# A LUTA CONTRA O TERRORISMO E A PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE CRÍTICA DE UM PRECEDENTE DO TRIBUNAL CONSTITUCIONAL ALEMÃO (*BUNDESVERFASSUNGSGERICHT*)

CHRISTIAN FRAU OBRADOR CHAVES*

RESUMO: Este artigo busca, com fundamento no princípio da proporcionalidade, que constitui um dos pilares do Estado Democrático de Direito, realizar uma análise crítica de precedente do Tribunal Constitucional Alemão que declarou inconstitucional lei de transposição da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho que dispõe, em seu art. 6º, sobre a retenção de dados pessoais, por período não inferior a 6 (seis) meses e não superior a 2 (dois) anos, no máximo, a contar da data da comunicação. A legislação, em vigor desde 2008 e julgada inconstitucional, em março de 2010, foi implementada com a justificativa de que a informação armazenada poderia ajudar a identificar organizações criminosas e terroristas.
PALAVRAS-CHAVE: Terrorismo; Proteção de dados; Princípio da proporcionalidade; Tribunal Constitucional Alemão; Precedente.

ABSTRACT: This article aims, based on the principle of proportionality, which is a pillar of the democratic rule of law, conduct a critical analysis of previous German Constitutional Court declared unconstitutional the law transposing Directive 2006/24/EC of the European Parliament and Council, which has, in its art. 6, on the retention of personal data for a period not less than 6 (six) months and not exceeding (2) two years up to the date of the notice. The legislation in force since 2008 and ruled unconstitutional in March 2010 was implemented with the justification that the stored information could help identify criminal and terrorist organizations.
KEYWORDS: Terrorism; Data protection; Principle of proportionality; German Constitutional Court; Precedent.



*Artigo recebido em 4.09.2010 e aprovado para publicação pelo Conselho Editorial em 29.09.2010.*
* Procurador da Fazenda Nacional e Mestrando em Direito Público – PUCRS.

inconstitucional lei que determina o armazenamento, pelo período de 6 (seis) meses, de dados de telecomunicação; Considerações Finais: A luta contra o terrorismo e a proteção de dados pessoais; Referências Bibliográficas.

SUMMARY: Introduction; 1 Charter of Fundamental Rights of the European Union; 2 Regulatory evolution; 2.1 The federal German data protection (Bundesdatenschutzgesetz, BDSG) and the decision on the population census (Volkszählungsurteil); 2.2 Policy on Data Protection (Directive 95/46/EC of 24 October 1995); 2.2.1 The European model of data protection; 2.2.2 Role of Community Policies; 2.2.3 Scopes Policy 95/46: protection and free flow of data; 2.2.4 Definition of "personal data" and areas excluded from protection; 2.3 Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications; 2.4 The September 11 and the 2006/24/EC Directive on data retention (amending Directive 2002/58/EC); 3. Decision of the German Constitutional Court, for violation of duty of proportionality, declaring unconstitutional the law that provides storage for a period of 6 (six) months of data telecommunication; Conclusion: The fight against terrorism and protection of personal data; References.

## INTRODUÇÃO

O presente trabalho busca realizar uma breve análise de decisão (*BvR 11/2010 de 2 de março de 2010*) da mais alta corte da Alemanha, o Tribunal Constitucional Alemão, que declarou inconstitucional o armazenamento de dados sobre conexões telefônicas e de internet, haja vista a incompatibilidade com a lei fundamental alemã de obrigar companhias telefônicas e de comunicações a armazenar durante 6 (seis) meses todos os contatos telefônicos, e-mails e conexões com a rede mundial efetuados no país.

A legislação que vigorava desde janeiro de 2008 tinha por objeto transpor os ditames expostos na Diretiva 2006/24/CE do Parlamento Europeu e do Conselho da União Européia relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicação. O disposto no considerando n. 9 da Diretiva mencionada externa o motivo de sua essencial implementação, mediante os seguintes argumentos:

> Nos termos do artigo 8.o da Convenção Europeia dos Direitos do Homem (CEDH), qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência. ***As autoridades públicas só podem interferir no exercício deste direito nos termos previstos na lei e, quando essa ingerência for necessária, numa sociedade democrática, designadamente, para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infracções penais, ou a protecção dos direitos e das liberdades de terceiros. Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente directiva.***[1] A aprovação de um instrumento de conservação de dados que obedeça aos requisitos do artigo 8.o da CEDH é, pois, uma medida necessária.

