige o trabalho de funcionários de setores diversos, além do apoio de sistemas de informações hospitalares. Conhecer, ainda que em linhas gerais, o fluxo de dados pessoais nessa instituição hospitalar é um passo necessário para apresentar propostas de promoção da LGPD nesse ambiente.

Primeiramente, cabe identificar setores e sujeitos que mais atuam no tratamento de dados pessoais no HUCF. A recepção é responsável pelo cadastro (coleta) de dados de identificação e de contato referentes aos pacientes que chegam ao hospital. A atualização dos dados relativos à saúde é feita por colaboradores de setores operacionais, através de prontuários médicos. As atividades do Serviço de Arquivo Médico e Estatística (SAME) e da Gerência de Tecnologia da Informação (GTI) na coleta e no armazenamento de informações dos pacientes também são fundamentais para a gestão dos dados pessoais dos pacientes. Por fim, quando se trata das informações dos colaboradores do hospital, a gerência de pessoas é a responsável por organizá-las. Nesses processos, os registros de informações (ou seja, dados) podem estar presentes tanto em arquivos físicos quanto em itens digitais de informação.

A partir de documentos cedidos pelo HUCF, é possível traçar aspectos sobre como alguns tipos de dados pessoais são tratados na instituição. Observa-se que, para fins de aplicação deste nosso estudo, “tipo de dado pessoal” é a caracterização do dado de acordo com a informação que ele carrega. São tipos de dados pessoais, por exemplo, o nome, o número no Cadastro de Pessoa Física (CPF), a ocupação profissional do titular, o resultado de um exame médico, bem como outros dados que representem informações referentes a pessoas físicas identificadas ou identificáveis. Eis, portanto, alguns exemplos de tipos de dados pessoais tratados no HUCF, tanto referente a seus usuários, quanto a seus colaboradores:

Quadro 4: Comparativo sobre o tratamento de dados pessoais dos pacientes do HUCF

Tipo de dado pessoal	Ocasião da coleta	Finalidade da coleta	Meio de coleta	Período de retenção do armazenamento
Nome, idade, sexo, cor, tipo sanguíneo, doador, filiação, estado civil, nome do cônjuge (se tiver), identidade, contato, endereço, etc.	Apresentação de documentação no momento do cadastro	Cadastro para atendimento em unidade hospitalar	Apresentação de documentação no momento do cadastro	Permanente
Nome social (se for o caso)	Apresentação de documentação no momento do cadastro	Cadastro para atendimento em unidade hospitalar	Não-informado	Permanente
Carteira Nacional de Saúde	Pesquisa no site do CADSUS	Não informado	Pesquisa no site do CADSUS	Não informado

Tipo de dado pessoal	Ocasião da coleta	Finalidade da coleta	Meio de coleta	Período de retenção do armazenamento
Login	Apresentação de documento no momento do cadastro	Cadastro para acesso de Sistema Informatizado	Não informado	Permanente
"Prestador" (identificação de colaborador)	Recuperação de acessos	Cadastro para acesso de Sistema Informatizado	Planilha	Enquanto existir vínculo com a instituição
Nome, CPF, data de nascimento, profissão	Apresentação de documento no momento do cadastro	Cadastro para acesso de Sistema Informatizado	Apresentação de documento no momento do cadastro	Permanente
***E-mail*, telefone**	Apresentação de documento no momento do cadastro	Cadastro para acesso de Sistema Informatizado	Informado pelo titular	Permanente
N° de matrícula (para acadêmicos)	Não informado	Cadastro para acesso de Sistema Informatizado	Importação de sistema acadêmico	Permanente

Ante a apresentação dos dois quadros anteriores, que comparam alguns dos aspectos referentes ao tratamento de determinados exemplos de tipos de dados, percebe-se que a ocasião da coleta é diversa. Dados presentes em documentos de posse do próprio titular, como nome, tipo sanguíneo, telefone e e-mail são coletados em ocasião da apresentação documental desses registros. Outros, para serem conhecidos, precisam de uma maior intervenção da instituição, como é o caso do cadastro no SUS (CADSUS) (provavelmente, porque é mais simples ou mais confiável que a instituição consulte por conta própria do que o solicite ao usuário) e o "prestador" (porque é a própria instituição que produz esse registro). Por isso, a ocasião da coleta está diretamente relacionada com o meio de coleta de cada tipo de dado. Quanto à finalidade da coleta, ela é pressuposta para execução das atividades na instituição, como atendimento hospitalar (no caso de atendimento de usuários) e acesso aos sistemas de informação hospitalares (SIHs) do hospital (no caso de colaboradores). Ainda, o tratamento de dados no HUCF envolve o armazenamento, que é imprescindível para fins de registro e organização informacional. Esse armazenamento pode ser permanente ou, em alguns casos, temporário (como na hipótese de guarda de "prestador" – número de identificação – do colaborador).

Para além das informações presentes nos quadros, salienta-se que a coleta não se dá através do consentimento do titular, como aduz o art. 7°, inciso I, da LGPD – hipótese bastante comum na iniciativa privada, como no cadastro de usuário em *websites* ou na compra de produtos, por exemplo. Em planilhas apresentadas pelo pessoal competente do HUCF, declara-se que a base legal que fundamenta o tratamento de dados de colaboradores e usuários (pacientes) da instituição é o legítimo interesse. De acordo com os documentos cedidos pelo HUCF, a justificativa de fundamentar-se nessa hipótese de tratamento é a "segurança, controle de acesso e utilização de recursos institucionais". Seguindo essa lógica, a título de exemplo, no caso dos colaboradores, um dos motivos para o legítimo interesse é a inscrição de informações nos cadastros trabalhistas, para que esses sejam titulares de direitos e deveres enquanto funcionários desta instituição. Além disso, o cadastro é necessário

para que eles possam acessar os sistemas de informações hospitalares (SIHs), a partir da apresentação de suas credenciais na *interface* dessas plataformas.

Entretanto, especificamente quanto aos dados de usuários (pacientes), entende-se que a base legal justificada pelo HUCF não é a mais adequada, visto que o legítimo interesse deve ser usado para casos especiais que justifiquem o tratamento (e estejam fora de outras hipóteses previstas em lei). Além disso, o legítimo interesse não possui embasamento legal para o tratamento de dados de saúde, visto que esses são dados sensíveis, que não estão previstos no rol das bases legais no artigo 11. Assim, entende-se que a base legal que melhor fundamenta o tratamento de dados de pacientes, legitimando suas operações, é a "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (Brasil, 2018a, art. 7°, inc. VIII; art. 11º, II, 'f'). Diferentemente do legítimo interesse, a tutela da saúde se aproxima melhor da razão pela qual dados de pacientes são coletados, produzidos e/ou utilizados no HUCF, além de ser base legal apropriada também ao tratamento de dados sensíveis.

Ainda sobre a dinâmica de gestão de dados no hospital, consideradas as terminologias da LGPD, frisa-se que a GTI é mera responsável técnica pelo tratamento. Como o controlador e o operador são figuras com personalidade jurídica própria, é a Unimontes quem controla e opera o tratamento de dados, pois o HUCF é a unidade administrativa que integra a universidade. Reitera-se, aqui, o entendimento da ANPD, anteriormente citado, no sentido de que colaboradores de uma instituição não são agentes de tratamento, mas apenas atuam sob o poder diretivo da entidade controladora (Brasil, 2021b), que, neste caso, é a Unimontes.

Em relação ao armazenamento, todos os dados são armazenados nos bancos de dados localizados no *Data Center*, de responsabilidade da GTI. Diariamente, é feito *backup* dos registros informacionais para discos de armazenamento, com um período de retenção de 7 dias. Não há descarte para dados em *backup*, nem exclusão definitiva, independentemente do tipo de dado.

A respeito dos demais controles de segurança sobre esses dados pessoais, há autenticação de usuário por meio de *login* e senha nos SIHs internos e do SUS, já que a apresentação de credenciais pode diminuir as chances de terceiros acessarem essas plataformas. Ademais, procura-se utilizar *firewall* e antivírus, além de bloqueio a acessos externos nos SIHs utilizados pela instituição. Ainda assim, subsiste risco de: invasão a esses sistemas; coleta de dados por agentes não-autorizados; possibilidade de perda das informações por falha nos equipamentos (incidente que pode ser contornado com restauração de cópia de segurança).

Do ponto de vista dos SIHs, o HUCF adota o Sistema Soul MV (ou apenas Sistema MV) como auxílio para a execução de suas principais atividades. Esse sistema de informações hospitalares utiliza um menu padrão, onde se pode ver as opções em sua *interface*. Ele gerencia informações em todas as instâncias da instituição, sejam de planejamento, administrativas, financeiras, de apoio ou clínicas. O colaborador conta com o auxílio de um manual de uso fornecido pelo desenvolvedor do Sistema Soul MV, para melhor aprender como manusear esse sistema, além de documentos, normas e formulários que orientam a sua atuação dentro do hospital. Dentre as suas funcionalidades, é interessante citar:

. Recursos de apoio ao atendimento (urgência e emergência, ambulatório, in-

ternação, centro cirúrgico e obstétrico), como central de agendamento e classificação de risco.

. Prontuário Eletrônico do Paciente (PEP), controle de infecção e gerenciamento de unidades.

. Auxílio no diagnóstico e na terapia, no laboratório de análises clínicas, no banco de sangue e no diagnóstico por imagem.

. Auxílio nos serviços de faturamento de internação (autorização de internação hospitalar - AIH) e de ambulatório (autorização de procedimento ambulatorial - APA e boletim de produção ambulatorial - BPA).

. Auxílio na logística do almoxarifado e da farmácia.

. Útil a serviços de apoio, como Setor de Nutrição e Dietética, Central de Materiais Esterilizados, Manutenção, Lavanderia e Rouparia, Diretoria Clínica e Diretoria Geral.

. Apoio na gestão de usuários e auditoria de tabelas.

. Fornece sistemas estratégicos de Gestão de Documentos, Gestão de Riscos e Gestão de Ocorrências.

Outro SIH importante para as atividades do HUCF é o Sistema Integrado de Dados (ou apenas Sistema Integrado). Ele foi desenvolvido pelo próprio hospital e é utilizado para gestão do pessoal. Faz o controle dos setores, das funções, das escalas de trabalho, dos afastamentos, dos registros de ponto, do controle de senhas da telefonia, dos relatórios gerenciais, além de servir como meio de fazer comunicados aos funcionários. O Sistema Integrado possui um menu de opções em formato taxonômico – dividido em níveis e subníveis, como se fossem categorias e subcategorias. A figura a seguir representa a estrutura do menu do Sistema Integrado:

Figura 2: Parte do menu do Sistema Integrado de Dados do HUCF

Fonte: informações cedidas pela GTI/HUCF, 08 fev. 2021.

Sobre o fluxo de informações dos pacientes, aponta-se que a atualização de dados cadastrais é feita nas recepções (da internação, da urgência e emergência ou dos ambulatórios). No momento da entrada do paciente ao hospital, também é feita a consulta do seu cadastro no SUS ("Cartão SUS") através do sistema CADSUS. Também se utiliza o Prontuário Médico Eletrônico do Sistema MV (MV PEP). Essa funcionalidade reúne os dados do paciente, especialmente o seu histórico médico, de maneira simplificada e acessível aos funcionários. Durante o cuidado do paciente, os profissionais de saúde que tratam daquele usuário têm acesso ao prontuário (limitado à atuação do seu setor e às suas atribuições médico-hospitalares). Portanto, observa-se que os sistemas de informações hospitalares têm sido bastante úteis para a gestão da informação dessa complexa instituição embora já haja uma preocupação com a segurança de dados pessoais, haja vista que as alternativas utilizadas pelo hospital (*antivírus* e *firewall*) não são suficientes para afastar totalmente os riscos de violação de dados.

Nessa toada, é preciso efetivar a consolidação da LGPD nessa instituição, enquanto demanda jurídica e social para preservação da privacidade de pacientes, de funcionários e de outras pessoas que estabeleçam relações com o hospital (como doadores de órgãos a pacientes e acompanhantes). Diante dessa necessidade, a Unimontes implementou, em 2020, o Grupo de Trabalho para implementação da LGPD (GT-LGPD/Unimontes). Desde então, o grupo tem se empenhado no desenvolvimento de ações para colocar as unidades da universidade (inclusive HUCF) em conformidade com as exigências da nova lei (Unimontes, 2020).

7.3 Executando as etapas de construção de taxonomias

Como já fora apontado, o mapeamento pode tomar a estrutura taxonômica como referência para organização hierárquica de dados pessoais em categorias diversas (que podem ser organizadas em múltiplas dimensões). O resultado desse processo é um mapa de dados pessoais construído sob uma taxonomia em ambiente digital. Para construção do referido sistema, considera-se a metodologia autoral de elaboração de taxonomias, já apresentada nesta obra.

Para melhor ilustrar como uma taxonomia de mapeamento de dados pessoais deve ser elaborada e aplicada em uma organização, tomamos como instituição-modelo o Hospital Universitário Clemente de Faria (HUCF). Os aspectos institucionais do hospital, bem como o modo com que dados pessoais transitam entre suas atividades médico-operacionais e administrativas, tornam-se os subsídios informativos necessários para demonstrar como um modelo de taxonomia pode ser implantado para os fins aqui propostos.

1) Análise da instituição e planejamento

Em síntese, como demonstrado na descrição do HUCF, esse é um hospital que, com diversas unidades de atendimento em Montes Claros, atende todo o norte de Minas Gerais, buscando realizar milhares de operações médico-hospitalares todos os anos. A importante atuação na região exige o tratamento de diversos tipos de dados pessoais (desde dados cadastrais de usuários e colaboradores até informações sensíveis relativas à saúde), o que exige a adoção de sistemas que auxiliem na adequação às normas de proteção de dados pessoais.

A intenção é que a taxonomia seja utilizada como instrumento para mapeamento de dados pessoais, que é uma das mais importantes ações no processo de *compliance*. Funcionando como um mapa de dados em ambiente digital, facilmente editável em SIH, a taxonomia permitirá que a equipe responsável pela implantação da aludida lei no HUCF conheça melhor os tipos de dados pessoais de acordo com categorias em organização multifacetada.

