Estudos Jurídicos

ISSN Eletrônico 2175-0491

O DIREITO À PROTEÇÃO DE DADOS FRENTE A MEDIDAS DE SEGURANÇA E INTERVENÇÃO ESTATAL

THE RIGHT TO DATA PROTECTION FROM SAFETY MEASURES AND STATE INTERVENTION

Regina Linden Ruaro[1]

Daniel Piñeiro Rodriguez[2]

Recebido em: 05/2010
Avaliado em: 06/2010
Aprovado para publicação em: 09/2010

RESUMO

O presente artigo[3] propõe um estudo acerca do direito fundamental à privacidade frente a medidas de segurança, com o intuito de perceber qual o nível de tal tutela no tocante às interferências estatais. Para tanto, toma-se como paradigma as recentes diretivas da União Européia, a jurisprudência internacional atinente ao tema, traçando as origens do direito à autodeterminação informativa e como se relaciona com a atual sociedade vigilância. Por fim, far-se-á uma breve análise do cenário brasileiro, com o escopo de esboçar a realidade do ordenamento pátrio, possibilitando a identificação de novas formas de prevenir - e não meramente reparar - ações atentatórias aos direitos e liberdades fundamentais referentes aos dados pessoais que entidades públicas e privadas dispõem a respeito de determinado indivíduo. Na pesquisa foram utilizados os métodos comparativo e monográfico, tendo em vista a busca de resultado através da comparação entre diversas linhas doutrinárias e da interpretação sistemática dos ordenamentos jurídicos brasileiro e europeu. (tipológico).

PALAVRAS-CHAVE: Proteção de dados. Vigilância estatal.

ABSTRACT

This article presents a study of the fundamental right to privacy in relation to security measures, in order to understand the extent of this right with regard to State interference. It takes as a paradigm the recent directives of the European Union, the international jurisprudence on this theme, tracing the origins of the right to informative self-determination and how it relates to today's surveillance society. Finally, it gives a brief analysis of the Brazilian scenario, outlining the reality of the country's laws, enabling the identification of new ways of preventing – rather than simply repairing – actions against the fundamental rights and liberties relating to the personal information that public and private entities hold on each individual. The research uses the methods of comparison and essay, seeking results through the comparison of various doctrinal lines and from a systematic interpretation of the Brazilian and European legal systems. (Typological).

KEY-WORDS: Data protection. State Surveillance.

RESUMEN

El presente artículo[4] propone un estudio acerca del derecho fundamental a la privacidad frente a medidas de seguridad con el objetivo de percibir cuál es el nivel de tal tutela en lo tocante a las interferencias estatales. Para ello, se toman como paradigma las recientes directivas de la Unión Europea, la jurisprudencia internacional atinente al tema, trazando los orígenes del derecho a la autodeterminación informativa y cómo se relaciona con la actual sociedad de vigilancia. Por último, se hará un breve análisis del panorama brasileño, con el objetivo de esbozar la realidad del ordenamiento patrio, posibilitando la identificación de nuevas formas de prevenir - y no meramente de reparar - acciones atentatorias a los derechos y libertades fundamentales referentes a los datos personales de los que entidades públicas y privadas disponen respecto a determinado individuo. En la investigación se utilizaron los métodos comparativo y monográfico, teniendo en vista la búsqueda de resultado a través de la comparación entre diversas líneas doctrinarias y de la interpretación sistemática de los ordenamientos jurídicos brasileño y europeo (tipológico).

PALABRAS CLAVE: Protección de datos. Vigilancia estatal.

INTRODUÇÃO

Os riscos à esfera privada com os quais a sociedade moderna se depara são, nos dias de hoje, constituídos e interligados por vários elementos. Podem ser apontados, dentre eles, o crescente desenvolvimento tecnológico, diferentes interesses econômicos e políticos, a constante "necessidade" de controle estatal sobre as relações particulares e, fundamentalmente, o fato de que a maioria da população não mais leva a sério sua esfera privada.[5] Em verdade, ao mesmo tempo em que a maioria dos indivíduos luta para manter sua esfera íntima longe do "painel" do Grande Irmão[6], também não contesta as permanentes intrusões perpetradas pelo Estado à guisa de combate ao terrorismo ou a qualquer prática antidemocrática.

Trata-se, em verdade, de um novo tempo, caracterizado fundamentalmente pela quebra da tradição ocidental. A lei básica da física de que dois corpos não podem ocupar um mesmo espaço ao mesmo tempo é superada pela noção de espaço virtual, cujo *locus* é ocupado por centenas de milhares de pessoas a todo instante. O eu interior descrito por Freud parece já não ser o foco do nosso desejo, porque sequer compreendemos o outro, que hoje habita diversas redes sociais disseminadas na Internet.

É neste novo ambiente - que verdadeiramente se estrutura como um espaço habitável e de interação humana - que despejamos dados pessoais, como, por exemplo, nossos gostos, nosso estado civil, aspirações e profissões. Note-se que não se está a negar os benefícios das novas tecnologias. Hoje está proibido o retrocesso e é impensável, num mundo globalizado e com fronteiras encurtadas, abrir mão das novas tecnologias; abrir mão seria tomar o trem em sentido contrário ao da história. Elas estão aí, para o bem ou para o mal da humanidade.

É por demais evidente a existência das grandes vantagens que o avanço tecnológico proporcionou a todos, sendo várias as comodidades inseridas em nosso cotidiano, dentre as quais a economia nas comunicações e a possibilidade de comunicação em tempo real. Pergunta-se, entretanto, qual o preço desse conforto. A resposta mais evidente é aquela que aponta para um só rumo: o virtual e o moderno tornaram possível a exata compreensão de todos os nossos comportamentos individuais. Mais do que nunca, o agir humano é observado, registrado e classificado.[7] Câmeras de vídeo observam espaços públicos cada vez maiores, tornando possível descrever para onde todos se locomovem e com quem cada um mantém contato. Um estudo na Inglaterra revelou, por exemplo, que cada cidadão britânico é filmado por 300 câmeras diferentes em um só dia.[8] Além disso, constata-se hoje um grande aumento da prática denominada "biometria", que consiste em métodos de identificação automática dos cidadãos a partir de suas características físicas.

Assim, parece que somente quando não houver razões que justifiquem a invasão por parte do Estado em nosso direito de privacidade/intimidade é que a sociedade – e cada indivíduo isoladamente

ISSN Eletrônico 2175-0491

– perceberá quão significativos são tais fatores, momento este em que serão tomadas posturas limitativas a este fenômeno. Enquanto isso, o comportamento social aos poucos se adapta à vigilância e ao monitoramento cotidiano, ao passo que se perdem progressivamente algumas conquistas do Estado Democrático de Direito.[9]

O direito à proteção de nossos dados pessoais no sistema jurídico brasileiro é tratado de forma superficial em legislações esparsas e fragmentadas, como no Código de Defesa do Consumidor e em leis penais. Lamentavelmente, sua existência só assume importância diante de eventos danosos à nossa individualidade, à privacidade e à intimidade, quando então alguns de nós buscamos recompor o dano através de ações judiciais.

