

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE GRADUAÇÃO EM DIREITO
CURSO DE DIREITO**

JHONATA ASSMANN

**O DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO GERMÂNICO
E BRASILEIRO**

FLORIANÓPOLIS – SC

2014

JHONATAASSMANN

O DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO GERMÂNICO E
BRASILEIRO

Trabalho de Conclusão apresentado ao
Curso de Graduação em Direito da UFSC,
como requisito à obtenção do título de
Bacharel em Direito.

Orientador: Prof. Dr. Airton Lisle Cerqueira L. Seelaender

FLORIANÓPOLIS – SC

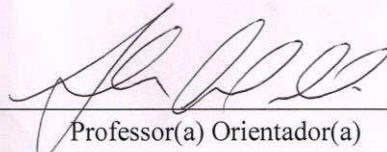
2014

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COORDENADORIA DE MONOGRAFIA

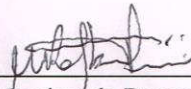
TERMO DE APROVAÇÃO

A presente monografia intitulada "**O direito fundamental à autodeterminação informativa no direito germânico e brasileiro**", elaborada pelo(a) acadêmico(a) **Jhonata Assmann**, defendida em **07/02/2014** e aprovada pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 10 (DEZ), sendo julgada adequada para o cumprimento do requisito legal previsto no artigo 9. da Portaria n. 1886/94/MEC, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução n. 003/95/CEPE.

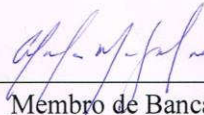
Florianópolis, 7 de Fevereiro de 2014.



Professor(a) Orientador(a)
Airton Lisle Cerqueira Leite Seelaender



Membro de Banca
Marcos Rotta Pucci



Membro de Banca
Laila Maia Galvão

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. Airton Lisle Cerqueira L. Seelaender, de quem partiu a sugestão sobre o tema da pesquisa e quem soube, mesmo com as limitações de tempo de ambas as partes, dar norte e motivar-me à feitura deste trabalho.

Ao meu amigo Guilherme Keime Goto, parceiro no momento mais importante e a quem pretendo retribuir com generosidade sua prova de amizade.

Aos colegas de universidade, especialmente aos apaixonados pela ciência jurídica.

Aos membros da banca, por aceitarem o desafio de participar desse momento tão importante da minha trajetória.

E, mais do que quaisquer outros, aos professores da minha vida, os meus pais, Katia e Selmiro, que abriram mão do orgulho e de suas profissões para poderem prover aos seus filhos educação em seu sentido mais amplo. As gotas de suor debaixo do sol ardente, o peso das caixas de isopor, as (tantas) noites varadas foram dedicadas para que eu e minhas irmãs tivéssemos uma vida autodeterminada.

LISTA DE ABREVIATURAS

Abs. – *Absatz* (parágrafo)

Art. – *Artikel* (artigo, usado no texto constitucional)

BDSG – *Bundesdatenschutzgesetz* (Lei Federal de Proteção de Dados Pessoais alemã)

BVerG – *Bundesverfassungsgericht* (Tribunal Constitucional Federal alemão)

BVerGE – *Bundesverfassungsgerichtsentscheidung* (Decisão do Tribunal Constitucional Federal alemão)

BVerGE (65), 1 – *Volkszählungsurteil* (Decisão sobre a Lei do Censo)

BVerGE (27) - *Mikrozensusurteil* (Decisão sobre a Lei da Realização Estatística Representativa da População e da Atividade Econômica (micro-censo))

CC – Código Civil

c.c – combinado com

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

GG – *Grundgesetz* (Lei Fundamental, equivalente à Constituição alemã)

STF – Supremo Tribunal Federal

TCF – Tribunal Constitucional Federal alemão

O poder dos atos jurídicos e da ciência é limitado. Os mesmos podem regular e promover o movimento que se desenvolve pelas trilhas já existentes, mas não são capazes de derrubar os diques que impedem a torrente do direito de abrir os novos caminhos.

Rudolf von Ihering, em “A Luta Pelo Direito”

RESUMO

Há trinta anos o direito a autodeterminação informativa foi enunciado pelo Tribunal Constitucional alemão (*Bundesverfassungsgericht*) como consectário do direito fundamental ao livre desenvolvimento da personalidade e inviolabilidade da dignidade humana (Art. 1 I e 2 I GG). Essa conclusão levou a mudanças sensíveis no entendimento sobre proteção de dados pessoais. O direito à autodeterminação informativa, nessa nova senda, é visto como um requisito para a liberdade em um Estado Democrático de Direito. Ampliou, assim, a área de proteção jurídica desse direito, influenciando a legislação sobre a proteção de dados alemã, a legislação sobre o tema a nível europeu e a jurisprudência dominante sobre o tema até hoje. O ordenamento jurídico pátrio, ao seu turno, ainda não possui uma (necessária) legislação sobre proteção de dados pessoais: dispõe, como principais instrumentos nesta área, do *habeas data* e de disposições no Código de Defesa do Consumidor (CDC). Consequentemente, apresenta-se o direito à autodeterminação informativa no direito brasileiro essencialmente em sua dimensão subjetiva (como *Abwehrrecht*) – e de maneira ineficiente. A complexidade, os constantes desenvolvimentos tecnológicos e a dimensão socioeconômica da manipulação de dados evidenciam, contudo, a necessidade de concretização do direito à autodeterminação informativa em sua dimensão objetiva, por meio de legislação sobre o tema.

Palavras-chave: Direito à autodeterminação informativa; direito fundamental; *Bundesdatenschutzgesetz*; CDC; *habeas data*.

ZUSAMMENFASSUNG

Vor dreißig Jahren wurde das Recht auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht (BVerfG) von der freien Entfaltung der Persönlichkeit (Art. 2 I GG) abgeleitet. Diese Herleitung führte zu einem nachhaltigen Wandel im Datenschutzrecht. Das Recht auf informationelle Selbstbestimmung wurde so zu einer der Bedingungen für einen freien und demokratischen Rechtsstaat. Mit dieser Konstitutionalisierung hat das BVerfG den Schutzbereich des Selbstbestimmungsrechts deutlich erweitert. Beispielsweise hat es die Gesetzgebung mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) beeinflusst, wie auch die bis heute herrschende Rechtsprechung über das Thema Datenschutz nachhaltig, auf nationaler wie auch europäischer Ebene, geprägt. Das brasilianische Datenschutzrecht besitzt seinerseits keine spezifische Kodifikation im Bereich des Datenschutzes und nutzt aus diesem Grund das verfassungsrechtliche Instrument des *habeas datas*, sowie einige Rechtsvorschriften wie das Verbraucherschutzgesetz (CDC). Folglich wirkt das Recht auf informationelle Selbstbestimmung im brasilianischen Recht grundsätzlich in seiner subjektiven Dimension (als Abwehrrecht). Die Komplexität, ständige Neuerungen auf diesem Gebiet und die wirtschaftlichen Dimensionen der Datenverarbeitung zeigen die Notwendigkeit auf, das Selbstbestimmungsrecht in seiner objektiven Dimension zu konkretisieren.

Stichworte: Selbstbestimmungsrecht; Grundrecht; Bundesdatenschutzgesetz; CDC; *habeas data*.

SUMÁRIO

INTRODUÇÃO	10
1 DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMATIVA.....	13
1.1 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DE DADOS	13
1.1.1 Panorama geral	13
1.1.2 A autodeterminação informativa no desenvolvimento legislativo da proteção de dados.....	15
1.2 DETERMINAÇÃO CONCEITUAL: AUTODETERMINAÇÃO INFORMATIVA COMO DIREITO FUNDAMENTAL	20
1.3 CONVERGÊNCIAS COM O DIREITO À PRIVACIDADE	27
2 PROTEÇÃO DOS DADOS PESSOAIS E DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO GERMÂNICO	29
2.1 PANORAMA GERAL.....	29
2.2 PANORAMA JURISPRUDENCIAL.....	31
2.2.1 O <i>Mikrozensusurteil</i>	31
2.2.2 A <i>Volkszählungsurteil</i>	33
2.3. A <i>BUNDESDATENSCHUTZGESETZ</i> – BDSG.....	41
3 PROTEÇÃO DOS DADOS PESSOAIS E DIREITO A AUTODETERMINAÇÃO INFORMATIVA NO DIREITO BRASILEIRO.....	44
3.1 PANORAMA GERAL.....	44
3.2 O HABEAS DATA.....	47
3.3. O CÓDIGO DE DEFESA DO CONSUMIDOR	50
4 DESAFIOS À TUTELA DO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO BRASIL	53
4.1. UMA CRÍTICA AOS PRINCIPAIS INSTITUTOS DISPONÍVEIS PARA PROTEÇÃO DE DADOS E CONCRETIZAÇÃO DO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO BRASILEIRO ...	53
4.2 A NECESSIDADE DE LEGISLAÇÃO SOBRE A PROTEÇÃO DE DADOS NO BRASIL.....	55
4.3. BREVES NOTAS PARA O DESENVOLVIMENTO DO DEBATE QUANTO AO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO BRASIL.....	58
CONCLUSÃO	60
REFERÊNCIAS BIBLIOGRÁFICAS	62

INTRODUÇÃO

O livre desenvolvimento da personalidade afigura-se como indispensável para o desenvolvimento de uma sociedade democrática e plural e relaciona-se diretamente com o direito à autodeterminação informativa, o qual apresenta uma dimensão subjetiva – que protege o indivíduo de intromissões indevidas a seus dados pessoais e, igualmente, em sua dimensão positiva, ordena ao legislador, *et cetera*, a produção de normas que regulem a utilização de dados pessoais, dimensão essa que independe de seus titulares e que visa a criar normas protetivas (sobretudo preventivas).

O silêncio legislativo no Brasil para com a adequada da proteção de dados pessoais contrasta com a atualidade do tema: se antes de avanços tecnológicos¹ os principais ataques ao espaço privado do indivíduo eram a violação do domicílio e da correspondência, hoje é o acesso indevido a informações pessoais, cujo resultado é a formação de perfis virtuais cujos titulares desconhecem a existência e que restringem de maneira concreta sua liberdade².

A pesquisa realizada nesta monografia situa-se no campo do direito constitucional, em especial no estudo dos direitos fundamentais e baseia-se no problema de, no ordenamento jurídico brasileiro, o direito fundamental à autodeterminação manifestar-se essencialmente no seu *status* negativo (*Abwehrrecht*), preterida sua dimensão positiva.

A hipótese central é de que um diploma legal para a proteção de dados traria, de maneira ampla, “regras do jogo”, cuja função preventiva regularia ataques à esfera privada dos cidadãos - concretizando assim a dimensão objetiva do direito à autodeterminação informativa.

O objetivo é justamente demonstrar, a partir de um diálogo com elementos jurisprudenciais e legislativos alemães - especialmente a Lei Federal de Proteção de Dados alemã (*Bundesdatenschutzgesetz*) e a *Volkszählungsurteil* - a necessidade de

¹ Cf. CAAR (2003), pela internet e com processadores ultrapotentes, big data, data warehouse, business intelligence, entre outros, são capazes de armazenar, agrupar e interpretar dados pessoais com extrema eficiência.

² Embora não seja objeto do presente trabalho, é de mencionar-se o caso recente das restrições de crédito a cidadãos cujos perfis econômico-financeiros (alheios ao seu conhecimento e anuência) eram traçados por uma empresa de análise de capacidade creditícia.

uma codificação adequada ao tema proteção de dados pessoais para garantir-se a dimensão objetiva do direito fundamental à autodeterminação informativa. Projeta-se, como objetivo secundário, sugerir pontos de desenvolvimento no debate jurídico pátrio sobre o tema.

No primeiro capítulo pretende-se expor o pano de fundo do debate sobre o direito à autodeterminação informativa. Traçar-se-á um breve panorama histórico, para então apresentar um conceito de autodeterminação informativa. Apontar-se-á, igualmente, convergências e pontos distintivos desse direito em relação ao direito à privacidade.

No segundo capítulo expõe-se um panorama geral sobre a proteção de dados no direito germânico. Com especial enfoque na decisão do Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*) sobre a Lei do Censo – a chamada *Volkszählungsurteil*.

No terceiro capítulo traz-se, sinteticamente, o panorama geral da proteção de dados no Brasil, com enfoque no remédio constitucional *habeas data*, assim como no Código de Defesa do Consumidor.

Por fim, o quarto capítulo envolve-se com um desiderato menos descritivo: procura-se fazer uma crítica aos instrumentos normativos brasileiros referentes à proteção de dados, para então abordar-se a necessidade de uma legislação sobre a proteção de dados pessoais no Brasil, além sugerir-se, brevemente, pontos de discussão para o desenvolvimento da matéria no ordenamento jurídico pátrio.

O estudo será desenvolvido com base no método dedutivo, utilizando procedimentos de pesquisa legislativa e pesquisa bibliográfica, analisando-os sob o prisma dos conceitos referentes ao tema da presente monografia.

Fontes primárias são as obras de Leonardo Martins: sua tese de doutoramento, intitulada *Die Grundrechtskollision. Grundrechtskonkretisierung am Beispiel des 41 1 BDSG*³, assim como *Os cinquenta anos da Jurisprudência do Tribunal Constitucional Federal alemão* (2005). A obra de Danilo Doneda, *Da privacidade à proteção de dados pessoais* (2006), o *Kommentar* de Herbert Auernhammer sobre a *Bundesdatenschutzgesetz* (BDSG), assim como os artigos de

³ Defendida na Humbolt Universität zu Berlin: “Colisão de direitos fundamentais: concretização de direitos fundamentais a partir do exemplo do 41 I da Lei Federal de Proteção de Dados” (tradução livre).

Thomas Petri⁴, Gerrit Hornung e Cristoph Schnabel⁵ foram igualmente basilares para a construção deste trabalho.

⁴ Wertewandel im Datenschutz und die Grundrechte (2010).

⁵ Data protection in Germany I: The population census decision and the right to informational self-determination (2009).

1 DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMATIVA

1.1 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DE DADOS

1.1.1 Panorama geral

O direito à autodeterminação informativa – capacidade de o indivíduo determinar em princípio sobre a exibição e uso de seus dados pessoais⁶ - não pode ser dissociado das mudanças de valores político-econômicas desde o surgimento efervescente das legislações sobre proteção de dados no final da década de sessenta, cujas causas são, entre outras, o desenvolvimento tecnológico, a propagação dos meios de comunicação em massa e a crescente mobilidade geográfica.

Pelo menos os dois primeiros constroem um cenário para a necessidade de uma efetiva proteção de dados. Destarte, o debate acerca da mudança de valores (*Wertewandel*) na Academia⁷ e na legislação de proteção de dados (*Datenschutzrecht*) alemães exemplificam reações, em parte, para os mesmos desenvolvimentos sociais. Isso não significa, contudo, que ambas as reações sejam de iguais características: A discussão científica serve para a análise desses processos de transformação, enquanto o *Datenschutzrecht* provê mecanismos de governança (*Steuerungsprozessen*)⁸.

A legislação para proteção de dados é, enquanto *Steuerungsprozess* para os novos desenvolvimentos tecnossociais, uma reação do Estado à constatação de a manipulação automatizada de dados oferecer não apenas grandes chances mas também riscos aos indivíduos e/ou limitações à liberdade desses. Aqui já fica claro que a proteção a dados é uma proteção a direitos fundamentais, pois procura resolver o problema da obtenção automatizada de perfis de personalidade alheia ao

⁶ Uma conceituação mais ampla e contextualizada é objeto da próxima sessão (1.2) deste trabalho.

⁷ Cf. PETRI, 2010, p. 26.

