PATRICIA ELIANE DA ROSA SARDETO

TRATAMENTO INFORMATIZADO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE

Florianópolis
2004

PATRICIA ELIANE DA ROSA SARDETO

TRATAMENTO INFORMATIZADO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE

Dissertação apresentada ao Curso de Pós-graduação em Direito da Universidade Federal de Santa Catarina, como requisito à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Aires José Rover.

Florianópolis
2004

COMISSÃO EXAMINADORA

_____

_____

_____

Florianópolis, ____ de _____ de 2004.

DEDICATÓRIA

Dedico este trabalho a Deus, por sua inspiração divina, ao meu esposo Marcelo e toda minha família, pelo apoio e compreensão e ao meu filho Luis Felipe, pelo presente que foi sua chegada.

AGRADECIMENTOS

Ao Dr. Aires José Rover, pela orientação paciente e compreensiva, pelos ensinamentos compartilhados e pela eterna amizade.

Aos professores, pela visão crítica de seu ensinamento jurídico.

Aos meus colegas de curso, pelo compartilhar de idéias, sempre tão instigadoras, e pelos bons momentos que passamos juntos.

À Camila e Cláudia, por toda hospitalidade e carinho com que me acolheram em Florianópolis.

Por fim, à minha mãe, pela disponibilidade em passar horas agradáveis com o neto, sem a qual não seria possível o término desta.

SUMÁRIO

SARDETO, Patricia Eliane da Rosa. ***Tratamento informatizado de dados pessoais e o direito à privacidade***. 2004. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis.

RESUMO

O presente trabalho teve por escopo traçar um panorama legal e doutrinário a respeito da proteção conferida aos dados pessoais no estrangeiro e no Brasil. Investigar a influência da tecnologia na sociedade e as implicações da denominada sociedade informacional. Analisar a informatização de dados e seu tratamento. Contextualizar a privacidade na atual sociedade, acompanhando sua evolução conceitual. Desmistificar o aparente paradoxo entre privacidade e liberdade. Constatar a natureza e a extensão da tutela jurídica estrangeira ao titular de dados pessoais. Apresentar o direito à privacidade como via assecuratória dos dados pessoais no Brasil, enquanto não se elabora legislação específica. Constatou-se a necessidade de elaboração de lei relativa à proteção de dados pessoais, embora o Brasil tenha condições de assegurar proteção ao titular de dados pela invocação do direito à privacidade, previsto na Constituição Federal e no Código Civil.

Palavras-chave: informatização e tratamento de dados; proteção aos dados pessoais no Brasil; direito à privacidade.

SARDETO, Patricia Eliane da Rosa. ***Automatisierte Datenverarbeitung und das Privatheitsrecht***. 2004. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis.

ZUSAMMENFASSUNG

Das Anliegen dieser Arbeit ist es, eine gesetzliche und grundsätzliche Übersicht über den Datenschutz im In- und Ausland zu zeichnen. Den Einfluss der Technologie in der Gesellschaft erforschen und die Folgen der sogenannten informationellen Gesellschaft ergründen. Informatizierung und Verarbeitung von Daten analysieren. Den Kontext darstellen zwischen Privatheit in der heutigen Gesellschaft, begleitet von der begrifflichen Entwickung. Das scheinbare Paradox zwischen Privatheit und Freiheit entmystifizieren. Das Wesen und das Ausmass der juristischen ausländischen Unterstützung der Betroffenen der Personaldaten in Brasilien darstellen, solange kein spezifisches Gesetz verabschiedet ist. Es wurde die Dringlichkeit eines Gesetzesentwurfes für den Datenschutz festgestellt, obwohl es in Brasilien möglich ist, die Personaldaten der Betroffenen zu schützen, wie es in der Verfassung und Grundgesetz vorgesehen ist.

Schlussworte: Informatizierung und Verarbeitung von Daten; Datenschutz in Brasilien; Privatheitsrecht

INTRODUÇÃO

O tratamento informatizado de dados pessoais constitui tema extremamente atual, porém ainda pouco desenvolvido pela doutrina pátria, encontrando-se apenas uma ou outra abordagem de forma isolada.

Diante dessa lacuna doutrinária e da relevância do assunto o presente trabalho se propõe a verificar se, mesmo diante da ausência de regulamentação específica relativa ao tratamento informatizado de dados pessoais, estes podem ser protegidos invocando-se o direito à privacidade.

Para tanto, lançou-se mão do método dedutivo, à medida que partiu-se de um contexto amplo, representado pelo ordenamento jurídico europeu, para se chegar a análise da proteção conferida pelo Brasil ao titular de dados.

Primeiramente incursiona-se na denominada *sociedade informacional*, procurando desvendar as características dessa sociedade, a influência exercida pelas tecnologias da informação em seu seio e o valor atribuído à informação a partir dos dados pessoais. A crescente informatização ocorrida tanto no setor público quanto privado tem contribuído para a dissiminação desenfreada do tratamento de dados pessoais, sem que o direito consiga acompanhar seu ritmo.

Talvez um dos maiores problemas com relação à proteção dos dados pessoais esteja justamente centrado na possibilidade indiscriminada de sua recolha. Isso porque, as tecnologias existentes capacitam o interessado a coletar os dados pessoais que lhe interessam, sem que o titular desses dados tenha ciência de tal prática invasiva.

Não apenas a coleta indiscriminada de dados pessoais merece atenção especial, senão que também a Internet, com toda sua potencialidade lesiva.

A par desse cenário, é natural que os estudiosos do Direito venham buscando regulamentar o tratamento de dados pessoais, de forma a conferir ao seu titular, ao menos, a observância de seu direito à privacidade. Há cerca de três décadas o ordenamento jurídico estrangeiro já se encontra trilhando esse caminho de regulamentação, pelo que é indispensável lançar um olhar sobre o que já se tem. Essa é a proposta do segundo capítulo ao relatar a origem e evolução da tutela jurídica no direito internacional, destacando o posicionamento de alguns países da União Européia e ainda dos Estados Unidos, bem como incursionando pelo direito pátrio e identificando alguns institutos que, de certa forma, garantem a proteção do titular de dados pessoais.