O público-alvo da taxonomia é o Grupo de Trabalho em LGPD da Unimontes (GT-LGPD/Unimontes), responsável pela implantação das regras e ações concernentes à legislação em toda a universidade, inclusive no hospital. A finalidade desse SOC é o reconhecimento (ou, na linguagem da literatura de *compliance* em LGPD, o mapeamento) dos dados a partir de categorias diversas, permitindo que a equipe responsável pelo *compliance* no hospital compreenda os aspectos de cada tipo de dado e, assim, aplicar medidas de segurança e privacidade que forem necessárias.

Quanto à sua aplicação, a taxonomia seria implantada como sistema de informações hospitalares. Nesses ambientes computacionais, os termos de uma taxonomia podem hospedar "*links*" que levam a outros locais do espaço virtual. Nesse sentido, a intenção desta proposta é que os termos desse SOC possam levar a páginas em que se possa registrar medidas de segurança e privacidade de dados, executadas ou a serem providenciadas pelo hospital, aproveitando-se do próprio funcionamento digital da taxonomia para fazer o controle dessas ações de *compliance*.

2) Coleta de termos

Os termos são os elementos hospedados em uma categoria e, em ambiente digital, podem servir como *links* que levam a outras páginas do sistema, tal como é a intenção deste modelo. Cada termo representa um tipo de dado que é tratado no hospital. Para os fins deste estudo, entende-se "tipo de dado pessoal" como a identificação do dado de acordo com a informação que ele carrega no sentido mais estrito possível.[2] São tipos de dados pessoais, por exemplo, o nome, o número no Cadastro de Pessoa Física (CPF), a ocupação profissional do titular, o resultado de um exame médico, bem como outros dados que representem informações referentes a pessoas físicas identificadas ou identificáveis. Neste modelo, cada termo serve como *link* para a página editável pelos usuários da taxonomia para registro de medidas de segurança que são ou podem ser adotadas em relação àquele tipo de dado específico, além de orientações para execução dessas ações técnicas e administrativas de *compliance*.

Na pretensa taxonomia, trabalha-se com um universo de termos que foram coletados a partir da análise dos processos operacionais e do fluxo informacional no hospital, bem como a partir das propostas de categorias de dados pessoais, estudadas anteriormente. Ou seja, tanto informações primárias extraídas de documentos fornecidos pela instituição e de respostas a questionamentos institucionais feitos

[2] "Tipo de dado pessoal" não se confunde com a categorização de dados pessoais de acordo com o seu conteúdo (apresentada posteriormente). Enquanto essa última é uma forma de classificação mais ampla de dados de acordo com o seu conteúdo informacional (por exemplo, informações cadastrais, informações médicas, etc.), aquela primeira é uma identificação mais restrita, referindo-se à específica informação apresentada pelo dado. Por exemplo, endereço é um tipo de dado pessoal, classificado como informação cadastral de acordo com o critério de conteúdo desse tipo de dado.

pelo autor, quanto conceitos presentes na bibliografia sobre dados pessoais, serviram como fontes informacionais para a coleta de termos. Alguns termos, ainda, apesar de não terem sido citados nos documentos apresentados pelo HUCF, foram incluídos devido à sua pertinência e importância (a exemplo de termos como "nome", "sexo", "endereço" e "telefone", que identificam e fornecem informações de contato de titulares de dados em fluxo na instituição, além de "termo de consentimento", importante documento na realização de procedimentos de saúde).

Quanto às garantias da OC, que balizam não apenas a coleta dos termos, mas toda a estrutura do SOC, são utilizadas as garantias de literatura, organizacional e cultural. A primeira se pauta na literatura especializada em LGPD e *compliance*, aplicada, neste caso, na identificação de determinados atributos de dados pessoais, especialmente aqueles com repercussão jurídica (como identificação de titulares e bases legais). Também são considerados termos próprios da literatura em sistemas de informação hospitalar e do próprio vocabulário médico, já que há dados relativos à saúde detectados no mapeamento. Por sua vez, a garantia organizacional, nesta proposta, tem como escopo a realidade de processos operacionais e de fluxos informacionais do HUCF. Logicamente, por conseguinte, as escolhas para organização do conhecimento aqui traçadas refletem a situação linguística do sistema jurídico sobre proteção de dados e da instituição, já que o modelo de taxonomia serve para uma finalidade específica a determinada instituição, em certa localidade e em uma época específica. Portanto, não há como desconsiderar a existência da garantia cultural para o modelo aqui apresentado, como decorrência natural das duas primeiras garantias.

3) Análise e controle dos termos coletados

Os termos listados na etapa anterior são, nesta fase, analisados e passam por controle terminológico, considerando as garantias da OC anteriormente destacadas. O idioma utilizado é a língua portuguesa, exceto quando determinada terminologia estrangeira é de conhecimento comum dos seus usuários ou o termo é de amplo uso pela literatura técnica (que são os casos de "*login*" e "*e-mail*"). Em regra, apenas a primeira letra dos descritores é maiúscula, exceto em "Cartão Nacional de Saúde (Cartão SUS)", por ser assim descrito pela linguagem institucional. Privilegia-se a forma masculina (quando possível) e em singular. Evita-se o uso de jargões, locuções verbais e adverbiais, bem como abreviaturas, para facilitar a compreensão e a navegação dos usuários pelos termos categorizados. Exceções ao evitamento de siglas e abreviaturas ocorre com a presença de "CPF", "MASP" e "SUS" entre os descritores.

Em diversos termos, recorreu-se aos parênteses para: a) diferenciação de termos, quando mesmos tipos de dados poderiam se referir a mais de um titular, de modo que se procurou diferenciá-los por parênteses para evitar duplicidades dentro de uma mesma categoria e tratar cada qual como se fosse um termo próprio, como em "nome (acompanhante)", "nome (doador)", "nome (colaborador)", "nome (paciente)"; b) detalhamento de termo, para servir como apoio à sua identificação, como em "registro de nascimento" (recém-nascido); c) para identificação de sinônimo, como em "Carteira Nacional de Saúde (Cartão SUS)" e "Registro funcional (MASP)". Nesta fase, nenhum dos termos listados na etapa anterior foram excluídos, de modo que todos foram eleitos para compor a taxonomia. Como resultado, chegou-se a uma lista de 74 termos, descritos e com pertinentes observações na lista a seguir:

Quadro 6: Lista e descrição de termos componentes da taxonomia

Termo	Descrição
Afastamento	Informação sobre afastamento de colaborador, registrado no Sistema Integrado.
Agendamento de exame	Registro de agendamento de exame no âmbito da Gerência de Apoio Diagnóstico.
Anamnese	É uma "entrevista" com o paciente, na qual são coletadas informações sobre seu histórico clínico e social, a fim de identificar suas necessidades. Assim como vários outros registros de informação no hospital, é dado pessoal relativo à saúde. No HUCF, é realizado por profissional de saúde, geralmente em ambulatório.
Autorização de cirurgia	É gerada como registro quando da verificação de necessidade de procedimento cirúrgico através de diagnóstico médico.
Autorização de internação hospitalar	De acordo com a literatura, este "é o documento hábil para identificar o paciente e os serviços prestados sob o regime de internação hospitalar e fornecer informações para o gerenciamento do sistema de informação da unidade hospitalar. É gerado quando ocorre uma internação em um prestador público ou privado" (Hospital Brasília, 2019, p. 1).
Avaliação nutricional	Avaliação de estado nutricional de paciente, feito por nutricionista (Silva; Sampaio, 2012), gerando documento que tem o paciente como titular. É, desse modo, dado pessoal relativo à sua saúde.
Avaliação profissional	Registro de avaliação profissional de colaborador que, por se referir a ele, é considerado dado pessoal.
Boletim de produção ambulatorial	Registro de atendimento realizado em ambulatório para prestação de contas ao SUS.
Carteira Nacional de Saúde (Cartão SUS)	Documento de identificação do usuário do SUS, comprovando que tal titular utiliza dos programas públicos de saúde.
Contrato de colaborador	É o contrato de vínculo de trabalho entre servidor contratado ou estagiário e a instituição hospitalar. O próprio registro do contrato é, em si, dado pessoal, porque representa informação acerca de uma relação laboral em que figura o colaborador (que é pessoa natural).
Controle de acesso	Registro de controle de acesso às dependências do hospital, referindo-se aos funcionários da instituição e sendo gerido no Sistema Integrado.
Cor de pele	Informação sobre cor de pele incluída no cadastro de paciente. É uma informação sensível, porque se refere a aspectos biológicos do indivíduo.
CPF (acompanhante)	Número em Cadastro de Pessoa Física de acompanhante de paciente, utilizado para identificação do indivíduo.
CPF (colaborador)	Número em Cadastro de Pessoa Física de colaborador, utilizado para identificação do indivíduo.

Termo	Descrição
CPF (doador)	Número em Cadastro de Pessoa Física de doador de órgãos, utilizado para identificação do indivíduo.
CPF (paciente)	Número em Cadastro de Pessoa Física de doador de órgãos, utilizado para identificação do indivíduo.
Data de nascimento/idade (acompanhante)	Data de nascimento e idade de acompanhante, postas em um mesmo descritor. Optou-se por colocá-las juntas, a fim de simplificar a organização do conhecimento e a recuperação da informação nesta proposta, já que a idade é decorrência lógica da data de nascimento.
Data de nascimento/idade (colaborador)	Data de nascimento e idade de colaborador, postas em um mesmo descritor.
Data de nascimento/idade (doador)	Data de nascimento e idade de doador de órgãos, postas em um mesmo descritor.
Data de nascimento/idade (paciente)	Data de nascimento e idade de paciente, postas em um mesmo descritor.
Declaração de nascido vivo (recém-nascido)	Declaração emitida pela instituição, de acordo com padrões estabelecidos pelo Ministério da Saúde, que, dentre outras finalidades, serve como documento obrigatório para registro civil de recém-nascido (Brasil, 2022c). Seu titular é o neonato, que é paciente.
Diagnóstico médico	Registro da identificação de enfermidade do paciente através dos sinais e sintomas apresentados pelo seu organismo (Hurtado, 2016).
E-mail	Registro de endereço eletrônico de colaborador, necessário para contato.
Encaminhamento de paciente externo	Guia de encaminhamento de paciente eterno ao HUCF. É dado pessoal porque diz respeito à condição do indivíduo de usuário encaminhado ao hospital.
Encaminhamento para internação	Guia de encaminhamento para internação hospitalar. É dado pessoal porque evidencia condição de necessidade de internação de paciente, importando em informação relativa à sua pessoa.
Endereço (acompanhante)	Endereço de domicílio de acompanhante, necessário para sua identificação, localização e contato.
Endereço (colaborador)	Endereço de domicílio de colaborador, necessário para sua identificação, localização e contato.
Endereço (doador)	Endereço de domicílio de doador, necessário para sua identificação, localização e contato.

Termo	Descrição
Endereço (paciente)	Endereço de domicílio de paciente, necessário para sua identificação, localização e contato.
Escala de plantão	Escala de trabalho em plantão de colaboradores. É registro de informação pessoal porque explicita horários e outras condições de trabalho em regime de plantão dos escalados.
Escala de trabalho	Escala de trabalho convencional (em turnos) de colaboradores.
Estado civil/nome do cônjuge	Informação sobre estado civil de paciente, juntamente com o nome de seu cônjuge (se casado), para fins de cadastro do usuário. São dados distintos, mas que, para efeitos de organização, foram colocados no mesmo descritor para facilitar a organização terminológica. São dados pessoais pois representam informação sobre o paciente, mas também sobre seu cônjuge.
Estado clínico	Informação sobre o estado de saúde de paciente.
Frequência de colaborador	Registro de frequência de colaborador ao trabalho.
Gravação de câmera de segurança	Imagens de circuito de segurança das dependências do hospital. Qualquer pessoa no âmbito do hospital (seja usuário, colaborador, acompanhante ou doador) pode ter sua imagem gravada. Este tipo de dado é gerenciado pelo Centro de Processamento de Dados.
Gravação telefônica	Dados de voz em ligações telefônicas estabelecidas em âmbito do HUCF, gravados para finalidade de registro da comunicação. Este tipo de dado também é gerenciado pelo Centro de Processamento de Dados.
Histórico médico	Histórico médico de paciente, gerenciado no Prontuário Médico do Sistema MV (MV PEP).
Identidade	Número de identificação de paciente no Registro Geral de cidadãos, necessário para cadastro do usuário.
Login	Credenciais de *login* em SIHs do hospital.
Mapa dietético	Prescrição de dieta adequada ao paciente de acordo com a sua avaliação nutricional.
Matrícula acadêmica (estagiário)	Número de matrícula acadêmica, necessária para identificação de colaborador quando for estagiário.
Nome (acompanhante)	Nome civil de acompanhante de paciente, necessário para sua identificação.
Nome (colaborador)	Nome civil de colaborador, necessário para sua identificação.
Nome (doador)	Nome civil de doador, necessário para sua identificação.

Termo	Descrição
Nome (paciente)	Nome civil de paciente, necessário para sua identificação.
Nome social	Nome de paciente transgênero de acordo com sua identidade de gênero.
Prestador	Registro identificador de colaborador para recuperação de acessos.
Ocupação profissional	Identificação de ocupação profissional de colaborador do hospital.
Registro de doação de órgãos	Informação referente à doação de órgãos, dizendo respeito tanto ao doador quanto ao paciente beneficiário.
Registro de nascimento (recém-nascido)	Certidão de nascimento, utilizado para cadastro de recém-nascido, que também é paciente, no hospital (razão pela qual se descreve seu titular em parênteses). O próprio registro do nascimento é, em si, dado pessoal.
Registro de ocorrência	Ocorrência de ato/fato envolvendo colaborador.
Registro de ponto	Registros de entrada e saída de colaborador em relógio de ponto, para controle da jornada de trabalho de colaboradores.
Registro de transfusão sanguínea	Registro de transfusão sanguínea. É dado pessoal, pois diz respeito à ação realizada por pessoa natural, o doador.
Registro funcional (MASP)	O registro funcional é um número identificador do servidor público. No âmbito do HUCF, utiliza-se o MASP (Matrícula do Servidor Público).
Relatório de alta hospitalar	A alta hospitalar ocorre após o tratamento clínico do paciente, quando comprovado que ele possui condições de retornar para casa. Como finalidade de registro, é feito um relatório, que é um tipo de dado pessoal por detalhar a condição de saúde do usuário.
Resultado de endoscopia	Resultado imagenológico de exame de endoscopia, em que se examina o trato de cavidades no corpo do paciente, especificamente no trato digestivo (Silva; Silva; Viana, 2011).
Resultado de exame parasitológico	Resultado de exame em que se busca verificar presença de parasitas no organismo do paciente (Silva; Silva; Viana, 2011).
Resultado de hemograma	Resultado de exame de análise de sangue.
Resultado de radiologia	Resultado de qualquer dos diversos tipos de exames radiológicos, isto é, de raios X (Silva; Silva; Viana, 2011).
Resultado de ultrassonografia	Resultado de exame de ultrassonografia, que consiste em "método diagnóstico que, mediante a emissão de ondas sonoras de alta frequência, permite a visualização de órgãos internos do corpo" (*sic*) (Silva; Silva; Viana, 2011, p. 841).