⁸ Cf. PETRI, 2010, p. 26.

contexto situacional das informações obtidas. A proteção a dados pessoais é, em síntese, uma reação às mudanças no campo social e estatal⁹.

Na busca de sintetizar o emaranhado de normas nacionais, supranacionais e decisões jurídicas, movimentos tecnológicos e sociais que perpassam o tema, a serem expostos a seguir como parte do desenvolvimento histórico da proteção de dados e do direito a autodeterminação informativa, observa-se, em um primeiro momento, surgir a iniciativa de governos em obter mais informações sobre os cidadãos para prover com maior acurácia direitos decorrentes do *welfare state* predominante na Europa continental durante as décadas de sessenta e sessenta, obtenção essa por meio das novas tecnologias de informação disponíveis. Por outro lado há uma oposição popular à obtenção, armazenamento e manipulação indiscriminados por parte de agentes estatais¹⁰. No âmbito político, surgem leis de proteção de dados para impor mecanismos de controle e expor “regras do jogo” do tratamento de dados¹¹. Tais legislações, contudo, não estavam estruturadas o suficiente para salvaguardar a privacidade dos cidadãos e direitos fundamentais, de maneira que decisões judiciais as conformam constitucionalmente com vistas a garantir, assim, os direitos dos cidadãos, seja em face do Estado, inicialmente, e depois de instituições privadas¹². Essas decisões, em destaque a *Volkszählungsurteil*¹³, vinculam a legislação, que, por sua vez, influencia o uso as tecnologias de informação, restringindo-lhe alcance para, assim como o aparato normativo, proteger o livre desenvolvimento da personalidade, igualdade e outros valores de matriz constitucional.

⁹ Cf. PETRI, 2010, p. 26, no original: **Das Datenschutzrecht stellt eine Form für den Steuerungsprozess neuer technisch-gesellschaftlicher Entwicklungen dar**. Es ist eine Reaktion des Staates auf die Feststellung, dass die automatisierte Datenverarbeitung nicht nur große Chancen bietet, sondern für den Einzelnen auch mit erheblichen Risiken und Freiheitsbeschränkungen verbunden ist. Hier wird bereits deutlich, dass der Datenschutz im Kern Grundrechtsschutz ist, weil er versucht, insbesondere die Probleme der automatisierten Schaffung von Persönlichkeitsbildern und den dadurch häufig bedingten Verlust des situationsbedingten Kontextes von einmal erfassten Informationen im Sinne der Freiheit.

¹⁰ Foram ajuizadas mais de duas mil Reclamações Constitucionais contra a Lei do Censo alemã, o que denota não apenas uma insatisfação jurídica, mas igualmente política dos cidadãos.

¹¹ Exemplo é a Lei Federal de Proteção de dados, a Bundesdatenschutzgesetz, de 1977.

¹² Os Estados, com seus grandes bancos de dados - como o SAFARI francês - surgiam como principais potenciais violadores da privacidade e do direito a autodeterminação informativa. Grandes empresas de tecnologia e processamento de dados, na Era da Informação, surgem nesse contexto em um segundo momento.

¹³ BVerGE 65, 1 (1983), acerca da constitucionalidade da Lei de Censo alemã.

Se se questionar o porquê desse desenvolvimento na Europa, especialmente, e também nos Estados Unidos (e não no Brasil, por exemplo¹⁴), sob o ponto de vista das condições político institucionais que passava o país nas décadas de sessenta a oitenta, em uma ditadura militar, cujo último interesse é fortalecer a posição jurídica dos cidadãos enquanto detentor de direitos, pode-se chegar à conclusão de que é necessário um ambiente de razoável estabilidade democrática, como gozava (e goza) o continente europeu, para que o debate sobre a proteção de dados enquanto proibição de intromissão do Estado na esfera privada.

1.1.2 A autodeterminação informativa no desenvolvimento legislativo da proteção de dados

A primeira legislação acerca da proteção de dados pessoais deu-se no estado americano da Califórnia em 1968 e abrangia aspectos do direito de acesso a registros públicos. Também a *Fair Credit Reporting Act* (1970) e *Privacy Act* (1974) regulam apenas parcialmente o tema a proteção de dados para instituições financeiras e na administração pública. A primeira tentativa de abordar a problemática da proteção de dados de maneira ampla ocorreu na Grã-Bretanha com a *Data Surveillance Bill* (1969)¹⁵.

Na província canadense de Ontário (1969) buscou-se abordar o tema, mas no curso do processo legislativo a lei não foi aprovada. Uma solução abrangente para tanto o setor público quanto o privado surge com a Lei de Dados sueca de 1973. Na Alemanha, a lei de proteção de dados do estado de Hessen (1970) foi a primeira legislação alemã a ocupar-se com a proteção de dados pessoais. Tratava sobre o uso de manipulação mecânica de dados na administração pública do estado de Hessen. Também a *Rheinland-Pfalzische Gesetz* contra o uso abusivo de dados (1974) limitava-se a regular a administração pública daquele estado¹⁶.

Tais iniciativas refletem o estado da tecnologia e a visão do jurista à época, notadamente vinculada à experiência do *National Data Center* e similares,

¹⁴ Vide Cap. III: O ordenamento pátria possui poucos instrumentos para proteção de dados pessoais – sequer uma legislação específica sobre o tema – o único na América Latina, inclusive, a não possui-lo.

¹⁵ Cf. AUERNHAMMER, 1993, p. 9.

¹⁶ Cf. AUERNHAMMER, 1993, p. 11.

marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçados pela coleta ilimitada de dados pessoais, uma operação que então era realizada basicamente pelo Estado. Tais leis são conhecidas hoje como leis de primeira geração, e proteção de dados pessoais, em uma classificação habitualmente utilizada pela doutrina¹⁷.

Essas legislações propunham-se a regular grandes polos manipuladores de dados: sua essência consistia na concessão de permissões de funcionamento e no controle do uso de informações pessoais pelo Estado e suas estruturas administrativas. Eram também pautadas em normas protetivas amplas, centradas no processamento de dados, apenas. Por outro lado, regras concretas e específicas eram destinadas aos responsáveis pelo processamento dos dados.

Este enfoque era natural, visto a motivação desta lei ter sido a “ameaça” representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática destas leis era condicionada pela informática – nelas, tratava-se dos “bancos de dados”, e não da “privacidade”, desde seus princípios genéricos até os regimes de autorização e modalidades de tratamentos de dados, a serem determinados *ex ante*, sem prever a participação do cidadão nesse processo (foi também por esse motivo que foram estabelecidos os primeiros comissários de proteção de dados pessoais)¹⁸.

Foi o *estado da tecnologia* que determinou a ineficácia desse primeiro grupo de normas, na medida em que seu regime baseado em autorizações, cujo acompanhamento demandava grande empenho por parte das autoridades responsáveis pelo controle, não logrou acompanhar o grande número de bancos de dados que surgiam à época.

A lei francesa de proteção de dados é o marco inaugural de um segundo momento legislativo referente à proteção de dados. A *Liberté e Informatique* de janeiro de 1978 vale para a manipulação automatizada de dados pessoais nas esferas pública e privada e prevê um processo de registro por meio de uma comissão de controle estatal¹⁹. Considera-se agora, em vez da “ameaça” computacional, a privacidade como uma liberdade negativa a ser exercida pelo próprio cidadão. Também a lei austríaca, as constituições da Espanha e Portugal caminham nesse sentido.

Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses; além disso, o controle nos moldes das leis anteriores tornou-se inviável, dada a fragmentação dos polos de

¹⁷ Cf. DONEDA, 2006, p. 207.

¹⁸ Cf. DONEDA, 2006, p. 210.

¹⁹ Cf. AUERNHAMMER, 1993, p. 10.

tratamento dos dados pessoais. **Assim, criou-se um sistema que fornece instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela** (grifo nosso)²⁰.

Pulveriza-se o mecanismo de autorização para o funcionamento de bancos de dados e a atividade de supervisão das autoridades de controle para facilitar a administração pública. Ocorre que Estas leis apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para sua efetiva participação na vida social.

Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para o seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão – ou seja, a atuação direta da “liberdade” do cidadão de interromper o fluxo para o exterior de suas informações pessoais – implicava, não raro, na sua exclusão de algum aspecto da vida social ou em algum tipo de prejuízo mensurável²¹.

Percebe-se que a informação, embora seja extensão da personalidade e deva ser protegida na esfera da privacidade, possui uma relevante dimensão econômico-social, razão pela qual alguns críticos chegam a proclamar um direito fundamental a manipulação de dados²².

Paradigmática é uma terceira fase da legislação de proteção de dados, pois influenciada pela decisão do *Bundesverfassungsgericht* que deu *status* constitucional ao tema da proteção de dados, ao enunciar a partir do direito fundamental ao livre desenvolvimento da personalidade e da dignidade humana. Essa terceira fase vê a proteção de como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes e assim proporcionando o efetivo e pleno exercício da autodeterminação informativa²³.

A autodeterminação informativa, de fato, surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas

²⁰ Cf. DONEDA, 2006, p. 210.

²¹ Cf. DONEDA, 2006, pp. 210-211.

²² Cf. GIESSEN, 2007, fala de um Grundrecht auf Datenverarbeitung (direito fundamental a manipulação de dados).

²³ Cf. DONEDA, 2006, p. 211.

na estrutura destas novas leis. O tratamento dos dados pessoais era visto como u processo, que não se encerrava na simples permissão ou não da pessoa para a utilização de seus dados pessoais, porém procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros; estas leis incluem também garantias específicas, como o dever de informação²⁴.

A participação do cidadão passa a ter destaque a partir desse momento legislativo. Percebeu-se, no entanto, que na realidade não seriam muitas as pessoas dispostas a exercitar suas prerrogativas de autodeterminação informativa, dado que os custos envolvidos, sejam eles econômicos ou sociais, geralmente as compeliam a aquiescer com situações que não eram as ideais. A autodeterminação informativa, portanto, continuava sendo privilégio de uma minoria decidida a enfrentar tais custos²⁵.

As “leis de quarta geração” procuraram suprir as lacunas de uma abordagem individualizada, com forte pragmatismo e instrumentalização de patamar coletivo da proteção de dados, concretizando a dimensão objetiva do direito a autodeterminação informativa.

Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição de uma pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito a autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual na autodeterminação informativa. Isto ocorre porque se parte do pressuposto que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser obtida exclusivamente de uma decisão individual²⁶.

Fortalece-se aqui um modelo baseado nas autoridades independentes para a atuação da lei – tanto mais necessárias com a diminuição do poder de barganha do indivíduo para autorização ao processamento de seus dados; há também o surgimento de uma normativa complexa, com regras específicas para alguns setores envolvidos no processamento de dados. Isso representaria para os cidadãos

²⁴ Cf. DONEDA, 2006, pp. 211-212.

²⁵ GARTH; CAPELETTI situam esse problema apontado por DONEDA no âmbito do acesso à justiça: “O prêmio para qualquer indivíduo buscar esta correção é pequeno demais para induzi-lo a tentar uma ação: trata-se, em muitos casos, de uma demanda judicial não-econômica. Assim, “embora as pessoas na coletividade tenham razões bastantes para reivindicar um interesse difuso, as barreiros à sua organização podem, ainda assim, evitar que esse interesse seja unificado e expresso”.

²⁶ Cf. DONEDA, 2006, p. 213.

instrumentos garantidores de maior eficácia dos princípios presentes nas leis de proteção de dados²⁷.

A partir da década de noventa a proteção dos dados também é normatizada no espaço europeu por meio da normativa 95/46/EG e a normativa 2002/58/EG (*e-commerce*) ampliaram a área de abrangência do direito a proteção de dados pessoais ao romper a tradicional distinção entre a área pública e privada.

O Art. 8º da carta de direitos fundamentais da União Europeia de 18 de dezembro de 2000 estipula um direito fundamental à proteção de dados pessoais. Com a entrada em vigor do Contrato de Lisboa torna-se tal direito um componente do ordenamento jurídico europeu originário firmando impulso para posteriores desenvolvimentos da legislação acerca dos dados pessoais (tradução livre)²⁸.

²⁷ Seguindo a inteligência de GARTH; CAPELETTI, 1998, p. 15, pode-se situar esse fenômeno sob o ponto de vista dos entraves ao acesso à justiça: “Supondo que o cidadão decida superar esses primeiros custos, deparar-se-á com agentes públicos, com todo o seu aparato funcional e prerrogativas processuais, ou agentes privados como provedores de internet e bancos, os quais Capeletti e Garth alcunham “litigantes habituais”.

²⁸ Cf. PETRI, 2010, p. 27, no original: Art. 8 Charta der Grundrechte der Europäischen Union vom 18.12.2000 sieht ausdrücklich ein Grundrecht auf Datenschutz vor. Mit Inkrafttreten des Vertrags von Lissabon wird es Bestandteil des Europäischen Primärrechts sein und weitere Impulse für eine Fortentwicklung des Datenschutzes setzen können.

1.2 DETERMINAÇÃO CONCEITUAL: AUTODETERMINAÇÃO INFORMATIVA COMO DIREITO FUNDAMENTAL

Entende-se relevante na determinação conceitual saber em quais valores constitucionais encontra a autodeterminação informativa guarida. A partir daí, constatado seu fundamento na *Grundgesetz*, trabalhá-lo como direito fundamental em suas dimensões, para que se possa determinar seu âmbito de proteção (*Schutzbereich*).

Direitos fundamentais são direitos públicos subjetivos de pessoas (físicas ou jurídicas), contidos em dispostos constitucionais e, portanto, encerram o caráter normativo supremo dentro do Estado, tendo como finalidade limitar o exercício do poder estatal em face da liberdade individual²⁹. O direito a autodeterminação informativa (*informationelles Selbstbestimmungsrecht*) não possui previsão textual na Lei Fundamental alemã (*Grundgesetz*): sua construção é jurisprudencial e dogmática³⁰, mas decorre de alguns de seus valores mais caros.

Para o *Bundesverfassungsgericht*, o **livre desenvolvimento da personalidade**, dadas as condições da manipulação de dados, **pressupõe** a proteção do indivíduo contra o levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Essa proteção seria abrangida pelo direito fundamental do Art. 2 I³¹ c. c. Art. 1 I³² GG. O direito fundamental (a autodeterminação informativa) **garante o poder do cidadão de determinar em princípio, ele mesmo, sobre a exibição e o uso de seus dados pessoais** (grifos nossos)³³.

²⁹ Cf. MARTINS, 2011, p. 49.

³⁰ O Bundesverfassungsgericht enunciou-o quando do julgamento acerca da constitucionalidade da Lei de Censo (Volkszählungsurteil), o qual merecerá especial atenção no capítulo seguinte.

³¹ Art. 2 I, GG: Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt (livre desenvolvimento da personalidade).

³² Art. 1 I, GG: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. (inviolabilidade da dignidade humana)

³³ BVerGE 65, 1, tradução de MARTINS, 2005, p. 238.

Essa ideia não deve, contudo, à interpretação simplista de que a capacidade de disposição sobre seus próprios dados signifique o exercício à autodeterminação informativa e a encerre enquanto conceito³⁴.

What the expression 'informational self-determination' means is rather that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined'³⁵.

Para que exista um livre desenvolvimento da personalidade faz-se necessário um espaço de autonomia, enquanto “qualidade que a vontade tem de ser lei para si mesma (independentemente de uma qualidade qualquer dos objetos do dever)”, diferentemente da vontade heterônoma, jurídica. Essa definição kantiana de autonomia coincide com a definição de liberdade de Rousseau, entendida como “obediência à liberdade que cada um dá a si mesmo”³⁶.

