A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

PROTECTION OF PERSONAL DATA AS A FUNDAMENTAL RIGHT

Danilo Doneda*

Resumo: O tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco. A possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes. Este artigo analisa os contornos jurídicos das informações pessoais e dos bancos de dados e explora suas principais definições no direito interno e internacional, a fim de identificar os princípios mais aparentes de uma tendência de consideração da proteção de dados pessoais como direito fundamental. A principal conclusão é que apenas sob o paradigma da interceptação, da escuta, do grampo - situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.

Palavras-chave: Direitos fundamentais. Dados pessoais. Privacidade.

Abstract: The treatment of personal data, particularly with automated processes, is a activity with risk. The possibility of unified control of the various activities of people in many situations of life, facilitate the knowledge of his public conduct and private, to the smallest detail. This article examines the legal contours of personal information and databases, and explores its main concepts in domestic and international law in order to identify the principles of a tendency to consider the protection of personal data as a fundamental right. The main conclusion is that only under the paradigm of interception, listening, clip - situations that are only a portion of the problems that may occur in treatment of personal data with the use of new technologies - can not provide effective protection to personal data in the extent that the importance of this subject assumes today.

Keywords: Fundamental rights. Personal data. Privacy.

* Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro; Professor de Direito na Fundação Getúlio Vargas do Rio de Janeiro; danilo@doneda.net

Introdução

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação.[1] Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável.

O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.

1 Bancos de dados

A ferramenta que possibilita a sistematização de volumes que podem chegar a ser gigantescos de informação e que teve seu potencial exponencialmente incrementado com o advento da informática foi, propriamente, o banco de dados.

Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. Sabe-se há um bom tempo que a informação pode gerar proveito, como resulta claro ao verificar que é milenar a prática de coleta sistematizada de informações por alguma modalidade de censo populacional, instrumento de imensa serventia para governantes de qualquer época – a ponto de os registros históricos a respeito não serem poucos.[2]

A informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna em elemento fundamental de um crescente número de relações e aumenta sua possibilidade

[1] Sobre a expressão "sociedade da informação", v. Lyon (1998, p. 384-402); v. Tb. Castells (1999).
[2] Desde o censo solicitado pelo imperador Yao na China de 2238 a.C., o de Moisés em 1700 a.C., passando pelo famoso censo ordenado por Augusto e mencionado pelo Evangelho de Lucas.

de influir em nosso cotidiano,[3] em um crescente que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais[4] – conforme notou Stefano Rodotà ainda em 1973, "[...] a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada."[5]

Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.

2 Informação e dados pessoais

A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. É importante estabelecer esse vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem esse vínculo objeto; também a produção intelectual de uma pessoa, em si considerada, não é *per se* informação pessoal (embora o fato de sua autoria o seja). Podemos concordar com Pierre Catala, que identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> Mesmo que a pessoa em questão não seja a "autora" da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade.[6]

O Conselho Europeu, por meio da Convenção de Strasbourg, de 1981, ofereceu uma definição que condiz com essa ordem conceitual. Nela, informação pes-

[3] "La informazione come servizio postula l'informazione come bene. L'assenza di tutela degli investimenti nel settore significherebbe creare una zona franca dominata da un precario parassitismo, con grave danno sia per le imprese sia per l'intero sistema, anche istituzionale, che fa perno sulla partecipazione informata." Perlingieri (1990, p. 329).
[4] Limberger (2007, p. 58 ss.).
[5] Rodotà (1973, p. 14).
[6] Catala (1983, p. 20).

soal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação."[7] É explícito, portanto, o mecanismo pelo qual é possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

Em relação à utilização dos termos "dado" e "informação", vale uma especificação. O conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica certa promiscuidade na sua utilização. Ambos os termos servem para representar um fato, determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser considerado.

Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos em um autor que o entende como uma informação em estado potencial, antes de ser transmitida,[8] o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. A doutrina não raro trata estes dois termos – dado e informação – indistintamente, ou então, procede a uma diferenciação algo empírica que merece ao menos ser ressaltada.

Deve-se lembrar ainda que o termo "informação" presta-se igualmente em certos contextos a representar diversas ordens de valores. Assim, a "liberdade de informação" como fundamento de uma imprensa livre, bem como seu correspectivo "direito à informação"[9] podem possuir conteúdo específico e que é mais remotamente relacionado ao tema deste artigo, como no caso do dever de informação pré-contratual do Código de Defesa do Consumidor.

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Com o aludido aumento da importância da informação de uma forma geral, foi justamente em torno dela que a temática da privacidade passou a orbitar, em especial ao se tratar de dados pessoais.[10] Esta guinada, que acabou por plasmar o próprio conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas poderiam ser a concepção de uma *informational privacy* nos Estados Unidos, cujo "núcleo duro" é composto

[7] Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º.
[8] Wacks (1989, p. 25).
[9] Sobre o tema, v. Carvalho (1999).
[10] Sobre o tema, v. Doneda (2006).

pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Federal alemão[11] e a Diretiva 95/46/CE da União Europeia (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), com todas as suas consequências.

O ponto fixo de referência nesse processo é que, entre os novos prismas para enquadrar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias.

Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. Esta vinculação do tratamento de dados pessoais com o controle foi bem caracterizada pelo Ministro Ruy Rosado de Aguiar, ainda em decisão de 1995:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.[12]

[11] A sentença de 15 de dezembro de 1983 do Tribunal Constitucional Federal alemão consolidou a existência de um "direito à autodeterminação informativa" (*informationelle selbstestimmung*), que consistia no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa.

[12] STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.

3 **Desenvolvimento das leis de proteção de dados**

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos e é caso emblemático de uma tendência que, a princípio, parecia apenas destinada a mudar determinado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados.[13] Esse desenvolvimento foi intenso nas cerca de quatro décadas que a disciplina ostenta. A mudança do enfoque dado à proteção de dados nesse período pode ser brevemente entrevista na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger,[14] que vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais.

A primeira dessas quatro gerações de leis[15] era composta por normas que refletiam estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos.[16] Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas. Esta primeira geração de leis vai, aproximadamente, até a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado dessa tecnologia, sem que se soubesse ao certo suas consequências, fez com que se optasse por princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados,[17] além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados. Esse enfoque era natural, visto a motivação dessas leis ter sido a "ameaça" representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática de tais leis era algo tecnocrático e condicionado pela informática – nelas, tratavam-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo.[18]

[13] Piñar Mañas (2005, p. 19-36).
[14] Mayer-Scönberger (1997, p. 219-242).
[15] Exemplo dessas leis de primeira geração são a Lei do *Land* alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados, sueca, que foi o Estatuto para bancos de dados de 1973 – *Data Legen 289,* ou *Datalag*, além do *Privacy Act* norte-americano de 1974.
[16] Sampaio (1997, p. 490).
[17] Cf. Spiros Simitis (1997, p. 565).
[18] Viktor Mayer-Scönberger. General development of data protection in Europe, cit., p. 223-224.

Essas leis de proteção de dados de primeira geração não demoraram muito a se tornar ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento. A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da "diáspora" dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*,[19] além da já mencionada *Bundesdatenschutzgesetz*. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da Lei Francesa).[20]

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 centros de tratamento dos dados pessoais. Assim, criou-se um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela.

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 a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado quanto os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente a sua exclusão de algum aspecto da vida social. Uma terceira geração de leis, surgida na década de 1980, procurou sofisticar a tutela dos dados pessoais, que continuou centrada no cidadão, porém passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera 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 – proporcionando o efetivo exercício da autodeterminação informativa.

A autodeterminação informativa 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 na estrutura dessas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pes-

[19] Lei 78-17 de 6 de janeiro de 1978.