Termo	Descrição
Resultado de urinálise	Resultado de exame de urina, que analisa aspectos físicos, químicos e microbiológicos dessa substância para avaliar funções renais e outras questões anatômicas (Silva *et al.,* 2021).
Sexo (acompanhante)	Identificação de sexo de acompanhante de paciente.
Sexo (colaborador)	Identificação de sexo de colaborador.
Sexo (doador)	Identificação de sexo de doador.
Sexo (paciente)	Identificação de sexo de paciente.
Situação funcional	É o estado em que se encontra o servidor (se ativo, aposentado, demitido, exonerado, etc.).
Solicitação de exame	Guia de solicitação de exame para paciente. É dado pessoal porque indica necessidade de exame clínico do usuário, o que é informação referente a ele.
Telefone (acompanhante)	Contato telefônico de acompanhante de paciente, para fins de comunicação.
Telefone (colaborador)	Contato telefônico de colaborador, para fins de comunicação.
Telefone (doador)	Contato telefônico de doador, para fins de comunicação.
Telefone (paciente)	Contato telefônico de usuário do hospital, para fins de comunicação.
Termo de consentimento (acompanhante)	Documento pelo qual o paciente ou seu representante toma ciência dos riscos de determinado procedimento médico e concorda com a sua realização (Conselho Federal De Medicina, 2016). “Consentimento”, nesse sentido, não se confunde com o “consentimento” para coleta de dados, uma das bases legais da LGPD, que não é verificada no tratamento de dados pessoais no HUCF. Neste caso, o descritor refere-se a termo assinado por acompanhante do paciente, de modo que se configura como dado pessoal referente ao acompanhante e ao paciente.
Termo de consentimento (paciente)	Também é termo de consentimento livre e esclarecido, porém assinado pelo próprio paciente. Apesar de não ter sido evidenciado nas informações fornecidas pelo hospital, optou-se por incluir este elemento na taxonomia em razão da sua utilização em serviços de saúde em geral.
Tipo sanguíneo	É a tipagem sanguínea do paciente, sendo dado pessoal relativo à saúde do titular.

Fonte: elaboração própria, 2023.

4) Definição de categorias gerais e específicas

Para facilitar o mapeamento de dados, preferiu-se que a estrutura taxonômica possuísse apenas dois níveis organizacionais: as categorias gerais (aqui chamadas de facetas) e as categorias específicas dentro de cada faceta. Em regra, cada categoria específica possui um conjunto de objetos mutuamente excludentes, de forma que cada tipo de dado é encontrado em apenas uma categoria em cada faceta. Essa regra, contudo, comporta exceções, como se destacará mais à frente. Ainda, em determinadas facetas, por haver termos que não se enquadrariam em nenhuma das suas categorias pré-estabelecidas, preferiu-se incluir a categoria "outros".

Ademais, todos os termos escolhidos estão presentes em todas as facetas, enriquecendo as possibilidades de recuperação informacional. Por exemplo, "resultado de radiologia" pode ser incluído na categoria "tutela da saúde" na faceta "base legal", ao passo que é possível alocá-lo na categoria "imagem" na faceta "formato". Passando por um caminho ou outro, chega-se ao mesmo termo, que, ao ser clicado na *interface* do SIH, leva à página de registros de ações de *compliance* efetivamente e/ou pretensamente aplicadas pelo GT-LGPD/Unimontes em relação àquele tipo de dado.

Na definição das facetas, aproveitou-se das propostas de categorias para mapeamento de dados apresentadas por Pohlmann (2019), Komnenic (2022) e o Guia de Elaboração de Inventário de Dados da ANPD (Brasil, 2021a). Considerou-se, também, a realidade dos processos operacionais e do fluxo de dados no HUCF. As facetas definidas foram as seguintes: "conteúdo", "titular", "base legal", "natureza jurídica", "formato" e "sistema de informação".

A faceta "conteúdo" estabelece categorização de acordo com o tipo de informação materializada no dado. Trata-se de uma organização de dados pessoais considerando seu conteúdo de maneira mais ampla, não se confundindo com a noção de "tipo de dado pessoal", que remete à específica informação registrada (como nome, telefone, sexo, avaliação profissional, etc.). Suas categorias são as seguintes:

1) Informação cadastral: Informações de identificação pessoal e de contato registradas em cadastro de paciente, acompanhante, doador ou colaborador (ex. apelido, Cartão SUS, nome, sexo, telefone). São necessárias para realização de serviços hospitalares (no caso de pacientes, doadores e acompanhantes) ou mesmo para registro, controle e contato das pessoas envolvidas nas atividades da instituição.
2) Informação médica: São as informações de conteúdo médico-hospitalar, referentes a condições de saúde e a procedimentos clínicos envolvendo usuários da instituição. Nesse rol, inclui-se agendamento de exames, anamnese e resultados de exames.
3) Informação profissional: Dizem respeito ao cotidiano, às funções, ao desempenho e ao exercício profissional de colaboradores (servidores efetivos e contratados, terceirizados, estagiários e voluntários). Logicamente, alguns tipos de colaboradores titulam dados pessoais específicos à sua condição profissional. Por exemplo, apenas estagiários possuem matrícula acadêmica, enquanto apenas servidores efetivos e contratados possuem registro funcional (MASP).

4) Outros: Na distribuição de termos às categorias, “gravação de câmera de segurança” e “gravação telefônica” não se enquadram em nenhum dos outros tipos categóricos. Por serem utilizados para ações distintas entre si (a primeira por questão de segurança nas dependências das instituições e a segunda para registro de diálogos telefônicos), optou-se por incluí-los nesta categoria.

Há a faceta “titular”, terminologia presente no texto da LGPD e que diz respeito à pessoa natural, a quem os dados se referem (Brasil, 2018a, art. 5°, inc. V). As categorias específicas dessa faceta são:

1) Acompanhante: Hospeda termos relativos a dados de acompanhante de paciente, tais como seu nome, CPF, data de nascimento, gravações de imagem e voz, além de termos de consentimentos (para procedimentos clínicos) assinados pelo acompanhante do paciente.
2) Colaborador: Compreende dados relativos ao colaborador, tanto aqueles de conteúdo cadastral (como identificação e informações de contato), quanto aqueles de teor profissional (como credencial de *login*, escalas, controle de acesso e registros de ocorrência). Reitera-se que pode ser considerado colaborador, no âmbito do HUCF, servidor efetivo ou contratado, terceirizado e estagiário.
3) Doador: Diante do fornecimento de serviço público de doação de órgãos no HUCF, entendeu-se que o doador de órgãos (incluindo, aqui, de sangue) é um titular que deve ser tratado sob uma categoria própria. As informações sobre o doador compreendem desde aquelas de teor médico (como registros das doações e transfusões sanguíneas) até aquelas de conteúdo cadastral (como nome, sexo, data de nascimento/idade, dentre outras), além de gravações de som e imagem dessa pessoa.
4) Paciente: Pacientes são os usuários internos e externos (encaminhados) ao HUCF, beneficiários dos serviços médico-hospitalares fornecidos pela instituição, incluindo-se também os recém-nascidos. Assim como na categoria anterior, compreende informações de saúde, cadastrais, além de gravações telefônicas e de câmera de segurança.
5) Outros: Incluída como “categoria residual”, na mesma lógica da faceta anterior. Nesta faceta, inclui-se o termo “estado civil/nome do cônjuge”.

Observa-se que, em todas essas categorias, figuram os termos “gravação de câmera de segurança” e “gravação telefônica”, pois todas essas pessoas podem ter suas imagens capturadas pelo sistema de monitoramento do hospital, bem como suas vozes em registros de ligações telefônicas com o hospital. Também se observa que dados básicos de identificação e de contato foram convencionalmente estendidos a todos os titulares, ainda que não estivessem explícitas nos documentos fornecidos pelo HUCF. São eles: nome, data de nascimento/idade, sexo, endereço e telefone.

Vale enfatizar, ainda, que “termo de consentimento (acompanhante)” é uma exceção à regra geral de que um mesmo termo não se repete numa mesma faceta. Em relação ao seu titular, esse tipo de dado pessoal refere-se tanto ao acompanhante (por ser a pessoa que permite a realização do procedimento) quanto ao paciente. Já “termo de consentimento (paciente)” encontra-se apenas na categoria “paciente”, pois

apenas esse permite a realização do procedimento, não envolvendo informação sobre seu acompanhante, como aponta o quadro de descrição de termos.

Outra faceta é "base legal", que se refere à hipótese legal que justifica o tratamento de dados segundo a LGPD. Se não estiver adequado a alguma base legal, o tratamento de dados pessoais é considerado ilegítimo e, portanto, não pode ocorrer. Digno observar que, a partir das informações coletadas na pesquisa perante o HUCF, a base legal do consentimento não foi identificada em nenhum processo informacional.[3] Cada categoria dessa faceta é uma base legal, na qual se enquadra o respectivo dado pessoal representado. Como as bases legais são hipóteses taxativas (limitadas), não há razão para inclusão da categoria "outros", primeiro porque todos os tipos de dados levantados até aqui se incluem em alguma das quatro categorias seguintes, segundo porque bastaria incluir uma nova base legal como categoria em caso de inclusão de novos termos que não se encaixassem nas hipóteses já existentes. Em síntese, as categorias definidas para essa faceta são as seguintes:

1) Execução de contrato: Essa base legal legitima a coleta/produção e o tratamento de dado pessoal quando necessário para execução de contrato ou de seus procedimentos preliminares ou conexos. O único termo incluído nesta categoria é "contrato de colaborador", visto que a explicitação da relação contratual de trabalho é um dado pessoal por si só, sendo um pressuposto formal para que o colaborador preste serviços ao hospital.
2) Legítimo interesse: Como anteriormente explicado nesta obra, o legítimo interesse só pode ser evocado pelo agente de tratamento quando houver justificativa plausível para o tratamento de dados pessoais. Neste modelo de taxonomia, "login" e "prestador" são dados produzidos pela própria instituição, referentes ao colaborador e cuja finalidade é servir como credenciais para acesso a SIHs. Já os termos "gravação telefônica" e "gravação de câmera de segurança" envolvem os interesses institucionais e, de certo modo, públicos (porque o HUCF é uma entidade estatal) de registro de gravações telefônicas e monitoramento de prédios do hospital.
3) Obrigação legal ou regulatória: Base legal que justifica o tratamento de dados pessoais quando esse for necessário para execução de obrigações legais/regulatórias do controlador. No caso da taxonomia, compreende os deveres nas relações de trabalho entre a Unimontes (que representa administrativa e juridicamente o HUCF) e os seus colaboradores. Nesse sentido, dados cadastrais, de avaliação, de organização das jornadas de trabalho, de controle de acesso de funcionários, dentre outras relativas ao trabalho, decorrem de deveres jurídicos dessa entidade estatal.
4) Tutela da saúde: A justificativa legal para coleta/produção de dados pessoais, bem como outras operações de tratamento, em razão da sua necessidade para realização de serviços de saúde prestados por profissional competente.

[3] Todas as atividades médico-operacionais ou administrativas da instituição envolvem bases legais que não exigem termo de consentimento para coleta/tratamento de dados pessoais. Mesmo registros informacionais que envolvem alguma anuência (como autorizações de cirurgia e internação) não solicitam concordância do cidadão para tratamento de seus dados, mas para a realização do referido procedimento médico-hospitalar. Esse entendimento pauta-se em uma discussão estritamente lógico-jurídica, que foge do propósito central desta obra e, portanto, não precisa ser aqui delongada.

No escopo desta taxonomia, não se pode confundir a natureza desta categoria com a de "informações médicas" da faceta "conteúdo". Pelo contrário, "tutela da saúde" compreende informações cadastrais e médicas, seja de pacientes, doadores ou acompanhantes, desde que a finalidade do seu uso seja a realização de serviços de saúde.

Neste modelo taxonômico, convenciona-se chamar de "natureza jurídica" a ampla diferenciação feita pela LGPD entre dados sensíveis e não-sensíveis, possuindo caráter de faceta, graças à necessidade de maior proteção daquele primeiro tipo (conforme já destacado no início desta obra). Nesse sentido, as categorias dessa faceta são denominadas:

1) Não-sensível: Compreende todos os tipos de dados que não são sensíveis de acordo com a LGPD (como endereços de residência e de e-mail, registros profissionais dos colaboradores, informações de contato, nomes, dentre outros). A definição dos termos que compõem esse conjunto foi feita pelo critério de exclusão, isto é, aqueles que não são sensíveis foram aqui incluídos.
2) Sensível: São aqueles dados passíveis de discriminações abusivas e/ou ilegais (Mulholland, 2018). Neste modelo de SOC, incluem-se os tipos de dados relativos à saúde (como "estado clínico" e "tipo sanguíneo") e ao sexo dos titulares.