A comunicação livre em uma sociedade democrática tem como requisito o livre desenvolvimento da personalidade para que haja um debate plural – cujas ideias postas em contraponto aperfeiçoam-se em um processo dialético. Instrumento necessário para concretização desses valores – constitucionalmente expressos – é o direito à autodeterminação informativa, que, enquanto direito fundamental, impõe limites ao Estado pela realização de suas dimensões negativa e positiva.

O Estado Democrático de Direito baseia-se, em grande medida, na participação de todos os cidadãos e sua legitimidade lastreia-se no respeito à liberdade individual de cada pessoa. **O direito à autodeterminação informativa não só é concedido para o bem do indivíduo, mas também em prol de um interesse público - para garantir um sistema de comunicação livre e democrático.** Portanto, é possível, principalmente para justificar interferências no direito à autodeterminação informativa se uma consideração de ambos os princípios mostra que o público interesse prevalece sobre os interesses legítimos do indivíduo. No entanto, a ideia básica é sempre a mesma: a pessoa em causa é para manter o controle de seus próprios dados (tradução livre)³⁷.

³⁴ O Bundesverfassungsgericht valeu-se da expressão personbezogene Daten, a qual, para PAHLEN-BRANT (2008), é relacionada à pessoa seja 1) por seu conteúdo, por meio de afirmações sobre a pessoa (Aussage über die Person): “A possui uma carteira de motorista”, por exemplo; 2) pela finalidade da manipulação de dados (Zweck der Verarbeitung), como no caso da vigilância por vídeo; ou 3) pelo resultado da manipulação, quando como consequência secundária de uma manipulação de dados seja possível formular afirmações sobre uma determinada pessoa. Neste último caso em especial é possível perceber a fragilidade da ideia de autodeterminação informativa como mera disposição sobre os próprios dados.

³⁵ ROUVROY; POULLET, 2009, p. 57.

³⁶ Cf. BOBBIO, 1997, pp. 62-63.

³⁷ Cf. HORNUNIG e SCHNABEL, 2009, p. 87, no original: *The democratic constitutional state relies to a great extent on the participation of all citizens and its legitimacy is based on respecting each person's individual liberty. As said before, the right to informational self-determination is not only granted for the sake of the individual, but also in the interest of the public, to guarantee a free and democratic communication order. Therefore, it is primarily possible to justify interferences in the right to informational self-determination if a consideration of both principles shows that the public interest outweighs the legitimate interests of the*

Esse conceito de autodeterminação informativa é muito díspar da ideia de privacidade como um *right to be alone*. O indivíduo é protegido contra interferências em assuntos pessoais, criando assim uma esfera em que ele pode se sentir seguro de qualquer interferência. Ao mesmo tempo, a proteção de dados é também uma pré-condição para a participação imparcial dos cidadãos nos processos políticos do Estado de direito democrático.

A autodeterminação informativa, como direito fundamental, tem como principal conferir aos indivíduos uma posição jurídica de direito subjetivo, em sua maioria de direito material, mas às vezes de natureza processual e assim limitar a atuação de órgãos do Estado³⁸, a chamada (*Abwehrrecht gegen staaatliche Grundrechtseingriffe*). É amplamente aceita na doutrina e jurisprudência a existência de dois “conteúdos” ou dimensões: as jurídico-subjetivas e as jurídico-objetivas, a serem aplicadas a esse direito.

Como principais desdobramentos dessa dimensão jurídico-subjetiva, têm-se o clássico direito de resistência contra a intervenção estatal e, também, os direitos à prestação de tutela estatal.

A função ou dimensão subjetiva dos direitos fundamentais é aquela que corresponde, principalmente, ao status negativus da clássica lição do status (statuslehre) de GEORG JELLINEK. Trata-se da dimensão chamada “clássica”, porque o seu conteúdo normativo se refere ao direito do titular de resistir à intervenção estatal em sua esfera de liberdade individual. Esta dimensão tem um correspondente teórico que é a teoria liberal dos direitos fundamentais. Fala-se também, neste contexto, em função “clássica”, quando o direito fundamental oferece ao titular a faculdade jurídica de resistência contra intervenção estatal³⁹.

Na relação jurídica de direito público havida entre o indivíduo e o Estado em razão das normas de direito fundamental, ao indivíduo é conferido um status de liberdade negativa (liberdade *de* alguma coisa, liberdade *contra* certos imperativos definidos pelo poder público)⁴⁰, cabendo ao Estado obrigação *de não fazer*, de não acessar a esfera individual protegida pela norma de direito fundamental, salvo se houver uma legitimação constitucional para tanto. Esse é o efeito, por excelência, desta dimensão dos direitos fundamentais.

individual. However, the basic idea is always the same: the data subject is to maintain control of his/her own data).

³⁸ Cf. MARTINS, 2011, p. 57.

³⁹ Cf. MARTINS, 2005, p. 80.

⁴⁰ Cf. MARTINS, 2005, p. 80.

No âmbito da autodeterminação informativa, essa dimensão realiza-se na imposição de um *espaço informativo* que o Estado não pode acessar sem justificativa legal e que permite ao titular do direito exigir em juízo sua guarda.

Em segundo lugar, a dimensão subjetiva também aparece naqueles casos onde os direitos fundamentais embasam pretensões jurídicas próprias do *status positivus*, onde ao indivíduo é conferido um status de liberdade positiva (liberdade *para* alguma coisa),

a qual pressupõe ação estatal, tendo como efeito a proibição da omissão por parte do Estado. Fala-se assim, de vários conteúdos, como, por exemplo, os direitos de participação e garantias processuais, onde a mais central é a pretensão à proteção de direitos pelo Judiciário, os direitos de tutela estatal contra agressões aos direitos fundamentais advindas de particulares⁴¹.

A *dimensão objetiva* dos direitos fundamentais fornece, ao seu turno, critérios de controle da ação estatal, vinculativos mesmo sem uma intervenção concreta, cujo efeito é precipuamente preventivo.

A *Função ou dimensão jurídico-objetiva* dos direitos fundamentais encerra outras funções, algumas também já tornadas “clássicas”, como as garantias de organização. Como “dimensão objetiva”, define-se a dimensão dos direitos fundamentais, **cuja percepção independe de seus titulares, vale dizer, dos sujeitos de direito**⁴².

Há três grandes funções pertencentes à dimensão objetiva dos direitos fundamentais. Primeiramente, o caráter de *normas de competência negativa*, que significa que aquilo que está sendo dado ao indivíduo, em termos de liberdade para a ação e em termos de livre arbítrio, está sendo, objetivamente, retirado do Estado, em termos de atribuição de competência.

Tal efeito ocorre independentemente do fato de o titular do direito exigi-lo em juízo. Por isso, o conceito ou caráter objetivo (dimensão objetiva) dos direitos fundamentais é relevante principalmente para o controle abstrato de normas, onde se controla a norma objetivamente e não a partir do ensejo de um caso particular. Não obstante, essa dimensão pode surgir também no bojo da interpretação e aplicação normativa. O controle abstrato de constitucionalidade de normas é dever do próprio Estado, que está vinculado a um espécie de auto-controle em função dos direitos fundamentais. Trata-se neste mister, de um “processo objetivo”, cujo objeto é o interesse público de se extirpar um estado normativo de inconstitucionalidade. Por outro lado, a minoria política, representada na Câmara Federal (*Bundestag*), é também, no entanto, parte legítima no controle abstrato de constitucionalidade⁴³.

⁴¹ Cf. MARTINS, 2005 p. 81.

⁴² Cf. MARTINS, 2005, p. 81 (grifos nossos).

⁴³ Cf. MARTINS, 2005, p. 82.

Como *critério para a interpretação e configuração do direito infraconstitucional*, nos seus efeitos *horizontal e de irradiação dos direitos fundamentais*, relacionados ao vínculo específico do Poder Judiciário aos direitos fundamentais, há, em um segundo desdobramento, a obrigação estatal de interpretar e aplicar todo o direito infraconstitucional em especial pelas cláusulas gerais (*Generalklauseln*), de modo consoante aos direitos constitucionais.

Na “interpretação conforme a Constituição”, existe a obrigação da “interpretação consoante os direitos fundamentais” (*grundrechtskonforme*), como subespécie da interpretação conforme a Constituição. É o que o Estado faz (deve fazer), em princípio, de forma objetiva, ou seja, sem a necessidade de provocação por parte do titular por direito. Neste caso, entretanto, a dimensão subjetiva também vem logo à tona, após a prolação da sentença pelo juiz que, ao interpretar o direito infraconstitucional, onde um direito fundamental for, ao menos, tangenciado, ignore os efeitos citados. Ao fazê-lo o juiz intervém de forma potencialmente violadora nos direitos fundamentais envolvidos⁴⁴.

O efeito dessa dimensão direito fundamental é chamada “horizontal”, pois vincula além do Estado, também terceiros (particulares). Para Auernhammer, diferentemente dos agentes públicos, pessoas e instituições de direito privado não são vinculados diretamente a direitos fundamentais previstos na *Grundgesetz*, dado que a vinculação direta destes a direitos fundamentais conduziria a uma limitação da autonomia privada, a qual possui igualmente amparo constitucional⁴⁵.

O dever estatal de tutela, (*staatliche Schutzpflichten*), por fim, enquanto desdobramento da dimensão objetiva, refere-se ao dever do Estado de resguardar, de modo ativo, os direitos fundamentais. Cabe ao Estado forçar a observância desses direitos de maneira preventiva, por meio da proteção de mecanismos legislativos preventivos.

A este contexto pertencem o desenvolvimento da energia atômica, da tecnologia eletromagnética, os riscos a saúde provocados por poluição química, **o desenvolvimento da tecnologia da informação, que permite a criação de perfis, a alienação total da identidade por meio do arquivamento de dados pessoais e o controle do indivíduo por certos “banqueiros de dados”** etc. O dever de tutela corresponde aqui a um dever de garantia da segurança (por exemplo, no caso da defesa de dados) ou ao dever geral de prevenção de riscos (por exemplo, no caso da prevenção contra riscos do uso da energia atômica) (grifo nosso)⁴⁶

⁴⁴ Cf. MARTINS, 2005, p. 82.

⁴⁵ 1993, p. 6, no original: Zwar gelten die Grundrechte im Privatrecht nach herrschender Meinung nicht unmittelbar; vielmehr kommt ihnen nur eine mittelbare Drittwirkung zu. Anders als die Öffentliche Hand werden private Person en und Institutionen durch die in den Grundrechten des Burgers enthaltenen Wertentscheidungen nicht nach Art. 1 Abs. 3 GG unmittelbar gebunden.

⁴⁶ Cf. MARTINS, 2005, p. 85. Este autor defende a ideia da irreparabilidade do dano à privacidade em sua tese de doutoramento

Trata-se da função de resistência ampliada àqueles casos nos quais os particulares passaram a ameaçar a liberdade tutelada. Esta função exige do Estado que ele aja contra as seguintes situações de ameaça de um direito fundamental:

Se a possível violação, que possa resultar do desenvolvimento da situação de ameaça, for irreparável. É o que ocorre, por exemplo, sobretudo no caso da ameaça ao direito à vida.

Quando o desenvolvimento em si, que parte da simples ameaça chegando à possível violação, for incontrollável. É o que ocorre em muitos casos envolvendo a utilização da técnica, como por exemplo, junto ao efeito cascata que o levantamento e o processamento de dados pessoais provocam. **O seguinte questionamento revela a importância da verificação desta incontrollabilidade para a verificação da necessidade do cumprimento do dever estatal de promover a segurança: quem levantou os dados pessoais? Com que objetivo? O titular do direito à intimidade, nestes casos, não pode nem sequer reagir, pois: reagiria contra quem? Quem sabe o quê sobre ele? (grifo nosso)**⁴⁷

Esse breve desenvolvimento da teoria dos direitos fundamentais é necessário para chegar ao necessário ponto do *dimensionamento objetivo do direito fundamental à autodeterminação informativa*: há, sob o ponto de vista do dever estatal de tutela, dada a incontrollabilidade do desenvolvimento das tecnologias da informação, um dever de legislação sobre a matéria proteção de dados pessoais, para que se evitem danos causados por particulares (e também pelo Estado)⁴⁸.

Assim, o direito à autodeterminação informativa é um direito público subjetivo depreendido de dispostos constitucionais que guarnecem o livre desenvolvimento da personalidade e da dignidade humana e, portanto, encerram valores supremos dentro do Estado, tendo como finalidade limitar o exercício do poder estatal em face da liberdade individual de dispor sobre seus dados pessoais

1) pela vedação à intromissão injustificada à esfera de privacidade dos cidadãos;

2) pela interpretação garantidora da autodeterminação informativa nas cláusulas gerais de normas infraconstitucionais (*selbstbestimmungsrechtskonform*)⁴⁹;

⁴⁷ DONEDA (2006) aponta com acerto que ferramentas disciplinadas do Código de Defesa do Consumidor (CDC) e o próprio habeas data pressupõem um binômio restritivo acesso/retificação. O dever estatal surge em um cenário em que se torna muito difícil detectar quem são aqueles que têm acesso a dados pessoais.

⁴⁸ Na Alemanha, esse dever estatal de tutela derivado do da dimensão objetiva dos direitos fundamentais é realizada pela Lei Federal de Proteção de Dados (Bundesdatenschutzgesetz).

⁴⁹ Termo cunhado pelo autor.

3) por meio de uma legislação sobre dados pessoais que previna de sua violação (dever estatal de tutela).

1.3 CONVERGÊNCIAS COM O DIREITO À PRIVACIDADE

O direito à privacidade associada ao isolamento e à reclusão, o *right to be alone*, tem como pano de fundo um modelo liberal, cuja tutela de direitos circunscrevia-se ao indivíduo: a casa como asilo inviolável, o sigilo de correspondência ou mesmo o sigilo profissional. Nesse sentido, pode ser definida como modo de ser da pessoa que consiste na exclusão do conhecimento de outrem de quanto se refira à mesma pessoa⁵⁰, ou mesmo a esfera secreta da vida do indivíduo na qual se tem o poder legal de evitar os demais⁵¹. Apresenta-se, nesse aspecto, como um *Abwehrecht*, *status* negativo que impõe ao Estado uma obrigação de não violar a correspondência, o domicílio, etc.

Sob esse prisma, propõem TROJANOW e ZEH⁵² o seguinte exemplo paradigma: um determinado cidadão contrata alguém para fazer a limpeza de sua casa e dirige-se ao trabalho. No meio do caminho recorda ter esquecido alguns documentos e retorna. Ao chegar a seu quarto, depara-se com o contratado livremente vasculhando sua vida privada em arquivos do computador da família. Evidentemente, à pergunta de se se tomaria alguma medida repressiva para coibir tal conduta, a resposta seria normalmente afirmativa, pois se trata de uma esfera íntima dentro da qual não se quer intromissão indesejada por ninguém. É um *locus* sobre o qual se tem o poder de evitar os demais, um espaço de privacidade.

As modernas tecnologias da informação permitem que governos e empresas adentrem aos “arquivos da vida privada” de milhões de cidadãos sem que se tenha a mínima consciência disso. Sabe-se que essa invasão existe – e ela reduz inclusive a expectativa por privacidade⁵³ –, mas um indivíduo isoladamente possui condições técnicas para tomar conhecimento de se *precisamente ele* tem sua privacidade devastada.

A conclusão é de que as ferramentas que dispunha o direito a privacidade seriam eficazes contra o primeiro, mas não contra o segundo. Por isso

a proteção da privacidade, elemento essencial da personalidade, merece tutela integrada, sendo um dos casos em que ela é mais necessária. A

⁵⁰ DE CUPIS apud SILVA, 2008, p. 207.