Porém, a existência de certas previsões legais no direito pátrio não garantem, de forma eficiente, o titular de dados pessoais contra a violação de sua privacidade, de modo que é o direito à privacidade que tem esse grande desafio. Assim, primeiramente se busca conceituar esse direito, analisando sua evolução em face da evolução tecnológica e determinando sua abrangência, para depois situá-lo no rol dos direitos fundamentais, destacando sua plena eficácia.

A questão última que se aventa é a possível colisão entre os diretos fundamentais, haja vista ser a Constituição do Brasil uma constituição pluralista, abarcando diversos interesses.

Em que pese o desejo de estender a pesquisa e tornar o conteúdo desse trabalho mais completo, a ainda incipiente literatura a respeito dificultou seu aprofundamento. Porém, o objetivo primeiro – despertar o leitor para a importância do tema e a possibilidade de invocação do direito à privacidade na proteção dos dados pessoais – espera-se, tenha sido atingido.

1 A SOCIEDADE INFORMACIONAL E O TRATAMENTO INFORMATIZADO DE DADOS PESSOAIS

Diante dos avanços tecnológicos, principalmente das tecnologias da informação, cresce a necessidade de se compreender a extensão do fenômeno informacional, em especial sua penetrabilidade na sociedade, bem como o grau de importância conferido à informação por esta sociedade informacional.

1.1 A sociedade informacional e suas características

Freqüentemente a inovação tecnológica é considerada a responsável pelas mudanças sociais, chegando até mesmo a identificar determinados períodos da história. Assim ocorreu com a sociedade comercial, a sociedade industrial e atualmente com a sociedade informacional[1].

[1] Antes da Sociedade informacional é possível identificar, seguindo o raciocínio de Peter Drucker, uma sociedade comercial, desencadeada pela Revolução Comercial em meados do século XVII e que prosseguiu até o início do século XVIII, e uma sociedade industrial, desencadeada pela Revolução Industrial em meados do século XVIII e ganhando novo impulso por volta do ano de 1870 quando novas indústrias foram criadas empregando um tipo diferente de força motriz e fabricando produtos novos e em grande quantidade, como a indústria química e farmacêutica, automotiva, de produtos eletrônicos, dentre outras. (DRUCKER, 2001, p. 168)

Em que pese a enorme influência da tecnologia sobre a sociedade é preciso registrar que a tecnologia não é o único fator a ensejar mudanças, sob pena de se cair no determinismo tecnológico.[2]

Porém, em função de sua relevância, o paradigma tecnológico - propulsor da sociedade informacional - merece destaque, pois concretizou um novo estilo de produção, comunicação, gerenciamento e vida. Organizado com base nas tecnologias da informação[3], o novo paradigma surgiu na década de 1970[4] nos Estados Unidos e vem crescendo de forma exponencial, segundo Castells (2003, p. 68), em razão de sua capacidade de criar uma interface entre campos tecnológicos mediante uma linguagem digital comum na qual a informação é gerada, armazenada, recuperada, processada e transmitida.

Aliás, é justamente a aplicação dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação que caracteriza a atual revolução tecnológica, e não a centralidade de conhecimentos e informação.[5]

Drummond (2003, p. 2), alheio à justificativa de Castells, se insurge contra a denominação de *sociedade da informação ou informacional,* registrando que embora o acesso à informação nunca tenha sido tão grande e tão facilitado, tal fato não é suficiente para emprestar o nome à atual sociedade. Prefere denominá-la

[2] Castells (2003, p.43) vai além para afirmar, que a tecnologia não determina a sociedade e nem a sociedade escreve o curso da transformação tecnológica, uma vez que vários são os fatores envolvidos no processo.

[3] As tecnologias da informação compreendem as tecnologias em microeletrônica, computação (hardware e software), telecomunicações/radiodifusão, optoeletrônica e engenharia genética.

[4] Em 1971 foi inventado o microprocessador (principal dispositivo de difusão da microeletrônica); em 1975 o microcomputador; e em 1977 foi introduzido o primeiro microcomputador comercial de sucesso, o Apple II, e a Microsoft começava a produzir sistemas operacionais para microcomputadores.

[5] Para Castells as novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos, tanto que usuários e criadores podem tornar-se a mesma coisa.

de *sociedade tecno-comunicacional*, primeiro porque o que circula na rede Internet e através de outras mídias e/ou modalidades de comunicação, não é necessariamente informação, mas sim, comunicação e segundo porque as novas tecnologias não carregam, em si mesmas, tamanha quantidade de informação suficiente para nomear o novo paradigma de nova sociedade da informação.

A justificativa de Drummond é válida à medida que se insurge à pretensão de algumas denominações e suas conseqüentes teorias, que atribuem à informação a exclusividade na construção/caracterização dessa nova sociedade em formação, não sendo esta porém, a posição que ora se defende, haja vista a convicção, na linha de Castells, da existência de outros fatores, igualmente relevantes, a contribuírem para o surgimento e desenvolvimento da sociedade informacional.

Castells (2003, p. 51), ao fundamentar a existência da sociedade informacional, não de uma, mas de várias, afirma que as sociedades podem ser caracterizadas ao longo de dois eixos, os modos de produção (capitalismo e estatismo) e os modos de desenvolvimento (industrialismo e informacionalismo) e que "a nova estrutura social está associada ao surgimento de um novo modo de desenvolvimento, o informacionalismo, historicamente moldado pela reestruturação do modo capitalista de produção, no final do século XX". E esclarece

> *No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. (CASTELLS, 2003, p. 53)*

O informacionalismo, nos moldes traçados por Castells, é que fundamenta a tese da existência de uma sociedade informacional, onde o termo informacional pretende indicar o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas no período histórico atual.