É de fundamental importância para o estudo aqui proposto deixar expresso desde já que compartimos da compreensão de que o direito à proteção de dados pessoais constitui direito fundamental autônomo nos moldes do concebido pelo sistema europeu que será adiante analisado. É um direito de caráter instrumental, devendo ser tutelado pelo Estado de modo a demandar um dever ora de prestação, ora de abstenção.

Avançar nesta linha de compreensão possibilita para os cidadãos demandar o Estado, a fim de obter a tutela devida em matéria de proteção de dados pessoais, em outras palavras, implica aceitar que esse, no Brasil, decorre das disposições constitucionais referentes à intimidade e à privacidade, sem com elas se confundir.

É neste contexto – que, ao primeiro olhar, vale referir, parece assemelhar-se mais com previsões fictícias do que com um cenário presente – que se propõe travar um debate acerca da importância dos direitos fundamentais à privacidade e à intimidade, bem como da real necessidade de inserir em seu perímetro – ou, ao revés, extrapolá-lo – uma noção de dados pessoais.

A pesquisa lança uso do método dedutivo, pois figura como premissa maior o sistema europeu que trata do tema, por ser este o modelo paradigma do estudo. Acessoriamente, utiliza-se na pesquisa o método dialético, uma vez que o objeto de estudo merece constante debate, tornando-se necessário o confronto de opiniões e correntes doutrinárias, bem como o manancial de decisões produzido pela jurisprudência nacional e estrangeira, tudo para que o tema seja amplamente analisado, em todos os seus aspectos.

1 O DIREITO FUNDAMENTAL À PRIVACIDADE E À INTIMIDADE E O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

Para a análise do tema, começa-se por discutir a diferença existente entre o "direito à intimidade e o direito à vida privada". Não há dúvidas de que ambos constituem direitos da personalidade[10], mas isto não permite concluir serem sinônimos ou mesclados conceitualmente.

A intimidade pode ser definida como o "modo de ser de determinado indivíduo, consistindo fundamentalmente na exclusão do conhecimento pelos demais daquilo que somente a ele diz respeito".[11] Corresponde a todos os fatos, informações, acontecimentos ou eventos que a pessoa deseje manter em seu foro íntimo. Danilo Doneda ensina, neste ponto, que mais do que qualquer outra coisa, a expressão "intimidade" relaciona-se com o direito à vida tranquila, ou, também, com o *right to be let alone*.[12] Nesta senda, Hannah Arendt salienta que se trata de um conceito moderno, explorado primeiramente por Jean-Jacques Rousseau, para quem a intimidade se contrapõe substancialmente ao conceito daquilo que é social.[13] Em contrapartida, "vida privada" denota a existência de duas esferas – esta e a da vida pública. Assim, a diferenciação entre ambas resume-se, justamente, na oposição entre a vida doméstica e a vida política, na medida em que existem como entidades distintas e separadas desde, pelo menos, a antiga cidade-estado.[14] [15]

Muito se debate acerca da distinção entre tais esferas que se mostram desde os primórdios inseparáveis e interligadas. Para Peter Schaar, a esfera privada é o retiro do individuo e, ao mesmo tempo, o pressuposto para desenvolver livremente suas opiniões e posturas. Sem esse espaço minimamente protegido - vale dizer, um espaço em que não haja constante observação e em que se possa refletir sobre suas experiências e preferências pessoais -, também não é possível a existência de uma esfera pública[16].

De qualquer forma, a esfera privada e o seu significado, nos dias atuais, não podem ser dissociados do surgimento da sociedade burguesa. Isto porque, na maioria das sociedades industriais, não era possível qualquer intromissão da individualidade humana no ciclo de produção – pelo menos não no sentido atual da expressão. Com a transição para tal estrutura e concepção social, naturalmente não desapareceram as classes até então existentes, mas a sua realidade se transformou, e junto com ela suas configurações axiológicas[17]. Não por acaso a discussão acadêmica acerca da proteção da privacidade teve seu marco inicial justamente neste contexto, com o ensaio apresentado pelos professores Samuel Warren e Louis Brandeis, datado de 1890 e publicado na Revista de Direito da Universidade de Harvard.[18] Este estudo, que nos remete ao antigo paradigma de "zero-relationship", demonstra a precocidade do debate, que pode ser justificada pelo fato de que, já no final do Século XIX, o desenvolvimento tecnológico começava a acelerar seus passos rumo à realidade que a sociedade globalizada amargou experimentar, qual seja, a gradativa diminuição da sensação de "estar sozinho".[19]

Foi a partir do Século XX, entretanto, com o uso dos meios de comunicação em massa, que ocorreram as maiores mudanças na relação entre esferas pública e privada, momento em que suas fronteiras se estreitaram ao ponto de quase se tornarem imperceptíveis. A realidade globalizada tomou proporções ainda maiores nos anos setenta, momento em que os avanços tecnológicos iniciaram o seu processo de transformação da sociedade. Se até determinado momento histórico a proteção jurídica do direito à privacidade se mostrava suficiente, com o desenvolvimento da informática, passam a ser armazenados um número ilimitado de dados de todas as naturezas, os quais circulam entre Estados, particulares e empresas privadas, muitas vezes sem qualquer tipo de controle.[20] Benedikt Buchner, em sua obra "Informationelle Selbstbestimmung im Privatrecht", comparando o contexto dos precursores da matéria com o experimentado atualmente, afirma que:

> […] Waren für Warren und Brandeis tecnische Neuerungen wie die Photographie und gesellschaftliche Entwicklungen wie die Sensationspresse der Auslöser für ihre Forderung nach rechtlicher Fortentwicklung, so sind diese technischen Neuerungen und gesellschaflichen Entwicklungen heute durch die elektronische Datenverarbeitung und den Wandel von der Industrie- zur Informationsgesellschaft in gleicher Weise gegeben.[21]

Neste contexto é que começa a surgir a necessidade de proteção aos dados pessoais. Armando Veiga[22] aduz que até mesmo o direito à intimidade já poderia ser referido como fruto de uma noção pré-informática, uma vez que não mais responderia a certas reivindicações jurídicas, como a necessidade de se reconhecer ao indivíduo o direito de controlar as informações a ele atinentes, ou, ainda, a de limitar o período de tempo de conservação de dados em arquivos públicos e privados.