[20] Como representante desta geração de leis, podemos mencionar também a Lei Austríaca (*Datenschutzgesetz* (DSG), Lei de 18 de outubro de 1978, n. 565/1978); além de que as constituições portuguesa e espanhola apontam nesse sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde.

soais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

A autodeterminação informativa era, porém, o privilégio de uma minoria que decidia enfrentar os custos econômicos e sociais do exercício dessas prerrogativas. Verificado esse caráter exclusivista, uma quarta geração de leis de proteção de dados, como as que existem hoje em vários países, surgiu e caracterizou-se por procurar suprir as desvantagens do enfoque individual existente até então. Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Entre as técnicas utilizadas, essas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nessa relação que não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa. Outra técnica é, paradoxalmente, a própria redução do papel da decisão individual de autodeterminação informativa. Isso ocorre por conta do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual – como é o caso para certas modalidades de utilização de dados sensíveis.

Outra característica é a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessária com a diminuição do poder de "barganha" com o indivíduo para a autorização ao processamento de seus dados, e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que um tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas europeias em matéria de proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas.

4 Princípios de proteção de dados pessoais

A aludida "progressão generacional" das leis sobre proteção de dados pessoais faz referência, não por acaso, a uma linguagem própria da informática e exprime a lógica da busca por modelos jurídicos mais ricos e completos.[21] Não obstante essa sua marcada mudança de perfil com os anos, é possível reagrupar materialmente seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em diversos graus em ordenamentos vários – no que podemos verificar uma forte manifestação da convergência das soluções legislativas quanto à matéria em diversos países, bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais.

[21] Cf. Rodotà (1999, p. 103).

Destes princípios, alguns se encontram já presentes nas leis de primeira e segunda geração, desenvolvidos pelas leis posteriores. Uma busca mais larga poderá, porém, retraçar suas origens em uma série de discussões que, na segunda metade da década de 1960, acompanhou a tentativa do estabelecimento do *National Data Center*, que consistiria basicamente em um gigantesco e jamais realizado banco de dados sobre os cidadãos norte-americanos para uso da administração federal.[22]

Após o fracasso da tentativa de instituição deste banco de dados centralizado, vários dos temas que foram levantados em meio à discussão sobre sua possibilidade continuaram a ser desenvolvidos, pois se o *National Data Center* particularmente não vingou, a realidade era que muitos outros bancos de dados pessoais de menor âmbito iam se estruturando. Uma das áreas na qual essa discussão ecoou com maior força foi a da saúde, pela justificada preocupação com o tratamento de dados médicos por sistemas informatizados. No início da década de 1970, a *Secretary for health, education and welfare* reuniu uma comissão de especialistas que divulgou, em 1973, um estudo que concluiu pela relação direta entre a privacidade e os tratamentos de dados pessoais, além da necessidade de estabelecer a regra do controle sobre as próprias informações:

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei.[23]

Uma concepção como esta requer que sejam estabelecidos meios de garantia para o cidadão, que efetivamente vieram descritos como:

> - Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.

[22] O *National Data Center* foi projetado para reunir as informações sobre os cidadãos norte-americanos disponíveis em diversos órgãos da administração federal em um único banco de dados – a partir de um projeto original, que pretendia unificar os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Garfinkel (2000, p. 13). Após acirradas discussões sobre a ameaça potencial que representaria às liberdade individuais, o governo norte-americano desistiu do projeto. V. Miller (1971).
[23] EUA (1973).

> - Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.
> - Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.
> - Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve toar as devidas precauções para evitar o mau uso destes dados.[24]

Tais regras, de caráter marcantemente procedimental,[25] apresentaram um conjunto de medidas que passou a ser encontrado em várias normativas sobre proteção de dados pessoais, às quais se passou a referir como *Fair Information Principles*. Esse "núcleo comum" encontrou expressão como um conjunto de princípios a serem aplicados na proteção de dados pessoais principalmente com a Convenção de Strasbourg[26] e nas *Guidelines* da OCDE,[27] no início da década de 1980. É possível elaborar uma síntese destes princípios:[28]

a) *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
b) *Princípio da exatidão*: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
c) *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
d) *Princípio do livre acesso*, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter có-

[24] Idem.
[25] Assim enquadrariam-se com maior facilidade no espírito da cláusula do *due process* norte-americano. Bennett (1992, p. 98).
[26] Convenção nº 108 do Conselho Europeu – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.
[27] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, disponível em: <www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. Estes princípios seriam: (1) collection limitation principle; (2) data limitation principle; (3) purpose specification principle; (4) use limitation principle; (5) security safeguard principle; (6) openness principle; (7) individual participation principle. Wuermeling (1996, p. 416).
[28] Cf. Stefano Rodotà. *Repertorio di fine secolo*, cit. p. 62. José Adércio L. Sampaio. *Direito à intimidade e à vida privada*. cit., p. 509 ss.

pias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;

e) *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos. Alguns países que sofreram uma mudança de regime político que lhes proporcionou a reelaboração de suas cartas fundamentais foram os primeiros nos quais foi possível observar uma tendência à consideração da problemática relacionada à informática e à informação pessoal em nível constitucional. Nesse sentido, nas Constituições da Espanha[29] e de Portugal[30] se encontram dispositivos destinados a afrontar os problemas da utilização da informática, e, no caso da Constituição portuguesa, uma referência explícita à proteção de dados pessoais.

[29] A Constituição Espanhola de 1978 contém os seguintes dispositivos:
Art. 18. – [...] 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
[...] Art. 105. – [...] b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

[30] A Constituição Portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:
"Artigo 35. (Utilização da informática)
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

É possível considerar a Convenção de Strasbourg como o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais. Em seu preâmbulo, a convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao artigo 8º da Convenção Europeia para os Direitos do Homem.[31] Posteriormente, também transparece, com clareza, presença dos direitos fundamentais na Diretiva 95/46/CE sobre proteção de dados pessoais na União Europeia.[32] Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

O documento europeu que levou mais adiante essa sistemática foi, certamente, a Carta dos Direitos Fundamentais da União Europeia, proclamada em 7 de dezembro de 2000. Seu artigo 8º, que trata da "proteção de dados pessoais", inspira-se no artigo 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286º do tratado instituidor da União Europeia.[33] Não obstante, nota-se um duplo matiz: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio mediante o estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais.[34]

---

[31] Cujo teor é o seguinte:
1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

[32] Mencione-se, de passagem, que a expressão "direitos fundamentais" é evocada por seis vezes nas considerações iniciais da Diretiva.

[33] De seguinte teor:
"Artigo 286º.
1. A partir de 1 de Janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.
2. Antes da data prevista no nº. 1, o Conselho, deliberando nos termos do artigo 251º., criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adoptará as demais disposições que se afigurem adequadas".

[34] Este caráter levou alguns autores a desencorajarem a leitura da diretiva em chave de direitos fundamentais do homem em relação à informação pessoal, apesar de reconhecerem que, "dal punto di vista più genuinamente privatistico, non v'è dubbio che la direttiva [...] sia destinata a diventare un punto di riferimento fondamentale nella ricostruzione sistematica dei diritti della personalità, almeno nella misura in cui il concetto di personalità si trovi a far i conti con la realtà informatica e telematica". v. Francesco Macario." (MACARIO, 1997, p. 8-9).

5 **Proteção de dados no ordenamento brasileiro**

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

A bem da verdade, pode-se encontrar uma menção ao caráter de direito fundamental da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo Governo Brasileiro em 15 de novembro de 2003. No item 45 da referida Declaração lê-se que:

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.

A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão[35] e do direito à informação,[36] que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de *habeas data* (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro.[37]

[35] Constituição Brasileira, art. 5º, IX; art. 220.
[36] Constituição Brasileira, art. 5º, XIV; art. 220; incluindo o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos (art. 5º, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5º, XXXIV).
[37] Cf. Carvalho (2003, p. 77-119).