⁵¹ DOTTI apud SILVA, 2008, p. 207.

⁵² 2011, pp. 80-90.

⁵³ Cf. ROUVROY; POULLET, 2009.

cotidiana redefinição de forças e meios que possibilitam a intromissão na esfera privada dos indivíduos, demanda uma tutela de caráter amplo. Face à miríade de possibilidades de manipulação de informações pessoais em bancos de dados informatizados, muitas delas originando alguma espécie de desnudamento de assuntos privados, sequer se pode pretender possuir a noção exata de seus efeitos quanto à privacidade. A única tutela eficaz é a que é dinâmica e integral. Tal tutela somente pode ser obtida contando-se com um instrumento jurídico adequado à esta dinâmica, que deve ser flexível o suficiente para poder ser aplicado em situações inéditas, onde novas formas de ofensas à privacidade ocorram de formas que antes não eram cogitadas. Para obtermos esta tutela deve ser utilizada a cláusula geral, entendida como "a formulação de uma hipótese legal que, em termos de grande generalidade, abrange e submete a tratamento jurídico todo um domínio de casos"⁵⁴.

Nesse enredo, a necessidade de funcionalização da proteção da privacidade faz surgir uma disciplina de proteção de dados pessoais, que compreende pressupostos ontológicos idênticos aos atos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias – especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem de conceitos pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa⁵⁵.

Privacidade e autodeterminação informativa protegem a linha de separação que evita a migração de informações sensíveis, descontextualizadas, de um contexto para outros. A proteção dos dados pessoais, como funcionalização da privacidade, é essencial para um desenvolvimento livre e autodeterminado do indivíduo. O desenvolvimento autodeterminado, ao seu turno, é pré-requisito para uma ordem de comunicação livre e democrática.

É esse o núcleo essencial que faz a autodeterminação informativa e a privacidade convergirem: ambas têm raiz constitucional e são meios necessários para um arranjo de liberdades que circundam a cláusula geral de personalidade.

⁵⁴ Cf. DONEDA, 2006, p. 27.

⁵⁵ Cf. DONEDA, 2006, p. 30.

2 PROTEÇÃO DOS DADOS PESSOAIS E DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO GERMÂNICO

2.1 PANORAMA GERAL

Apesar de ter-se apresentado um cenário das “gerações” de proteção de dados em âmbito europeu no primeiro capítulo, reputa-se necessário apontar os principais estágios de desenvolvimento da proteção de dados *na Alemanha*. Para Petri⁵⁶, são basicamente cinco.

Fase 1. A decisão sobre o *Mikrozensus* de 16 de julho de 1969 abre caminho para a proteção de dados na Alemanha. O Tribunal Constitucional Federal confirma haver uma esfera intocável da vida privada que é garantida contra o poder público. Determina assim que o Estado não pode de forma obrigatória registrar e catalogar a personalidade dos cidadãos. Essa decisão põe o direito fundamental a proteção dos dados como decorrente da dignidade da pessoa humana e do direito à autodeterminação informativa, motivo por que se firmou como um claro impulso para as primeiras leis de proteção a dados pessoais no continente europeu.

Fase 2. A Lei Federal de proteção de Dados Pessoais (*Bundesdatenschutzgesetz*) inaugura em 1977 o marco legislativo sobre proteção de dados na Alemanha. De acordo com o parágrafo primeiro do BDSG 1977 “é tarefa da proteção de dados pessoais e a proteção de dados pessoais contra seu abuso”.

Fase 3. Em dezembro de 1983, o TCF alemão, no *Volkszählungsurteil*, declara a raiz constitucional do direito a proteção de dados pessoais, o que amplia a área de proteção jurídica desse direito consideravelmente. A proteção de dados pessoais não é mais vista apenas como proteção à privacidade contra investidas do Estado – configura-se agora como um direito à autodeterminação informativa, derivado do Art. 2 Abs. 1 e Abs. 1 GG.

Fase 4. Desde a metade dos anos 90 a proteção dos dados também é normatizada no espaço europeu. A normativa 95/46/EG e a normativa 2002/58/EG (e-commerce) ampliam a área de abrangência do direito a proteção de dados pessoais alemão na medida em que quebram a tradicional distinção entre a área

⁵⁶ 2010, em Wertewandel im Datenschutzrecht.

pública e privada. Artigo 8º da Carta dos Direitos Fundamentais da União Europeia, 18.12.2000 especificamente prevê o direito fundamental à privacidade.

Fase 5. Em 2008, na decisão cunhada de *Online-Durchsuchungsurteil*, o BVerfG enuncia, a partir do direito fundamental ao livre desenvolvimento da personalidade e da dignidade humana (Art. 2 I e Art. 1 I GG), um novo direito fundamental (o primeiro após o direito a autodeterminação informativa). O *IT-Grundrecht*, como é denominado o *direito fundamental à garantia da confiabilidade e integridade de sistemas*, protege a confiabilidade de sistema de informação. Isso significa, *et cetera* que apenas pessoas autorizadas podem ter acesso às informações disponíveis no sistema. Além disso, a integridade dos sistemas de informação também deve ser garantida por meio de medidas preventivas.

O presente capítulo ocupa-se de aspectos relevantes da jurisprudência e legislação concernentes à proteção de dados e do direito a autodeterminação informativa no direito germânico.

Do conjunto de decisões sobre o tema, acima mencionados, abordar-se-ão a *Mikrozensusurteil*, que firmou as bases de uma interpretação constitucionalizada da proteção de dados a partir do livre desenvolvimento da personalidade. Sua *teoria das esferas* foi superada pela *Volkszählungsurteil* de 1983, que estatuiu uma área de proteção jurídica (*Schutzbereich*) mais ampla e dinâmica ao evocar da dignidade humana e do livre desenvolvimento da personalidade o direito à autodeterminação informativa (*Recht auf informationelle Selbstbestimmung*), que é âncora constitucional da proteção de dados no direito alemão.

Em uma segunda seção, apontar-se-ão aspectos da Lei Federal de Proteção de Dados alemã, a *Bundesdatenschutzgesetz*, concretizadora do dever estatal de tutela decorrente da dimensão objetiva do direito fundamental à autodeterminação informativa.

2.2 PANORAMA JURISPRUDENCIAL

2.2.1 O Mikrozensusurteil

O *Volkszählungsurteil* consolida a jurisprudência acerca do que o Art. 2 I GG assegura o livre desenvolvimento da personalidade (*freie Entfaltung der Personlichkeit*). Contudo, antes de 1983 já interpretava o Tribunal Constitucional Federal o livre desenvolvimento da personalidade como direito à autodeterminação informativa. Valia-se, para isso, da “teoria das esferas” (*Spharentheorie*), de acordo com a qual a personalidade possuiria ao menos três esferas: uma íntima, uma privada e outra social⁵⁷.

A esfera íntima permaneceria intocável (*untastbar*), ao representar o núcleo essencial (*Wesensgehalt*) do Art. 2 I GG. A intromissões na esfera privada aplicar-se-ia o princípio da proporcionalidade (*Verhältnismassigkeitsgrundsatz*); intromissões à esfera social, ao seu turno, seriam mais toleradas, pois presentes informações necessárias à formulação de políticas públicas.

Nesse sentido a decisão, em controle concreto de constitucionalidade, sobre a lei do “micro-senso” de 1957 (BverfGE 27, 1), que previa uma multa para casos de recusa a respostas sobre viagens de férias e repouso, o TCF considerou, em suma, que os dados levantados não atingiam **a esfera íntima e inviolável do indivíduo** e que a intervenção estava justificada por ser formalmente permitida pelo Art. 2 I GG e materialmente proporcional para abastecer o Estado com dados necessários ao planejamento da ação estatal.(...) Embora a pesquisa tenha se referido a um âmbito de vida privada, não obrigou o entrevistado nem a revelações sobre **sua esfera íntima nem concedeu ao Estado visão que não acessível ao mundo exterior** e que, assim, não tem por sua natureza caráter sigiloso (grifo nosso)⁵⁸.

Note-se que o TCF afasta a tese de atingimento à esfera íntima, inviolável, e à esfera privada. Entendeu-se tratar de informações pertencentes à esfera mais frágil de proteção, a social (*Sozialsphere*), motivo por que justificada a intervenção, sem prejuízo ao livre desenvolvimento da personalidade.

⁵⁷ Cf. MARTINS, 2001, p. 71.

⁵⁸ Cf. MARTINS, 2001, pp. 215-218.

Em outra decisão, a *Scheidungsakte-Beschluss*, segue o TCF a linha interpretativa de que nem todas as áreas da vida privada estariam protegidas pelo direito fundamental ao livre desenvolvimento previsto no Art. 2 I GG. Restrições firmar-se-iam possíveis quando relevante interesse coletivo estivesse em jogo, ressalvada a análise de proporcionalidade e desde que não houvesse agressão à esfera íntima⁵⁹.

A jurisprudência baseada na teoria das esferas, até o advento da *Volkszählungsurteil* majoritária no TCF, revelou-se, no entanto, insuficiente para resolver os problemas dogmáticos relativos à concretização do livre desenvolvimento da personalidade. Não houve definição ou exemplo para a esfera íntima. Para a esfera social, por exemplo, não houve exemplificação consistente⁶⁰.

Para a questão da proteção de dados, as limitações da teoria das esferas afiguram-se ainda mais notáveis. A utilização da teoria das esferas significa que nem toda informação privada precisa ser protegida, senão apenas aquelas que possam ser consideradas da esfera íntima⁶¹.

Nos fundamentos da *Volkszählungsurteil*, um dos principais argumentos que supera a teoria das esferas⁶² é atestar que não há mais dados que sejam inofensivos, desmerecedores de proteção, na medida em que se pode obter, a partir do cruzamento de vários desses dados, uma informação cujo conteúdo pertenceria à esfera íntima. Em suma: o direito à autodeterminação informativa enquanto direito fundamental enunciado pelo TCF na *Volkszählungsurteil*, representa a superação da teoria das esferas enquanto critério de aferição de lesão à privacidade dos cidadãos.

⁵⁹ Cf. MARTINS, 2001, p. 72, no original: *Jedoch steht nicht der gesamte Bereich des privaten Lebens unter dem absoluten Schutz des Grundrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 und 19 Abs. 2 GG (vgl. auch BVerfGE 6, 389 (433); 27, 1 (6 f.)). Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger (BVerfGE 4, 7 (15 f.); 27, 1 (7)) muß vielmehr jedermann staatliche Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismasskeitsgebote erfolgen, soweit sie nicht den unantastbaren Bereich privater Lebensgestaltung beeinträchtigen. Dabei kann von den Grundsätzen, die das Bundesverfassungsgericht in seiner bisherigen Rechtsprechung über die verfassungsrechtliche Zulässigkeit von Eingriffen in die körperliche Unversehrtheit entwickelt hat (BVerfGE 16, 194 (201 f.); 17, 108 (117 f.); 27, 211 ff.), ausgegangen werden. Jedoch ist dem Schutz der Integrität der menschlichen Person in geistig-seelischer Beziehung ein besonders hoher Wert beizumessen (vgl. auch BGHSt 19, 325 (331 ff.); BVerwGE 19, 179 (184 ff.); Maetzel, DVBl. 1966, S. 665).*

⁶⁰ SCHLINK apud. MARTINS, 2001, p. 72, no original: *Tonbandaufnahme existiert, wo das Argument allerdings nicht entscheidungserheblich war.*

⁶¹ Martins, 1991, p. 71. „Die Anwendung der Spharentheorie bedeutete, dass nicht jede private Information geschützt werden muss, sondern nur diejenigen, die der Intimsphäre zugerechnet werden können“ (tradução livre).

⁶²

É do contexto, fundamentos e consequências dessa decisão que a presente pesquisa irá ocupar-se.

2.2.2 A *Volkszählungsurteil*

Em 1983, o governo federal alemão planejava conduzir um recenseamento geral da população. No entanto, houve grande insatisfação popular pelo receio de uma excessiva vigilância e a sensação de que um censo seria uma invasão injusta à privacidade. Estes sentimentos levaram a um acalorado debate público, o que resultou em apelos por um boicote e no ajuizamento de Reclamações Constitucionais no *Bundesverfassungsgericht*, o qual decidiu que a Lei Censo Demográfico era parcialmente inconstitucional e, portanto, foi anulada, pondo fim ao censo temporariamente. Nesta decisão, chamada de *Volkszählungsurteil*, o Tribunal Constitucional Federal cunhou um novo direito fundamental: a autodeterminação informativa, âncora legal para proteção de dados na Constituição alemã. A decisão é, até o momento, a mais importante decisão na história da proteção de dados alemã, o que significa que entender essa decisão é crucial para compreender a visão alemã sobre proteção de dados⁶³.

O parlamento federal alemão aprovou uma lei para o censo da população a ser realizado no ano seguinte, cuja aprovação foi unânime. As poucas intervenções durante o debate parlamentar não faziam alusão à proteção de dados - focou-se essencialmente em questões de financiamento do censo. Não era esse clima de apatia que vigia na sociedade alemã à época.

Em contraste com a ausência de discussões polêmicas no *Bundestag*, houve um grande debate na sociedade sobre os riscos de proteção de dados, bem como a utilidade do censo populacional. A oposição compôs uma corrente divergente, mas não logrou convencer o *Bundesregierung* a abandonar ou mesmo sequer alterar seus planos. Além de um ceticismo geral em relação às possibilidades de planejamento central, os argumentos dos adversários focavam a problemática de proteção de dados. Havia temores que os dados poderiam ser “reassociados” aos

⁶³ Cf. HORNUNG; SCHNABEL, 2009, p. 85.

indivíduos [...]. Os dados, ressalte-se, não visavam apenas a fins estatísticos, mas também à comparação e correção de registros de residentes⁶⁴.

Além do debate político, a Lei do Censo também foi contestada perante o *Bundesverfassungsgericht*. Em dezembro de 1983, o tribunal publicou sua decisão. Foi declarada constitucional a finalidade precípua da Lei do Censo, mas exigiram-se salvaguardas processuais e organizacionais com vistas à de direitos fundamentais. A transferência de dados para as autoridades locais, por exemplo, foi considerada igualmente inconstitucional, pois violaria as fronteiras entre a coleta de dados para fins estatísticos anônimos e o processamento de dados pessoais por parte dessas autoridades. A resposta do Parlamento não tardou a vir.

Mesmo que o resultado da decisão possa ser considerado uma grande vitória para os opositores, o censo não foi interrompido, somente retardado. Uma nova lei foi aprovada em 1985 no *Bundestag*, levada agora em conta a decisão do *Bundesverfassungsgericht*, - e o censo populacional efetivamente ocorreu em maio de 1987. Essa nova lei foi igualmente contestada perante o tribunal, mas os juízes a consideraram constitucional⁶⁵.

No *Volkszählungsurteil*, o TCF firmou as bases da proteção de dados alemã em âmbito 1) constitucional ao enunciar um direito fundamental à autodeterminação informativa (*Recht auf informationelle Selbstbestimmung*) e 2) infraconstitucional ao ditar regras e princípios que influenciaram diretamente na reformulação da Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*).

O direito à autodeterminação informativa e um direito geral à privacidade não estão textualmente explícitos na *Grundgesetz*. Os fundamentos para a autodeterminação informativa tornar-se um direito constitucional residem no argumento adotado pelo TCF de que proteção do indivíduo contra o levantamento, armazenagem, uso e transmissão irrestritos de dados pessoais é pressuposto para livre desenvolvimento da personalidade.