"Formato", outra faceta desta proposta, diz respeito ao formato em que o tipo de dado majoritariamente se encontra. Aqui, não se faz distinção entre suportes digitais e físicos, pois os registros de informação podem ser impressos ou digitalizados pelo pessoal do hospital, de acordo com as suas necessidades. Porém, isso não impede que, em fases posteriores do processo de *compliance* no HUCF, sejam discriminadas medidas de segurança e privacidade específicas para suportes analógicos e digitais. Para melhor localização e compreensão do formato de cada tipo de dado, escolheu-se dividi-los em:

1) Audiovisual: São aqueles registros em formato de áudio e/ou vídeo, quais sejam, "gravação de câmera de segurança" e "gravação telefônica";
2) Imagem: Compreende aqueles dados que são completa ou majoritariamente registrados em imagem estática (figuras). Foram identificados como representações informacionais imagéticas apenas os resultados de exames de endoscopia, radiologia e ultrassonografia;
3) Texto: Nesta faceta, incluem-se os dados que são representações total ou majoritariamente textuais, tanto em meio digital quanto físico. Todos os outros termos, que não foram incluídos nas categorias anteriores são, por decorrência lógica, compreendidos pela categoria "texto".

Por fim, há a faceta "sistema de informação". Como demonstra a descrição do HUCF apresentada neste estudo, o referido hospital aproveita-se de SIHs em todas as suas áreas. Nesse sentido, a partir da interpretação de quais são as espécies de informações trabalhadas em cada sistema, é possível atribuir tipos de dados pessoais geridos em cada um deles:

1) DATASUS: Responsável por gestão de dados do Sistema Único de Saúde, o HUCF explicita, em documentos apresentados ao autor, que possui acesso ao DATASUS. Identificou-se apenas a Carteira Nacional de Saúde (Cartão SUS) como tipo de dado originário do DATASUS que adentra o fluxo informacional do hospital;
2) Sistema Integrado: Sistema interno desta instituição, possui como foco a gestão de dados referentes aos seus colaboradores. Em razão disso, compreende tanto suas informações cadastrais (como "nome" e "telefone") quanto as de teor profissional (tais como "afastamento" e "frequência de colaborador");
3) Sistema MV: Sistema voltado à gestão hospitalar, onde se encontra, inclusive, as ferramentas de prontuário eletrônico (MV PEP). Compreende informações cadastrais (como "CPF" e "apelido"), mas também todas as informações de teor médico;
4) Outros: De acordo com as informações apresentadas pela instituição, gravações telefônicas e de câmeras de segurança não são gerenciadas em nenhum dos sistemas anteriores. Ainda assim, são armazenados no *Data Center* da GTI, assim como todos os outros dados em fluxo na organização. Por essa razão, optou-se por inclui-los na categoria "outros".

5) Ordenação e padronização gramatical das categorias

O controle terminológico, não apenas das facetas, como também das categorias específicas, seguiu a mesma lógica do que foi feito com os termos da taxonomia: privilegiou-se a forma masculina, no singular (com exceção de "outros" em duas facetas), em português, em linguagem clara e compreensível ao público-alvo da taxonomia. Evitou-se o uso de siglas e abreviaturas (com exceção de "DATASUS" e "Sistema MV", por serem nomenclaturas de amplo conhecimento da organização).

Chegou-se ao número de seis facetas, organizados de acordo com critério de relevância de cada atributo para a finalidade de mapeamento de dados, sendo elas: "conteúdo", "titular", "base legal", "natureza jurídica", "formato" e "sistema de informação". Seguiu-se um raciocínio lógico para a ordenação dessas facetas, começando das informações mais básicas (como seu conteúdo, seu titular, base legal e natureza jurídica conforme LGPD, por exemplo) até características mais específicas, mas que podem ser úteis, tanto para navegação do usuário, quanto para identificação de demandas específicas de *compliance* para determinados grupos de tipos de dados (como formato e SIH utilizado).

Quanto às categorias específicas, foram ordenadas em ordem alfabética, com exceção de "outros" nas facetas "conteúdo", "titular" e "sistema de informação", incluídas no último lugar de seu nível classificatório como forma de facilitar a recuperação da informação. Como já argumentado, se nenhuma das categorias navegadas contempla a entidade, "outros" faz a função de categoria "residual", devendo hospedar-se sempre após a última categoria temática.

Considerando as categorias gerais e específicas aqui apresentadas, apresenta-se o seguinte modelo de estrutura taxonômica, dentro dos quais são incluídos termos representativos de espécies de dados mapeados:

- **Conteúdo**
    - **Informação cadastral**
    - **Informação médica**
    - **Informação profissional**
    - **Outros**
- **Titular**
    - **Acompanhante**
    - **Colaborador**
    - **Doador**
    - **Paciente**
    - **Outros**
- **Base legal**
    - **Execução de contrato**
    - **Legítimo interesse**
    - **Obrigação legal ou regulatória**
    - **Tutela da saúde**
- **Natureza jurídica**
    - **Não-sensível**
    - **Sensível**
- **Formato**
    - **Audiovisual**
    - **Imagem**
    - **Texto**
- **Sistema de informação**
    - **DATASUS**
    - **Sistema integrado**
    - **Sistema MV**
    - **Outros**

6) Definição de relacionamentos semânticos entre os termos

Neste momento, são definidos os relacionamentos semânticos (hierárquicos, de equivalência e associativos, que já apresentamos anteriormente) entre os termos escolhidos para compor as taxonomias. A hierarquia própria da estrutura taxonômica implica em relações de subordinação entre categoria e termo e em relações de coordenação entre entidades de um mesmo nível classificatório. Nesse sentido, a própria forma da taxonomia já evidencia relacionamentos hierárquicos, sem necessidade, em nosso entendimento, de evidenciar notações por relações dessa natureza. Ademais, quanto às relações de equivalência, a fim de garantir maior facilidade na navegação pela taxonomia, não foram incluídos termos equivalentes, o que não afasta essa pos-

sibilidade em futuras atualizações do modelo aqui proposto, de acordo com a conveniência da equipe de *compliance* da instituição.

Os relacionamentos associativos, especificamente aqueles entre termos relacionados (notação TR), são úteis para esta proposta, pois indicam ao usuário a relação entre distintos tipos de dados que, em uma análise superficial, aparentariam não possuir conexão entre si. Foram evidenciados, portanto, os seguintes relacionamentos associativos, justificados por algum tipo de relação entre termos (que não compreende caráter hierárquico e de equivalência):

Quadro 7: Relações associativas entre termos da taxonomia e suas justificativas

Relações associativas		Justificativa
Nome (paciente)	Apelido	Identificam o paciente, sendo que o primeiro termo é uma identificação oficial (formal) e o segundo é uma identificação informal.
Nome (paciente)	Nome social	Enquanto o primeiro é o nome civil do paciente transgênero, o segundo é o nome pelo qual gostaria de ser chamado, de acordo com a sua identidade de gênero.
E-mail	Telefone (colaborador)	Ambas são informações de contato de colaborador, podendo ser úteis quando observadas em conjunto.
Identidade	CPF (paciente)	Ambos são registros de identificação do paciente.
Controle de acesso	Frequência de colaborador	A frequência do colaborador ao trabalho pressupõe a identificação de seus horários de entrada e saída das dependências do hospital.
Controle de acesso	Registro de ponto	Também o registro de ponto trabalha com horário e identificação de servidores que entram e saem do hospital, ainda que para finalidades de diferenças: um para segurança, outro para verificação do adequado cumprimento da jornada de trabalho.
Escala de trabalho	Escala de plantão	Ambas são escalas de trabalho, sendo que a primeira trabalha com turnos convencionais e a segunda organiza a distribuição de horários em plantões.
Registro funcional (MASP)	Matrícula acadêmica (estagiário)	No tratamento de dados do HUCF, são utilizadas para a mesma finalidade: número de identificação. Enquanto o primeiro é próprio do servidor público efetivo ou contratado, o outro é utilizado por estagiários (que possuem matrícula acadêmica em instituição de ensino).
Agendamento de exame	Solicitação de exame	Referem-se à realização de exames clínicos, sendo que um refere-se à solicitação de exame por profissional competente e o outro ao agendamento feito pelo hospital. Ainda assim, são tipos de dados pessoais distintos, pois representam momentos e circunstâncias distintos no processo de atendimento do usuário no hospital.

Relações associativas		Justificativa
Anamnese	Diagnóstico médico	A anamnese compreende a análise da condição do paciente, enquanto o diagnóstico é a conclusão alcançada pelo médico, com apoio de exames e outros procedimentos clínicos. Originam-se, portanto, de diferentes atos no processo de diagnóstico, implicando em informações pessoais de teor distinto.
Autorização de cirurgia	Autorização de internação hospitalar	A cirurgia indicada por aquele primeiro termo, em certos casos, é a finalidade da internação hospitalar referenciada pelo segundo descritor.
Estado clínico	Histórico médico	Enquanto o estado clínico indica a situação atual do paciente, o histórico médico é informação sobre as condições de saúde pretéritas do usuário.
Mapa dietético	Avaliação nutricional	Enquanto a avaliação nutricional verifica o estado nutricional do paciente e as suas necessidades, o mapa dietético é a prescrição nutricional do paciente no HUCF.
Termo de consentimento (paciente)	Termo de consentimento (acompanhante)	O primeiro é assinado pelo próprio paciente, enquanto o segundo é assinado pelo seu acompanhante. Ainda assim, suas finalidades são as mesmas: assegurar anuência do usuário ou seu representante acerca do procedimento clínico a ser realizado.
Gravação de câmera de segurança	Gravação telefônica	Possuem aspecto comum de ser gravações, ainda que em formatos e usos distintos.

Fonte: elaboração própria, 2023.

Neste ponto da elaboração do modelo, é possível apresentar a estrutura taxonômica, contemplada tanto pelas relações hierárquicas entre facetas, categorias e termos (evidenciadas pela sua própria estrutura, não por notações), quanto pelas relações associativas retromencionadas (identificadas pela notação TR):

CONTEÚDO

Informação cadastral

Apelido TR Nome (paciente)

Carteira Nacional de Saúde (Cartão SUS)

Cor de pele

CPF (acompanhante)

CPF (colaborador)

CPF (doador)

CPF (paciente) *TR Identidade*

Data de nascimento/idade (acompanhante)

Data de nascimento/idade (colaborador)

Data de nascimento/idade (doador)

Data de nascimento/idade (paciente)

Declaração de nascido vivo (recém-nascido)
E-mail *TR Telefone (colaborador)*
Endereço (acompanhante)
Endereço (colaborador)
Endereço (doador)
Endereço (paciente)
Estado civil/nome do cônjuge
Identidade *TR CPF (paciente)*
Nome (acompanhante)
Nome (colaborador)
Nome (doador)
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Registro de nascimento (recém-nascido)
Sexo (acompanhante)
Sexo (colaborador)
Sexo (doador)
Sexo (paciente)
Telefone (acompanhante)
Telefone (colaborador) *TR E-mail*
Telefone (doador)
Telefone (paciente)

Informação médica

Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Boletim de produção ambulatorial
Diagnóstico médico *TR Anamnese*
Encaminhamento de paciente externo
Encaminhamento para internação
Estado clínico *TR Histórico médico*
Histórico médico *TR Estado clínico*
Mapa dietético *TR Avaliação nutricional*
Registro de doação de órgãos

Registro de transfusão sanguínea
Relatório de alta hospitalar
Resultado de endoscopia
Resultado de exame parasitológico
Resultado de hemograma
Resultado de radiologia
Resultado de ultrassonografia
Resultado de urinálise
Solicitação de exame *TR Agendamento de exame*
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

Informação profissional

Afastamento
Avaliação profissional
Contrato de colaborador
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
Escala de plantão *TR Escala de trabalho*
Escala de trabalho *TR Escala de plantão*
Frequência de colaborador *TR Controle de acesso*
Login
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Ocupação profissional
Prestador
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Situação funcional

Outros

Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*

TITULAR

Acompanhante

CPF (acompanhante)
Data de nascimento/idade (acompanhante)
Endereço (acompanhante)

Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*
Nome (acompanhante)
Sexo (acompanhante)
Telefone (acompanhante)
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*

Colaborador

Afastamento
Avaliação profissional
Contrato de colaborador
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
CPF (colaborador)
Data de nascimento/idade (colaborador)
E-mail *TR Telefone (colaborador)*
Endereço (colaborador)
Escala de plantão *TR Escala de trabalho*
Escala de trabalho *TR Escala de plantão*
Frequência de colaborador *TR Controle de acesso*
Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*
Login
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Nome (colaborador)
Ocupação profissional
Prestador
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Sexo (colaborador)
Situação funcional
Telefone (colaborador)*TR E-mail*

Doador

CPF (doador)
Data de nascimento/idade (doador)
Endereço (doador)
Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*

Nome (doador)
Registro de doação de órgãos
Registro de transfusão sanguínea
Sexo (doador)
Telefone (doador)

Paciente

Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Apelido *TR Nome (paciente)*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Boletim de produção ambulatorial
Carteira Nacional de Saúde (Cartão SUS)
Cor de pele
CPF (paciente) *TR Identidade*
Data de nascimento/idade (paciente)
Declaração de nascido vivo (recém-nascido)
Diagnóstico médico *TR Anamnese*
Encaminhamento de paciente externo
Encaminhamento para internação
Endereço (paciente)
Estado civil/nome do cônjuge
Estado clínico *TR Histórico médico*
Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*
Histórico médico *TR Estado clínico*
Identidade *TR CPF (paciente)*
Mapa dietético *TR Avaliação nutricional*
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Registro de nascimento (recém-nascido)
Relatório de alta hospitalar
Resultado de endoscopia
Resultado de exame parasitológico
Resultado de hemograma
Resultado de radiologia
Resultado de ultrassonografia

Resultado de urinálise
Sexo (paciente)
Solicitação de exame *TR Agendamento de exame*
Telefone (paciente)
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

Outros

Estado civil/nome do cônjuge

BASE LEGAL

Execução de contrato

Contrato de colaborador

Legítimo interesse

Login
Gravação telefônica *TR Gravação de câmera de segurança*
Gravação de câmera de segurança *TR Gravação telefônica*
Prestador

Obrigação legal ou regulatória

Afastamento
Avaliação profissional
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
CPF (colaborador)
Data de nascimento/idade (colaborador)
E-mail *TR Telefone (colaborador)*
Endereço (colaborador)
Escala de plantão *TR Escala de trabalho*
Escala de trabalho *TR Escala de plantão*
Frequência de colaborador *TR Controle de acesso*
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Nome (colaborador)
Ocupação profissional
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Sexo (colaborador)
Situação funcional
Telefone (colaborador) *TR E-mail*