[1] Sem grifo no original.

Numa conjuntura em que a fronteira entre o material e o virtual é muito tênue, e em que as pessoas e as organizações atuam com uma agilidade crescente no domínio informático e das telecomunicações, também é reconhecido que as novas tecnologias consubstanciam uma ferramenta suscetível de ser utilizada, para fins ilícitos, que, por sua vez, devem ser no máximo possível, sempre tendo em mente os direitos fundamentais subjacentes, combatidos.

A proteção de dados sensíveis, da reserva da intimidade da vida privada, da correspondência e das telecomunicações assume uma relevância reconhecida no contexto da salvaguarda dos direitos fundamentais, por isso qualquer espécie de restrição a esses direitos reconhecidamente de jaez fundamental deve ser feita dentro de um contexto limitado pelo exame com base nos critérios da proporcionalidade. O Tribunal Constitucional Alemão andou bem ao declarar inconstitucional a lei de transposição da Diretiva n 2006/24/CE.

A essencial proteção de dados sensíveis com a não menos essencial proteção da segurança nacional apresenta um conflito aparente entre princípios com assento constitucional que merece uma solução adequada, necessária e proporcional em seu sentido eminemente estrito. A real necessidade de dotar os Estados membros da União Europeia de instrumentos eficazes de combate à criminalidade e ao terrorismo não pode servir de justificativa para solapar consagrados direitos fundamentais a muito custo conquistados, sob pena de atávico retrocesso e grasso avilto à evolução constitucional. Sob essa ótica que se passa a comentar o precedente alemão.

## 1. CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPÉIA

Antes de adentrarmos na análise da decisão do Suprema Corte Alemã, uma breve digressão histórica mostra-se salutar como forma de demonstrar o acerto na declaração de inconstitucionalidade da lei de transposição da Diretiva 2006/24/CE. A Carta dos Direitos Fundamentais da União Européia, proclamada em 7 de dezembro de 2000, no Capítulos das "Liberdades", consagrou o direito fundamental à proteção de dados:

> *Artigo 8º - Protecção de dados pessoais*
>
> *1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*
>
> *2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei.*
>
> *Todas as pessoas têm o direitode aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.*
>
> *3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.*

No momento de sua promulgação inicial a Carta representava um compromisso político, sem efeitos jurídicos obrigatórios. O Tratado de Lisboa – que alterou o Tratado da União Européia – reconheceu os direitos enunciados na Carta e conferiu-lhes força jurídica. Por isto, a Carta foi adaptada e reproclamada em 12 de dezembro de 2007. Com a entrada em vigor do Tratado de Lisboa, em 1º de dezembro de 2009,

passou a vincular juridicamente os Estados membros. A Polônia e o Reino Unido obtiveram um regime de exceção.

Portanto, atualmente a proteção de dados está alçada, no âmbito da União Européia, à condição de direito fundamental[2].

## 2. EVOLUÇÃO NORMATIVA

A primeira lei de proteção de dados foi formulada pelo estado alemão de Hessen, em 1970. A primeira legislação nacional foi editada pela Suécia, em 1973[3].

### 2.1 A lei federal alemã de proteção de dados (*Bundesdatenschutzgesetz, BDSG*) e a decisão sobre o censo populacional (*Volkszählungsurteil*)

A lei federal alemã de proteção de dados, na sua forma original, foi promulgada em 1977 (a lei foi posteriormente revisada em 1990, e alterada em 1994, 1997 e 2002). Entretanto, o direito alemão de proteção de dados só alcançou um desenvolvimento mais acentuado e uma articulação com a Lei Fundamental a partir da sentença proferida em 1983 pelo Tribunal Constitucional Federal a respeito da lei do censo populacional (*Volkszählungsurteil*).