Ainda segundo o autor o conteúdo real da sociedade informacional precisa ser determinado pela observação e análise, restando evidente, no entanto, que umas das características principais dessa sociedade é a lógica de sua estrutura básica em redes (daí o emprego da denominação “sociedade em rede”), bem como a presença dos movimentos sociais e do Estado.

Aliás a presença do Estado tem grande relevância no destino de uma sociedade, uma vez que este pode tanto promover o desenvolvimento quanto a estagnação tecnológica e conseqüentemente possibilitar ou não o acesso de seus cidadãos às inovações tecnológicas e à inserção no futuro informacional.

Nesse sentido Castells bem resume o papel desempenhado pelo Estado

> *De um lado, o Estado pode ser, e sempre foi ao longo da história, na China e em outros países, a principal força de inovação tecnológica; de outro, exatamente por isso, quando o Estado afasta totalmente seus interesses do desenvolvimento tecnológico ou se torna incapaz de promovê-lo sob novas condições, um modelo estatista de inovação leva à estagnação por causa da esterelização da energia inovadora autônoma da sociedade para criar e aplicar tecnologia. (CASTELLS, 2003, p.47)*

Tal constatação acerca do papel do Estado bem se comprova pela postura do governo norte-americano, que é um excelente exemplo de incentivo às

inovações tecnológicas no campo da tecnologia da informação. Desde o princípio o Estado patrocinou as pesquisas da ARPA (Agência de Projetos de Pesquisa Avançada) do Departamento de Defesa dos Estados Unidos, que acabaram por possibilitar a criação da Internet, e fomentou as pesquisas acadêmicas, formando um corpo de pesquisadores especializados[6].

De outro lado, a postura do Brasil, por exemplo, que fechou-se à concorrência internacional em fins da década de 80 e início da década de 90, sem contar com qualquer infraestrutura a fornecer aporte à indústria nacional de hardware e software. A conseqüência desta postura política do Estado brasileiro foi, sem dúvida, um hiato, uma descontinuidade no desenvolvimento tecnológico do país. Com muito custo o país tem procurado compensar a desvantagem tecnológica, porém um grande empecilho ainda é a falta de prioridade no setor educacional.

Além de possibilitar uma infra-estrutura tecnológica mínima - sistemas de comunicação e informática acessíveis, de baixo custo e de alta qualidade -, o Estado tem a responsabilidade e a obrigação de fomentar a educação em todos os níveis, a fim de garantir a formação de recursos humanos. Apenas uma sociedade que prioriza a educação terá futuro num mundo onde a informação e seu processamento são cruciais ao desenvolvimento.

1.2 O valor da informação a partir dos dados pessoais

[6] Em 1990, dados coletados pela UNESCO informavam que os recursos humanos científicos e técnicos, proporcionalmente à população, eram 15 vezes maiores na América do Norte do que o nível médio nos países em desenvolvimento e que os gastos com P&D na América do Norte representavam mais de 42% do total mundial, ao passo que os gastos na América Latina e na África, somados, atingiam um total inferior a 1% do mesmo total. (Castells, 2003, p. 175)

A par das peculiaridades da sociedade informacional é fácil constatar que informações são mercadoria de valor, sobre a qual as tecnologias disponíveis se debruçam. As pessoas (umas mais, outras menos) já sentem os efeitos (benéficos e maléficos) da utilização em larga escala das informações, e a velocidade com que estas se processam, revela a eficiência da lógica de rede.

Castells (2003, p. 108), ao tratar das características do novo paradigma tecnológico – a tecnologia da informação – sustenta que a informação é a sua matéria-prima, de forma que as tecnologias agem sobre a informação e não apenas a informação para agir sobre a tecnologia, como nas revoluções tecnológicas anteriores.

Tanto isso é verdade que a atividade comercial já se encontra extremamente dependente das informações fornecidas por grandes bancos de dados de consumidores, disponíveis em serviços como o SCPC (Serviço Central de Proteção ao Crédito) no Brasil, da mesma forma que a Administração Pública, o Estado e os cidadãos dependem de informações para implementação das políticas públicas, garantia da ordem pública e exercício da cidadania, respectivamente.

Os serviços, de uma forma geral, encontram-se automatizados e *on line,* e oferecem comodidade e agilidade ao usuário, necessitando apenas que este municie seu banco de dados com algumas informações, ou mais precisamente, com alguns dados. Tecnicamente os conceitos de informação e dado são distintos.

Segundo esclarece Stair (1998, p. 4), *informação* “é um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor do fato em si”. Daí a grande quantidade de dados que as pessoas são, diariamente, solicitadas

a fornecer, pois quanto maior o número de dados pessoais, melhor a informação obtida e consequentemente mais valiosa.

Por sua vez, Stair (1998, p.4) completa definindo *dados* como “os fatos em sua forma primária, como por exemplo, o nome de um empregado e o número de horas trabalhadas em uma semana, números de peças em estoque, ou pedidos de venda”. Sendo fatos, os dados apenas terão valor se organizados ou arranjados de uma maneira significativa, a fim de se tornarem uma informação.

Daí a incessante busca pela coleta de dados pessoais, pois a informação obtida com o tratamento desses dados fornece inúmeras possibilidades ao seu detentor, tanto lícitas quanto ilícitas.

A par destes dois conceitos preliminares é possível, com base em algumas regulamentações acerca da proteção de dados pessoais, identificar alguns elementos essenciais a definição de dados pessoais. Em que pese a versão de língua portuguesa da Diretiva[7] 95/46/CE da União Européia (2003a), definir em seu art. 2º, “a”, dados pessoais como “qualquer informação relativa a uma pessoa singular identificada ou identificável[8]”, trazendo como sinônimas as expressões dados e informações, deve-se entender o sentido do termo informações de forma genérica, como fatos ou indicações, e não propriamente no sentido técnico, de produto final obtido pela organização e relação dos fatos, como anteriormente exposto.