Tutela da saúde

Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Apelido *TR Nome (paciente)*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Boletim de produção ambulatorial
Carteira Nacional de Saúde (Cartão SUS)
Cor de pele
CPF (acompanhante)
CPF (doador)
CPF (paciente) *TR Identidade*
Data de nascimento/idade (acompanhante)
Data de nascimento/idade (doador)
Data de nascimento/idade (paciente)
Declaração de nascido vivo (recém-nascido)
Diagnóstico médico *TR Anamnese*
Encaminhamento de paciente externo
Encaminhamento para internação
Endereço (acompanhante)
Endereço (doador)
Endereço (paciente)
Estado civil/nome do cônjuge
Estado clínico *TR Histórico médico*
Histórico médico *TR Estado clínico*
Identidade *TR CPF (paciente)*
Mapa dietético *TR Avaliação nutricional*
Nome (acompanhante)
Nome (doador)
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Registro de doação de órgãos
Registro de nascimento (recém-nascido)
Registro de transfusão sanguínea
Relatório de alta hospitalar
Resultado de endoscopia
Resultado de exame parasitológico

Resultado de hemograma
Resultado de radiologia
Resultado de ultrassonografia
Resultado de urinálise
Sexo (acompanhante)
Sexo (doador)
Sexo (paciente)
Solicitação de exame *TR Agendamento de exame*
Telefone (acompanhante)
Telefone (doador)
Telefone (paciente)
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

NATUREZA JURÍDICA

Não-sensível

Afastamento
Apelido *TR Nome (paciente)*
Avaliação profissional
Carteira Nacional de Saúde (Cartão SUS)
Contrato de colaborador
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
CPF (acompanhante)
CPF (colaborador)
CPF (doador)
CPF (paciente) *TR Identidade*
Data de nascimento/idade (acompanhante)
Data de nascimento/idade (colaborador)
Data de nascimento/idade (doador)
Data de nascimento/idade (paciente)
Declaração de nascido vivo (recém-nascido)
E-mail *TR Telefone (colaborador)*
Endereço (acompanhante)
Endereço (colaborador)
Endereço (doador)
Endereço (paciente)

Escala de plantão *TR Escala de trabalho*
Escala de trabalho *TR Escala de plantão*
Estado civil/nome do cônjuge
Frequência de colaborador *TR Controle de acesso*
Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*
Identidade *TR CPF (paciente)*
Login
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Nome (acompanhante)
Nome (colaborador)
Nome (doador)
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Ocupação profissional
Prestador
Registro de nascimento (recém-nascido)
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Situação funcional
Telefone (acompanhante)
Telefone (colaborador) *TR E-mail*
Telefone (doador)
Telefone (paciente)

Sensível

Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Boletim de produção ambulatorial
Cor de pele
Diagnóstico médico *TR Anamnese*
Encaminhamento de paciente externo
Encaminhamento para internação
Estado clínico *TR Histórico médico*
Histórico médico *TR Estado clínico*

Mapa dietético *TR Avaliação nutricional*
Registro de doação de órgãos
Registro de transfusão sanguínea
Relatório de alta hospitalar
Resultado de endoscopia
Resultado de exame parasitológico
Resultado de hemograma
Resultado de radiologia
Resultado de ultrassonografia
Resultado de urinálise
Sexo (acompanhante)
Sexo (colaborador)
Sexo (doador)
Sexo (paciente)
Solicitação de exame *TR Agendamento de exame*
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

FORMATO

Audiovisual

Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*

Imagem

Resultado de endoscopia
Resultado de radiologia
Resultado de ultrassonografia

Texto

Afastamento
Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Apelido *TR Nome (paciente)*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Avaliação profissional
Boletim de produção ambulatorial

Carteira Nacional de Saúde (Cartão SUS)
Contrato de colaborador
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
Cor de pele
CPF (acompanhante)
CPF (colaborador)
CPF (doador)
CPF (paciente) *TR Identidade*
Data de nascimento/idade (acompanhante)
Data de nascimento/idade (colaborador)
Data de nascimento/idade (doador)
Data de nascimento/idade (paciente)
Declaração de nascido vivo (recém-nascido)
Diagnóstico médico *TR Anamnese*
E-mail *TR Telefone (colaborador)*
Encaminhamento de paciente externo
Encaminhamento para internação
Endereço (acompanhante)
Endereço (colaborador)
Endereço (doador)
Endereço (paciente)
Escala de plantão *TR Escala de trabalho*
Escala de trabalho *TR Escala de plantão*
Estado civil/nome do cônjuge
Estado clínico *TR Histórico médico*
Frequência de colaborador *TR Controle de acesso*
Histórico médico *TR Estado clínico*
Identidade *TR CPF (paciente)*
Login
Mapa dietético *TR Avaliação nutricional*
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Nome (acompanhante)
Nome (colaborador)
Nome (doador)
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Ocupação profissional
Prestador

Registro de doação de órgãos
Registro de nascimento (recém-nascido)
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro de transfusão sanguínea
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Relatório de alta hospitalar
Resultado de exame parasitológico
Resultado de hemograma
Resultado de urinálise
Sexo (acompanhante)
Sexo (colaborador)
Sexo (doador)
Sexo (paciente)
Situação funcional
Solicitação de exame *TR Agendamento de exame*
Telefone (acompanhante)
Telefone (colaborador) *TR E-mail*
Telefone (doador)
Telefone (paciente)
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

SISTEMA DE INFORMAÇÃO

DATASUS

Carteira Nacional de Saúde (Cartão SUS)

Sistema Integrado

Afastamento
Avaliação profissional
Contrato de colaborador
Controle de acesso *TR Frequência de colaborador TR Registro de ponto*
CPF (colaborador)
Data de nascimento/idade (colaborador)
E-mail *TR Telefone (colaborador)*
Endereço (colaborador)
Escala de plantão *TR Escala de trabalho*

Escala de trabalho *TR Escala de plantão*
Frequência de colaborador *TR Controle de acesso*
Login
Matrícula acadêmica (estagiário) *TR Registro funcional (MASP)*
Nome (colaborador)
Ocupação profissional
Prestador
Registro de ocorrência
Registro de ponto *TR Controle de acesso*
Registro funcional (MASP) *TR Matrícula acadêmica (estagiário)*
Sexo (colaborador)
Situação funcional
Telefone (colaborador) *TR E-mail*

Sistema MV

Agendamento de exame *TR Solicitação de exame*
Anamnese *TR Diagnóstico médico*
Apelido *TR Nome (paciente)*
Autorização de cirurgia *TR Autorização de internação hospitalar*
Autorização de internação hospitalar *TR Autorização de cirurgia*
Avaliação nutricional *TR Mapa dietético*
Boletim de produção ambulatorial
Cor de pele
CPF (acompanhante)
CPF (doador)
CPF (paciente) *TR Identidade*
Data de nascimento/idade (acompanhante)
Data de nascimento/idade (doador)
Data de nascimento/idade (paciente)
Declaração de nascido vivo (recém-nascido)
Diagnóstico médico *TR Anamnese*
Encaminhamento de paciente externo
Encaminhamento para internação
Endereço (acompanhante)
Endereço (doador)
Endereço (paciente)
Estado civil/nome do cônjuge
Estado clínico *TR Histórico médico*
Histórico médico *TR Estado clínico*

Identidade *TR CPF (paciente)*
Mapa dietético *TR Avaliação nutricional*
Nome (acompanhante)
Nome (doador)
Nome (paciente) *TR Apelido TR Nome social*
Nome social *TR Nome (paciente)*
Registro de doação de órgãos
Registro de nascimento (recém-nascido)
Registro de transfusão sanguínea
Relatório de alta hospitalar
Resultado de endoscopia
Resultado de exame parasitológico
Resultado de hemograma
Resultado de radiologia
Resultado de ultrassonografia
Resultado de urinálise
Sexo (acompanhante)
Sexo (doador)
Sexo (paciente)
Solicitação de exame *TR Agendamento de exame*
Telefone (acompanhante)
Telefone (doador)
Telefone (paciente)
Termo de consentimento (acompanhante) *TR Termo de consentimento (paciente)*
Termo de consentimento (paciente) *TR Termo de consentimento (acompanhante)*
Tipo sanguíneo

Outros

Gravação de câmera de segurança *TR Gravação telefônica*
Gravação telefônica *TR Gravação de câmera de segurança*

7) Validação

Na validação, verifica-se se o sistema já representa com fidelidade a realidade informacional da instituição em que será implantado, o que foi feito através de uma revisão entre os documentos cedidos pelo HUCF e as entidades contidas na estrutura taxonômica. Observou-se que a estrutura taxonômica é adequadamente representativa das tipologias de dados pessoais em fluxo, considerados os vastos registros sobre dados pessoais e atividades operacionais que lhes envolvem, informações que foram fornecidas pelo hospital.

8) Definição da forma de apresentação da taxonomia e tecnologia de suporte

Propõe-se que a estrutura taxonômica seja implantada como um SIH, assim como os que já existem no HUCF, a exemplo do Sistema MV e do Sistema Integrado (cuja estrutura é taxonômica, com itens dispostos em níveis classificacionais). Aliás, esse último foi criado pela equipe de Tecnologia da Informação da própria instituição, como apontam as informações oferecidas pelo hospital, o que permite inferir que tal organização possui condições de implantar o modelo aqui sugerido em ambiente computacional.

A ideia é que, assim como no Sistema Integrado, a equipe de *compliance* em LGPD (usuários do sistema) tenha à sua disposição uma estrutura taxonômica, servindo neste caso como mapa de dados pessoais, além de permitir registros de ações de *compliance* em relação a cada tipo de dado (função esta que extrapola os limites da organização do conhecimento).

Sugere-se a inclusão de uma opção de "exibir itens" (representada pelo ícone +) e "ocultar itens" (representada pelo ícone -) entre os níveis classificacionais, para facilitar a navegação do usuário. Essa ferramenta, que "amplia" ou "restringe" a visualização de itens informacionais da taxonomia, já existe, por exemplo, na estrutura do Sistema Integrado.

Como medida de segurança, deve haver controle sobre acesso dos usuários do sistema. Assim, é interessante que cada membro da equipe de *compliance* no HUCF possua um *login* para acessar o sistema, mapear o fluxo de dados da instituição e realizar os devidos ajustes. Essa configuração exige uma arquitetura computacional mais rebuscada no sistema, mas já é realidade em outras SIHs da instituição como o Sistema MV.

9) Publicação

Como a intenção deste estudo não é fazer efetiva implantação da taxonomia aqui proposta, mas utilizá-la como modelo de SOC adequado ao apoio no processo de *compliance* em LGPD, não houve publicação no HUCF. Deve-se enfatizar, contudo, que ela deve ser implementada como SIH com restrito acesso à equipe de *compliance* de dados pessoais na instituição, garantidas a sua segurança e estabilidade computacional. Além disso, frente às constantes mudanças no fluxo informacional de uma organização, seu uso deve ser permanente.

10) Determinação de ações de gerenciamento

Por ser um SOC definitivo, já que o processo de *compliance* em LGPD nunca se encerra, sempre necessitando de novas análises e atualizações do mapa de dados e da identificação de ações de segurança e privacidade, devem ser definidas práticas de gerenciamento da taxonomia. Assim que publicada, recomenda-se a realização de reuniões de instrução aos usuários sobre como utilizar o sistema taxonômico e aproveitar suas funcionalidades para pensar adequadas medidas de *compliance* de acor-

do com as diversas dimensões que os tipos de dados podem ser observados. Além disso, é útil a elaboração de manuais de uso, que orientem com maior profundidade sobre a utilização desse SOC.

Quanto aos papéis de gerenciamento da taxonomia, devem ser definidos os responsáveis pela sua gestão e manutenção. No caso do modelo sugerido ao HUCF, são os próprios usuários da taxonomia, a equipe de *compliance* em LGPD (GT-L-GPD), já que são eles os responsáveis pelo mapeamento de dados, atividade que gera a estrutura de categorias. Também devem ser definidas as funções de registro das medidas de segurança e privacidade a cada tipo de dado nos termos taxonômicos, de controle de acesso ao SIH e de determinação de periodicidade de manutenções. A realização de reuniões periódicas para cuidar da taxonomia também deve ser pré-estabelecida entre os usuários e gerenciadores desse sistema.

11) Manutenção

A manutenção da taxonomia deve ser feita pelas pessoas escolhidas na etapa anterior. Esta fase não envolve apenas ações de garantias de segurança e estabilidade computacional do SIH em que a taxonomia se encontra, mas também a periódica atualização do mapa de dados (tanto em relação aos seus termos, quanto em relação às facetas e categorias). Ou seja, enquanto o primeiro mapeamento de dados pessoais serve para estruturar a taxonomia, os próximos têm a função de atualizá-la.

7.4 Benefícios de uma taxonomia para mapeamento de dados na instituição-modelo

O modelo de sistema de organização do conhecimento aqui sugerido volta-se ao uso corporativo, logo, possui aplicação restrita a uma instituição. Sua finalidade é bem definida: servir como suporte para o mapeamento de dados pessoais na medida em que se estrutura como um mapa de dados interativo, cujos *links* dos termos podem levar a páginas que permitem registro de ações de segurança e privacidade realizadas e/ou pretendidas em relação a cada tipo de dado organizado.

Para se alcançar esse propósito em uma instituição hospitalar, há desafios atinentes à própria construção de taxonomias: investimento de tempo, recursos tecnológicos e de pessoal para a execução desta tarefa; necessidade de destinação de pessoal competente para gerenciamento e atualização do sistema. Da mesma maneira, o primeiro mapeamento de dados pessoais, de onde saem os primeiros descritores e categorias do SOC, também apresenta desafios e riscos à instituição: gasto de tempo para o mapeamento; risco de desatualização dos registros com o tempo (já que os dados continuam em fluxo); possibilidade de que nem todos os tipos de dados sejam detectados (Furtado, 2020). Esses óbices, no entanto, são transponíveis através da persistência da instituição em construi-lo e em atualizá-lo em seus aspectos computacionais e de organização informacional.