Em 1982, o Parlamento federal alemão aprovou uma lei convocando um plebiscito populacional a ser realizado no ano seguinte. Essa lei permitia que os dados recolhidos no censo fossem rastreados até os cidadãos recenseados e fossem empregados para outras finalidades que não o recenseamento, como, e.g, pelas autoridades locais para corrigir os cadastros de moradores dos Municípios. Após uma campanha pública contra a lei esta foi questionada perante o Tribunal Constitucional Federal. A decisão do Tribunal Constitucional Federal, de 25.12.1983, apoiou os propósitos estatísticos da lei, mas declarou que os direitos fundamentais dos cidadãos deveriam ser salvaguardados contra possíveis abusos. Assim, a transferência de dados obtidos no recenseamento do governo federal para autoridades locais foi declarada inconstitucional[4].

A sentença do Tribunal Constitucional Federal anulou parcialmente a lei de censo populacional e forjou a noção de um *direito constitucional de auto-determinação informativa*, estruturando os fundamentos da proteção de dados alemã[5].

### 2.2 Diretiva sobre Proteção de Dados (Diretiva 95/46/CE, de 24 de outubro de 1995)

#### 2.2.1 O modelo europeu de proteção de dados

O modelo de proteção de dados adotado pela União Européia tem como pressuposto que a privacidade é uma questão de **direitos fundamentais**, não podendo ser deixada sob a regulação exclusiva do mercado.

A Europa optou por um modelo de **compreensivo** de proteção, adotando uma

---

[2] Têmis Limberger, *Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI,* p. 218.
[3] Fred H. Cate, *The EU data protection directive, information privacy, and the public interest,* p. 431.
[4] Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive,* p. 293.
[5] Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive,* p. 292.

norma geral de proteção de dados que regula, compreensivamente, a coleta, uso e disseminação de informações pessoais, tanto pelo setor público como pelo setor privado, bem como instituindo um órgão ou agência encarregado de supervisionar o cumprimento da legislação[6].

Ao mesmo tempo, o modelo de proteção de dados adotado pela União Européia pode ser qualificado como **flexível**, uma vez que permite a coleta e o tratamento de dados mediante um controle público, cabendo ao gestor do banco de dados notificar a autoridade pública responsável quando da inclusão, alteração e exclusão de informações. Distingue-se, assim, de um modelo rigoroso – até então adotado pelos países escandinavos –, o qual veda, em princípio, a coleta de dados, salvo exceções ou autorizações específicas em sentido contrário[7].

Diferentemente da Europa, os Estados Unidos adotaram uma abordagem dita **setorial**, que combina **autoregulação** dos agentes do mercado com leis restritas a setores específicos. Compreende-se que "o mercado deve liderar"[8]. Para o modelo norte-americano a privacidade é encarada, de certa forma, como um *bem* que o consumidor pode negociar com o fornecedor, dela podendo abrir mão, desde que consentidamente[9].

### 2.2.2 Função das Diretivas comunitárias

A regulação da proteção de dados foi encaminhada por meio de uma Diretiva comunitária. As Diretivas têm como destinatários os Estados membros da União Européia. Depois de adotada a Diretiva a nível europeu, cada Estado-Membro deve garantir a sua transposição para o respectivo sistema jurídico nacional.

A diretiva prevê um resultado final, mas a forma e os métodos da sua aplicação são da responsabilidade de cada Estado membro.

Em princípio a Diretiva é concretizada através de medidas nacionais (legislação nacional), mas quando a Diretiva confere direitos diretos às pessoas, estas podem invocá-los perante um juiz. Ainda, se alguém considerar que sofreu perdas devido à aplicação incorreta da Diretiva pelo Estado membro, pode mover um processo por perdas e danos nos tribunais nacionais[10].