[7] As Diretivas são espécies normativas gerais da União Européia, que precisam ser transpostas para o direito nacional.

[8] Identificável é todo aquele que possa ser identificado, direta ou indiretamente, por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Pode-se retirar desta definição, que por sinal é bastante abrangente, pois admite que qualquer informação deva ser considerada como um dado pessoal, desde que se refira a uma pessoa identificada ou passível de identificação, três elementos básicos, a saber, *a admissibilidade de qualquer tipo de informação, o caráter personalíssimo dos dados* e *a identificabilidade/determinabilidade do titular dos dados*.

A admissibilidade de qualquer tipo de informação, não importando sua natureza, se decorrente de circunstância objetiva ou subjetiva, bem como o suporte mediante o qual é coletada, impede que a proteção aos dados pessoais seja limitada. O caráter personalíssimo dos dados está a indicar que se tratam de dados pessoais, ou seja, referente a um indivíduo, um ser humano. A identificabilidade ou determinabilidade do titular dos dados revela a possibilidade, perfeitamente viável diante dos avanços tecnológicos, de se identificar uma pessoa através de uma informação que a princípio não ensejaria sua identificação, como por exemplo, um número de telefone, uma placa de automóvel, um endereço de e-mail, o DNA ou a impressão digital.

Seguindo a orientação da Diretiva, a lei portuguesa de proteção de dados (Lei 67/98), em seu art. 3º, "a", define *dados pessoais* como "qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (titular de dados)". Já a lei alemã de proteção de dados, em seu art. 3º, 1, define

como “indicações individuais sobre circunstâncias subjetivas ou objetivas de uma pessoa física determinada ou determinável (titular de dados)[9]”.

Sendo assim, é possível se conceituar dados pessoais como todo tipo de indicação, independentemente de sua natureza e do suporte mediante o qual é coletada, de caráter personalíssimo e passível de identificar o titular de dados[10].

Os dados pessoais ainda comportam uma espécie que é a dos dados pessoais sensíveis, prevista também nas legislações citadas. A Diretiva os enumera no n. 1, do art. 8º, como aqueles dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical e relativos à saúde e à vida sexual. A lei portuguesa faz sua previsão no art. 7º, ampliando seu rol para prever também aqueles referentes à filiação partidária, vida privada, bem como os dados genéticos.

A par dessas noções, a classificação proposta por Bautista, citado por Carvalho, é bastante ilustrativa. Bautista classifica os dados em três graus diferentes, em função do grau de intimidade envolvido.

> *1. os considerados indiferentes; 2. os sensíveis em relação a um contexto; e 3. os sensíveis por si mesmos. Entre os indiferentes estão o nome, sobrenome, idade, profissão, domicílio, data de nascimento, sexo, grau de escolaridade, etc, que são normalmente fornecidos e têm reduzida potencialidade de causar qualquer dano. Os sensíveis em um determinado contexto são os tributários, situação financeira, dados clínicos, que, de acordo com o modo de utilização, podem se tornar mais ou menos sensíveis. Os dados sensíveis pela sua natureza são os relacionados a opiniões políticas, crenças religiosas, vida sexual, condenações reabilitadas, origem racial, que representam sério risco de dano aos direitos da personalidade. Geralmente os dados sensíveis pela sua natureza não podem constar de bancos de dados. Os indiferentes, ao*

[9] “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältinisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffner)”.

[10] Castro (2004) os define como toda informação (ainda que anônima) com a qual se possa, através de associações e cruzamento de dados, identificar-se uma pessoa, como, por exemplo, o DNA, a impressão digital, ou dados incompletos de um indivíduo.

> *contrário, escapam de qualquer controle pela banalização de sua utilização. Os contextualmente sensíveis normalmente só podem ser utilizados para determinado fim legítimo. (BAUTISTA apud CARVALHO, 1999, p. 119)*

Embora Carvalho sustente que os dados considerados indiferentes escapam de qualquer controle – e em certa medida é possível concordar com essa afirmação – algumas considerações são necessárias. É certo que dados como nome, sobrenome, idade, profissão, domicílio, data de nascimento e sexo são constantemente requisitados ao seu titular diante das mais variadas situações do dia-a-dia e por isso mesmo fornecidos com muita naturalidade.

É utópico pensar que nos dias atuais qualquer pessoa possa relacionar-se em sociedade sem partilhar alguns de seus dados pessoais. Portanto, o fornecimento ou a disponibilização de alguns dados pessoais é questão de sobrevivência, pois “somos aquilo que nossos dados dizem de nós”.

No entanto, é perigoso afirmar que esses dados tidos como indiferentes escapam de qualquer controle. A possibilidade de violação da privacidade de seu titular existe, embora bem mais reduzida, de modo que há a necessidade de certo controle sobre esses dados. Primeiramente o próprio titular deve se precaver, fornecendo apenas os dados realmente necessários e solicitando informações a respeito de sua destinação. Em segundo lugar compete aos órgãos de controle ou ao Judiciário fiscalizar e punir a comercialização de bancos de dados.

1.3 A informatização de dados e seu tratamento

A evolução tecnológica experimentada pela humanidade nas últimas décadas foi fantástica. Desde o surgimento do primeiro computador eletrônico em

1946, conhecido como ENIAC (Eletronic Numerical Integrator and Calculator), que possuía aproximadamente 18 mil válvulas, pesava 30 toneladas e chegava a consumir 150 KWs, até a popularização dos computadores pessoais (Personal Computer – PC), que teve grande impulso em 1981 com o lançamento do PC da IBM, menos de quatro décadas se passaram. As duas décadas seguintes só aumentaram o potencial dos computadores e fizeram da informática[11] uma companheira do dia-a-dia.