1.1 O Surgimento do direito à autodeterminação informativa

Como referido anteriormente, em 1890, o artigo pioneiro dos norte-americanos Samuel Warren e Louis D. Brandeis, "The Right to Privacy", trouxe a ideia de um direito básico à proteção da pessoa e de um direito de estar sozinho. Partindo deste ponto inicial é que se desenvolveu o pensamento de que o indivíduo teria o direito de decidir sobre a publicização de informações pessoais relevantes sobre sua pessoa. Teria aqui suas raízes[23] o que o Tribunal Constitucional Federal alemão anos após, em 1983, logrou definir como o "direito à autodeterminação informativa."

Salienta-se que antes mesmo da referência expressa à sua figura no sistema jurídico alemão, o Tribunal Constitucional já abordava o assunto de diferentes formas, de modo que não houve propriamente a "criação" daquele direito em um único precedente; o que se fez, isto sim, foi reconhecer *status* de direito fundamental a uma construção que já contava com certa elaboração jurídica.[24] É o que se depreende da análise de precedentes anteriores à Sentença da Lei do Censo ("Volkszählungsurteil") – a seguir analisada – na medida em que referiam um direito à autodeterminação do indivíduo sobre deus dados pessoais.

Na "Mikrozensus-Entscheidung"[25], por exemplo, foi garantido o direito de autodeterminação dos indivíduos no sentido de poder controlar e fiscalizar o levantamento de seus dados pessoais e relativos à sua vida privada. Ressaltou-se a ideia de que toda pessoa precisaria permanecer, para o efetivo desenvolvimento livre e responsável de sua personalidade, em uma espécie de "espaço interno", em que ela domina e controla a si própria e do qual ela possa se retirar sem sofrer influências externas. Tal espaço deveria permitir que se ficasse em paz e que se aproveitasse um direito de estar só.[26]

ISSN Eletrônico 2175-0491

Em decisões posteriores também se utilizou o elemento específico da autodeterminação no tocante ao direito geral de personalidade, de forma que, cada vez mais, o Tribunal Constitucional Federal da Alemanha lançou mão de diferentes formatações desta figura jurídica. Na grande maioria dos casos, era suscitada no sentido de que o individuo poderia escolher como ser representado ou visto por terceiros ou pelo público como um todo.[27] Uma autodeterminação assim descrita abrangeria o direito à própria imagem e àquilo que é dito, bem como a possibilidade de dispor sobre a representação de si mesmo.[28]

Em 1977, a Alemanha já apresentava uma lei federal sobre a matéria – a primeira do mundo a tratar da proteção de dados pessoais, originária da "Land de Hesse" –, mas que se mostrou incapaz de fornecer garantias suficientes aos cidadãos e também de enfrentar a "Lei do Censo".

Valendo-se desta lei, o Estado alemão pretendia finalizar um censo geral em 1983, que tinha como objetivo principal, a partir de 160 perguntas, confrontar os dados fornecidos com os do registro civil. Além disso, as perguntas eram de cunho pessoal, que iam desde as aspirações profissionais do indivíduo até suas práticas religiosas e políticas. Ademais disso, outros pontos suscitaram controvérsia, como a possibilidade de transmissão dos dados colhidos a autoridades federais e a outros Estados, e até mesmo a previsão de multa àqueles que não respondessem ao Censo, culminando com a inserção de mecanismos que favorecessem a denúncia destas pessoas.[29]

Despontou então um generalizado sentimento de insegurança, temendo-se a criação de um Estado superinformado, iniciando-se um processo que terminou com a sentença da Corte Constitucional, suspendendo provisoriamente o censo e, posteriormente, julgando-o inconstitucional, sob o argumento principal de que:

> [...] caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos, estaria caracterizada a diversidade de finalidades, que impediria o cidadão de conhecer o efetivo uso de suas informações. [...] O rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares de dados.[30]

Este é considerado o marco oficial em que surge o direito à autodeterminação informativa, que seria, segundo a sentença, "O direitos dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados". A partir desta ideia, o sujeito passa a dispor de quando e sob que circunstâncias poderá dar-se conhecimento de seus dados pessoais.[31]

Especificamente no direito alemão, a decisão é considerada a Magna Carta do seu desenvolvimento, na medida em que sua declaração trouxe suporte para a discussão constitucional sobre a intervenção e o controle Estatal neste âmbito. A partir de então, passou-se a exigir que cada limitação ou restrição ao direito à autodeterminação informativa tivesse base jurídica constitucional.[32] Benedikt Buchner ressalta, ainda, a necessidade de clareza na atuação do Poder Público ao restringir o direito, bem como congruência entre o motivo legal e a efetiva coleta. Há, portanto, uma exigência de conformidade e clareza no que toca ao uso de informações pessoais que resultem numa menor proteção do cidadão.[33]

Assim, a proteção dos dados pessoais é a regra, e a intervenção estatal se dá em casos excepcionais. Significa que o ente público deve sempre, no tratamento destas informações, atuar em consonância com as previsões e as autorizações legais, respeitando também o princípio da proporcionalidade.[34]

1.2 A Proteção de Dados Pessoais no Sistema Europeu

O direito à proteção de dados pessoais começou a ser desenvolvido na Europa a partir do final da década de 1960. Podem ser descritos como seus antecedentes históricos tanto o artigo 12 da Declaração Universal dos Direitos do Homem, como o artigo 8º do Convênio para Proteção de Direitos Humanos e Liberdades Fundamentais, pactuado em Roma, no ano de 1950. Figuram também nesta lista de influências os artigos 17 e 18 do Pacto de Direitos Civis e Políticos, firmado em Nova Iorque no ano de 1966. [35] [36]

Em 23 de janeiro de 1970, a Resolução nº. 428 da Assembleia Parlamentar do Conselho da Europa, também conhecida como "Declaração sobre os meios de comunicação em massa e os Direitos Humanos" ("Declaration on mass communication media and Human Rights"), trouxe novamente à

discussão o tema da necessidade de proteger a vida privada em face dos novos meios informáticos, salientando que "onde sejam implementados bancos de dados regionais, nacionais ou internacionais, o indivíduo não poderá ser totalmente exposto pela acumulação de informações atinentes à sua vida privada". Impôs, ademais, que tais arquivos deveriam ter seu conteúdo restringido o máximo possível, de acordo com a finalidade de sua criação.[37] [38]

Posteriormente, em 1981, o Conselho da Europa dispôs por meio do Convênio nº 108[39] sobre a proteção dos indivíduos quanto ao tratamento de dados pessoais. Este foi o primeiro texto jurídico unificado acerca da matéria, que se propôs a garantir, no território de cada país-membro, o respeito aos direitos e às liberdades fundamentais de todas as pessoas, independentemente de suas nacionalidades ou residências, atendendo, também, à proteção do tratamento automatizado de dados pessoais.[40] [41]