### 2.2.3 Escopos da Diretiva 95/46: proteção e livre circulação de dados

A Diretiva foi adotada em 1995 e obrigou os Estados membros a adaptarem as suas legislações nacionais no prazo de 3 (três) anos, que se esgotou em 24 de outubro de 1998. Não abrange as pessoas coletivas e não interfere com a legislação que se destina à sua proteção[11]. Apresenta como objetivo primordial a "proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida

---

[6] David Banisar, *Privacy and data protection around the world*, p. 1.
[7] SILVEIRA, Paulo A. Caliendo Velloso da. *Proteção de dados no direito comparado.* AJURIS, Porto Alegre, v. 71, nov. 1997, p. 323.
[8] http://en.wikipedia.org/wiki/Data_Protection_Directive
[9] Detlev Zwick e Nikhilesh Dholakia, *Contrasting european and american approaches to privacy in electronic markets: property right versus civil right*, pp. 118-119.
[10] *Data Protection in the European Union*, p. 4.
[11] "(...) a legislação para a protecção das pessoas colectivas relativamente ao tratamento de dados que lhes dizem respeito não é afectada pela presente directiva" (considerando n. 23).

privada", no que se refere ao tratamento de dados pessoais (art. 1º, 1).

Tal proteção, todavia, não deve impedir e necessita ser conciliada com a livre circulação de dados pessoas entre os Estados-membros (art. 1º, 2).

A Diretiva parte do princípio de que a diferença do nível de proteção entre os países membros União Européia pode impedir a circulação de dados, prejudicando o desenvolvimento da atividade econômica no plano comunitário (assim o seu considerando de n. 7[12]). Assim, a Diretiva visa a harmonizar as legislações nacionais para evitar que tais barreiras interfiram com a livre circulação de dados.

**2.2.4 Definição de "dados pessoais" e situações excluídas da proteção**

A Diretiva define como dados pessoais passíveis de proteção quaisquer informações relativa a uma pessoa singular, que esteja identificada ou que seja identificável, direta ou indiretamente, por características físicas, psíquicas, econômicas, culturais ou sociais (art. 2º, a). A Diretiva regula o tratamento de dados (*processing*, na versão inglesa), assim considerada toda operação realizada sobre dados pessoais, incluindo sua coleta, organização, conservação, consulta, utilização, transmissão, difusão e apagamento (art. 2º, b).

A Diretiva é "tecnologicamente neutra", no sentido de que as suas disposições se aplicam independentemente do meio tecnológico utilizado para armazenar e processar os dados (sistema informatizado, cartões de papel, etc.)[13].

Não são protegidos pela Diretiva os tratamentos de dados que dizem respeito à segurança do Estado e aqueles efetuados por pessoas singulares no exercício de atividades estritamente pessoais ou domésticas (art. 3º, 2).

**2.3 Diretiva 2002/58/CE, de 12 de julho de 2002, sobre privacidade e comunicações eletrônicas**

Trata-se da Diretiva sobre *Internet e* serviços telefônicos. Esta Diretiva regula o processamento de dados pessoais e a proteção da privacidade nas comunicações eletrônicas, transformando os princípios estabelecidos na Diretiva 95/46/CE e na Carta dos Direitos Fundamentais da União Européia em regras específicas para o setor de telecomunicações. Substitui a Diretiva 97/66/CE.

**2.4 O 11 de Setembro e a Diretiva 2006/24/CE sobre conservação de dados (altera a Diretiva 2002/58/CE)**

O 11 de Setembro criou na Europa a oportunidade para modificar a agenda política e incrementar mudanças que já vinham ocorrendo no sentido de uma maior "securitização" da sociedade européia. Tornou-se mais difícil para as forças políticas

[12] "(...) nas diferenças entre os Estados-membros quanto ao nível de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domónio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de actividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de protecção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;"

[13] *Data Protection in the European Union*, p. 8.

oporem-se à coleta, retenção e compartilhamento de informações pelas autoridades de segurança[14]. Tal mudança foi acompanhada de uma nova tendência na segurança pública denominada "dataveillance" (vigilância de dados), que contempla a análise de dados por meio da convergência de tecnologias e bancos de dados para vigiar pessoas ou grupos suspeitos que possam representar risco potencial à segurança. A vigilância de dados usa novas tecnologias para identificar grupos de risco com base em diferentes padrões de "comportamento suspeito" ao nível dos bancos de dados privados e públicos[15].