Castells (2003, p. 304), analisando o processo de trabalho no paradigma informacional, constata que o amadurecimento da revolução das tecnologias da informação na década de 1990 transformou o processo de trabalho, quando então as máquinas baseadas em microeletrônica já se encontravam introduzidas nas indústrias e os computadores em rede difundiram-se pelas atividades relacionadas a processamento da informação. Ou seja, indústrias e prestação de serviços se rendiam à informatização.

Assim é que o fenômeno da informatização vem ganhando cada vez mais espaço na sociedade atual, ao passo de ser inconcebível, hoje, uma grande empresa, um governo, uma escola, que não esteja informatizada, para citar apenas alguns exemplos. Informatizar virou sinônimo de eficiência gerencial, redução de custos, maior produtividade, maior e melhor controle sobre as operações desenvolvidas e maior precisão.

[11] É a ciência do tratamento lógico e automático da informação entendida, esta última, como suporte dos conhecimentos e das comunicações. Sua parte mais visível são os computadores, mas a informática está presente também no estudo e desenvolvimento de softwares, equipamentos periféricos de entrada e saída de informação, robôs, linguagens e técnicas de programação, microeletrônica e todas as aplicações que de alguma forma fazem o tratamento automático da informação, de componentes para cafeteiras elétricas a equipamentos de bordo de aviões.

Alimentar, com dados, os milhares de computadores distribuídos pelo mundo é a grande prioridade do homem no momento, bem como transformar esses dados em informação diferenciada e conseqüentemente valiosa[12]. Stair constata tal fenômeno assim consignando

> *Todos os dias somos solicitados a divulgar dados sobre nós mesmos. Na maioria das vezes, o fazemos sem pensar duas vezes. Aceitamos a solicitação como necessária, e, mais importante, os dados serão usados apenas para a finalidade para a qual foram fornecidos. O que não conseguimos perceber é que, atualmente, mais do que nunca, nossos dados estão sendo processados e compartilhados, muitos deles sem a nossa permissão ou conhecimento. As empresas descobriram que a venda de dados é um negócio lucrativo. Infelizmente, os dados que elas vendem são nossos. Dados demográficos, sobre tendências de compras e preferências pessoais tornaram-se valiosos para as organizações que tentam vender seus produtos em um mercado altamente competitivo. Por esta razão, a indústria de dados é muito lucrativa. (STAIR, 1998, p. 112)*

Para tanto, a utilidade dos bancos de dados[13] informatizados é notória. Através destes é possível recolher um grande número de informações, processá-las, agrupá-las e relacioná-las das mais diferentes formas e em tempo irrisório.

Todas essas possibilidades traduzem-se na palavra tratamento, que na visão de Sousa (1986, p. 74) compreende a recolha, arquivamento, tratamento e transmissão de dados. Portanto, o tratamento de dados pode assumir tanto um caráter amplo quanto restrito. No primeiro engloba todo o processo envolvendo os

---

[12] "Os dados – apenas dados primários – têm pouco valor além de si mesmos. Por exemplo, considere pedaços de madeira como dados. Neste estado, a madeira tem pouco valor além de seu valor inerente como um simples objeto. Entretanto, se alguma relação for definida entre os pedaços de madeira, eles ganharão valor. (...) Com a informação é exatamente o mesmo. Regras e relações podem ser estabelecidas para organizar os dados em informação útil e valiosa." (STAIR, 1998, p. 4/5)

[13] Um banco de dados é uma coleção organizada de fatos e informações (STAIR, 1998, p. 13) ou segundo definição da Diretiva 95/46/CE para bancos de dados pessoais, prevista no art. 2, "c", "qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico".

dados, desde sua recolha até a informação obtida ao final e/ou sua transmissão/compartilhamento; no segundo contempla as possibilidades de trabalho propriamente dito com os dados.

A Diretiva 95/46/CE da União Européia define *tratamento de dados pessoais* como

> *Qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição. (UNIÃO EUROPÉIA, 2003a)*

Como se percebe a Diretiva optou por não diferenciar os meios pelos quais os dados são tratados, se automatizados ou não, a fim de garantir total proteção à privacidade do indivíduo.[14]

É, porém, com o tratamento informatizado de dados pessoais que, hodiernamente, a sociedade externa sua preocupação. Stair (1998, p. 119 e 351) cita alguns exemplos acerca do potencial dos bancos de dados informatizados e de seu tratamento, que embora se refiram à análise do mercado de consumo, não importando a identificação do titular dos dados, servem de parâmetro (assustador) para o campo dos dados pessoais.

Um deles é o dispositivo PDV (ponto de venda), instalado na caixa registradora do supermercado, que pode informar quantas caixas de um produto de determinada marca forma vendidos em uma determinada loja em um determinado

[14] O item n. 27 da exposição de motivos da Diretiva deixa essa opção bem clara. “Considerando que a proteção das pessoas se deve aplicar tanto ao tratamento automatizado de dados como ao tratamento manual; que o âmbito desta proteção não deve, na prática, depender das técnicas utilizadas, sob pena de se correr o sério risco de a proteção poder ser contornada (...)”.

dia, dentre outras possibilidades; outro são as empresas de marketing de televisão, que ajudam as redes de televisão a decidir que programas estão tendo resultado positivo e quais não estão, medindo os níveis de audiência e as reações das propagandas; outro é a implementação de um VLDB (*very large database* – banco de dados muito grande), capaz de armazenar de algumas centenas de gigabytes (um gigabyte = um bilhão de bytes[15]) a alguns terabytes (um terabyte = um trilhão de bytes)[16]