A Diretiva Comunitária 95/46/1995, que regulamenta o tratamento e a livre circulação dos dados pessoais, marcou o direito comunitário europeu, na medida em que estabeleceu o dever dos Estados de criarem códigos de condutas nacionais e comunitários, para que fosse possível dar maior efetividade às disposições da Diretiva. Apesar de não apontar direitos atinentes à proteção de dados pessoais e quais os seus limites, a norma apresentou princípios que deveriam ser observados nas legislações internas, para que se possibilitasse a defesa dos interesses protegidos.[42] Além disso, acentuou que a proteção dos dados pessoais deveria ser aplicada tanto ao tratamento automatizado de dados como ao tratamento manual, da mesma forma que a observância de suas determinações deveria se dar tanto pelo setor público quanto pelo setor privado.[43]

Posteriormente, a Diretiva 97/66CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, complementa a norma anterior, trazendo, por exemplo, determinações de segurança em determinados setores. Assim, dispõe que, havendo risco especial de violação da segurança de rede dos serviços de telecomunicações acessíveis ao público, o seu fornecedor estará obrigado a informar tal fato aos assinantes e quais as possíveis soluções, incluindo os respectivos custos da reparação pretendida.[44]

Em 2002, foi promulgada outra diretiva atinente ao tema – Diretiva 2002/58/CE –, visando à regulamentação da proteção de dados pessoais no âmbito da comunicação eletrônica. Em que pese não tenha inovado o ordenamento da comunidade europeia, permitiu a adequação das finalidades presentes na Diretiva 95/46/CE à realidade tecnológica não presente à época de sua promulgação.[45]

1.2.1 A Diretiva 2006/24/CE e a devastação da esfera privada

Por derradeiro, a Diretiva 2006/24/CE, que dispõe sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, salienta a necessidade da tutela do direito à privacidade e à intimidade por parte dos Estados-membros. Em seu artigo 4º, determina que os dados referidos na diretiva – decorrentes de comunicações eletrônicas, por exemplo – só poderão ser transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. A norma refere, ainda, que tal procedimento deverá ser analisado tendo em vista a sua necessidade.

No entanto, a mesma diretiva permite que sejam disponibilizados determinados dados para efeitos de investigação, de detecção e de repressão de crimes graves. Em suas considerações, a de número 9 afirma que "a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros".[46] O artigo 6º prevê, por fim, que esta conservação pode se estender até 24 meses.

O período de armazenamento de dados tem sido um ponto de discussão importante entre os países-membros da comunidade europeia, visto que a Diretiva traz uma lista de dados específicos a serem conservados, como números de telefones, códigos de identificação atribuídos aos computadores que navegam na Internet, e até mesmo a data e horário que determinada pessoa acessou (*login*) ou desconectou (*log off*) a rede mundial.[47]

Relativamente ao excesso de tempo de armazenamento de dados, Armando Veiga cita dois estudos relevantes: um deles realizado pela Faculdade de Direito de Erasmus de Roterdan, e o outro apresentado pela Presidência do Reino Unido da União Européia. Enquanto o primeiro, a partir

ISSN Eletrônico 2175-0491

do estudo de 65 casos concretos, apontou que o tempo de três meses seria suficiente para que se desse o fornecimento dos dados buscados, o segundo demonstrou que 85% das informações solicitadas poderiam ser recolhidas em apenas seis meses, ou até doze meses, em casos de crimes graves.[48] Entretanto, ainda que questionado pela Autoridade Européia de Dados (AEPD) e pelo Comitê Econômico e Social[49], o Conselho da União Européia manteve o limite máximo de 24 meses.

A questão do tempo de armazenagem dos dados pessoais suscita a grande dúvida dos estudiosos, questionando se, mesmo em tempos em que o "inimigo" não é facilmente determinado, a sua conservação pelo período de dois anos, com o objetivo de combater manifestações terroristas[50], não afrontaria brutalmente o direito à privacidade e à intimidade.

Tanto atentados terroristas físicos quanto os denominamos *cyber-attacks* tornam-se cada vez mais frequentes, o que motivou a elaboração de Parecer do Conselho Europeu intitulado "*How to prevent cybercrime against state institutions in member and observer States.* [51] "Com políticas severas de combate ao terrorismo, entretanto, os danos daí decorrentes poderiam ser irreversíveis na medida em que, a pretexto de proteção, todos os indivíduos seriam potencialmente "perigosos". Não pode ser outro o entendimento, haja vista a postura atual manifestada pelo governo britânico, que pretende criar um arquivo contendo todas as comunicações móveis e transferência de dados nos últimos seis meses, seja pelo uso da Internet ou telefone.[52]

A crítica a medidas como esta aparece de todos os lados: até que ponto o monitoramento de *sites* de relacionamento, utilizados por cerca de metade dos habitantes da Inglaterra[53], poderá resolver ou prevenir crimes de Estado e de ataques em massa? Se este é um perigo possível, há outro que o antecede e é certo: o perigo de criação de um ente público superinformado, conhecido e já experimentado nos regimes totalitários.

No famoso caso "Amann vs. Suíça" (Sentença BJC-242, do Tribunal Europeu de Direitos Humanos – TEDH), Hermann Amann vendeu, por telefone, um aparelho eletrônico a uma pessoa situada na antiga União Soviética. Esta chamada foi interceptada pelo Ministério da Confederação da Suíça (Ministério Público) que a identificou como proveniente da embaixada soviética. A partir deste contexto, a polícia de Zurique preparou um relatório sobre o Senhor Amann, que o cadastrou com um "contato da embaixada russa", tendo lhe atribuído o número (1163:0)614[54]. O caso chegou ao TEDH e foi julgado em 16 de fevereiro de 2000. O peculiar deste precedente, e que convida à reflexão acerca da eficiência de controle de dados pelo Estado, é que o aparelho vendido por Amann era um depilador elétrico.

2 PROTEÇÃO DE DADOS, SEGURANÇA E INTERVENÇÃO ESTATAL: NADA A ESCONDER?

Cada vez mais, na discussão sobre proteção de dados, vem à tona o velho ditado popular de que "quem não tem nada a esconder, não precisa invocá-la" Porém, Peter Schaar[55] destaca os milhares de reclamações anuais feitas pelos cidadãos às autoridades de proteção de dados na Europa, por exemplo, quanto ao abuso na sua utilização dos próprios. Frequentemente isso ocorre em relação a informações médicas sensíveis, ou outros dados que mereçam proteção especial.

Outro ponto comumente levantado é a clássica fórmula "proteção de dados é proteção de criminosos" ("Datenschutz ist Täterschutz"), classificando a tutela como empecilho na luta contra o crime organizado, terrorismo, crimes sexuais, etc. Uma observação mais atenta é capaz de perceber outros problemas relacionados ao fenômeno, que ganha grande peso na mídia. O caso Stephanie (2006), por exemplo, costuma acalentar estas discussões.