Em resposta aos ataques terroristas ocorridos em Madri (2004) e Londres (2005) a União Européia aprovou, em 2006, a Diretiva 2006/24/CE. O propósito dessa Diretiva é promover a cooperação na investigação e persecução criminal dentro da União Européia. Ela determina que os fornecedores de serviços de telecomunicação devem conservar os dados de maioria das espécies de comunicação eletrônica (ligações telefônicas, emails, textos, telefonia pela Internet, redes de comunicação social) por um período de 6 meses a 2 anos. Esses dados incluem a identificação do emitente e do receptor, a identificação do equipamento usado, da hora, data e duração da comunicação, e das coordenadas geográficas de dispositivos móveis usados durante a comunicação. Não está abrangido pela Diretiva o conteúdo da comunicação[16].

## 3. DECISÃO DO TRIBUNAL CONSTITUCIONAL ALEMÃO QUE, POR OFENSA AO DEVER DE PROPORCIONALIDADE, DECLARA INCONSTITUCIONAL LEI QUE DETERMINA O ARMAZENAMENTO, PELO PERÍODO DE 6 (SEIS) MESES, DE DADOS DE TELECOMUNICAÇÃO

Em março de 2010, o Tribunal Constitucional Federal alemão declarou inconstitucional a lei alemã de transposição da Diretiva 2006/24/CE, que tratava sobre a conservação de dados sensíveis, determinando que todos fossem definitivamente apagados. A mais alta Corte Alemã, com supedâneo no exame de proporcionalidade[17], considerou que a lei carecia de medidas de segurança de dados, transparência e proteção legal.

A lei de armazenamento de dados correspondia a uma diretriz de combate ao terrorismo. Segundo o Tribunal Constitucional, a lei não garantia "a restrição de seu uso", por parte das autoridades; permitia uma intromissão na vida cotidiana dos alemães "com dimensões até agora desconhecidas pela legislação" e provocava nos cidadãos "um sentimento ameaçador de ser observado", que prejudicava "a percepção de seus direitos fundamentais".

Com respaldo no princípio da proporcionalidade, a Suprema Corte da Alemanha asseverou que, em nome da prevenção/precaução, os dados pessoais somente podem ser utilizados em situações excepcionais. Apenas, quando houver um perigo concreto à vida, à integridade física, à liberdade de uma pessoa ou um concreto risco à

[14] Michael Levi e David S. Wall, *Technologies, security, and privacy in the post 9-11 European information society*, p. 203.
[15] Michael Levi e David S. Wall, *Technologies, security, and privacy in the post 9-11 European information society*, pp. 199-200.
[16] Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, pp. 299-300.
[17] Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, p. 314.

segurança pública, pode-se quebrar o constitucional direito à privacidade/proteção de dados pessoais (*the right of privacy*). Acrescentou que provavelmente a decisão irá afetar a utilização de dados pelos serviços de inteligência; contudo, tal fato não cria um ambiente constitucionalmente aceitável capaz de afastar genericamente qualquer análise, sob a ótica da proporcionalidade, de requisitos mínimos e conclusivos de que, no caso concreto, a segurança pública merece maior proteção que a privacidade.

Ressalva feita pelo Tribunal Constitucional Alemão, concernente aos custos suportados pela empresas responsáveis pelo armazenamento dos dados pessoais, merece destaque. Alerta que os custos decorrentes do armazenamento devem ser levados em consideração pelas empresas, haja vista que esses (custos) representam um risco inerente à própria atividade empresarial, devendo ser, caso haja custos, repassados no preço do serviço.

Em suma, sob todos os aspectos o Tribunal Constitucional Alemão considerou inconstitucional a legislação de transposição da Diretiva 2006/24/CE, em face de que o Estado, despautado de critérios objetivos e claros, não pode, sob o argumento da prevenção/precaução ao terrorismo, invadir a esfera privada do cidadão. O dever de proporcionalidade deve nortear toda a atividade legislativa, sem o qual se mostra incontornável o vício aos preceitos constitucionais.

## CONSIDERAÇÕES FINAIS: A LUTA CONTRA O TERRORISMO E A PROTEÇÃO DE DADOS SENSÍVEIS

Como bem apontado pelo Corte Alemã: *The whole legislation lacks a structure complying with the principle of proportionality* (toda legislação carece de uma estrutura em conformidade com o princípio da proporcionalidade). Ou seja, o legislador não pode se afastar do dever de proporcionalidade. Não pode esquecer que as normas, por mais altos que sejam os reclamos sociais, devem espraiar segurança jurídica e respeito à norma constitucional que lhes serve de suporte de validade.