A despeito dessas dificuldades, o SOC proposto apresenta condições de apoiar a aplicação da LGPD em uma instituição hospitalar, tomando-se o HUCF como marco empírico do modelo aqui elaborado. O primeiro uso deste SOC é a organização

do conhecimento institucional sobre os dados pessoais em fluxo no hospital, conhecimento este socializado e disperso entre os setores corporativos e que, por meio da taxonomia, centraliza-se em uma estrutura classificatória voltada ao uso da equipe de *compliance* em LGPD. No que tange ao estabelecimento de conceitos e relações conceituais nesse sistema, destaca-se, também, a importância das relações associativas entre os descritores, que facilitam a visualização de tipos de dados relacionados entre si e, portanto, a recuperação informacional.

O segundo uso, que decorre da sistematização digital de termos em categorias sob múltiplas dimensões (facetas), é a capacidade instrumental de que itens categorizados funcionem também como *links* que levem a páginas em que a equipe de *compliance* possa registrar ações de segurança e privacidade adotadas e/ou a serem planejadas em relação a cada tipo de dado. Por exemplo, clicando no termo "prestador", em qualquer das suas posições nos níveis de classificação taxonômica, chega-se à mesma página onde se possa registrar medidas de *compliance* presentes e/ou futuras em relação àquele tipo de dado. Essa ferramenta permite que o GT-LGPD/Unimontes possa ter controle das diversas ações de implantação da norma de proteção de dados, considerando as especificidades de cada tipo de dado em seus diversos atributos (representados pelas suas categorias). Ainda é justo destacar que a construção da taxonomia em SIH, além de viabilizar computacionalmente o controle de acesso de usuários, torna esse SOC mais perene e estável que uma simples planilha de mapeamento de dados, por exemplo. Dessa forma, facilita atualizações periódicas no mapa de dados, conforme é sugerido pela literatura de *compliance* em LGPD. Apesar dos benefícios e das sugestões em relação à taxonomia digital, a aplicação computacional desse sistema não é foco desta obra.

Assim, a discussão de ordem teórico-metodológica estabelecida neste estudo, com um modelo representativo de sua futura aplicação, não se esgota em si, mas permite que esta pesquisa tenha uma contribuição pragmática à realidade. Fica provado que um processo de organização do conhecimento, qual seja, a classificação em estrutura taxonômica, auxilia na construção e na visualização de um mapa de dados pessoais como suporte ao *compliance* em instituições hospitalares. Diante do que fora descrito, o modelo de SOC proposto não se restringe à representação do conhecimento sobre os aspectos de dados pessoais no hospital (por meio da estrutura taxonômica), mas também permite a recuperação das informações nele organizadas (graças à possibilidade de armazenamento de itens informacionais, amplamente citada pela literatura especializada).

Como abordado por Keinert (2018), a promoção da proteção de dados pessoais não passa apenas por uma abordagem normativa (de observância da lei), mas também tecnológica (de promoção de medidas técnico-computacionais de segurança) e comportamental (conscientização das pessoas sobre a importância da privacidade informacional). O SOC sugerido contribui para todas essas dimensões: primeiro, o dever de registro de operações de dados, por meio de seu mapeamento, passa a ser exercido pela instituição (Brasil, 2018a, art. 37); em segundo lugar, também é executada a gestão de medidas de segurança e privacidade; e, por fim, a equipe de *compliance* passa a reconhecer melhor quais são as necessidades para proteção de dados pessoais específicas a cada tipo de dado.

Em um hospital de tamanha importância regional como o HUCF, é de grande valia a presença desse SOC como suporte à efetivação de uma das fases mais desa-

fiadoras no processo de implantação da LGPD. Por se tratar de hospital público, as funcionalidades da taxonomia, assim como a maior segurança e estabilidade dos seus registros (graças à sua implantação em SIH), causam impacto positivo não apenas à instituição que se beneficia de um *compliance* mais seguro e otimizado, mas à Administração Pública como um todo. Em outro plano, toda a população norte-mineira, que de maneira direta ou indireta se beneficia com os serviços do HUCF, é privilegiada pelo papel de um sistema como esse, que visa, enfim, a proteção de dados pessoais dos cidadãos. Ademais, não se pode olvidar que as entidades públicas também se submetem às sanções da LGPD (com exceção das multas), de modo que a má adequação à lei nessas instituições também pode acarretar em punições administrativas.

Por fim, destaca-se que, ao ser aplicada em outros hospitais públicos, a taxonomia pode necessitar de adequações de acordo com cada realidade informacional. Ainda assim, os mesmos benefícios verificados em âmbito do HUCF podem ser observados em outras instituições hospitalares, que, além de trabalharem com fluxos informacionais semelhantes (já que são todas instituições de saúde), também possuem inestimável valor social.

8

Considerações finais

Na sociedade informacional, marcada pela massiva utilização de tecnologias de informação e comunicação, muitas são as mudanças nas relações humanas no que tange às trocas informacionais. Dentre elas, destaca-se a crescente utilização de dados pessoais, que são registros de informação referentes a pessoas naturais identificadas ou passíveis de identificação (identificáveis), tratados tanto por pessoas físicas, quanto por organizações públicas ou privadas. Com os insurgentes interesses econômicos, mas também políticos e até mesmo privados, sobre os dados pessoais, os riscos de violações aumentam, colocando em risco a privacidade dos cidadãos.

Nessa conjuntura, centenas de países se movimentam no sentido de criar e efetivar leis de proteção de dados pessoais. No Brasil, não seria diferente: surgiu, em 2018, a Lei Geral de Proteção de Dados Pessoais, que inova no ordenamento jurídico nacional ao institucionalizar regras gerais para o tratamento de dados pessoais não apenas no Brasil, mas também, em alguns casos, fora dele. Para que a instituição que trata esses tipos de dados se adeque às exigências dessa norma, é necessária a execução de um programa de adequação (*compliance*) em LGPD, que compreenda etapas de avaliação da instituição, registro de operações de tratamento, criação de relatórios de impacto de proteção de dados, bem como a adoção de medidas de segurança e privacidade informacionais.

Nessa toada, esta obra recorreu à dimensão instrumental (aplicada) da organização do conhecimento, disciplina localizada no campo científico da Ciência da Informação, para propor o desenvolvimento de um modelo de taxonomia capaz de dar suporte a instituições hospitalares em *compliance* com a LGPD. Como marco empírico desta proposta de ordem teórico-metodológica, mas de reflexos concretos e pragmáticos, escolheu-se o Hospital Universitário Clemente de Faria (HUCF), vinculado à Universidade Estadual de Montes Claros (Unimontes).

Tomando como referência o HUCF, fica evidente a necessidade de mapear dados pessoais para conhecer melhor as especificidades dessas instituições e, assim, propor adequadas ações de *compliance*. Diante dos tipos de SOCs, percebe-se uma maior predisposição das taxonomias em satisfazer essa necessidade de organização do conhecimento corporativo acerca dos dados pessoais.

O principal aspecto taxonômico que parece, ainda neste ponto do trabalho, chamar a nossa atenção é a estrutura desse SOC: com uma organização baseada em níveis classificatórios, uma taxonomia pode organizar tipos de dados pessoais em diversas categorias, dando forma a um mapa de dados pessoais que possa apoiar a

implantação da LGPD. E assim foi feito. A partir de uma proposta metodológica autoral de construção de taxonomias corporativas digitais (voltada a finalidades gerais), criada a partir da comparação e da análise de metodologias de outros autores, procurou-se desenvolver um modelo aplicável à intenção de mapear dados pessoais, tomando-se o HUCF como modelo pragmático para tanto. Sob a lógica de classificação facetada, trabalhou-se com facetas que representam distintas dimensões categoriais sobre as quais um tipo de dado possa ser categorizado e analisado.

Em sequência, é ilustrado o processo de desenvolvimento da pretensa taxonomia, com foco não apenas em seus aspectos computacionais (que não faz parte do escopo de nossa investigação), mas preocupando-se com seus aspectos de organização do conhecimento: controle terminológico, categorização, hierarquização de termos e determinação de relações semânticas. Na nossa proposta, o público-alvo desse modelo de taxonomia seria a equipe de *compliance* de dados pessoais (no caso do HUCF, o GT-LGPD/Unimontes).

Com base no modelo assentado na realidade administrativa e informacional do HUCF, foi possível detectar dois principais usos da taxonomia para mapeamento de dados pessoais:

a) Categorização de tipos de dados (na forma de termos) em distintas dimensões (facetas) para servir como suporte no mapeamento de dados pessoais, em um primeiro momento, e como referência para atualização do mapa de dados construído sobre essa estrutura taxonômica digital, já depois de publicada;

b)Possibilidade de transformar termos em *links* que levem a páginas onde os usuários da taxonomia possam registrar ações de segurança e privacidade adotadas ou planejadas especificamente àquele tipo de dado (considerando suas peculiaridades e atributos, evidenciados pelas suas categorias). Essa função extrapola os limites da OC, mas demonstra ser útil na adequação institucional à LGPD, na medida em que facilita o registro de ações de *compliance*, unificando-os em um mesmo local. Ademais, com a possibilidade de criação de credenciais para acesso à taxonomia, mostra-se ainda mais seguro fazer o controle das ações de *compliance* nessa mesma ferramenta virtual.

Associados, esses dois usos do SOC proposto implicam na maior aderência de determinadas políticas técnicas (computacionais) e administrativas (gerenciais) de segurança e privacidade, graças à verificação de determinado atributo (categoria) daquele tipo de dado. Por exemplo, para verificar se os tratamentos sob legítimo interesse possuem justificativas plausíveis, pode-se utilizar o mapa de dados para localizar essa categoria e seus dados. Clicando-se nesses termos, pode-se abrir página de registro em que o usuário anote a razão para o tratamento sob tal base legal, sendo que esse procedimento é uma medida de segurança e privacidade, observando as exigências da LGPD.

Em conclusão, a pesquisa da qual se origina esta obra sucedeu a demonstrar como a taxonomia (enquanto SOC) pode apoiar hospitais (na instituição-modelo, o HUCF) na implantação da LGPD. A indagação central desta obra, apresentada no

capítulo de apresentação, foi esclarecida. Em síntese: cria-se uma taxonomia corporativa e digital que estruture mapas de dados pessoais da instituição em que se aplica, servindo como apoio para que a equipe de *compliance* possa avaliar os tipos de dados em fluxo na organização e pensar em ações específicas às características de cada item de informação.

Em última análise, esta obra foi capaz de demonstrar que é possível associar a organização do conhecimento com as demandas contemporâneas da sociedade informacional, mesmo aquelas de fora da Ciência da Informação (como é o caso das exigências jurídicas de uma lei). Servindo ao conhecimento socializado e registrado (acerca de tipos de dados pessoais em fluxo numa instituição), a CI (na dimensão instrumental da organização do conhecimento) caminha rumo à interdisciplinaridade com o Direito. Logo, esse campo científico contribui para o desenvolvimento do mundo três (do conhecimento sobre categorias de dados em uma área corporativa) e sua repercussão no mundo dois (na mente dos usuários da pretensa taxonomia) e no mundo um (onde residem os dados), refletindo no que, outrora, foi teorizado por Popper (2006).

Referências

ACCIOLY, Dante. Comissão aprova MP que cria órgão para a proteção de dados. **Senado Notícias**, Brasília, 07 mai. 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/05/07/comissao-aprova-mp-que-cria-orgao-para-protecao-de-dados. Acesso em: 10 mar. 2021.

AGANETTE, Elisângela Cristina. **Taxonomias corporativas**: um estudo sobre definições e etapas de construção fundamentado na literatura publicada. 2010. Dissertação (Mestrado em Ciência da Informação) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2010. Disponível em: http://repositorios.questoesemrede.uff.br/repositorios/handle/123456789/916?show=full. Acesso em: 29 jul. 2021.

AGANETTE, Elisângela Cristina; TEIXEIRA, Lívia Marangon Duffles. Taxonomias corporativas: uma proposta de procedimento operacional para construção baseada na teoria e na prática. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 18., 2017, Marília. **Anais** [...]. Marília: Universidade Estadual de São Paulo, 2017, não paginado. Disponível em: http://enancib.marilia.unesp.br/index.php/XVIII_ENANCIB/ENANCIB/paper/view/34. Acesso em: 28 jul. 2021.

ARAÚJO, Carlos Alberto Ávila. **O que é Ciência da Informação**. Belo Horizonte: KMA, 2018.

ARAÚJO, Paula Carina de.; FERNEDA, Edberto; GUIMARÃES, José Augusto Chaves. The relation between the domains of Information Retrieval and Knowledge Organization in International Journals. **Brazilian Journal of Information Studies: Research Trends**, Marília, v. 10, n. 2, p. 82-88, 2016.

ARGUDO, Sílvia; CENTELLES, Miquel. Metodología para el diseño de taxonomías corporativas. **Investigación Bibliotecológica**, Cidade do México, v. 19, n. 39, p. 158-177, jul./dez. 2005. Disponível em: http://rev-ib.unam.mx/ib/index.php/ib/article/view/4082. Acesso em: 06 ago. 2021.

BARITÉ, Mario *et. al*. **Diccionario de organización del conocimiento**: Clasificación, Indización, Terminologia. Montevídeo: CSIC, 2015.

BARITÉ, Mario. Organización del conocimiento: un nuevo marco teórico-conceptual en Bibliotecología y Documentación. *In:* CARRARA, Kester (org.). **Educação, Universidade e Pesquisa**. Marília: Unesp, Marília Publicações; São Paulo: FAPESP, 2001. p. 35-60.

BARRETO, Aldo de Albuquerque. A condição da informação. **São Paulo em Perspectiva**, São Paulo, v. 16, n. 3, p. 67-74, jul. 2002. Disponível em: https://www.scielo.br/j/spp/a/5Q85NCzRFvJ8BLjjd54jLMv/?lang=pt. Aceso em: 21 jun. 2021.

BARRETO, Aldo de Albuquerque. Uma história da ciência da informação. *In:* TOUTAIN, Lídia Maria Batista Brandão (org.). **Para Entender a Ciência da Informação**. Salvador: EDUFBA, 2007, p. 13-34. Disponível em: https://repositorio.ufba.br/ri/bitstream/ufba/145/1/Para%20entender%20a%20ciencia%20da%20informacao.pdf. Acesso em: 28 jun. 2021.