Essa proteção é abrangida pelos direito fundamentais dos Art. 2 I e Art. 1 I da *Grundgesetz*, quais sejam, o livre desenvolvimento da personalidade e a inviolabilidade da dignidade humana, os quais compõem um *direito geral de personalidade*, que, por sua vez, possui diversas implementações – uma das quais o direito à autodeterminação informativa.

⁶⁴ Cf. HORNUNG; SCHNABEL, 2009, p. 85.

⁶⁵ Cf. HORNUNG; SCHNABEL, 2009, p. 85.

Pode-se afirmar, portanto, que o direito de autodeterminação informativa é a âncora constitucional para a proteção de dados e uma parte do direito geral de personalidade, ligado à ideia de dar a cada pessoa a possibilidade de desenvolver uma personalidade livre e autodeterminada.

O *Bundesverfassungsgericht* desenvolveu uma série de salvaguardas para proteger os cidadãos contra invasões desproporcionais em seu direito à autodeterminação informativa. Uma vez que o direito apresenta-se como um direito fundamental constitucional, intervenções só são possíveis para promover interesse jurídico geral (*Rechtsgut*) de *status* constitucional. Além disso, atos que intervenham no direito do cidadão à autodeterminação informacional devem ser baseados em lei que cumpra altos padrões de clareza e certeza. Estas exigências são devidas pelo fato de o direito a autodeterminação permitir aos cidadãos o livre desenvolvimento da personalidade⁶⁶.

Essas medidas são especialmente necessárias pelo fato de, argumenta o TCF, informações de um contexto poderem ser combinadas, sobretudo na estruturação de sistemas integrados, com outros bancos de dados, formando um quadro de personalidade sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso.

Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas⁶⁷.

A autodeterminação individual pressupõe, prossegue o TCF, que mesmo sob as condições da moderna tecnologia de processamento de informação, sejam garantidas ao indivíduo 1) sua liberdade de decisão sobre as ações a serem procedidas ou omitidas e, inclusive, 2) a possibilidade de se comportar realmente conforme tal decisão.

Quem não consegue determinar com suficiente segurança quais informações sobre a sua pessoa são conhecidas em certas áreas de seu meio social, e quem consegue avaliar com mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação⁶⁸.

⁶⁶ Cf. HORNUNG; SCHNABEL, 2009, p. 85.

⁶⁷ BVerGE 65, 1, tradução de MARTINS, 2005, p. 237.

⁶⁸ BVerGE 65, 1, tradução de MARTINS, 2005, p. 237.

Essa primeira interpretação denota o caráter constitucional do direito a autodeterminação informativa sob o ponto de vista do livre desenvolvimento da personalidade, ou seja, no âmbito da individualidade. Existe, contudo, uma outra dimensão, igualmente importante, que o *Selbstbestimmungsrecht* concretiza: uma dimensão de garantia de comunicação livre em uma sociedade plural.

Uma ordem social e uma ordem jurídica [...] na qual os cidadãos não sabem mais quem, o que, quando, e em que ocasião se sabe sobre eles, não seriam compatíveis com o direito a autodeterminação na informação. Quem estiver inseguro sobre as formas de comportamento divergentes são registradas o tempo todo e definitivamente armazenadas, utilizadas e transmitidas, tentará não chamar a atenção através de tais comportamentos⁶⁹.

Um cidadão que saiba poder ser registrada uma assembleia ou em iniciativa popular por autoridades, tenderia, para evitar problemas futuros, a desistir de exercer seus respectivos direitos fundamentais. Isso menoscabaria não apenas de desenvolvimento individual cidadão, mas também o do bem comum, porque a autodeterminação informativa é uma condição funcional elementar para uma comunidade democrática e livre, fundada na capacidade de ação e participação de seus cidadãos⁷⁰.

Assim, o conceito alemão de autodeterminação informativa é muito díspar da ideia de privacidade como um *right to be alone*. Ao contrário, autodeterminação informativa e a proteção de dados tem dois efeitos correspondentes. O indivíduo é protegido contra interferências em assuntos pessoais, criando assim uma esfera em que ele ou ela pode se sentir seguro de qualquer interferência. Ao mesmo tempo, a proteção de dados é também uma pré-condição para a participação imparcial dos cidadãos nos processos políticos do Estado de direito democrático⁷¹.

O Estado Democrático de Direito baseia-se, em grande medida, na participação de todos os cidadãos e sua legitimidade lastreia-se no respeito à liberdade individual de cada pessoa. O direito à autodeterminação informativa não só é concedido para o bem do indivíduo, mas também em prol de um interesse público - para garantir um sistema de comunicação livre e democrático. Portanto, é possível, principalmente para justificar interferências no direito à autodeterminação informativa se uma consideração de ambos os princípios mostra que o público interesse prevalece sobre os interesses legítimos do indivíduo. No entanto, a ideia básica é sempre a mesma: a pessoa em causa é para manter o controle de seus próprios dados (tradução livre)⁷².

⁶⁹ BVerGE 65, 1, tradução de MARTINS, 2005, p. 237.

⁷⁰ BVerGE 65, 1, tradução de MARTINS, 2005, p. 238.

⁷¹ Cf. HORNUNIG e SCHNABEL, 2009.

⁷² Cf. HORNUNIG e SCHNABEL, 2009, p. 85, no original: “The democratic constitutional state relies to a great extent on the participation of all citizens and its legitimacy is based on respecting each person’s

Daí porque o livre desenvolvimento da personalidade pressupõe resguardar o indivíduo contra o levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Tal proteção, abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG, garante o poder do cidadão de determinar em princípio, ele mesmo, sobre a exibição e o uso de seus dados pessoais⁷³.

O *Bundesverfassungsgericht* assevera que esse direito possui determinados limites, na medida em que mesmo determinados dados pessoais pertencem ao *fluido informacional* necessário para a organização social e formulação de políticas públicas por parte do Estado.

O indivíduo não tem um direito no sentido de um domínio absoluto, ilimitado sobre “seus” dados; ele é muito uma personalidade em desenvolvimento, dependente da comunicação dentro da comunidade social. A informação, também quando ela é relativa à pessoa, representa um recorte da realidade social que não pode ser associado exclusivamente ao indivíduo atingido [por causa da demanda de informações do Estado e de terceiros]. A *Grundgesetz*, como frisado várias vezes na jurisprudência do TCF, decidiu o conflito indivíduo – comunidade, orientado pela vinculação à coletividade da pessoa e sua participação interdependente na [mesma] coletividade **Por isso, em princípio, o indivíduo tem que aceitar limitações de seu direito à autodeterminação informativa em favor do interesse geral predominante** (grifo nosso)⁷⁴.

Essas limitações à autodeterminação informativa necessitam, contudo, prosseguir o TCF, de base legal constitucional, da qual resultam de forma clara e reconhecível para o cidadão os pressupostos e a extensão das limitações, atendendo-se ao princípio da clareza normativa do Estado de Direito

O *Bundesverfassungsgericht* aponta, igualmente, que legislador deve observar em sua regulamentação o princípio da proporcionalidade, “bastião” da dignidade constitucional e resultado da essência dos direitos fundamentais, pois a pretensão jurídica geral de liberdade do cidadão só pode ser limitada pelo Poder Público quando for imprescindível para proteção de relevantes bens jurídicos.

Em face dos expostos riscos criados pelo uso do processamento eletrônico de dados, argumenta o TCF, deve-se, *mais do antes*, tomar precauções

individual liberty. As said before, the right to informational self-determination is not only granted for the sake of the individual, but also in the interest of the public, to guarantee a free and democratic communication order. Therefore, it is primarily possible to justify interferences in the right to informational self-determination if a consideration of both principles shows that the public interest outweighs the legitimate interests of the individual. However, the basic idea is always the same: the data subject is to maintain control of his/her own data).

⁷³ BVerGE 65, 1, tradução de MARTINS, 2005, p. 238.

⁷⁴ BVerGE 65, 1, tradução de MARTINS, 2005, p. 239.

organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade⁷⁵.

Em que medida o direito de autodeterminação sobre a informação conjuntamente com o princípio da proporcionalidade e com o dever de criar medidas processuais de proteção, vão exigir do legislador com fundamento constitucional a regulamentação vai depender do tipo, do alcance e dos usos possíveis dos dados pesquisados, assim como do perigo de seu abuso [...]. O interesse comum preponderante existira geralmente apenas nos dados com significado social, excluindo-se informações íntimas inexigíveis e autoacusações (grifo nosso)⁷⁶.

Se forem consideradas necessárias intervenções em seus direitos, os cidadãos devem ser colocados em uma posição onde eles podem avaliar a riscos para a sua personalidade e que estejam relacionadas com um processamento dos seus dados pessoais. Assim, o alcance, a intensidade e os efeitos de processamento de dados devem ser transparentes.

Consequentemente, o *Bundesverfassungsgericht* considera terem intervenções secretas um impacto ainda maior sobre a autodeterminação informativa. Uma vez que ninguém pode absolutamente excluir a possibilidade de ser alvo de um ato secreto para obtenção de dados, o efeito intimidador de tais medidas é muito superior, o que, por sua vez, leva a um forte efeito negativo sobre a ordem de comunicação democrática como um todo. Portanto, os requisitos constitucionais para intervenções secretas são muito mais rigorosos (tradução livre)⁷⁷.

Outra questão para a qual o *Bundesverfassungsgericht* atenta são os perfis de personalidade. Dentro de um *profil* os dados são ligados intencionalmente a fim de se reunir informações adicionais, além das originais, obtidas a partir do cruzamento de dados disponíveis. Isso traz substanciais riscos para o indivíduo, pois através da combinação de informações aparentemente inofensivas podem-se gerar dados novos ou mesmo dados sensíveis.

Isso pode representar uma ameaça ao direito do indivíduo à autodeterminação informativa, o qual coloca o indivíduo em uma posição para, a princípio, decidir por si mesmo, se informação pessoal deva ser divulgada em seu ambiente social. Mesmo antes da *Volkszählungsurteil*, o *Bundesverfassungsgericht* decidiu que “se estaria a contradizer a garantia constitucional da dignidade da pessoa humana se o governo reivindicasse o direito de obrigatoriamente registrar e catalogar completamente a personalidade de um indivíduo, mesmo com a ferramenta do anonimato

⁷⁵ BVerGE 65, 1, tradução de MARTINS, 2005, p. 239.

⁷⁶ BVerGE 65, 1, tradução de MARTINS, 2005, p. 240.

⁷⁷ Cf. HORNUNIG e SCHNABEL, 2009, p. 86, no original: *Consequently, the Bundesverfassungsgericht considers secret interventions to have an even bigger impact on informational self-determination. Since nobody can absolutely rule out the possibility that he/she has been subject to a secret act of data collection, the intimidating effect of such measures is much higher, which in turn leads to a strong negative effect on the democratic communication order as a whole. Therefore, the constitutional requirements for secret interventions are much stricter.*

fornecida por um censo estatístico, uma vez que o indivíduo seria tratado como um objeto acessível para um inventário em todos os sentidos (tradução livre)⁷⁸.

O TCF, na *Volkszählungsurteil*, fundou também a ideia de separação de poderes informacional. O tribunal decidiu que o Estado não deveria ser considerado como uma entidade única na medida em que obtenha e manipule dados pessoais. Devido aos princípios como finalidade e proporcionalidade, o fim para a qual os dados são processados deve ser especificado no momento de coleta e nunca deve haver mais dados coletados do que o absolutamente necessário para atingir o desiderato especificado. Dado que a finalidade é definida pela competência específica da respectiva entidade pública, deve haver medidas organizacionais nos processos correspondentes [que garantam a não-comunicação de dados entre as entidades públicas]. **Isso leva à conclusão de que o Estado como um todo não pode ser considerado como um processador de dados.** Em vez disso, tem de haver uma **separação de poderes informacional, o que significa ser Estado composto por diversas entidades consideradas processadores de dados individualmente.** Qualquer transferência de dados de uma entidade estatal para outra é, portanto, um ato de processamento de dados que deve ser baseado em uma disposição legal que atende os altos padrões de clareza e certeza (grifo nosso)⁷⁹.

⁷⁸ Cf. HORNUNIG e SCHNABEL, 2009, p. 87, no original: *“This may pose a threat to the individual’s right to informational self-determination, which is supposed to put the individual in the position to, in principle, decide for him/herself which personal information is to be disclosed in his/her social environment. Even before the population census decision, the Bundesverfassungsgericht ruled that: “It would be contradicting the constitutional guarantee of human dignity for the government to claim the right to compulsorily register and index an individual’s complete personality even in the anonymity provided by a statistical census, since the individual would be treated as an object accessible to an inventory in every way”.*

⁷⁹ Cf. HORNUNIG e SCHNABEL, 2009, p. 87, no original: *“Another ‘invention’ the Bundesverfassungsgericht made in the population census decision was the concept of informational separation of powers. The court decided that the state was not to be considered as a single entity as far as the collection and the use of personal data is concerned the principles of purpose specification and proportionality, the purpose for which data is processed must be specified at the time of collection and there must never be more data collected than absolutely necessary for achieving the specified purpose. As the purpose is defined by the specific competence of the respective public authority, organisational measures must be in place to separate the corresponding processes. This leads to the conclusion that the state as a whole cannot be considered as one data processor. Rather there has to be an informational separation of powers, which means that the state consists of different entities which are all considered to be single data processors. Any data transfer from one state entity to another is thus an act of data processing which must be based on a legal provision which meets the high standards of clarity and certainty”.*

Essa paradigmática decisão adotou uma série de princípios de proteção de dados que agora podem ser considerados os princípios-chave da proteção de dados na Europa, uma vez que presentes na Diretiva de Proteção de Dados de 95/46/EC. Isto também inclui, ao lado do princípio da minimização dos dados, obrigações do *data controller* e os direitos do atingido, bem como os princípios da especificação da finalidade e da proporcionalidade.

Com base nas ideias de especificação da finalidade e proporcionalidade, o *Bundesverfassungsgericht* desenvolveu uma extensa proibição de retenção de dados. De acordo com o tribunal, a coleta de dados não-anônimos para propósitos não específicos ou fins a serem especificadas posteriormente seria uma violação a esses princípios. Uma exceção só pode ser feita por dados anônimos que são coletados por meio de estatísticas, uma vez que se encontra na natureza da estatística, para a qual nem todos os fins destino dos dados podem ser conhecidos no momento da obtenção⁸⁰.

Se se pudesse buscar resumir quais foram, dentre tantas, as principais contribuições da *Volkszählungsurteil* para o regime de proteção de dados, dir-se-ia ter-se dado caráter constitucional à matéria. A partir daí que somente por leis e obedecendo-se o princípio da proporcionalidade (*Verhältnismässigkeitsprinzip*). Uma das consequências práticas dessa decisão foi o fato de várias legislações precisarem passar por uma readequação constitucional (uma das quais a BDSG) para que se aprimorassem suas estruturas no que concerne à proteção de dados.

A validação de regras para se adequarem aos preceitos da proteção de dados pessoais para a ser uma etapa importante do processo legislativo. Igualmente as interpretações de textos legislativos devem ser *datenschutzfreundlich*⁸¹.

Para o presente trabalho, importante salientar o mandamento ao legislador de produzir/atualizar normas de organização e procedimentais para evitar-se o dano à autodeterminação informativa.

⁸⁰ Cf. HORNUNIG e SCHNABEL, 2009, p. 87.

⁸¹ Conceito à semelhança de dataprotectionfriendly.

2.3. A BUNDESDATENSCHUTZGESETZ – BDSG

Uma codificação do direito à proteção de dados, ou seja, uma lei que abranja essa matéria em todas as áreas, em todas as particularidades de maneira completa e definitiva *não é realizável*, pois a proteção de dados é matéria transversa que influencia um grande número de áreas jurídicas com particularidades diversas umas das outras. E esse também é o motivo pelo qual o direito à proteção de dados não pertença especificamente a qualquer dos tradicionais ramos do direito⁸².