O *habeas data*, instituto que no direito brasileiro tem a forma de uma ação constitucional, foi introduzido pela Constituição de 1988.[38] Com um *nomen iuris* original, introduziu em nosso ordenamento o direito de acesso, carregando consigo algo da carga semântica do *habeas corpus*. A sua influência em outras legislações latino-americanas chegou a provocar a discussão sobre a existência de um modelo de proteção de dados que circule dentro do subcontinente.[39]

Cabe ressaltar que o *habeas data* brasileiro surgiu basicamente como um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e sem maiores vínculos, portanto, com uma eventual influência da experiência europeia ou norte-americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época.

Posteriormente o *habeas data* foi regulamentado pela Lei 9.507, de 1997. A ação de *habeas data* visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente. Por meio dela, o cidadão pode acessar e retificar seus dados pessoais em bancos de dados "de entidades governamentais ou de caráter público" (posteriormente ampliou-se o sentido deste "caráter público", incluindo-se os bancos de dados referentes a consumidores, mesmo que administrados por privados). A ação não é acompanhada, porém, de instrumentos que possam torná-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais: além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, algo que se percebe em vários dos seus pontos estruturais, como a necessidade de sua interposição por meio de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados, ela é, substancialmente, um instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação. Não surpreende, portanto, que desde certo tempo a doutrina brasileira tenha assumido posição majoritariamente crítica em relação à ação, tratando-a ora como "um remédio de valia, no fundo, essencialmente simbólica", para Luís Roberto Barroso,[40] ora como "uma ação voltada para o passado", para Dalmo de Abreu Dallari.[41]

Parece existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais.

[38] Constituição Federal, art. 5º, LXXII:
"Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes 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."
[39] Sobre o tema, Puccinelli (1999).
[40] Barroso (1998, p. 212).
[41] Dallari (1997, p. 100).

Uma determinada leitura da sistemática da Constituição Brasileira parece encorajar essa perspectiva. Nela, a proteção da privacidade (por intermédio da menção à inviolabilidade da intimidade e da vida privada) encontra-se em um dispositivo (art. 5º, X), enquanto que outro dispositivo se refere à inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." (art. 5º, XII).

Tal técnica legislativa acabou por fundamentar uma interpretação no mínimo temerosa no que diz respeito à matéria: se, por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme o art. 5º, XII, que trata da inviolabilidade da comunicação de dados.

Tal interpretação, além de dissonante com a visão segundo a qual privacidade e informações pessoais são temas sempre mais relacionados e, em muitas ocasiões, quase que indistinguíveis entre si – conforme atesta o mencionado desenvolvimento de leis que tratam da proteção de dados pessoais e também os documentos transnacionais que associam o caráter de direito fundamental à proteção de dados pessoais –, traz consigo o enorme risco de acabar por se tornar uma norma que sugere uma grande permissividade em relação à utilização de informações pessoais.

Nesse sentido, recentemente, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais, endossando tese de Tércio Sampaio Ferraz Júnior, segundo a qual o ordenamento brasileiro tutelaria o sigilo das comunicações – e não dos dados em si.[42] Nesta decisão fica saliente a dificuldade em tratar do tema da infor-

[42] "Em primeiro lugar, a expressão 'dados' manifesta uma certa impropriedade (BASTOS; GANDRA, 1989, p. 73). Os citados autores reconhecem que por "dados" não se entende o objeto de comunicação, mas uma modalidade tecnológica de comunicação. Clara, nesse sentido, a observação de Manoel Gonçalves Ferreira Filho (1990, p. 38).— "Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. Os dados aqui são os dados informáticos (v. incs. XIV e LXXII)." A interpretação faz sentido. O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isso é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." Note-se, para a caracterização dos blocos, que a conjunção e uma correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que deveria ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo. Mas, se alguém entra nessa transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitima-

mação pessoal de forma diversa daquela binária – sigilo/abertura, público/privado – de forma que reflita a complexidade da matéria da informação.