BLACKBURN, Barb; SMALL-WOOD, Robert. A information organization and classification: taxonomies and metadata. *In:* SMALWOOD, Robert F. (org.). **Information Governance**: Concepts, Strategies and Best Practices. [*S.l.*]: Wiley, 2014, p. 355-384. Disponível em: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118433829.app1. Acesso em: 11 nov. 2021.

BOLZANI, Izabela. Novo vazamento expõe dados de mais de 100 milhões de contas de celular. **Folha de S. Paulo**, São Paulo, 10 fev. 2021. Disponível em: https://www1.folha.uol.com.br/mercado/2021/02/novo-vazamento-expoe-dados-de-mais-de-100-milhoes-de-contas-de-celular.shtml. Acesso em: 10 mar. 2021.

BOTELHO, Ernani Mendes. **Custeio baseado em atividades – ABC**: Uma aplicação em uma organização hospitalar universitária. 2006. Tese (Doutorado em Administração) – Universidade de São Paulo, São Paulo, 2006. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12139/tde-10042008-102523/publico/Tese.pdf. Acesso em: 07 jul. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia de Avaliação de Riscos de Segurança e Privacidade**. Brasília (DF): Presidência da República, nov. 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf. Acesso em: 18 jan. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD)**. Brasília (DF): Presidência da República, ago. 2020b. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 21 dez. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia de Elaboração de Programa de Governança em Privacidade**. Brasília, DF: Presidência da República, out. 2020c. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso em: 01 ago. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia de Elaboração de Inventário de Dados Pessoais**. Brasília, DF: Presidência da República, abr. 2021a. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf/@@download/file/guia_inventario_dados_pessoais.pdf. Acesso em: 01 ago. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: Presidência da República, mai. 2021b. Disponível em: https://www.gov.

br/anpd/pt -br/assuntos/noticias/2021- 05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 30 ago. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, versão 2.0**. Brasília, DF: Presidência da República, abr. 2022a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 19 jul. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. Brasília, DF: Presidência da República, jan. 2022b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 19 jul. 2022.

BRASIL. Câmara dos Deputados. **PL 4.060/2012**: ficha de tramitação. [20--]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066 . Acesso em: 28 mai. 2022.

BRASIL. Câmara dos Deputados. **PL 5.276/2016**: ficha de tramitação. [20--]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 28 mai. 2022.

BRASIL. Congresso Nacional. **Medida provisória n° 869, de 2018**: ficha de tramitação. [20--]. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 28 mai. 2022.

BRASIL. Conselho Nacional de Desenvolvimento Científico e Tecnológico. **Plataforma Lattes**. [20–]. Disponível em: https://lattes.cnpq.br/. Acesso em: 28 mai. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 mai. 2022.

BRASIL. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. **Portal de Periódicos da CAPES**. [20–]. Disponível em: https://www-periodicos-capes-gov-br.ez287.periodicos.capes.gov.br/index.php. Acesso em: 21 ago. 2021.

BRASIL. **Declaração de nascido vivo: manual de instruções para preenchimento**. 4. ed. Brasília: Ministério da Saúde, 2022c. Disponível em: https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/publicacoes-svs/vigilancia/declaracao-de-nascido-vivo-manual-de-instrucoes-para-preenchimento. Acesso em: 03 nov. 2022.

BRASIL. **Decreto n° 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Brasília: Presidência da República, 2020d. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em: 10 mar. 2021.

BRASIL. **Decreto n° 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.

Brasília: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 17 dez. 2021.

BRASIL. **Decreto-lei n° 2.848, de 7 de dezembro de 1940**. Código Penal. Presidência da República: Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 mai. 2022.

BRASIL. Deputado Milton Monti. **Projeto de lei n° __, de 2012**: dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Congresso Nacional, 2012a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=Tramitacao-PL+4060/2012. Acesso em: 10 mar. 2021.

BRASIL. **Emenda Constitucional n° 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. Brasília: Presidência da República, 2022d. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 23 mar. 2022.

BRASIL. Governo Federal. **Portal Gov.br**. [20--]. Disponível em: https://www.gov.br/pt-br. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Presidência da República: Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 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; [...]. Brasília: Presidência da República, 2011a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Presidência da República, 2012b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no pe-

ríodo da pandemia do coronavírus (Covid-19). Brasília: Presidência da República, 2020e. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 10 mar. 2021.

BRASIL. **Lei n° 14.058, de 17 de setembro de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 6 de julho de 2020. Brasília: Presidência da República, 2020f. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14058.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei n° 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 28 mai. 2022.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 10 mar. 2021.

BRASIL. **Medida provisória n° 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Presidência da República, 2018b. Disponível em: https://www.conjur.com.br/dl/presidente-temer-cria-autoridade.pdf. Acesso em: 10 mar. 2021.

BRASIL. **Medida provisória n° 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília: Presidência da República, 2020g. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 28 mai. 2022.

BRASIL. Ministério da Cidadania. **Tutorial**: consulta da situação do auxílio emergencial. Brasília: Presidência da República, 2020h. Disponível em: http://www.mds.gov.br/webarquivos/cidadania/auxilio_emergencial/tutorial-2013-consulta-da-situacao-do-auxilio-emergencial-2013-1805.pdf. Acesso em: 05 jul. 2021.

BRASIL. Ministério do Estado da Economia. **EM n° 00168/2020 ME**. Brasília: Presidência da República, 2020i. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Exm/Exm-MP-959-20.pdf. Acesso em: 10 mar. 2021.

BRASIL. Presidência da República. **Mensagem n° 451, de 14 de agosto de 2018**. Brasília: Presidência da República, 2018b. Disponível em: http://www.planalto.gov.br/

ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 10 mar. 2021.

BRASIL. Presidência da República. **Projeto de lei n° 5.276/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília: Presidência da República, 2016. 24p. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=Tramitacao-PL+5276/2016. Acesso em: 10 mar. 2021.

BRASIL. Senado Federal. **Projeto de Lei da Câmara n° 53, de 2018**: ficha de tramitação. [20–]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 28 mai. 2022.

BRASIL. Subchefia de Assuntos Parlamentares. **EMI n° 00086-MJ/MP/MCT/MC**. Brasília: Congresso Nacional, 2011b. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0usl7vcngx0f91d5td0oh9f-db21021054.node0?cod teor=912989 filename=Tramitacao-PL+2126/2011Acesso em: 10 mar. 2021.

BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD**: Lei Geral de Proteção de Dados Comentada. 2 ed. São Paulo: Revista dos Tribunais, 2019. *Ebook*, não paginado.

CAMARGO, Maria Fernanda Mayer de. **A construção de taxonomias para estruturação e recuperação de informações corporativas**. 2016. Dissertação (Mestrado em Ciência da Informação) – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2016. Disponível em: https://repositorio.ufmg.br/handle/1843/BUBD-AMWFJC. Acesso em: 29 jul. 2021.

CAMPOS, Maria Luiza de Almeida; GOMES, Hagar Espanha. Taxonomia e classificação: a categorização como princípio. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 8., 2007, Salvador. **Anais** [...]. Salvador: Universidade Federal da Bahia, 2007. 14p. Disponível em: http://www.enancib.ppgci.ufba.br/artigos/GT2--101.pdf. Acesso em: 24 jun. 2021. Acesso em: 17 dez. 2021.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Seqüência**, Florianópolis, n. 76, p. 213-240, ago. 2017. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/abstract/?lang=pt. Acesso em: 18 nov. 2021.

CARVALHO, Paulo Vicente Guimarães. **Revisão do Plano Diretor**: Hospital Universitário Clemente de Faria. 2008. Trabalho de conclusão de curso (Especialização em Gestão Hospitalar) – PROHOSP, Secretaria de Estado de Saúde de Minas Gerais, Montes Claros (MG).

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Editora Paz e Terra, 1999.

CHAUDRY, Abdus Sattar; LING, GohHui. Building taxonomies using organizational resources: a case of business consulting environment. **Knowledge Organization**,

Baden-Baden, v. 32, n. 1, p. 25-46, 2005. Disponível em: https://www.ergon-verlag.de/isko_ko/downloads/ko3220051c.pdf. Acesso em: 05 nov. 2021.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout so far. **The New York Times**, Nova Iorque, 4 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 10 mar. 2021.

CONSELHO FEDERAL DE MEDICINA. **Recomendação CFM n°1/2016**. Brasília: Conselho Federal de Medicina, 2016. Disponível em: https://portal.cfm.org.br/images/Recomendacoes/1_2016.pdf. Acesso em: 03 nov. 2022.

CONSUMERS INTERNATIONAL. **The state of data protection rules around the world**: a briefing for consumer organisations. [*S.l.*]: Consumers International, 2018. 6p. Disponível em: https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf. Acesso em: 10 mar. 2021.

CURRÁS, Emilia. The nature of information and its influence in human cultures. **Knowledge Organization**, Baden-Baden, v. 41, n. 1, p. 92-96, 2014. Disponível em: https://www.ergon-verlag.de/isko_ko/downloads/ko_41_2014_1_i.pdf. Acesso em: 08 nov. 2021.

DAHLBERG, Ingetraut. Teoria do conceito. **Ciência da Informação**, Rio de Janeiro, v. 7, n. 2, p. 101-107, 1978. Disponível em: http://revista.ibict.br/ciinf/article/view/115. Acesso em: 08 set. 2021.

DZIEKANIAK, Gisele; ROVER, Aires. Sociedade do conhecimento: características, demandas e requisitos. **DataGramaZero – Revista de Ciência da Informação**, [*s.l.*], v. 12, n. 5, não paginado, out. 2011. Disponível em: https://brapci.inf.br/index.php/res/v/7461. Acesso em 17 dez. 2021.

ESTADO DE MINAS GERAIS. Universidade Estadual de Montes Claros. **Cursos de graduação**. [20--]. Disponível em: https://unimontes.br/cursos/cursos-de-graduacao/. Acesso em: 28 mai. 2022.

ESTADO DE MINAS GERAIS. Universidade Estadual de Montes Claros. **Hospital Universitário Clemente de Faria**. [20--]. Disponível em: https://unimontes.br/unidades/hospital-universitario/. Acesso em: 28 mai. 2022.

FERREIRA, Daniela Assis Alves; MARQUES, Rodrigo Moreno; NATALE, Alexandra. A política de informação na arena da privacidade dos dados pessoais. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19., 2018, Londrina. **Anais** [...]. Londrina: Universidade Estadual de Londrina, 2018, p. 3119-3138. Disponível em: http://enancib.marilia.unesp.br/index.php/XIX_ENANCIB/xixenancib/paper/view/1417. Acesso em: 30 ago. 2021.

FERREIRA, Herbert Alcântara; LIMA, Rafael Antônio Gonçalves. **LGPD comentada artigo por artigo**. São Paulo: Fontenele Publicações, 2021.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados

na Lei Geral de Proteção de Dados. **Rev. Direito e Práx.**, Rio de Janeiro, v. 12, n. 2, 2021, p. 1002-1033. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/46944. Acesso em: 11 mai. 2022.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019, p. 677-715.

FURTADO, Tiago Neves. Registro das operações de tratamento de dados pessoais - *data mapping - data discovery*: por que é importante e como executá-lo. *In:* BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. **Data Protection Officer (Encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020, p. 85-104.

GILCHRIST, Alan. Thesauri, taxonomies and ontologies – an etymological note. **Journal of Documentation**, Bingley, v. 59, n. 1, p. 7-18, 2003. Disponível em: https://www.researchgate.net/publication/240602491_Thesauri_taxonomies_and_ontologies_-_An_etymological_note. Acesso em: 30 set. 2021.

GOMES, Hagar Espanha. Marcos históricos e teóricos da organização do conhecimento. **Informação & Informação**, Londrina, v. 22, n. 2, p. 33-66, mai./ago. 2017. Disponível em: https://brapci.inf.br/index.php/res/download/45074. Acesso em: 17 dez. 2021.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro – Volume 1 (Parte Geral)**. 18. ed. São Paulo: Saraiva Educação, 2021.

GUIMARÃES, José Augusto Chaves. Organização do conhecimento: passado, presente e futuro sob a perspectiva da ISKO. **Informação & Informação**, Londrina, v. 22, n. 2, p. 84-98, mai./ ago. 2017. Disponível em: http://www.uel.br/revistas/uel/index.php/informacao/article/view/31443. Acesso em: 17 dez. 2021.

GUIMARÃES, José Augusto Chaves. Slanted knowledge organization as a new ethical perspective. *In:* ANDERSEN, Jack; SKOUVIG, Laura (Org.). **The organization of knowledge: caught between global structures and local meaning**. Bingley: Emerald Publishing Limited, v. 12, p. 87-102, 2017.

HODGE, Gail. **Systems of Knowledge Organization for Digital Libraries**: Beyond Traditional Authority Files. Washington: The Digital Library Federation, 2000. Disponível em: https://www.clir.org/wp-content/uploads/sites/6/pub91.pdf. Acesso em: 04 out. 2021.

HOSPITAL BRASÍLIA. **Termo de autorização para internação**. Brasília: Hospital Brasília, 2019. Disponível em: https://hospitalbrasilia.com.br/pt/medicos-site/Documents/Termos%20de%20Consentimento/A008.2018.TERMO%20DE%20AUTORIZA%C3%87%C3%83O%20PARA%20INTERNA%C3%87%C3%83O.docx. Acesso em: 03 nov. 2022.

HUGHES, Eric. **A Cypherpunk's Manifesto**. 1993, não paginado. Disponível em: https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt. Acesso em: 17 nov. 2021.

HURTADO, Teobaldo Coronado. Diagnóstico médico. **Biociencias**, Barranquilla, v. 11, n. 1, p. 69-73, jan.-jun. 2016. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=5646110. Acesso em: 03 nov. 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2019**. Brasília: IBGE, 2021. 12 p. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf. Acesso em: 05 jul. 2021.

IRAMINA, Aline. RGPD V. LGPD: Adoção estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**. Brasília, v. 12, n. 2, p. 91-117, out. 2020. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/34692/27752. Acesso em: 25 mai. 2022.