A BDSG, embora regule de maneira ampla a proteção de dados pessoais, deixa espaço para leis específicas que melhor possam regular as matérias que lhes são próprias, em relação às quais tem aplicação subsidiária.

Outra decorrência da abrangência da proteção legal da BDSG é a utilização de conceitos jurídicos indeterminados e cláusulas gerais. Generalização e abstração normativa afiguram-se necessárias em uma sociedade dinâmica, na medida em que uma legislação não é capaz de descrever de maneira precisa todos os acontecimentos da sociedade⁸³.

A BDSG apresenta-se como sistema de segurança de proteção de dados, cuja finalidade é realizar o dever estatal de tutela. O princípio da vinculação à finalidade prescreve que o processamento de dados deve basear-se em um determinado propósito previamente definido. Qualquer outro uso dos dados depende do consentimento previamente voluntário do interessado.

A finalidade *da Bundesdatenschutzgesetz* é, de acordo com seu parágrafo primeiro, a “proteção do indivíduo contra prejuízos que possa sofrer no seu direito de personalidade, através do tratamento de seus dados pessoais”.

Outro princípio importante previsto na lei é o do evitamento e economia de dados, previsto no § 3⁸⁴:

A configuração e a seleção do sistema de processamento de dados têm por objetivo evitar o levantamento, processamento ou utilização de dados pessoais ou fazê-lo o mínimo possível. Especialmente, utilizando-se, tanto quanto possível, da possibilidade de anonimização e pseudonimização, desde que isso seja possível e que o esforço seja proporcional à finalidade protetiva.

⁸² Cf. AUERNHAMMER, 1993, p. 18.

⁸³ Cf. AUERNHAMMER, 1993, p. 20.

⁸⁴ Tomou-se a tradução de

O § 4 destaca o papel do consentimento e o dever de notificação, que encerra a ideia de transparência e descreve a exigência de que cada parte interessada deva saber quais os dados coletados. *In verbis*:

O consentimento é eficaz apenas quando se baseia na livre decisão do atingido. Este deve ser informado sobre a finalidade prevista para o levantamento, processamento ou utilização dos dados, tanto quanto sobre as conseqüências da recusa de seu consentimento, e desde que as circunstâncias do caso o exijam ou requeiram. O consentimento necessita da forma escrita, se outra forma especial não for apropriada em razão de circunstâncias específicas. Se o consentimento escrito necessitar ser dado junto com outros esclarecimentos, isso deverá ser especialmente salientado.

Os procedimentos automatizados de processamento de dados devem ser notificados, antes de sua implementação pelas entidades não públicas responsáveis, à repartição fiscalizadora competente, bem como, pelas entidades públicas da federação e pelas empresas dos Correios e de Telecomunicações, ao Delegado Federal de proteção de dados, conforme o disposto no §4.

Aos encarregados da proteção de dados pessoais, cuja missão é tornar efetiva a observância da BDSG, cabe, entre outros, de acordo com o § 4 g:

1. fiscalizar a aplicação do programa de processamento de dados regulamentado, com auxílio do qual os dados pessoais devem ser processados; com esta finalidade ele deve ser instruído oportunamente sobre projetos de processamento automatizado de dados pessoais.
2. informar aos encarregados do processamento de dados pessoais, através de medidas apropriadas, das disposições desta lei e de outros regulamentos sobre proteção de dados, com suas respectivas exigências especiais sobre proteção de dados.

Há também a previsão de que entidades públicas e não públicas que, por si ou por delegação, levantam, processam ou utilizam dados pessoais devam “adotar medidas técnicas e organizacionais necessárias para garantir a observância dos ditames desta lei” (§ 9), assim como a realização de *auditorias de proteção de dados*, a partir da qual “os provedores dos sistemas de programa e processamento de dados e as entidades responsáveis podem apresentar suas estratégias de proteção de dados, bem como sua configuração técnica para serem examinadas e avaliadas por peritos independentes e competentes” (§ 9 a).

Se houver prejuízo ao interessado quando, sem permissão ou incorretamente, no levantamento, processamento ou utilização de seus dados pessoais, a entidade, ou seus dirigentes, estarão obrigados a indenizar o atingido (§ 7).

O § 6 prevê um rol de direitos irrenunciáveis do atingido, que não podem ser restringidos através de negócio jurídico, como o direito à informação, retificação, apagamento ou bloqueio de dados.

3 PROTEÇÃO DOS DADOS PESSOAIS E DIREITO A AUTODETERMINAÇÃO INFORMATIVA NO DIREITO BRASILEIRO

3.1 PANORAMA GERAL

Embora a guarida à intimidade e à privacidade esteja prevista na Constituição Federal⁸⁵, no Código Civil (CC), na Lei de Acesso à Informação (Lei nº 12.527/11) e no Código de Defesa do Consumidor (CDC), a *proteção de dados pessoais* no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário.

Em nível constitucional não há menção específica à proteção de dados pessoais. Além do *habeas data*⁸⁶, a Constituição brasileira abarca o problema da informação através das garantias à liberdade de expressão e do direito à informação, que devem ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade⁸⁷, *v. g.*

[...] assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano moral, material ou à imagem, (inciso V); inviolável a liberdade de consciência e de crença [...], (inciso VI); livre a expressão da atividade intelectual, artística, científica e de comunicação, independente de censura ou licença, (inciso IX); inviolável a intimidade, a vida privada, a honra e a imagem das pessoas, assegurada a indenização pelo dano material ou moral decorrente de sua violação, (inciso X); inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas [...], (inciso XII); assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional (inciso XIV); direito de todos receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral [...], (inciso XXXIII).

A Constituição declara invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. Portanto, erigiu tais valores humanos à condição de direito individual, mas não o fez constar no caput do artigo. Por isso, considera-o um direito conexo ao da vida. Assim, ele figura no caput como reflexo ou manifestação deste⁸⁸.

O Código Civil assevera em seu art. 21: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências

⁸⁵ Não é recente a tutela constitucional da privacidade e intimidade: já previa o inciso VII do art. 118 da Constituição Política do Império do Brasil de 1824: Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar.

⁸⁶ Vide a próxima sessão (3.2.1)

⁸⁷ Cf. DONEDA, 2006, p. 323.

⁸⁸ Cf. SILVA, 2008, p. 205.

necessárias para impedir ou fazer cessar ato contrário a esta norma”. Tal regra tem efeitos sobre a proteção de dados, ainda que indiretos, por permitir ao juiz adotar medidas que coíbam ou ao menos inibam aqueles que, sem justificativa legal, visem a adentrar na esfera privada do cidadão. A inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas, que também possui previsão constitucional, foi regulada pela Lei Federal nº 9.296/96 que, em seu Art. 1º, parágrafo único, afirma que a proteção dada aos sistemas de telefonia também se aplica à interceptação de fluxo de comunicações em sistemas de informática e telemática⁸⁹.

A referida proteção também poderá ser garantida pelo Projeto de Lei nº 2.126/2011, o qual estipulará que tais dados somente podem ser fornecidos mediante ordem judicial⁹⁰.

O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos:

I – à inviolabilidade da intimidade e da vida privada, assegurado o direito à sua proteção e à indenização pelo dano material ou moral decorrente de sua violação;

II – à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

O art. 37 do Projeto de Lei nº 4.906/01⁹¹ estabelece: “o provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas”. O provedor de Internet, deste modo, não produz e não exerce qualquer controle ou juízo de valor sobre mensagens e conteúdos transmitidos entre um remetente e um destinatário. A eventual responsabilidade sobre o conteúdo transmitido é, portanto, do usuário que utilizou a infraestrutura de provimento de acesso à Internet, cuja identificação poderá ser requerida mediante ordem judicial, devido ao direito fundamental à privacidade e ao sigilo das comunicações⁹².

O art. 5º da CF, em seu inciso XXXIII, prescreve: “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do

⁸⁹ Cf. LIMA; MONTEIRO, 2013.

⁹⁰ O referido projeto de lei é conhecido como “Marco Civil na Internet”.

⁹¹ Tal Projeto de Lei reuniu os Projetos de Lei nº 1.483/99 e 1.589/99.

⁹² Cf. LIMA; MONTEIRO, 2013.

Estado”. À Lei Federal nº 12.527/11 cabe regulamentar tal inciso ao estabelecer procedimentos específicos para o cidadão requisitar dados que estejam em posse da Administração Pública, além de classificar os documentos do Estado em níveis diferentes de sigilo⁹³.

A obrigação de sigilo para os agentes do fisco (art. 178 do Código Tributário Nacional), o segredo de justiça, nos casos previstos no art. 155 do Código de Processo Civil, os tipos penais que tutelam a privacidade através da inviolabilidade de domicílio e correspondência (arts. 170 a 174), bem como leis setoriais como a Lei de Imprensa (Lei 5250/67) também tocam o tema proteção de dados.

A jurisprudência, merecedora de breve menção pela pouca profundidade com que aborda a matéria de proteção de dados pessoais, concentra-se basicamente em definir indenizações pecuniárias em face da violação à privacidade. Exceção à regra é jurisprudência firme do Tribunal Superior do Trabalho no sentido de coibir o estabelecimento de listas negras de trabalhadores, expondo assim dados sensíveis, que requerem especial proteção dado seu uso potencialmente discriminatório⁹⁴.

Dar-se-á maior atenção ao *habeas data* e ao Código de Defesa do Consumidor por serem, dos institutos disponíveis no ordenamento jurídico pátrio, aqueles que mais se aproximam da realização do direito a autodeterminação informativa.

⁹³ Cf. LIMA; MONTEIRO, 2013.

⁹⁴ **RECURSO DE REVISTA. DANO MORAL. -LISTAS NEGRAS-. OFENSA AO PRINCÍPIO QUE PROTEGE A DIGNIDADE DA PESSOA HUMANA (ARTIGO 1º, INCISO III, DA CONSTITUIÇÃO FEDERAL). PROVIMENTO.** A inclusão dos nomes de Empregados nas chamadas -listas negras-, por si só enseja o pagamento de indenização por dano moral, tendo em vista que a prática constitui ofensa ao princípio constitucional que protege a dignidade da pessoa humana (art. 1º inciso III, Constituição Federal), ainda que não haja comprovação no sentido de ter o Autor sofrido prejuízo concreto, no que se refere à conquista de nova colocação no mercado de trabalho. Recurso conhecido e provido para que sejam restabelecidos os comandos da sentença quanto ao deferimento da indenização por dano moral requerida (Processo RR-532/2003-091-09-00.0, Relatora Ministra Maria de Assis Calsing, 4 Turma, Data de Publicação: DJ 18/04/2008).

3.2 O HABEAS DATA

A finalidade precípua dos direitos fundamentais é conferir aos indivíduos uma posição jurídica de direito subjetivo, para limitar a atuação de órgãos do Estado (*Abwehrrecht gegen staatliche Angriffe*). Essa dimensão clássica, de *status* negativo, cujo conteúdo normativo se refere ao direito do titular de resistir à intervenção estatal, oferece ao titular a faculdade jurídica de resistência contra intervenção estatal.

A autodeterminação informativa, enquanto direito fundamental, abrange decidir sobre si próprio em princípio, quando e dentro de que limites fatos pessoais serão revelados. Diante disso, pergunta-se: se um cidadão brasileiro tem, no âmbito informacional, seu espaço de autonomia violado, de qual instrumento jurídico ele dispõe para limitar a atuação estatal e, por conseguinte, concretizar o direito a autodeterminação informativa em sua dimensão negativa?

O principal meio para a realização da dimensão negativa do direito a autodeterminação informativa no direito brasileiro é o *habeas data* (art. 5, LXII), remédio constitucional que tem como objetivo proteger a esfera íntima dos indivíduos contra: a) uso abusivo de registros de dados pessoais coletados por meios fraudulentos, ilegais ou ilícitos; b) introdução nesses registros de dados sensíveis (assim chamados os de ordem racial, opinião política e filosófica ou religiosa, filiação partidária ou sindical, orientação sexual, etc.); c) conservação de dados falsos ou com fins diversos dos autorizados em lei⁹⁵.

A Constituição de 1988 não traz um dispositivo autônomo que contemple o direito de reconhecer e de retificar dados pessoais, mas prevê sua garantia, outorgada no mesmo dispositivo que institui o remédio de sua tutela, *in verbis*:

Conceder-se-á *habeas data*:

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou bancos de dados de entidades governamentais ou de caráter público;
- b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (inciso LXXII do art. 5 da CF 88).

Dentro da expressão *entidades governamentais*, há de se compreender órgãos da administração direta e indireta.

⁹⁵ Cf. SILVA, 2008, p. 453.

Logo, a expressão “entidades de caráter público” não pode referir-se apenas a organismos públicos, mas a instituições, entidades e pessoas jurídicas de direito privado que prestem serviços públicos, envolvendo-se aí não apenas os concessionários, permissionários ou exercentes de atividades autorizadas, mas também agentes de controle e proteção de situações sociais e coletivas, como as instituições de cadastramento de dados pessoais para controle ou proteção de crédito ou divulgadores profissionais de dados pessoais, como as firmas de assessoria e fornecimento de malas-direta⁹⁶.

O processo do *habeas data* pode desenvolver-se em duas fases. Na primeira, o Juiz, de plano, manda notificar o impetrado para apresentar os dados do impetrante, constantes de seu registro, no prazo que estipule; juntados os dados, o impetrante terá ciência deles, devendo-se manifestar em um prazo determinado. Se nada tiver a retificar, di-lo-á e se arquivará o processo. Se tiver retificação a fazer, dirá quais são, fundamentadamente, mediante aditamento à inicial, e então o Juiz determinará a citação do impetrado para a contestação, se quiser, prosseguindo-se nos termos do contraditório⁹⁷.

A Lei 9507/97 prescreve o rito processual do *habeas data*, o qual pressupõe uma fase administrativa anterior iniciada com um requerimento do interessado à entidade depositária do registro ou banco de dados, que poderá ser deferido ou indeferido no prazo de 48 horas.

Se deferido o requerimento, o depositário do registro ou banco de dados marcará dia e hora para que o requerente tome conhecimento das informações. Constatada inexatidão de qualquer dado a seu respeito, o interessado, em petição acompanhada de documentos comprobatórios, poderá requerer sua retificação, que deverá ser feita, no máximo, no prazo de dez dias. Indeferido o acesso às informações, ou verificado o transcurso do prazo de mais de dez dias sem decisão, ou ainda se recusadas as anotações das explicações ou contestação apresentadas pelo requerente, então, sim, poderá ele recorrer ao poder judiciário, mediante petição na forma dos artigos 282 e 285 do Código de processo Civil, pleiteando a concessão de *habeas data* que lhe assegure acesso às informações, às retificações solicitadas, bem como às anotações pleiteadas. Ao despachar a inicial, o juiz ordenará que se notifique o coator do conteúdo da petição, entregando-lhe segunda via apresentada pelo impetrante, com a cópia dos documentos, a fim de que, no prazo de dez dias, preste as informações que julgar necessárias. Feita a notificação, o serventuário em cujo cartório corra o feito, juntará aos autos cópia autêntica do ofício endereçado ao coator, bem como prova de sua entrega a este ou da recusa, que seja de recebê-lo, seja de dar recibo. Se o juiz julgar procedente o pedido, marcará data e hora para que o coator apresente: a) ao impetrante as informações a seu respeito, constante de registro e bancos de dados; b) em juízo a prova de retificação ou da anotação feita nos assentamentos do impetrante. Da sentença cabe apelação, que só terá efeito devolutivo. O pedido de *habeas*

⁹⁶ Cf. SILVA, 2088, p. 455.