Em Dresden, um homem prendeu uma menina de 13 anos em seu apartamento por 36 dias, tendo sido torturada e abusada sexualmente diariamente. O criminoso fora condenado anteriormente por um crime sexual, mas mesmo assim não foi localizado nos registros policiais. Rapidamente depositou-se a culpa do sinistro na proteção de dados excessiva: as autoridades policiais alegaram que houve uma rápida alteração do cadastro de Mario M. para proteger sua privacidade, o que teria dificultado a sua captura. Entretanto, o Supervisor de Proteção de Dados do Estado logrou desmentir a justificativa, sustentando que a busca poderia ser feita até mesmo em um sistema *on-line* da repartição.[56]

As consequências de uma opinião social desse nível podem ser percebidas nos EUA, onde o nome e o endereço de criminosos sexuais são colocados por particulares à disposição para consulta em *sites* da Internet, sem um debate prévio que garanta a legitimidade democrática de tal medida e sem a segurança de que as informações ali constantes sejam verdadeiras. Também na Alemanha algumas posturas políticas contrariam princípios constitucionais face às reivindicações aguçadas da sociedade, ignorando as consequências que podem resultar dessa exposição pública. Procedimentos como estes afrontam não só uma sociedade e um ordenamento jurídico livres, mas também fariam nossas vidas mais inseguras: quando é retirada dos infratores a possibilidade de ressocialização e reinserção social, amplia-se o seu espaço de violência.[57]

A ideia de que a proteção de dados instiga o aumento da criminalidade persiste na população como um todo. Pesquisas[58] mostram, por exemplo, que predomina no ideário popular a crença de que houve um aumento no número de crimes sexuais contra crianças nos últimos 10 anos, quando, na verdade, esses números diminuíram.

O *ranking* mundial de proteção de dados[59], que escalona a tutela da esfera privada dos países de acordo com suas legislações protetivas, mostrava que, em 2006, a Alemanha estava em primeiro lugar, seguida pelo Canadá. Os EUA, a Inglaterra e a Rússia estavam entre os piores colocados. Tendo em vista este estudo, vê-se que a relação "proteção de dados – criminalidade" não pode ser tão estreita assim, pois em países com elevados índices de proteção da intimidade (Alemanha e Canadá) a criminalidade é muito menor do que aqueles em que praticamente não existe tal tutela, o que põe em dúvida se as milhares de câmeras dispostas na Inglaterra cumprem o papel a que se destinam.[60]

2.1 O passado alemão e a invasão da esfera privada pelo Estado

O bom desempenho da Alemanha nos estudos acerca da proteção da esfera privada talvez seja fruto das lembranças ainda vivas dos dois modelos de Estado de vigilância experimentado pelos alemães: o regime nazista e o DDR. As experiências brutais dos aparatos de repressão nazista fizeram reconhecer que uma polícia secreta poderosa, juntamente com todas as outras circunstâncias da época, deveria para sempre ser evitada.[61] [62] O segundo modelo de Estado de vigilância – o DDR – também provocou profundos danos à população. Escutas e grampos vigiavam todos os espaços privados. Ninguém estava a salvo de ver seus hábitos de higiene pessoal ou sua intimidade familiar observados e registrados. Depois da unificação do Estado alemão, continuou o debate acerca do tratamento de dados coletados. Em 1991, o parlamento alemão aprovou regramento específico sobre a documentação do Deutschen Demokratischen Republik: a Lei sobre os Documentos do Serviço de Segurança do Estado da antiga República Democrática Alemã – a "Stasi[63] – Unterlagen – Gesetz (StUG)". A norma separa o tratamento de dados quanto aos infratores, vítimas e outros interessados, e a todos os vigiados assiste o direito de inspeção sobre os dados coletados.

Os ensinamentos desse momento histórico também influenciaram diretamente o debate constitucional antes e depois da unificação de 3 de outubro de 1990. Todos os novos Estados (Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt e Thüringen) têm o direito à proteção de dados pessoais expressos em suas constituições. Também foi ventilada a discussão acerca de se ter ou não expressamente considerada na Lei Fundamental alemã o mesmo direito, mas se votou no sentido de que, depois do precedente do Tribunal Constitucional Federal Alemão, reconhecendo o direito à autodeterminação informativa – mesmo sem o nome expresso de proteção de dados –, já seria considerado como fundamental. [64]

2.2 Autodeterminação Informativa e Segurança do Estado

Informações estatais e interesses de vigilância passaram a ser tema constante na pauta política dos países europeus e dos Estados Unidos, sobretudo após os atentados de 11 de setembro de 2001. Seus reflexos não são identificados somente nos EUA, mas também na Alemanha. Os conflitos entre a efetivação da segurança nacional, de um lado; e o respeito à autodeterminação informativa dos indivíduos, do outro, foram sensivelmente aguçados a partir deste marco temporal.[65] As nações dos dois lados do Atlântico tiveram de fazer uso de instrumentos que possibilitassem uma maior

ISSN Eletrônico 2175-0491

fiscalização estatal nas relações privadas e comerciais – tudo com expressa autorização legal –, o que já sinalizava uma maior restrição vindoura ao direito à autodeterminação informativa face à segurança interna dos países.[66]

Nos Estados Unidos, há o famoso "Patriot Act" que, após o atentado de 11 de Ssetembro, teve por objetivo atacar o terrosimo e o seu financiamento, aumentando as possibilidades de poder e de controle estatal sobre imigrantes e estrangeiros. Para tanto, proporcionou o aumento do poder de agências do governo na interceptação telefones, *e-mails*, dados médicos, financeiros, etc., além de alterar muitas leis em relação à privacidade[67] (v.g. Electronic Communication Privacy Act, de 1986).[68] Esta postura estadunidense enfraqueceu em muito a tutela dada às garantias individuais e da privacidade. Podem ser constatadas, a partir dela, ofensas pelo menos às 1ª, 4ª e 14ª Emendas, frente a mandados amplos e abusivos, coletas de dados privados, detenções injustificadas, etc.[69]

Também na Alemanha o legislador reagiu rapidamente. Em janeiro de 2002 sobreveio a lei antiterrorismo ("Terrorismusbekämpfungsgesetz" - TBG), contendo numerosas alterações de outras leis federais. A partir dela destacou-se a ampliação das competências dos serviços secretos e uma maior limitação ao direito fundamental de sigilo no âmbito das telecomunicações.[70]

O desejo do Estado por mais controle e monitoramento, entretanto, não diminuiu com a aprovação da TBG. A sentença do Tribunal Constitucional Federal Alemão sobre vigilância acústica de casas particulares ("akustischen Wohnraumüberwachung"), de março de 2004, a introdução da biometria no tocante aos documentos de identificação, a obrigatoriedade de armazenamento de dados no âmbito das telecomunicações, já referida no ponto 1.2.1., por ocasião da Diretiva 2006/24/CE, são alguns dos exemplos de um passado recente que parece nos acompanhar por algum tempo, sem serem rompidas as tensões entre vigilância estatal e proteção da esfera privada.[71]

3 CONSIDERAÇÕES FINAIS

O sucesso de uma promessa estatal que almeje tutelar a esfera privada deve estar necessariamente calcado em uma estratégia de combate que alie ferramentas tecnológicas, econômicas, políticas e jurídicas, sem deixar de tomar em conta uma (re)significação do conceito da palavra "proteção". Na Era da Informação, tal termo somente conseguirá ser desvinculado de uma vigilância excessiva por parte Poder Público – podendo até mesmo ser invertido o resultado do jogo travado entre Estado, sociedade e particulares – quando a tecnologia e o Direito buscarem juntos respostas concretas, sem perder de vista o âmbito global que a proteção de dados inevitavelmente invoca.