A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a corrente mencionada, gozariam de uma proteção mais tênue. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar novamente o quanto hoje em dias as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas mediante a representação de sua personalidade, fornecida pelos seus dados pessoais, aprofundando ainda mais a íntima relação entre tais dados e a própria identidade e personalidade de cada um de nós.

Apenas sob o paradigma da interceptação, da escuta, do grampo – situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.

O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente o favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, ou seja, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa na vicissitudes da Sociedade da Informação.

Referências

BARROSO, Luís Roberto. Viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvim (Coord.). *Habeas data*. São Paulo: RT, 1998.

BENNETT, Colin. *Regulating privacy. Data protection and public policy in Europe and UnitedStates*. Itahaca: Cornell University Press, 1992.

BRASIL. *Constituição*: República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. *Diário da Justiça*, Brasília, DF, 20 mar. 1995.

mente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-lo! (FERRAZ JÚNIOR, 1993, p. 447).

CASTELLS, Manuel. *A sociedade em rede (A era da informação, economia, sociedade e cultura*). São Paulo: Paz e Terra, 1999. v. 1.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional. *Revista de Direito do Consumidor*, n. 46, p. 77-119, abr./jun. 2003.

CARVALHO, Luis Gustavo Grandinetti de. *Direito de Informação e Liberdade de Expressão*. Rio de Janeiro: Renovar, 1999.

CATALA, Pierre. Ebauche d' une théorie juridique de l'information. *Informatica e Dirito*, ano 9, p. 20, janv./avril 1983.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. *Revista de la Faculdade de derecho de La Pontifícia Universidade Católica del Peru*, n. 51, p. 100, 1997.

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

EUA. *Records, computers and the rights of citizens*. Reporto f the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*. 1993. v. 88.

GARFINKEL, Simson. *Database nation*. Sebastopol: O'Reillly, 2000.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*. Porto Alegre: Livraria do Advogado, 2007.

LYON, David. The roots of the information society Idea. In: O'SULLIVAN, Tim; JEWKES, Yvonne (Ed.). *The media studies reader*. London: Arnold, 1998.

MACARIO, Francesco. La protezione dei dati personali nel diritto privato europeo. In: CUFFARO, Vicenzo; RICCIUTO, Vicenzo. *La disciplina Del trattamento dei dati personali. Giappechelli*, 1997.

MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997.

MILLER, Arthur. *Assault on privacy*. Ann Arbor: University of Michigan, 1971.

PERLINGIERI, Pietro. L' informazione come bene giuridico. In: *Rassegna di diritto civile*. 2/90, p. 329.

PINÃR MAÑAS, José Luis. El derecho fundamental a la protección de dados personales (LOPD). In: _____ (Dir.). *Protección de datos de carácter personal en Iberoamérica*. Valencia: Tirant Lo Blanch, 2005.

PUCCINELLI, Oscar. *El habeas data em Indoiberoamérica*. Bogotá: Temis, 1999.

RODOTÀ, Stefano. *Elaboratori elettronici e controllo sociale*. Bologna: II Mulino, 1973.

_____. *Repentino di fine secolo*. Bari: Laterza, 1999.

SAMPAIO, José Adércio Leite Sampaio. *Direito à intimidade e à vida privada*. Belo Horizonte: Del Rey, 1997.

SIMITIS, Spiros. Il contesto giuridico e político della tutela della privacy. *Rivista Critica Del Diritto Privato*, 1997.

WACKS, Raymond. *Personal information*. Oxford: Clarendon Press, 1989.

WUERMELING, Ulrich. Harmonization of European Union Privacy Law. In: *14 John Marshall Journal of Computer & Information Law 411*, 1996.

Recebido em 18 de agosto de 2011
Aceito em 13 de setembro de 2011