⁹⁷ Cf. SILVA, 2008, p. 455.

data poderá ser renovado se a decisão denegatória não lhe houver apreciado o mérito⁹⁸.

Descrito o rito do *habeas data*, depara-se o cidadão brasileiro, no atual estado da tecnologia da informação, com o desafio de saber *quem detém seus dados pessoais*, com que objetivos, para, nesse caso, impetrar um *habeas data*. Sem saber quem possui acesso aos seus dados pessoais, não há como impetrá-lo. Igualmente, sem poder acessar as informações, por não se saber onde elas estão, como então poder retificá-las? Nesse caso a dimensão subjetiva do direito a autodeterminação torna-se obsoleta, ou, ao menos, ineficiente, com o instituto do *habeas data*.

⁹⁸ Cf. SILVA, 2008, p. 457.

3.3. O CÓDIGO DE DEFESA DO CONSUMIDOR

O ordenamento jurídico pátrio não possui uma legislação específica sobre proteção de dados pessoais. Isso não significa que a dimensão objetiva - cuja percepção independe de seus titulares, e que estatui previsões legislativas de modo a antecipar a violação do direito, no caso, a autodeterminação informativa – esteja em todo negligenciada pelo direito brasileiro.

O Código de Defesa do Consumidor, embora seja legislação setorial, impõe um conjunto de regras e princípios aos detentores de bancos de dados, cujo resultado é prevenir, dentro de seus limites (no âmbito da relação de consumo), danos à esfera privada dos consumidores, atuando assim, na legislação pátria, como principal instrumento de tutela da dimensão objetiva do direito a autodeterminação informativa.

A Seção VI do CDC trata especificamente sobre bancos de dados e cadastro de consumidores, em seus artigos 43 e 44, *in verbis*:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º 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.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º 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.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.

§ 1º É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.

§ 2º Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.

Para que os bancos de dados sejam considerados legítimos, à luz dessas normas, devem atender a certos requisitos. Há um *dever de comunicação prévia* ao

consumidor e, no caso de dados sensíveis, de obtenção da *anuência expressa* para a abertura do cadastro. Esse dever de comunicação se aplica ao organizador do banco de dados e ao fornecedor que deu origem à informação, pois ambos, em razão desta omissão, são responsáveis solidários por danos causados ao consumidor.

Os bancos de dados têm, igualmente, o *dever de garantir ao consumidor o acesso aos seus dados*, ao assegurar ao consumidor o direito de acesso irrestrito, imediato e gratuito às informações a seu respeito que se encontrem armazenadas, bem como às fontes do registro e à identificação dos destinatários das informações. A entidade arquivista tem, além disso, o *dever de manter apenas informações corretas, claras e atuais e o direito do consumidor à retificação de dados*; exige-se, ademais, *um acesso restrito dos arquivos de consumo a terceiros*; Destaca-se também o *prazo de permanência de informações negativas sobre o consumidor nos arquivos de consumo*. Quanto à responsabilidade, é objetiva e solidária, não podendo ser atenuada por instrumento contratual dada a sua natureza cogente e indisponível⁹⁹.

O princípio da finalidade pode depreendido através da aplicação da cláusula geral de boa-fé objetiva e da garantia constitucional de privacidade, a fim de que os dados sobre o consumidor sejam utilizados para os fins ensejadores de sua obtenção, sem desvirtuamento, o que pode servir como fundamentação para a coleta de dados sensíveis e da comercialização de bancos de dados de consumidores¹⁰⁰.

Ademais, a Portaria número 05 de 2002 do Ministério da Justiça alargou o rol de cláusulas abusivas do Art. 51 do CDC, ao considerar:

Art. 1º [...] abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que:

I – autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia;

II – imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor;

III – autorize o fornecedor a investigar a vida privada do consumidor.

É importante frisar o inciso III desta Portaria, que considera cláusula abusiva aquela que autoriza ao fornecedor a investigar a vida privada do consumidor. Esta

⁹⁹ Cf. DA CUNHA E CRUZ, 2007.

¹⁰⁰ Cf. DOENDA, 2006, p. 339.

orientação é frequentemente desrespeitada, em especial quando se utilizam meios eletrônicos, pois a coleta de dados e a transferência destes para terceiros é quase uníssona, mesmo que explicitada nos “termos de uso” dos serviços (quando existentes)¹⁰¹.

Impende frisar que o art. 43, § 4º, do CDC considera os bancos de dados de consumidores algo de caráter público. Desta forma, em uma interpretação integrativa da lei, o acesso aos bancos de dados de registros pessoais das relações de consumo é igualmente assegurado por meio de *habeas data*¹⁰².

O CDC prevê, ainda, em seus artigos 73 e 74, sanções para aqueles que dificultem o acesso ou retificação constantes em cadastros, registros ou bancos de dados. *In verbis*:

Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena Detenção de seis meses a um ano ou multa.

Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena Detenção de um a seis meses ou multa.

Embora seja questionável a efetividade da pena de detenção para os agentes que impeçam, dificultem ou mesmo deixem de corrigir imediatamente informações do consumidor constantes em cadastros – tal debate não pertence aos objetivos deste trabalho -, uma tal norma visa a inibir que os administradores de bancos de dados e registros violem os princípios do mínimo informacional e transparência.

¹⁰¹ Cf. LIMA; MONTEIRO, 2013.

¹⁰² Cf. LIMA; MONTEIRO, 2013.

4 DESAFIOS À TUTELA DO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO BRASIL

4.1. UMA CRÍTICA AOS PRINCIPAIS INSTITUTOS DISPONÍVEIS PARA PROTEÇÃO DE DADOS E CONCRETIZAÇÃO DO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO DIREITO BRASILEIRO

A falta de um diploma legal que aborde de maneira ampla e sistemática a proteção de dados pessoais, como visto, enseja a necessidade de um arranjo dogmático que dê extensividade a normas materiais, como o Código de Defesa do Consumidor - o qual toma como públicos bancos de dados de instituições creditícias, por exemplo - ou instrumentais, como o *habeas data*, os quais tocam de maneira refratária a proteção de dados pessoais, para que haja um “agasalho mínimo” ao tema na legislação pátria.

Sobre o *habeas data* brasileiro, embora seja *sui generis* e pioneiro no continente sul-americano, inspirado, “na esteira da inovação do constituinte brasileiro para superar o período ditatorial antecedente à democracia no Brasil”¹⁰³, falhou ao basear-se na suposição de que a natureza dos interesses em questão pudesse ser conjugada pelo binômio *acesso/retificação*.

No atual estágio do desenvolvimento econômico e tecnológico, é muito difícil precisar qual o agente que detém dados pessoais. Pode ser uma agência governamental de espionagem, um órgão de fiscalização tributária, ambos a nível público, ou mesmo empresas cujo *core business* é vender informações obtidas e armazenadas em grandes bancos de dados. Ou seja, se em primeiro momento a principal preocupação do legislador de proteção de dados, na década de setenta, era voltar-se contra grandes bancos de dados públicos e em um segundo momento contra os bancos de dados pulverizados em diversas instancias¹⁰⁴, hoje há grandes bancos de dados pulverizados, tanto em nível nacional quanto internacional. Portanto, é necessário superar a abordagem *acesso-retificação*.

¹⁰³ Cf. DONEDA, 2006, p. 355.

¹⁰⁴ Remete-se ao capítulo II deste trabalho.

Vencer os impasses e indefinições que circundam a proteção de dados pessoais no Brasil passa necessariamente pela redefinição do papel do *habeas data*, que poderia seguir dois caminhos para atingir tal objetivo: o primeiro seria pluralizar a ação de *habeas data*, fazendo-a atender, em cada uma de suas vertentes, a fins determinados pelos vários procedimentos necessários em um sistema moderno de proteção de dados pessoais; a segunda consistiria em relegar ao *habeas data* uma função instrumental, que atenderia basicamente ao direito de acesso e retificação, um instrumento entre outros em um sistema integrado de proteção de dados pessoais a ser necessariamente estruturado para além desta ação¹⁰⁵.

Na verdade, ambas as soluções têm em comum **a necessidade de uma maturação da disciplina de proteção de dados pessoais, a ser estruturada em torno dos princípios e deve contar com instrumentos que garantam sua eficácia – um dos quais pode ser o *habeas data***. A partir daí, a questão é saber se o *habeas data* ocupa uma função central nesse mecanismo, para o que ele deve ser pluralizado; ou se ocupa um espaço residual ente outros remédios, para que deve ser limitado (grifo nosso)¹⁰⁶.

O Código de Defesa do Consumidor, ao seu turno, embora seja a legislação que mais concretiza a dimensão positiva do direito à autodeterminação no ordenamento pátrio, é restrito, em regra, às relações de consumo. É, portanto, incapaz de regular, de maneira ampla e ordenada – inclusive por serem esparsos os dispositivos que abarcam proteção de dados pessoais – o conjunto das relações que perpassam o tema. Os demais diplomas legais, isoladamente, não criam um sistema unificado capaz de prevenir, de maneira eficiente, a obtenção, armazenamento e manipulação de dados.

Ao cabo dessa verificação, o caráter remedial do sistema de proteção de dados pessoais brasileiro é patente, e parece mais condizente com as concepções liberais que consideram a proteção de dados pessoais e a própria privacidade liberdades negativas. A normativa infraconstitucional não nos resulta compatível com a alçada de uma leitura constitucional dos interesses ligados à proteção de dados pessoais e que necessita de instrumentos adequados para atuação - se não por outro motivo, para proporcionar a efetiva atuação da Constituição no que tange à tutela da personalidade¹⁰⁷.

¹⁰⁵ Cf. DONEDA, 2006, p. 358.

¹⁰⁶ Cf. DONEDA, 2006, p. 359.

¹⁰⁷ Cf. DONEDA, 2006, pp. 358-359.

4.2 A NECESSIDADE DE LEGISLAÇÃO SOBRE A PROTEÇÃO DE DADOS NO BRASIL

Baseado na teoria geral dos direitos fundamentais, buscou-se no presente trabalho formular um conceito de autodeterminação informativa. Definiu-se direito a autodeterminação informativa como um direito público subjetivo depreendido de dispositivos constitucionais que guarnecem o livre desenvolvimento da personalidade e da dignidade humana e, portanto, encerram valores supremos dentro do Estado, tendo como finalidade limitar o exercício do poder estatal em face da liberdade individual de dispor sobre seus dados pessoais: 1) pela vedação à intromissão injustificada à esfera de privacidade dos cidadãos; 2) pela interpretação garantidora da autodeterminação informativa nas cláusulas gerais de normas infraconstitucionais; 3) por meio de uma legislação sobre dados pessoais que previna sua violação.

O dever estatal de tutela expresso na terceira proposição tem o desiderato de promover segurança, em uma atuação tipicamente preventiva, cuja vinculação valha tanto para entidades públicas quanto privadas.

O ordenamento jurídico brasileiro contempla a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental. Embora devesse corresponder a uma proteção integrada e dirigida pela tábua axiológica constitucional, atua de forma fracionada, em focos de atuação determinados – sejam estes a ação de *habeas data*, as previsões do Código de Defesa do Consumidor ou outras – que tendem a orientar-se mais pela lógica de seus específicos campos do que por uma estratégia baseada na tutela integral da personalidade através da proteção dos dados pessoais¹⁰⁸.

Isso não impede, contudo, que se aplique a inteligência desse conceito no ordenamento jurídico brasileiro – a partir de uma interpretação teleológica e sistemática da Constituição Federal pode-se, sim, enunciar um direito a autodeterminação informativa, que respalde as garantias de proteção de dados em face das crescentes ameaças que a manipulação de dados representa para os

¹⁰⁸ Cf. DONEDA 2006, pp. 27-28.

cidadãos brasileiros e que ameaçam fundamentos constitucionais como a democracia – da qual uma vontade autônoma livre de interferências é requisito.

Se se pode enunciar um direito a autodeterminação a partir dos valores fundamentais fixados na *carta de direitos* da ordem constitucional pátria, surge então para o Estado brasileiro o dever, por meio do seu poder Legislativo, produzir um corpo normativo capaz de resguardar a igualdade, liberdade e privacidade resultantes de uma adequada proteção de dados.

Em uma iniciativa conjunta do Ministério da Justiça e da Fundação Getúlio Vargas elaborou-se o anteprojeto da Lei Brasileira de Proteção de Dados Pessoais (ALBDP), que vem ao encontro da tese defendida neste trabalho: há uma premente necessidade de uma legislação sobre a proteção de dados, de modo a realizar a dimensão objetiva do direito fundamental à autodeterminação informativa enquanto dever estatal de tutela.

Mais do que isso, uma tal iniciativa estimula o debate sobre o tema da proteção de dados, que pode trazer como resultado o aperfeiçoamento tanto do anteprojeto em si como da própria consciência da dimensão ampla que a privacidade assumiu nos últimos anos.

Ademais, a aprovação de uma lei de proteção de dados fecundará a produção de literatura jurídica especializada sobre o tema e abrirá portas para um posicionamento jurisprudencial mais adequado à dinâmica da Era da Informação.

Nesse sentido, tem-se por acertado o enunciado do art. 1º, do Anteprojeto da Lei de Proteção de Dados pessoais ao prescrever que a “lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente **em relação à sua liberdade, igualdade e privacidade pessoal e familiar**, nos termos do art. 5º, incisos X e XII da Constituição Federal” (grifo nosso).

A essência da ALBDP está seu rol de princípios (art. 8), os quais norteiam, de maneira sistemática, os agentes que manipulem dados pessoais. *In verbis*:

I - **Princípio da finalidade**: a não utilização dos dados pessoais objeto de tratamento para finalidades distintas ou incompatíveis com aquelas que fundamentaram a sua coleta e que tenham sido informadas ao titular; bem como a limitação deste tratamento às finalidades determinadas, explícitas e legítimas do responsável;

II - **Princípio da necessidade**: a limitação da utilização de dados pessoais ao mínimo necessário, de forma a excluir o seu tratamento sempre que a finalidade que se procura atingir possa ser igualmente realizada com a utilização de dados anônimos ou com o recurso a meios que permitam a identificação do interessado somente em caso de necessidade;

III - **Princípio do livre acesso:** a possibilidade de consulta gratuita, pelo titular, de seus dados pessoais, bem como de suas modalidades de tratamento;

IV - **Princípio da proporcionalidade:** o tratamento de dados pessoais apenas nos casos em que houver relevância e pertinência em relação à finalidade para a qual foram coletados;

V - **Princípio da qualidade dos dados:** a exatidão dos dados pessoais objeto de tratamento, com atualização realizada segundo a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI - **Princípio da transparência:** a informação ao titular sobre a realização do tratamento de seus dados pessoais, com indicação da sua finalidade, categorias de dados tratados, período de conservação destes e demais informações relevantes;

VII - **Princípio da segurança física e lógica:** o uso, pelo responsável pelo tratamento de dados, de medidas técnicas e administrativas proporcionais **ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento**, constantemente atualizadas e aptas a proteger os dados pessoais sob sua responsabilidade da destruição, perda, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado;

VIII - **Princípio da boa-fé objetiva:** o respeito à lealdade e à boa-fé objetiva no tratamento de dados pessoais; e

IX - **Princípio da responsabilidade:** a reparação, nos termos da lei, dos danos causados aos titulares dos dados pessoais, sejam estes patrimoniais ou morais, individuais ou coletivos.

X – **Princípio da prevenção:** o dever do responsável de, para além das disposições específicas desta Lei, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (grifos nossos)¹⁰⁹.