A segurança nacional é um dever do Estado e um direito do cidadão. O Estado para proteger seu povo, diante do terrorismo e outras formas de atentados à segurança pública, precisa da prévia informação; precisa de antemão dos dados pessoais, caso contrário, o dever de proteção juridicamente eficaz torna-se imprestável, pois efetivamente falível. A posse da informação pelas autoridades e serviços de inteligência, de fato, é essencial. Não há, diante dos avanços tecnológicos utilizados pelo crime organizado e terroristas, como abrir mão da prévia informação. Não há dúvidas de que o cerne da inteligência é o cruzamento de dados pessoais negados, dados que o detentor da informação pode ser o próprio Estado ou um particular, que por ser igualmente detentor de dados sigilosos, deve disponibilizá-los às autoridades competentes, em nome da proteção da segurança nacional.

Por outro lado, qualquer avanço próximo ao núcleo essencial de um direito fundamental deve ser criteriosamente conduzido pelo princípio da proporcionalidade, "na sua função como critério de controle da legitimidade constitucional de medidas restritivas do âmbito de proteção dos direitos fundamentais"[18]. Assim, a opção do

[18] SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais.* 10. ed. Porto Alegre: Livraria do Advogado, 2009, p. 397.

legislador alemão de conservação dos dados, sem a observância dos potenciais riscos em matéria de proteção de dados pessoais, mormente, no que diz respeito a acessos indevidos, desvio de finalidade (*riscos estes que devem ser minimizados dada a natureza dos direitos em causa – direitos fundamentais*), viola os princípios da intimidade e da privacidade, os quais preponderam, no caso, no exame da proporcionalidade, sobre o dever de segurança pública e proteção contra o crime organizado.

O legislador, quanto ao prazo de conservação e a forma de obtenção dos dados, deve seguir os seguintes passos: (**1**) desvelar o meio adequado para a prossecução dos fins visados pela lei (salvaguarda de outros direitos ou bem constitucionalmente consagrados), (**2**) o meio necessário, porque os fins visados pela lei não podiam ser obtidos por outros meios menos onerosos para os direitos liberdades e garantias, e, por último, (**3**) os meios devem situar-se numa justa medida, impedindo-se a adoção de medidas legais restritivas desproporcionadas, excessivas, em relação aos fins obtidos.

Assenta-se que os direitos fundamentais não possuem o mesmo conteúdo, já que dele extraem-se exigências e concretizações em maior ou menor grau de intensidade, isto sem se falar na possibilidade de existirem direitos fundamentais sem um conteúdo visivelmente aferível. Os princípios, por força de sua essência, sujeitam-se a uma necessária relativização. No âmbito de uma hierarquia axiológica, a prevalência no confronto entre princípios e regras de mesma estatura e *locus* constitucional deve ser aferida, com fundamento no caso concreto, mediante uma atividade jurisdicional vinculada e com amparo no princípio da proporcionalidade, sob pena de falência do sistema constitucional vigente, que se pauta por valores, princípios e regras de fundamental importância para o Estado de Direito garantidor da realização efetiva dos direitos catalogados e não catalogados como fundamentais no corpo constitucional.

**Em face das considerações e comentários precedentes**, é latente que não se pode dispensar, em matéria de direitos fundamentais – até mesmo em face da necessidade de solucionar o caso concreto – um juízo de ponderação entre os prováveis princípios e/ou regras colidentes. Andou bem a Corte Constitucional Alemã em declarar a inconstitucionalidade de lei que, em nome da segurança nacional e do terror a possíveis atentados terrorismo, atribuía primazia à invasão da privacidade, quando em cotejo com a infeliz, porém, necessária, luta contra o terrorismo. Andou bem o Tribunal porque a "guerra" contra o terrorismo, por mais tristes que sejam os atentados, deve conter balizas determinadas e visualizáveis e com amparo judicial, no caso concreto, buscar a concordância prática dos princípios em conflito, primando por aquele que menos sofre restrição em seu núcleo essencial, sob pena de o acesso invasivo aos dados pessoais ser mais triste que os atentados terroristas.