Mais importante que tudo isto, entretanto, é a construção de uma nova premissa maior, em tempos de supervigilância. Para o efetivo e o livre exercício da tão almejada autodeterminação informativa, há que se substituir, no campo da proteção e da tutela, o papel do controle sufocante pelo da renovada "responsabilidade", não divorciada da realidade digital, mas sim consciente de suas proporções – que beiram o desconhecido. Não se quer, com isso, anular o dever de regulação atinente ao Estado, mas o que ocorre hoje é uma valorização excessiva das técnicas informáticas, girando em torno de acesso a novos espaços virtuais. Por que são estes os fatores aos quais se dedicam tantas atenções, ao desprezo da proteção da esfera privada?

Talvez a resposta a esta questão esteja no fato de que os próprios atingidos pela sociedade de vigilância já estejam completamente conectados e adaptados à transição onipresente de uma sociedade que tem como principal característica a coleta e o armazenamento de dados pessoais. Resulta daí que a discussão a ser travada não é apenas sobre vigilância, mas também como algumas respostas jurídicas poderão efetivamente intervir neste novo cenário. Para alguns autores[72], o papel da ética fica evidenciado na nova sociedade informatizada, de modo que somente nela estaria a esperança de estabilizar a já tão enfraquecida esfera privada. Nem por isso, no entanto, devem ser olvidados os esforços internacionais realizados neste sentido, e justamente por isto o direito comparado pode apontar uma das possíveis respostas a este problema. Se vivemos hoje em uma sociedade dinâmica e regida pela máxima de que "a informação é poder", qualquer posição que o Estado adote deverá, para responder aos anseios sociais, tomar em conta esta dinamicidade, por vezes tendo de avançar para além do discurso jurídico. Somente assim será possível caminhar em busca de uma solução compatível com os princípios da democracia e, ao mesmo tempo, que permita a necessária proteção dos dados pessoais.

REFERÊNCIAS

ARENDT, Hannah**.** *A condição humana***.** 8. ed. Rio de Janeiro: Forense, 1997.

BRANDEIS, Louis D. e WARREN, Samuel D. *The rigtht to privacy*. Disponível em: www.lawrence.edu/fast/boardmaw/privacy_brand_warr2.html. Acesso em: 16 de julho de 2008.

BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.*Mohr Siebeck, 2006.

COMPARATO**.** *Ética, direito, moral e religião no mundo moderno.* 2006.

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

FARIAS, Edilsom Pereira de. *Colisão de direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Sérgio Antônio Fabris, 1996.

HAINZENREDER, Eugênio. *O direito à intimidade e à vida privada do empregado frente ao poder diretivo do empregador*: o monitoramento do correio eletrônico no ambiente de trabalho. 2007, 157 f., Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007.

HAMMERSCHMIDT, Denise. *Intimidade genética & direito da personalidade.* Curitiba: Juruá, 2008.

LEVY, Pierre. *Cibercultura*. Rubí (Barcelona) Editorial: México: Universidad Autónoma Metropolitana - Iztapalapa, 2007.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*: a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MAÑAS, José Luis P. *El derecho fundamental a la protección de datos personales, algunos retos de presente y futuro***.** Revista Parlamentária de La Asamblea de Madrid, n. 13, dez. 2005.

_____. El derecho fundamental a la protección de datos personales. In: MAÑAS, José Luis P. *Protección de datos de caráter personal en Iberoamérica*. Valencia: Tirant lo Blanch, 2006.

MILLER, Arhur R. *The assault in privacy*: computers, data banks and dossiers. s.l.: The University of Michigan Press, 1971.

PANITZ, João Vicente Pandolfo. *Proteção de dados pessoais*: a intimidade como núcleo do direito fundamental à privacidade e a garantia constitucional à dignidade. 2007. 115 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007.

ORWELL, George**.** *1984.* São Paulo: Editora Nacional, 1998.

PASQUALINI, Alexandre. *Hermenêutica e sistema jurídico.* Porto Alegre: Livraria do Advogado, 1999.

RAMIRO, Mônica Arenas. *El derecho fundamental a la protección de datos personales em Europa.* Valencia: Tirant la blanch, 2006.

RODOTÁ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden. O conteúdo essencial dos direitos fundamentais à intimidade e à vida privada na relação de emprego: o monitoramento do correio eletrônico pelo empregador. In: SARLET, I. W. (Org.). *Direitos fundamentais, informática e comunicação*: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007. Vol. 1, cap. 9.

_____. Responsabilidade Civil do estado por dano Moral em Caso de Má Utilização de Dados Pessoais. In: *Direitos Fundamentais e Justiça.* n. 1-out/dez. Porto Alegre: 2007.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais.* Porto Alegre: Livraria do Globo, 1998.

SCHAAR, Peter. *Das Ende der Privatsphäre*: der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007.

ISSN Eletrônico 2175-0491

SILVA, José Afonso. *Curso de direito constitucional.* 20. ed. São Paulo: Malheiros Editores, 2001.

TÉLLEZ, Fernando A. Protección de datos personales: la directiva comunitária, su influencia y repercusiones em latinoamérica. In: MAÑAS, José Luis P. *Protección de datos de caráter personal en Iberoamérica.* Valencia: Tirant lo Blanch, 2006.

TRAVIESO. Juan Antonio. La protección de datos personales en América latina: unidos o desprotegidos hacia una red iberoamericana de protección de datos personales. In: MAÑAS, José Luis P. *Protección de datos de caráter personal en Iberoamérica.* Valencia: Tirant lo Blanch, 2006.

VEIGA, Armando; RODRIGUES, Benjamin Silva. *A monitorização de dados pessoais de tráfego nas comunicações electrónicas.* Raízes Jurídicas, Curitiba, v. 3, n. 2, jul/dez, 2007.

WESTIN, Alan. *Privacy and Freedom.* New York: Atheneum, 1967.

NOTAS

1 Pós-Doutora em Direito pelo Centro de Estúdios Universitários de San Pablo - Espanha. Doutora em Direito pela Universidad Complutense de Madrid - Espanha. Professora Titular da PUCRS. Procuradora Federal. Fone: (51) 3320.3500. *E-mail*: ruaro@pucrs.br.