Em se tratando de dados pessoais, a proteção à privacidade do indivíduo deve ser complementada pela observância de certas condições para seu tratamento. São condições gerais de licitude, verdadeiros princípios, a nortearem o tratamento dos dados pessoais[17]. Destacam-se:

a) *princípio da lealdade[18] e da licitude*: por lealdade deve se entender o tratamento ético, com respeito à pessoa do titular; já a licitude trata do aspecto legal, das condições estabelecidas em uma determinada lei ou norma com tal força;

b) *princípio da recolha para fins determinados, explícitos e legítimos[19]*: a determinabilidade dos fins conduz o titular dos dados à certeza de que seus dados serão tratados para uma finalidade específica, de forma que quanto mais explícita esta finalidade maior o grau de determinação. A melhor maneira de se

[15] Um byte equivale a oito bits juntos e pode representar uma letra, um dígito numérico ou um caracter. Bit é um dígito binário, ou 1 ou 0. (STAIR, 1998, p. 409)

[16] Wal-Mart, American Express e TRW (empresas de crédito) são exemplos de empresas que possuem VLDBs.

[17] Princípios livremente elaborados pela autora com base no art. 6 da Diretiva 95/46/CE.

[18] A lei francesa estabelece o dever de lealdade na coleta de dados, punindo aquele que realizar coleta de modo fraudulento, desleal ou ilícito com pena de cinco anos de prisão, e multa de 300.000 euros.

[19] A lei francesa estabelece o respeito à finalidade declarada, punindo aquele que usar o dado pessoal de forma distinta daquela que foi originalmente objetivada e declarada com pena de cinco anos de prisão e multa de 300.000 euros, e aquele que conservar dados, por prazo superior ao informado, com pena de três anos de prisão e multa de 45.000 euros.

explicitar os fins a que se destina a recolha é trazê-los de forma expressa, a fim de que não pairem dúvidas. Por fim, a legitimidade pode ser reconhecida pelo *consentimento*[20] *inequívoco do titular*[21].

c) *princípio da adequação, da pertinência e da racionalidade dos dados*: os dados pessoais, objeto da recolha, devem se adequar às finalidades explicitadas e determinadas pelo responsável, guardando pertinência com seu tratamento. Sendo assim, apenas devem ser coletados aqueles dados necessários ao atendimento da finalidade visada, sem que haja excessos;

d) *princípio da exatidão dos dados*: assegura que os dados pessoais inexatos e incompletos sejam excluídos/deletados, compreendendo também a sua atualização, se necessário;

e) *princípio da garantia do tratamento seguro*: incumbe ao responsável pelo tratamento assegurar a observância de todos os princípios elencados, bem como a adoção das medidas, técnicas ou não, tendentes a impedir o acesso não autorizado aos dados recolhidos.

Sampaio identifica alguns princípios comuns, presentes em diversos graus nas legislações européias, assim resumidos:

> *1 - Princípio da publicidade (ou da transparência), pelo qual a existência e a utilização de qualquer banco de dados com informações pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para funcionar; da necessidade do registro público de sua existência; do envio de relatórios periódicos ao Estado ou aos interessados; ou ainda*

[20] Consentimento é qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento, conforme definição do art. 2, "h", da Diretiva 95/46/CE.

[21] Existem algumas situações excepcionais, previstas na Diretiva 95/46/CE, nas quais, mesmo sem o consentimento do titular, há legitimidade no tratamento dos seus dados, como por exemplo, para proteger interesses vitais do próprio titular.

> *exigindo que seja dada ciência aos envolvidos que tenham dados pessoais sendo utilizados. 2 - Princípio da boa-fé (ou da finalidade), pelo qual todo procedimento ligado ao banco de dados deve ser realizado com o objetivo de realizar a finalidade proposta para o sistema, que deve ser conhecida previamente pelos titulares das informações do sistema. Dentro deste princípio estão inclusos ainda a limitação de coleta e armazenamento somente dos dados que tenham sido obtidos licitamente e que tenham relação com o objetivo; ainda limita o período de tempo que estes dados poderão ficar armazenados e também equipara o fornecimento destes dados a terceiros como violação do princípio. 3 - Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados onde suas informações estão armazenadas, com a conseqüente possibilidade de controle destes dados: as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas. 4 - Princípio da segurança física e lógica, pelo qual o administrador do banco de dados é responsável pela sua proteção contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. (SAMPAIO, 1998, p. 509)*

A observância desses princípios pelo responsável pelo tratamento dos dados é de suma importância na cruzada contra a violação da privacidade do titular de dados pessoais. No entanto, cabe ressaltar a importância de se respeitar o princípio elencado no item “b”, que trata da legitimidade da recolha e da necessidade do consentimento inequívoco do titular dos dados. Em países onde o tratamento de dados pessoais ainda não se encontra devidamente regulado, é imprescindível, pelo menos, que o titular de dados pessoais seja instado a dar seu consentimento para o tratamento de seus dados.

Para tanto, é obrigação do responsável pelo tratamento prestar as seguintes informações[22], a fim de garantir ao titular toda segurança e certeza ao consentir que seus dados sejam tratados: a identidade do responsável pelo tratamento, as finalidades do tratamento, os destinatários dos dados, o caráter

[22] A lei francesa estabelece o dever de prestar informação às pessoas, sendo que a falta de informação implica em pena de multa no valor de 1.500 euros.

obrigatório ou facultativo da resposta e possíveis conseqüências se não responder, a possibilidade de acessar os dados que lhe digam respeito e os retificar.[23]

Caso os dados não sejam recolhidos junto ao seu titular as mesmas informações devem ser prestadas pelo responsável pelo tratamento no momento em que os dados forem registrados ou, se estiver prevista a comunicação de dados a terceiros, no momento da primeira comunicação dos dados.