## REFERÊNCIAS BIBLIOGRÁFICAS

BANISAR, David. *Privacy and data protection around the world.* 1999. Disponível em: http://www.pco.org.hk/textonly/english/infocentre/files/banisar-paper.doc. Acesso em 15 maio 2010.

BYGRAVE, Lee A. *Data protection law: approaching its rationale, logic and limits.* The Hague: Kluwer Law International, 2002.

CASTRO, Luiz Fernando Martins. Proteção de dados pessoais: panorama internacional e brasileiro. *Revista CEJ*, Brasília, v. 6, n. 19, pp. 40-45, outubro-dezembro/2002.

CATE, Fred H. *The EU data protection directive, information privacy, and the public interest.* 1995. Disponível em: http://www.fredhcate.com/Publications/Iowa95.pdf. Acesso em 15 maio 2010.

DESIMONE, Christian. *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive.* German Law Journal, v, 11, n, 3. (2003). Disponível em: http://www.germanlawjournal.com/pdfs/Vol11-No3/PDF_Vol_11_No_03_291-318_Articles_de%20Simone.pdf. Acesso em 15 maio 2010.

European Communities. *Data Protection in the European Union.* 2003. Disponível em: http://www.windowsecurity.com/uplarticle/anti-spam/data_protection_legal_eu.pdf. Acesso em 15 maio 2010.

JUDT, Tony. *Pós-guerra: uma história da Europa desde 1943.* Trad. José Roberto O´Shea. Rio de Janeiro: Objetiva, 2008.

LEVI, Michael; WALL, David S. *Technologies, security, and privacy in the post 9-11 European information society*. 2004. Disponível em: http://www.leeds.ac.uk/law/staff/lawdw/Jlsart4.pdf. Acesso em 15 maio 2010.

LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In: *Direitos fundamentais, informática e comunicação:* algumas aproximações. Org. SARLET, Ingo Wolfgang. Porto Alegre: Livraria do Advogado, 2007.

_____. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. *Revista de Direito do Consumidor*, São Paulo, ano 17, n. 67, julho-setembro/2008.

MAXEINER, James R. *Freedom of Information and the EU Data Protection Directive.* 1995. Disponível em: http://www.law.indiana.edu/fclj/pubs/v48/no1/maxeiner.html. Acesso em 17 maio 2010.

MORO, Sérgio Fernando. *Jurisdição Constitucional como Democracia.* São Paulo: Revista dos Tribunais, 2004.

PIÑAR MAÑAS, José Luis. *La red iberoamericana de protección de datos: declaraciones y documentos.* Valencia: Tirant lo Blanch, 2006.

SALBU, Steven. R. *The european union privacy directive and international relations.* Dezembro/2001. Disponível em: http://deepblue.lib.umich.edu/bitstream/2027.42/39802/3/wp418.pdf. Acesso em 15 maio 2010.

SARLET, Ingo Wolfgang; FIGUEREDO, Mariana Filchtiner. *Reserva do possível, mínimo existencial e direito à saúde: algumas aproximações,* in *Direitos fundamentais*: orçamento e reserva do possível. Porto Alegre: Livraria do Advogado, 2008.

SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais.* 10. ed. Porto Alegre: Livraria do Advogado, 2009.

_____. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. Porto Alegre: Livraria do Advogado Ed., 2007.

SILVEIRA, Paulo Antônio Caliendo Velloso da. *Direito Tributário e análise econômica do Direito:* uma visão crítica. Rio de Janeiro: Elsevier, 2009.

_____. Proteção de dados no direito comparado. *Revista da Ajuris*, Porto Alegre, ano 24, nº 71, pp. 302-343, novembro/1997.

ZWICK, Detlev; DHOLAKIA, Nikhilesh. *Contrasting european and american approaches to privacy in electronic markets: property right versus civil right.* Disponível em: http://www.yorku.ca/dzwick/Electronic_Markets_Privacy.pdf. Acesso em 15 maio 2010.