2 Mestrando em Direito do Estado pela PUCRS. Bolsista CNPq. Fone: (51) 3320.3500. *E-mail*: daniel.rodriguez@ acad.pucrs.br

3 O ensaio ora apresentado é extrato de pesquisa científica financiada pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), contemplada pelo Edital MCT/CNPq Nº 014/2008 – Universal.

4 El ensayo aquí presentado es extracto de una investigación científica financiada por el Consejo Nacional de Desarrollo Científico y Tecnológico (CNPq), contemplada por el Edicto MCT/CNPq Nº 014/2008 – Universal.

5 SCHAAR, Peter. *Das Ende der Privatsphäre*: der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 11.

6 ORWELL, George. *1984*. São Paulo: Editora Nacional, 1998.

7 SCHAAR, Peter. *Das Ende der Privatsphäre***:** der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p.14.

8 Information Comissioner: A Report on the Surveillance Society. September, 2006.

9 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 12.

10 RUARO, Regina Linden. Responsabilidade Civil do Estado por dano Moral em Caso de Má Utilização de Dados Pessoais. In: *Direitos Fundamentais e Justiça*. n.1-out/dez. Porto Alegre: 2007.

11 FARIAS, Edilsom Pereira de. *Colisão de direitos:* a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Sérgio Antônio Fabris Edito, 1996, p. 104.

12 DONEDA. *Da privacidade à proteção de dados pessoais*. 2006, p. 68.

13 ARENDT, Hannah. *A condição humana.* 8. ed. Rio de Janeiro: Forense, 1997, p. 48.

14 ARENDT, Hannah. *A condição humana*. 8. ed. Rio de Janeiro: Forense, 1997, p. 21.

15 Ressalta-se, quanto à vida privada, a decisão tomada no caso Christine Goodwin VS. Reino Unido. O Tribunal Europeu dos Direitos Humanos considerou, na Sentença BJC259, de 11 de julho de 2002, por unanimidade, que o Reino Unido violou a vida privada de Christine Goodwin, um transexual masculino que se submeteu à cirurgia de mudança do sexo. A reclamante continuou sendo considerada homem pela ordem jurídica do Reino Unido após a cirurgia de transgenitalização e, por isso, teve de contribuir para a segurança social até a idade de 65 anos. Se a sua identidade de gênero fosse reconhecida pelo Reino Unido, ela teria de efetuar tais contribuições até a idade de 60 anos.

16 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p.15.

17 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p.17.

18 BRANDEIS, Louis D. e WARREN, Samuel D. *The rigtht to privacy*. Retirado do site: <www.lawrence.edu/fast/boardmaw/privacy_brand_warr2.html>, acesso em: 16 de outubro de 2008.

19 PANITZ, João Vicente Pandolfo. *Proteção de dados pessoais*: a intimidade como núcleo do direito fundamental à privacidade e a garantia constitucional à dignidade. 2007. 115 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007.

20 RAMIRO, Mônica Arenas. *El derecho fundamental a la protección de datos personales em Europa.* Valencia: Tirant la blanch, 2006.

21 "Assim como para Warren e Brandeis as inovações técnicas - tais como fotografia - bem como os desenvolvimentos sociais - como a imprensa sensacionalista – foram um gatilho para a sua pesquisa e evolução jurídica, da mesma forma são hoje as inovações técnicas e as tendências sociais, manifestadas através do processamento eletrônico de dados e da transformação de uma sociedade industrial para uma sociedade da informação" (tradução de Daniel Piñeiro Rodriguez). BUCHNER, Benedikt. Informationelle Selbstbestimmung im Privatrecht. Mohr Siebeck, 2006, p. 14.

22 VEIGA, Armando; RODRIGUES, Benjamin Silva. *A monitorização de dados pessoais de tráfego nas comunicações electrónicas*. Raízes Jurídicas, Curitiba, v. 3, n. 2, jul/dez, 2007, p. 59-110.

23 No entanto, em que pese seja do ordenamento jurídico americano o mérito de iniciar tais debates, em termos de *privacy* como um direito geral de personalidade, há de se ressaltar a problemática opção do senado estadunidense em não adotar um sistema de proteção de dados independente, o que refletiu principalmente nas questões de âmbito privado. Tal *deficit* de tutela foi levado em consideração pela União Européia, que tratou do assunto em diferentes convenções e diretivas, estabelecendo o dever te proteção dos dados pessoais em instituições públicas e também em organizações privadas (SCHAAR, Peter. *Das Ende der Privatsphäre*: der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 19-21).

24 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 41.

25 BVerfGE 27, 1 (7) – 16 de julho de 1969.

26 BVerfGE 27, 1 (7) – 16 de julho de 1969.

ISSN Eletrônico 2175-0491

27 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 42.

28 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 42.

29 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p.192.

30 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 45.

31 Cabe ressaltar que o americano Alan Westin, já em 1967, falava nesta figura jurídica. No entanto, ainda que não desenvolvida originariamente pela própria Corte Constitucional, a Sentença da Lei do Censo é apontada pela maioria maciça da doutrina como uma referência na proteção de dados pessoais (WESTIN, Alan. *Privacy and Freedom*. New York: Atheneum, 1967, p. 7).

32 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 43.

33 "[...] Aus dieser müssen sich gemäβ dem Gebot der Normenklarheit die Voraussetzungen und der Umfang einer Beschränkung des informationellen Selbstbestimmungsrechts klar und für den Bürger erkennbar ergeben (BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 43).

34 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 43.

35 TRAVIESO. Juan Antonio. *La protección de datos personales en América latina:* unidos o desprotegidos hacia una red iberoamericana de protección de datos personales. In: MAÑAS, José Luis P. *Protección de datos de caráter personal en Iberoamérica*. Valencia: Tirant lo Blanch, 2006, p. 85.

35 O artigo 17 do referido pacto assim dispõe: "Art. 17 - 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação".

36 Resolução n. º 428. Disponível em: http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta70/ERES428.html. Acesso em: 07 de abril de 2009.

37 O ponto C.5 do referido pacto assim preceitua: "Where regional, national or international computer-data banks are instituted the individual must not become completely exposed and transparent by the accumulation of information referring even to his private life. Data banks should be restricted to the necessary minimum of information required for the purposes of taxation, pension schemes, social security schemes and similar matters".

38 O Convênio 108, de 28 de janeiro de 1981 trata da Proteção das Pessoas a respeito do tratamento automatizado de Dados de Caráter Pessoal. A Espanha o ratificou dia 27 de janeiro de 1984 (BOE de 15 de novembro de 1985).