1.4 A coleta voluntária e involuntária de dados pessoais

A coleta de dados assume especial importância, à medida que é a porta de entrada para o tratamento dos dados e facilmente pode ser realizada de forma abusiva. Chama a atenção a disseminação dos *cookies* que, aparentemente inofensivos, podem causar sérios transtornos e ensejar o tratamento indevido de dados pessoais e a conseqüente violação da privacidade do titular dos dados. A maioria dos internautas nem desconfia de sua existência. No entanto, eles são verdadeiros espiões[24].

Rover, ao tratar do comércio eletrônico, já constata essa prática invasiva:

---

[23] Conforme preconiza o art. 10 da Diretiva 95/46/CE.

[24] "Nos Estados Unidos, 150.000 casas já estão equipadas com os novos aparelhos de TV interativos. Além de oferecer uma programação sob medida para o usuário, eles permitem acesso à internet e a vários outros serviços, como fazer compras e efetuar operações bancárias sem sair de casa. Mas esses dispositivos também registram cada toque no controle remoto e enviam de volta para a operadora dados sobre tudo o que foi visto pelo dono do equipamento – incluindo quanto tempo o telespectador gastou vendo novelas, futebol ou filmes eróticos. De posse das informações, as empresas conseguem identificar os hábitos dos consumidores diante de um aparelho de televisão e com isso podem oferecer-lhes novos produtos, compatíveis com suas preferências. Uma pessoa que goste de assistir a documentários, por exemplo, estará mais disposta a aceitar uma oferta desse tipo de programa que outra que prefira ver partidas de futebol ou corridas de carro". (LEPIANI, 2001, p. 79)

> *No mundo real, o consumidor pode ser um anônimo, na medida em que entra numa loja, olha os produtos que quer e vai embora, sem que ninguém saiba o que ele fez. Já no ambiente da Internet, ocorre exatamente o contrário, pois o administrador da página visitada saberá precisamente quais as características do consumidor. (ROVER, 2001, p. 51)*

Ocorre que mesmo os consumidores mais atentos ao problema podem sofrer com a recolha indiscriminada e invasiva de seus dados pessoais. Em seu artigo sobre Privacidade na Internet, Kaminski esclarece que c*ookie* é um pequeno *bit* de informação que um *web site* coloca no computador do usuário quando este acessa o *site*, sendo que ao retornar a esse mesmo *web site*, em outra oportunidade, o navegador remete as informações de volta ao *site*.

> *Normalmente o* cookie *é projetado para lembrar e dizer ao* site *algumas informações úteis sobre o consumidor. Por exemplo, uma livraria* online *provavelmente utiliza-se de* cookies *para armazenar em seu banco de dados os autores e os títulos de livros que o consumidor adquiriu, e quais suas preferências e hábitos de compra. Ao retornar à livraria virtual, o navegador poderá permitir ou não que o* site *da livraria tenha acesso ao* cookie*. O* site *então poderá compilar uma lista de livros do mesmo autor, ou livros por determinado assunto, e disponibilizar ao consumidor tal listagem. Esta atividade é invisível ao internauta, e a não ser que o navegador esteja configurado para alertar quando um* cookie *será armazenado no computador, o consumidor não saberá sobre a existência de tal* cookie*. Quando o consumidor retorna ao* site*, igualmente não saberá que o* cookie *está sendo lido e analisado. Do ponto de vista comercial neste exemplo, o consumidor simplesmente visita a livraria virtual, e uma listagem de livros de seu interesse magicamente aparece em sua tela. (KAMINSKI, 2003)*

O autor ainda informa que os c*ookies* normalmente são inofensivos, não podendo em tese obter informações sobre o internauta (a não ser que este autorize ou as forneça). No entanto, muitos serviços utilizam-se de *cookies* para criar um perfil de interesses baseado nos *sites* visitados, e quais ações foram adotadas nesses *sites*.

Drummond (2003, p. 98/107) identifica três momentos distintos com relação aos problemas advindos da utilização de *cookies*, a saber, o momento da coleta dos dados, o de seu armazenamento e o da sua posterior utilização. Sustenta que, a princípio, apenas no caso de posterior utilização dos dados é que poderá ocorrer violação à privacidade.

Isto porque, em linhas gerais, a coleta de dados pelos *cookies* não identifica efetivamente o usuário (consumidor), que permaneceria anônimo, e o seu armazenamento também não traria maiores implicações, haja vista estarem apenas guardados na máquina (do próprio usuário ou do *site*). Já quanto à utilização posterior, Drummond alerta para o fato de possível cruzamento de dados entre aqueles recolhidos pelos *cookies*, involuntariamente, e aqueles fornecidos pelos consumidores de forma voluntária.

> *Esse cruzamento de dados passa a apresentar um perfil complexo do usuário e coloca o sítio cibernético a um passo da ilicitude, principalmente em se tratando da possibilidade de comercialização de dados pessoais. (DRUMMOND, 2003, p. 103)*

Embora o autor citado apenas vislumbre a violação à privacidade em caso de posterior utilização indevida dos dados, não parece ser este o melhor posicionamento frente a vulnerabilidade do titular de dados. Uma vez recolhidos, os dados estão potencialmente disponíveis a serem tratados. Sendo assim, a mera recolha de dados, sem o consentimento do titular, constitui violação à privacidade e deve ser terminantemente coibida.

Que a coleta involuntária de dados pessoais é prática abusiva e invasiva não se discute, devendo ser totalmente rechaçada. Porém, também a coleta voluntária desses dados merece atenção especial.

Grande parte dos *sites* comerciais da *Web* solicitam o preenchimento de dados, a fim de formar seu cadastro de consumidores (banco de dados interno)[25] e diante das novidades que a rede oferece, muitos consumidores fornecem, sem maiores problemas, seus dados pessoais, mesmo aqueles que nem são de preenchimento obrigatório.

Antes de fornecer seus dados pessoais, o titular deveria se preocupar com a política de privacidade da página visitada[26], bem como fornecer apenas os dados estritamente necessários, pois a Internet, embora traga muitos benefícios, ainda é um ambiente de muitos riscos.