¹⁰⁹ Disponível em: <http://www.acessoinformacao.gov.br/acessoinformacaogov/publicacoes/anteprojeto-lei-protECAo-dados-pessoais.pdf>. Acesso em 29/01/2014.

4.3. BREVES NOTAS PARA O DESENVOLVIMENTO DO DEBATE QUANTO AO DIREITO À AUTODETERMINAÇÃO INFORMATIVA NO BRASIL

I

O conceito de direito a autodeterminação informativa, da maneira como foi enunciado – como garantia de o cidadão poder decidir por si e em princípio sobre a exibição e uso de seus dados pessoais – deve estar ligado ao contexto argumentativo do *Volkszählungsurteil*, sob pena de tornar-se uma ferramenta meramente retórica na construção jurídica nacional. “Autodeterminar” informações pessoais é, como visto, apenas uma faceta deste direito: em sentido amplo, significa não ser determinado, não ser mero objeto (com dignidade, autonomia ou personalidade violados) no que toque às informações pessoais. Sem esse pano de fundo, o debate sobre o tema tende a ser superficializado.

II

Apesar da construção legal, jurídica e doutrinária avançadas sobre o tema na Alemanha, uma população parece ter desacreditado dos benefícios da proteção de dados pessoais¹¹⁰. Se se puder extrair uma lição deste fenômeno, que seja no sentido de o poder público estimular um amplo debate sobre o tema. Uma parcela substancial do sucesso de políticas de proteção de dados reside na autoproteção (*Selbstschutz*).

III

Concernente à necessidade de uma legislação que realize o dever de tutela do direito fundamental à autodeterminação informativa, parece salutar o esforço realizado no Anteprojeto da Lei Brasileira de Proteção de Dados Pessoais, o qual deve ser debatido à luz das legislações mais avançadas sobre o tema, como a alemã.

IV

Para estudos futuros, propõe-se uma análise comparativa entre a BDSG e o Anteprojeto da Lei de Proteção de Dados Pessoais: Quais as convergências e

¹¹⁰ Cf PETRI (2010) e WAGNER (2010).

divergências essenciais entre esses diplomas? Quais os impactos para o direito à autodeterminação informativa? Respostas a essas perguntas podem oferecer pontos de desenvolvimento para o debate.

V

Sugere-se, por fim, pesquisas sobre o direito fundamental à garantia de confiabilidade e integridade de sistemas de informação. Foi o único direito fundamental enunciado a partir da cláusula de personalidade (art.2 I GG) desde o direito à autodeterminação informativa e expõe algumas lacunas deste perante as mais recentes inovações tecnológicas.

CONCLUSÃO

O direito à autodeterminação informativa como **poder decidir sobre si próprio em princípio, quando e dentro de quais limites dados pessoais podem ser revelados** surge no *Volkszählungsurteil* enquanto resposta (jurídica) à demanda de mais de duas mil reclamações constitucionais perante o Tribunal Constitucional Federal alemão. Essa decisão traz como pano de fundo a extensão do debate sobre os limites do Estado. Há um arsenal de argumentos em prol da “eficiência” da Administração, combate à criminalidade organizada e ao terrorismo¹¹¹, que têm servido como justificção para desrespeito ao espaço para o livre desenvolvimento da personalidade garantido pelo direito a autodeterminação informativa.

No âmbito jurídico, o que resguarda essa verdadeira “autonomia *kantiana*”, de raiz constitucional (também essa conclusão vem da *Volkszählungsurteil*), são eficácias advindas das dimensões subjetiva e objetiva dos direitos fundamentais.

A discussão acadêmica sobre o direito a autodeterminação informativa possui relevo na medida em que surge um perigoso movimento de normalização (*Normalisierung*) na sociedade¹¹² quanto à aceitação de medidas que restrinjam a autodeterminação informativa, pois 1) há considerável incorporação do *discurso do terror* como fator de legitimação para uma “necessária” violação de direitos¹¹³; 2) uma subestimação dos potenciais danos à liberdade e privacidade em favor de determinadas comodidades fornecidas pelo desenvolvimento tecnológico¹¹⁴; 3) pela redução da expectativa de privacidade.

No âmbito jurídico, urge a superação do entendimento da privacidade apenas em sua dimensão subjetiva, baseada em um modelo liberal individualista incapaz de regular os complexos processos tecnológicos que transpassam a vida de um cidadão diariamente.

¹¹¹ Cf. TROJANOW; ZEH, 2009, p. 75.

¹¹² Cf. PETRI, 2010, p. 29.

¹¹³ Cf. TROJANOW; ZEH, 2009, p. 81, refere-se à expressão *Angst sells*: o “medo vende” – a população só aceita políticas restritivas de liberdade quando aceitam o discurso de que há “inimigos infiltrados na sociedade” a serem “capturados” para livrar a “parte boa sociedade” de seus elementos “ruins” – note que esse discurso é típico de regimes totalitários.

¹¹⁴ Cf. WAGNER, 2010, *Für eine kleine Gewinnchance bei Preisausschreiben [...] geben Hunderttausende ganz persönliche Daten von sich Preis*: por uma pequena chance de obter descontos, milhares fornecem seus dados bastante privados (tradução livre).

Tal como no direito à vida, é irreparável o dano causado pelo ataque injustificado à privacidade¹¹⁵, bem como a outros direitos da personalidade. A reatividade de um *habeas corpus*, por exemplo, é insuficiente para proteger o cidadão: como saber quem tem qual informação, obtida de que maneira sobre si? Quem não responde a essa pergunta, não consegue determinar por si mesmo um importante desdobramento de sua personalidade – ao contrário, é determinado por um perfil elaborado a partir de seus dados pessoais. “Soltos por aí”, eles determinam se um cidadão possuirá acesso a crédito, se ele obterá visto para algum país, etc.

Solução para concretizar o direito a autodeterminação informativa não pode passar, por conseguinte, apenas por sua dimensão subjetiva: é por via da dimensão objetiva, no dever de proteção (*Schutzpflicht*), em cujo cerne reside a produção de normas que regulem o tema e previnam a violação ao direito, bem como definam instrumentos para regular a proteção de dados.

O Brasil, diferentemente da Alemanha, ainda não possui uma legislação sobre o tema. Aliás, é o único país no Mercosul a não possuí-la. A codificação sobre o a problemática de proteção aos dados pessoais (*Datenschutzproblematik*) é, assim, urgente e necessária, motivo por que iniciativas como Anteprojeto da Lei de Proteção de Dados Pessoais podem trazer efeitos positivos uma vez que se estabelecerá, de maneira ampla e *a priori* – portanto, preventivamente – o *modus* da obtenção, manipulação e armazenamento de dados, resguardando assim as dimensões subjetiva e objetiva do direito a autodeterminação informativa.

¹¹⁵ Cf. MARTINS, 2001, p. 79: Es handelt sich um eine logische Analogie zum Schutz des Lebens. Denn einmal aufgegeben, ist ein Geheimnis für immer tot und alle sich darauf beziehenden Persönlichkeitsrechte sind gleichermaßen betroffen.

REFERÊNCIAS BIBLIOGRÁFICAS

Anteprojeto da Lei de Proteção de Dados Pessoais. Disponível em:

<<http://www.acessoinformacao.gov.br/acessoinformacaogov/publicacoes/anteproje-to-lei-protacao-dados-pessoais.pdf>>. Acessado em: 26/01/2014.

AUERNHAMMER, Herbert. *Bundesdatenschutzgesetz; Kommentar*. 3. Auflage. Köln; Berlin; Bonn; Munchen: Heymann, 1993.

BARRAL, Welber. *Metodologia da Pesquisa Jurídica*. 2 ed. Florianópolis: Editora Fundação Boiteux, 2003.

BIAGGIONI, Andréa. Tradução da Primeira Seção da Bundesdatenschutzgesetz conforme o Modelo Funcionalista de Christiane Nord. Dissertação de Mestrado. Universidade Federal de Santa Catarina, Florianópolis, 2010.

BOBBIO, Norberto. *Direito e Estado no Pensamento de Emanuel Kant*. 4. ed. Brasília: Editora Unb, 1997.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. *Dicionário de Política*. 5. ed. São Paulo: Imprensa Oficial, 2004.

BRASIL. Constituição (1824). *Constituição Política do Imperio do Brazil (de 25 de Março de 1824)*. Rio de Janeiro, 22 jan. 1824. Disponível em: <http://www.planalto.gov.br/Ccivil_03/Constituicao/Constituicao24.htm>. Acesso em: 15/01/2014.

BRASIL. Constituição da República Federativa do Brasil. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20/01/2014.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 12 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/8078.htm>. Acesso em: 25/01/2014.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 28/01/2014.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 20/01/2014.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 22/12/2013.

BROSSETE, Josef, Dr. iur. *Der Wert der Wahrheit im Schatten des Rechts auf informationelle Selbstbestimmung*. Berlin: Duncker und Humblot, 1991.

CARR, Nicholas G. *TI já não importa mais*. Harvard Business Review Brasil. 2003.
DA CUNHA E CRUZ, Marco Aurélio Rodrigues. *A disciplina normativa brasileira sobre a intimidade e os bancos de dados*. Araucaria, 2007.

DEUTSCHLAND. *Grundgesetz für die Bundesrepublik Deutschland vom 1949*. Disponível em: <http://www.bundestag.de/bundestag/aufgaben/rechtsgrundlagen/grundgesetz/>. Acesso em 25/01/2014.

DEUTSCHLAND. *Bundesdatenschutzgesetz*. Disponível em: http://www.gesetze-im-internet.de/bdsg_1990/. Acesso em 25/01/2014.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. *A tutela dos dados pessoais na internet: o direito a autodeterminação informativa*. 2011. Disponível em: <<http://www.egov.ufsc.br/portal/conteudo/tutela-dos-dados-pessoais-na-internet-o-direito-a-autodeterminação-informativa>>. Acesso em: 27 jan. 2014.

FOUCAULT, Michel. *Überwachen und Strafen: Die Geburt des Gefangnisses*. 8. ed. Frankfurt: Suhrkamp, 1989.

GARTH, Bryan; CAPELETTI, Mauro. *Acesso à Justiça*. Porto Alegre: Sergio Antonio Fabris, 1988.

GIESEN, Thomas. Das Grundrecht auf Datenverarbeitung. *JZ*, Dresden, n. 19, p.918-927, 2007.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro. Volume I, Parte Geral*. 5. Edição. São Paulo; Editora Saraiva, 2007.

GROSSMANN, Luís Oswaldo. *Espionagem prejudica liberdade e muda sociedade, diz Snowden*. 2014. Disponível em: <<http://convergenciadigital.uol.com.br/>>. Acesso em: 27 jan. 2014.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law And Security Review*, Kassel, n. 25, p.84-88, 2009.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law And Security Review*, Kassel, n. 25, p.115-122, 2009.

KAUFMANN, Arthur. *Filosofia do Direito*. Lisboa: Fundação Calouste Gulbekian, 2004.

KG, M. Klauenberg. *Bundesdatenschutzgesetz*. 1977. Disponível em: <<http://www.klauenberg.de/bundesdatenschutz.htm>>. Acesso em: 20 jan. 2014.

LIMA, Caio César Carvalho; MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. *AtoZ: novas práticas em informação e conhecimento*, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <<http://www.atoz.ufpr.br>>. Acesso em: 25/01/2014.

MARTINS, Leonardo. (org.) *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*. Montevideú: Fundação Konrad Adenauer, 2005.

MARTINS, Leonardo; DIMOULIS, Dimitri. *Teoria Geral dos Direitos Fundamentais*. 3. edição. São Paulo: Editora Revista dos Tribunais, 2011.

MARTINS, Leonardo. *Die Grundrechtskollision. Grundrechtskonkretisierung am Beispiel des 41 1 BDSG*. Berlim: Humboldt-Universität zu Berlin, 2001.

MENDES, Gilmar Ferreira. *Direitos Fundamentais e Controle de Constitucionalidade*. 3 edição. São Paulo: Editora Saraiva, 2007.

MEYERHOLT, Ulrich. Vom Recht auf informationelle Selbstbestimmung zum Zensus 2011. *Dud: Datenschutz und Datensicherheit*, Oldenburg, n. 10, p.683-686, 2011.

PAHLEN-BRANDT, Ingrid. Datenschut braucht scharfe Instrumente Beitrag zur Diskussion um „personenbezogene Daten“. *Dud: Datenschutz und Datensicherheit*. Berlin, n. 1, p.34-40, 2008.

PETRI, Thomas. Wertewandel im Datenschutz und die Grundrechte. *Dud: Datenschutz Und Sicherheit*, Munchen, n. 1, p.25-29, 2010.

PILATI, José Isaac. *Teoria e Prática do Direito Comparado*. Florianópolis: OAB/SC Editora., 2000.

ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: GUTWIRTH, S.. *Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*. Heilderberg: Springer, 2009. p. 45-76.

RUARO, Regina Linden; RODRIGUEZ, Daniel Pinero. *Nada a esconder? O direito à proteção de dados frente a medidas de segurança pública e intervenção estatal*. 2013. Disponível em: <<http://www.ambito-juridico.com.br/>>. Acesso em: 12 jan. 2014.

SCHAAR, Peter. Ein Datenschutzrecht für das 21. Jahrhundert. *Dud: Datenschutz Und Sicherheit*, Berlin, n. 8, p.518-518, 2010.

SCHEMITSCH, Markward. *Identitätsdaten als Persönlichkeitsgüter*. 2004. 194 f. Tese (Doutorado) - Curso de Rechts- Und Wirtschaftswissenschaften, Technische Universität, Darmstadt, 2004.

SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. 31 edição. São Paulo: Malheiros editores, 2008.

SOUZA, Victor Roberto Corrêa de. O acesso à informação na legislação brasileira. *Rev. SJRJ*, Rio de Janeiro, v. 19, n. 33, p.161-181, abr. 2012.

TRIBUNAL SUPERIOR DO TRABALHO. *RECURSO DE REVISTA. DANO MORAL. - LISTAS NEGRAS-. OFENSA AO PRINCÍPIO QUE PROTEGE A DIGNIDADE DA PESSOA HUMANA (ARTIGO 1º, INCISO III, DA CONSTITUIÇÃO FEDERAL). PROVIMENTO*. A inclusão dos nomes de Empregados nas chamadas -listas negras-, por si só enseja o pagamento de indenização por dano moral, tendo em vista que a prática constitui ofensa ao princípio constitucional que protege a dignidade da pessoa humana (art. 1 inciso III, Constituição Federal), ainda que não haja comprovação no sentido de ter o Autor sofrido prejuízo concreto, no que se refere à conquista de nova colocação no mercado de trabalho . Recurso conhecido e provido para que sejam restabelecidos os comandos da sentença quanto ao deferimento da indenização por dano moral requerida. Processo RR-532/2003-091-09-00.0, Relatora Ministra Maria de Assis Calsing, 4 Turma, Data de Publicação: DJ 18/04/2008.

TROJANOW, Ilija; ZEH, Juli. *Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte*. 2. Auflage. München: Deutscher Taschenbuchverlag, 2011.

UNIÃO EUROPÉIA. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal*, Luxemburgo, L 281, 23 Nov. 1995, p. 0031 – 0050. Disponível em: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>>. Acesso em: 19/01/2014.

WAGNER, Edgar. Datenschutz bei Kundenkarten. *DuD: Datenschutz und Datensicherheit*, Mainz, p.30-33, 2010.

WEICHERT, Thilo. Cloud Computing und Datenschutz. *Dud: Datenschutz Und Sicherheit*, Kiel, n. 10, p.679-687, 2010.