39 Artigo 1º do Convênio 108.

40 Importante destacar, para uma melhor compreensão do funcionamento da normativa europeia, que no cenário europeu atual podem ser destacadas duas fontes principais de direito: as primárias, que se identificam com os atos jurídicos criadores de regras, previamente pactuadas pelos Estados-membros; e as derivadas, que são os regulamentos, diretivas, decisões, recomendações e ditames. Interessam ao presente estudo as diretivas comunitárias, que se caracterizam por seu poder vinculante aos Esta-

dos integrantes da União Européia quanto ao resultado, sendo permitido, no entanto, que cada nação escolha a melhor forma de alcançá-lo.

41 DONEDA. *Da privacidade à proteção de dados pessoais*. 2006, p. 238.

42 Considerando 27 da Diretiva 95/46CE sobre Proteção de Dados Pessoais. Disponível em: <http://www.inst-informatica.pt/v20/legislacao/docs/Directiva95_46_CE.pdf>. Acesso em: 10 de abril de 2009.

43 Diretiva 97/66/CE, publicada em 15 de dezembro de 1997. Disponível em: <http://www.anacom.pt/streaming/97.66.CE.pdf?categoryId=59229&contentId=93936&field=ATTACHED_FILE>. Acesso em: 14 de abril de 2009.

44 DONEDA. *Da privacidade à proteção de dados pessoais.* 2006, p. 239.

45 Diretiva 2006/24/CE, publicada em 15 de março de 2006. Disponível em: <http://www.cnpd.pt/bin/legis/internacional/DIR2006-24-CE.pdf>. Acessado em: 14 de abril de 2009.

46 Artigo 5º da Diretiva 2006/24/CE.

47 VEIGA, Armando; RODRIGUES, Benjamin Silva. *A monitorização de dados pessoais de tráfego nas comunicações electrónicas.* Raízes Jurídicas, Curitiba, v. 3, n. 2, jul/dez, 2007, p. 59-110.

48 Ibid., p. 59-110.

49 Considerando n. 9º da Diretiva 2006/24/CE.

50 Sobre este ponto, assim se manifestou a Comissão de Assuntos Políticos, em 27 de junho de 2007: "[…] In most cases, cyber-attacks do not have a political but an economic motive, and are aimed at ill-prepared small to medium-size business, with poor defence capabilities. However, politically motivated attacks do take place and include, amongst their most frequent targets, TV and radio channels, on-line newspapers and state-related websites. Instead, the large and well-protected military and government networks require relatively greater time, skill and experience to penetrate. However, cyber-attacks are becoming more and more sophisticated and are also capable of hitting these sensitive websites. Amongst the main targets are the United States, China, Brazil, Australia, the United Kingdom and Turkey […]". Disponível em: <http://assembly.coe.int/Documents/WorkingDocs/ Doc07/EDOC11333.pdf>. Acesso em: 23 de outubro de 2009.

51 Dados obtidos no jornal alemão Spiegel, publicado em 25 de março de 2009. Disponível em: <http://74.125.65.132/translate_c?hl=pt-BR&sl=de&u=http://www.spiegel.de/netzwelt/web/0,1518,615 336,00 .html&prev=/search% 3Fq%3DGro%25C3%259Fbritannien%2Bplant%2B%25C3%259 Cberwachung%2Bvon%2BSocial%2BNetworks%26hl%3Dpt-BR%26rlz%3D1T4ADBF_pt-BRBR294BR295&usg=ALkJrhgwhK8ePwEbmyvYu2YR5Far-Oldbw>. Acessado em 23 de outubro de 2009.

52 Dados obtidos no jornal alemão Spiegel, publicado em 25 de outubro de 2009. Disponível em: <http://74.125.65.132/translate_c?hl=pt.-&sl=de&u=http://www.spiegel.de/netzwelt/web/0,1518,615336.html&prev=/search%3Fq%3DGro%25C3%259Fbritannien%2Bplant%2B%25C3%259Cberwachung%2Bvon%2BSocial%2BNetworks% 26hl%3Dpt-BR%26rlz%3D1T4ADBF_pt-BRBR294BR295&usg=ALkJrhgwhK8ePwEbmyvYu2Y R5Far-Oldbw>. Acesso em: 23 de outubro de 2009.

53 Este número representava um código para as seguintes identificações: "país de regime comunista";, "União Soviética"; "espionagem demonstrada" e "diversos contatos com o bloqueio do Leste".

ISSN Eletrônico 2175-0491

54 SCHAAR, Peter. *Das Ende der Privatsphäre*: der Weg in die Überwachungsgesellschaft. C. ertelsmann (München) 2007, p. 22.

55 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p.23.

56 SCHAAR, Peter. *Das Ende der Privatsphäre*: der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p.24.

57 Informação disponível em: www.bmj.bund.de. Acesso em: 22 de novembro de 2009.

58 Disponível em: www.privacyinternational.org. Acesso em: 20 de setembro de 2010.

59 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 24-27.

60 O aparato estatal totalitário é descrito por Fábio Konder Comparato como uma "descomunal e inteligível máquina burocrática, cujos meandros parecem desafiar a lógica dos mais hábeis estadistas da época." (COMPARATO. *Ética, direito, moral e religião no mundo moderno*. 2006, p. 367).

61 A tomada do poder pelo movimento totalitário constituiu o momento decisivo de seu êxito ou fracasso. Uma vez em posse do controle estatal, existiam dois grandes perigos ao seu sucesso: a evolução rumo a um absolutismo – através do seu congelamento como governo, o que prejudicaria a sua abrangência no âmbito interno –, ou a sua evolução rumo a um nacionalismo, o que acabaria por frustrar a pretendida expansão externa. Para que esses dois insucessos fossem evitados, percebia-se fundamental a eterna variação de poder. Somente assim – deixando as massas desnorteadas em seu mundo fictício, que logo seria novamente reconfigurado – o líder totalitário seria capaz de evitar a normalização do novo modo de vida, de maneira que novos valores e formas de conviver com a falsa realidade fossem criadas. Esse é o fardo do regime totalitário: permanecer em eterno movimento (ARENDT. *Origens do totalitarismo*. 2004, p. 441).

62 Stasi (forma curta de Ministerium für Staatssicherheit, Ministério para a Segurança do Estado) era a principal organização de polícia secreta e inteligência da República Democrática Alemã, dissolvido em 1989.

63 SCHAAR, Peter. *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 29-31.

64 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Mohr Siebeck, 2006, p. 68.

65 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Mohr Siebeck, 2006, p. 68.

66 V.g., Electronic Communication Privacy Act, de 1986.

67 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p.234.

68 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p.235.

69 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Mohr Siebeck, 2006, p. 69.

70 BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, 2006, p. 69.

71 Cf. Peter Schaar, *Das Ende der Privatsphäre:* der Weg in die Überwachungsgesellschaft. C. Bertelsmann (München) 2007, p. 217 e ss.