JACINTHO, Eliana Maria dos Santos Bahia; GONZÁLEZ, José Antonio Moreiro. Aplicação de taxonomia nos portais corporativos: um olhar a partir das ofertas de emprego para arquivista. **Tendências da Pesquisa Brasileira em Ciência da Informação**, João Pessoa, v. 10, n. 1, p. 1-17, jan./jul. 2017. Disponível em: https://revistas.ancib.org/index.php/tpbci/article/view/432/431. Acesso em: 08 set. 2021.

KEINERT, Tania Margarete Mezzomo; CORRIZO, Carlos Tato. Dimensões da privacidade das informações em saúde. **Cadernos de Saúde Pública**, Rio de Janeiro, v.34, n. 7, p. 1-4, mai. 2018. Disponível em: https://www.scielo.br/j/csp/a/VQbX3mB7hz4rZvrYwHqG9Lx/?format=pdf&lang=pt. Acesso em: 17 dez. 2021.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Sandro. **LGPD**: Da teoria à implementação nas empresas. São Paulo (SP): Editora Rideel, 2021.

KOMNENIC, Masha. Complete GDPR Data Mapping Guide. **Termly**, mai. 2022. Disponível em: https://termly.io/resources/articles/gdpr-data-mapping/. Acesso em: 01 ago. 2022.

LAW, Thomas. **A Lei Geral de Proteção de Dados**: uma análise comparada ao novo modelo chinês. 2020. Tese (Doutorado em Direito Comercial) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2020. Disponível em: https://tede.pucsp.br/handle/handle/23402. Acesso em: 10 mar. 2021.

LE COADIC, Yves-François. **A ciência da informação**. Brasília: Briquet de Lemes, 1996.

LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. **Revista Fronteiras Interdisciplinares do Direito**, São Paulo, v.1, n.1, p. 178-196, 2019. Disponível em: https://revistas.pucsp.br/fid/article/view/41960. Acesso em: 10 mar. 2021.

LIMA, Gercina Ângela Borém.; RAGHAVAN, K. S. Categories in Knowledge Organization. **Advances in Knowledge Organization**, Baden-Baden, v. 14, p. 88-95, 2014. Disponível em: https://www.ergon-verlag.de/isko_ko/downloads/aiko_vol_14_2014_13.pdf. Acesso em: 03 nov. 2021.

LIMA, José Leonardo Oliveira.; ALVARES, Lilian. Organização e representação da informação e do conhecimento. *In:* ALVARES, Lilian (Org.). **Organização da Informação e do Conhecimento**: conceitos, subsídios interdisciplinares e aplicações. São Paulo: B4Editores, 2012, p. 21-34. Disponível em: https://www.researchgate.net/publication/281969932_Organizacao_e_representacao_da_informacao_e_do_conhecimento. Acesso em: 28 jun. 2021.

LOPES, Pâmela Tamires Dias; AGANETTE, Elisangela C.; MACULAN, Benildes Coura Moreira dos Santos. Análise da produção de teses e dissertações sobre taxonomias corporativas e facetadas em ciência da informação e ciência da computação. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 19, 2018, Londrina (PR). **Anais** [...]. Londrina: Universidade Estadual de Londrina, 2018, p.1169-1177. Disponível em: http://enancib.marilia.unesp.br/index.php/XIX_ENANCIB/xixenancib/paper/viewPaper/1549. Acesso em: 28 jul. 2021.

MACULAN, Benildes Coura Moreira dos Santos; ASSIS, Juliana de; ALVES, Alan Vasconcelos; PEREIRA, Fernanda. Taxonomia, folksonomia, acessibilidade e usabilidade: proposta de interseção na área de organização do conhecimento, com foco na recuperação de informação. *In:* SEMINÁRIO EM CIÊNCIA DA INFORMAÇÃO, 3., 2009, Londrina. **Anais** [...]. Londrina, 2009, não paginado. Disponível em: http://eprints.rclis.org/23854/. Aceso em: 24 jun. 2021.

MAIA, Carolina de Fátima Marques; FONSECA, Décio; CUNHA, Mônica Ximenes Carmelo da; DORNELAS, Jairo Simião. Gestão da informação hospitalar: uma proposta a partir do estudo de caso em um hospital universitário no Recife. **Revista Eletrônica de Sistemas de Informação**, Curitiba, v. 8, n. 2, artigo 3, p. 1-22, 2009. Disponível em: http://www.periodicosibepes.org.br/index.php/reinfo/article/view/560. Acesso em: 26 mai. 2021.

MAIA, Lucinéia Souza; LIMA, Gercina Ângela; MACULAN, Benildes Coura Moreira dos Santos. Taxonomia dos tipos de relações semânticas para a organização e a representação do conhecimento: uma proposta a partir da literatura. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 18., 2017, Marília. **Anais** [...]. Marília: Universidade Estadual de São Paulo, 2017. 26p. Disponível em: https://brapci.inf.br/index.php/res/download/125053. Acesso em: 03 ago. 2021.

MAROSO, Eduardo Pereira. Segurança da informação. *In:* LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. **LGPD - Lei Geral de Proteção de Dados**: sua empresa está pronta? São Paulo: Literare Books International, 2020. *Ebook*, não paginado.

MATHEWS, Lee. File with 1.4 billion hacked and leaked passwords found on the dark web. **Forbes**, [S.l.], 11 dez. 2017.Disponível em: https://www.forbes.com/sites/leemathews/2017/12/11/billion-hacked-passwords-dark-web/?sh=290bc3b721f2. Acesso em: 10 mar. 2021.

MAZZOCHI, Fulvio. Knowledge organization system (KOS). **Encyclopedia of Knowledge Organization**, 2017, não paginado. Disponível em: https://www.isko.org/cyclo/kos#ref. Acesso em: 09 set. 2022.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, [*s.l.*] 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de- 223-milhoes-de-brasileiros-o--que-se- sabe-e-o-que-falta-saber.ghtml. Acesso em: 10 mar. 2021.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo (SP), v.1009, p. 4-17, nov. 2019. Disponível em: https://www.brunomiragem.com.br/ wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 10 mar. 2021.

MOREIRA, Manoel Palhares; MOURA, Maria Aparecida. Construindo tesauros a partir de tesauros existentes: a experiência da TCI – Tesauro em Ciência da Informação. DataGramaZero – **Revista de Ciência da Informação**, [s.l.], v. 7, n. 4, ago. 2006. 16p. Disponível em: https://brapci.inf.br/index.php/res/v/6670. Acesso em: 24 jun. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: https://sisbib.emnuvens.com.br/ direitosegarantias/article/view/1603. Acesso em: 10 mar. 2021.

NETSHOES terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes. **G1**, [s.l.], fev. 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por- vazamento-de-dados-de--2-milhoes-de-clientes.ghtml. Acesso em: 10 mar. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Guidelines governing the protection of privacy and transborder flows of personal data**. Paris: Organisation for Economic Co-operation and Development, 2013. 37p. Disponível em: https://www.oecd.org/sti/ieconomy/2013- oecd-privacy-guidelines.pdf. Acesso em: 10 mar. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Brasília: Organização das Nações Unidas, 1948. Disponível em: https://www.unicef.org/brazil/ declaracao-universal-dos-direitos-humanos. Acesso em: 10 mar. 2021.

PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. **Agência Brasil**, Brasília, 19 out. 2015. Disponível em: https://agenciabrasil.ebc.com.br/geral/ noticia/2015-10/mj-finaliza-nova-versao-de- anteprojeto-sobre-protecao-de-dados-na-internet. Acesso em: 10 mar. 2021.

PIEDADE, Maria Antonietta Requião. **Introdução a teoria da classificação**. 2. ed. Rio de Janeiro: Interciência, 1983.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

PINHO, Fábio Assis. Prefácio. In: PINHO, Fabio Assis; GUIMARÃES, José Augusto Chaves (Org.). **Memória, tecnologia e cultura na Organização do Conhecimento - Estudos Avançados em Organização do Conhecimento**. v. 4. Recife: Editora UFPE, 2017, p. 3.

PINTO, Mariane Costa. Perspectivas em organização do conhecimento e informação. **Revista Analisando em Ciência da Informação**, João Pessoa, v. 8, n. 2, p. 06-15, jul./dez. 2020. Disponível em: http://arquivologiauepb.com.br /racin/edicoes/ v8_n2/racin_v8_n2_artigo01.pdf. Acesso em: 21 jun. 2021.

POHLMANN, Sérgio. **LGPD Ninja**: Entendendo e implementando a Lei Geral de Proteção de Dados nas Empresas. Nova Friburgo: Editora Fross, 2019.

POPPER, Karl. **Em busca de um mundo melhor**. São Paulo: Martins, 2006.

QUEIROZ, Daniela Gralha de Caneda; MOURA, Ana Maria Mielniczuk de. Ciência da Informação: história, conceitos e características. **Em Questão**, Porto Alegre, v. 21, n.3, p. 26-42, ago./dez. 2015. Disponível em: https://seer.ufrgs.br /index.php/EmQuestao/article/view/57516. Acesso em: 13 abr. 2021.

RUARO, Regina Linden; RODRÍGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. **Direito, Estado e Sociedade**, Rio de Janeiro, n. 36, p. 178-199, jan./jun. 2010. Disponível em: http://direitoestadosociedade.jur. puc-rio.br/ media/8ruaro_rodriguez36.pdf. Acesso em: 17 dez. 2021.

SANTOS, Matheus Eduardo Glok dos; SCHIMITT, Murilo de Oliveira. Lei Geral de Proteção de Dados (LGPD): impactos sobre a formação de mercados de serviços digitais. **Caderno PAIC**, v. 22, n. 1, 2021, p. 643-658. Disponível em: https://cadernopaic.fae.edu/ cadernopaic/article/view/457. Acesso em: 11 mai. 2022.

SARACEVIC, Tefko. Information Science. *In*: BATES, M. J.; MAACK, M. N. (Eds.) **Encyclopedia of Library and Information Science**. New York (Estados Unidos da América): Taylor & Francis, p. 2570-2586, 2009.

SCHENEIDER, Henrique Nou; SANTOS, Jacques Fernandes.; SANTOS, Vinicius Silva. Cultura juvenil, dependência digital e contingência. **Revista Científica do UniRios**, Paulo Afonso, v. 14, n. 23, p. 41-54, 2020. Disponível em: https://www.unirios.edu.br/revistarios/ media/revistas/2020/23/cultura_juvenil_dependencia_ digital_e_ contigencia.pdf. Acesso em: 05 jul. 2021.

SEREJO NETO, Edson. **Organização do conhecimento em ambientes web com base na teoria da classificação facetada**: estudo aplicado para a área de engenharia naval e offshore. 2014. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2014. Disponível em: http://www.repositorio-bc.unirio.br:8080/ xmlui/handle/unirio/11828. Acesso em: 12 ago. 2021.

SETZER, Valdemar W. **Dado, informação, conhecimento e competência**. 2015. Online, não paginado. Disponível em: https://www.ime.usp.br/~ vwsetzer/dado-info. html. Acesso em: 13 abr. 2021.

SILVA, Jonathas Luiz Carvalho; GOMES, Henriette Ferreira. Conceitos de informação na Ciência da Informação: percepções analíticas, proposições e categorizações. **Informação & Sociedade: Estudos**, João Pessoa (PB), v.25, n.1, p. 145-157, 2015. Disponível em: http://hdl.handle.net/20.500.11959/ brapci/93211. Acesso em: 13 abr. 2021.

SILVEIRA, Sergio Amadeu da. A noção de exclusão digital diante das exigências de uma cibercidadania. *In*: HETWOSKI, Tânia Maria (org.). **Políticas Públicas & Inclusão Digital**. Salvador: EDUFBA, 2008, p. 43-66.

SMIRAGLIA, Richard P. **The Elements of Knowledge Organization**. [*S.l.*]: Springer, 2014.

SOUZA, Renato Rocha; TUDHOPE, Douglas; ALMEIDA, Maurício Barcellos. Towards a taxonomy of KOS: dimensions for classifying Knowledge Organization Systems. **Knowledge Organization**, Baden-Baden, v. 39, n. 3, p. 179-192, 2012. Disponível em: https://www.ergon-verlag.de/isko_ko/downloads/ ko_39_2012_3_c. pdf. Acesso em: 11 nov. 2021.

SUENAGA, C. M. K.; RODRIGUES, M. R.; SANTOS, J. C. F.; CERVANTES, B. M. N. Sistemas de organização do conhecimento: taxonomia e mapa conceitual. *In*: SEMINÁRIO EM CIÊNCIA DA INFORMAÇÃO, 5., 2013, Londrina. **Anais** [...]: Londrina: Universidade Estadual de Londrina, 2013, p. 501-520.

TERRA, J. C. C.; SCHOUERI, R.; VOGEL, M. J. M.; FRANCO, C. **Taxonomia**: elemento fundamental para a Gestão do Conhecimento. [S.l.]: TerraForum Consultores, 2004. 8p.

TIDY, Joe. Marriot Hotels fined € 18.4m for data breach that hit millions. **BBC**, Londres, 30 out. 2020. Disponível em: https://www.bbc.com/news/technology-54748843. Acesso em: 10 mar. 2021.

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. **Agência Brasil**, Brasília, 07 mai. 2018a. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/ 2018-05/legislacao-de-protecao-de-dados-ja-e- realidade-em--outros-paises#. Acesso em: 10 mar. 2021.

VALENTE, Jonas. Temer sanciona lei de proteção de dados mas veta órgão regulador. **Agência Brasil**, Brasília, 14 ago. 2018b. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2018-08/temer-sanciona-lei-de-protecao-de-dados-mas-veta-orgao-regulador. Acesso em: 10 mar. 2021.

VASCONCELOS, Kleber. Os benefícios da implementação da LGPD. **Serpro**, Brasília, 26 out. 2020. Disponível em: https://www.serpro.gov.br/lgpd/ noticias/2020/benefi-cios-riscos-lgpd-empresas. Acesso em: 10 mar. 2021.

ZANATTA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). **Direito e Internet III: Marco Civil da Internet**, São Paulo: QuartierLatin, 2015, p. 447-470.

Campus Universitário Professor Darcy Ribeiro
Montes Claros - Minas Gerais - Brasil
CEP 39401-089 - CAIXA POSTAL 126
www.editora.unimontes.br
editora@unimontes.br


EDITORA
Unimontes