1.5 A Internet como ambiente de maiores riscos

Pode-se afirmar que as potencialidades do tratamento informatizado de dados se desenvolveram com o surgimento da Internet[27], especialmente a partir dos anos 90. Em 1989 nasceu o *World Wide Web* (usualmente www), a rede mundial, permitindo à Internet transformar-se num instrumento de *comunicação de massa* e como tal ser o meio ideal para a recolha, tratamento e distribuição dos dados pessoais informatizados.

---

[25] Esses dados são, pois, armazenados em um banco de dados da empresa, podendo ser utilizados pela própria empresa para e-marketing – criação de ofertas especiais para um conjunto de clientes baseadas em informações de um banco de dados - ou negociados com outra empresa ou interessado nesse banco de dados de consumidores.

[26] A ênfase é dada às compras pela Internet, em razão da prática freqüente de recolha de dados pessoais em *sites* de compra *on line*.

[27] A Internet originou-se das pesquisas realizadas pela ARPA (Agência de Projetos de Pesquisa Avançada) do Departamento de Defesa dos Estados Unidos com o intuito de criar um sistema de comunicação invulnerável a ataques nucleares. A primeira rede de computadores (ARPANET) entrou em funcionamento em 1. de setembro de 1969. Na década de 1980 a rede das redes se formou e passou a se chamar INTERNET, ainda sustentada pelo Departamento de Defesa e operada pela National Science Foudation. Porém, foi precisamente em 1995 que a Internet se consolidou, quando acabou sendo privatizada. (CASTELLS, 2003, p. 82)

A respeito da Internet Bensoussan, Iteanu e Ribas (apud Perez Luño, 2003) advertem que a facilidade de trocar informações à distância pode gerar situações de perigo para a proteção dos dados pessoais, uma vez que a Internet produz um efeito multiplicador dos atentados contra direitos, bens e interesses jurídicos, pois sua potencialidade na difusão ilimitada de imagens e informações tornam-na um veículo especialmente poderoso para perpetrar atentados criminais contra quatro tipos de bens jurídicos básicos, quais sejam:

(1) *a intimidade, a imagem, a dignidade e a honra das pessoas*, ao possibilitar a intromissão indevida em dados pessoais, sua transmissão não autorizada e a propagação de difamações, calúnias e injúrias, dentre outros;

(2) *a liberdade sexual*, ao permitir a propagação de imagens ou informações que sejam formas de exibicionismo, provocação sexual ou fomentem a pornografia entre os menores de idade;

(3) *a propriedade intelectual e industrial, o mercado e os consumidores*, uma vez que a Internet pode contribuir para a distribuição ilícita de obras registradas como propriedade ou industrial, à pirataria de programas, bem como a difusão de conteúdos publicitários ilegítimos;

(4) *a segurança nacional e a ordem pública*, enquanto que podem contribuir para facilitar atentados e desordens pública, inclusive atividades terroristas.

O citado autor ainda adverte quanto ao caráter internacional e ilimitado dessas condutas, o que torna mais difícil seu descobrimento, prevenção e

sanção, pois mesmo quando descobertas, os responsáveis podem não sofrer qualquer sanção em razão de conflito de jurisdição.

Também existe uma grande dificuldade em se determinar a responsabilidade jurídica desses crimes pela Internet, uma vez que existem diferentes operadoras nessa cadeia de comunicação, como o provedor da rede, o provedor de acesso, o provedor de serviço e o provedor de conteúdo.

Agrava o problema o fato de muitas vezes estes diferentes provedores encontrarem-se em países distintos, com legislações diferentes. Aliás, este é um outro problema, pois enquanto a Internet tem âmbito global e ilimitado, o mesmo não acontece com a capacidade de resposta jurídica, que se encontra fracionada pelas fronteiras nacionais.

Diante dessa realidade os operadores do direito, sociólogos, políticos e demais pessoas diretamente envolvidas nesse processo, são instados a oferecerem respostas adequadas a essa nova gama de comportamentos humanos que emerge.

Aliás, o professor Aires José Rover, em artigo tratando a respeito dos sistemas especialistas legais, já assinala neste sentido, quando sustenta a necessidade de se responder adequadamente às demandas da sociedade.

> *Hoje, mais do que em qualquer outro tempo na história jurídica da humanidade, há necessidade de enfrentar a complexidade tanto administrativa quanto técnica do sistema jurídico, respondendo adequadamente às demandas da sociedade. Deve exigir-se dos operadores do Direito respostas de qualidade que dêem conta dos conflitos. (ROVER, 2000, p. 207)*

Por esta razão é que a troca de conhecimentos e experiências é essencial. Nesse sentido, a experiência estrangeira pode oferecer alguns subsídios ao direito pátrio, uma vez que já enfrenta a questão do tratamento informatizado de dados pessoais há algum tempo.

2 PANORAMA LEGAL E DOUTRINÁRIO DA PROTEÇÃO AOS DADOS PESSOAIS

O avanço tecnológico e as transformações sociais requerem uma postura jurídica clara e objetiva, especialmente em relação à proteção dos dados pessoais, isso porque a realidade social já revela a prática corriqueira do tratamento de dados.

E para auxiliar na construção dessa postura jurídica é de grande valia a contribuição do direito internacional, que já enfrenta esta questão há mais de três décadas.

2.1 Origem e evolução da tutela jurídica no direito internacional

Os dados pessoais, informatizados ou não, são objeto de debate e normatização há algum tempo, especialmente na Europa. Com o avanço da tecnologia de informação e comunicação, a troca de dados entre diferentes países,

que diga-se, sempre existiu, adquiriu um volume e importância nunca antes visto, o que importou no surgimento de algumas regulamentações.

Perez Luño (1996, p. 35) afirma que a questão do fluxo internacional de dados (*transborder data flow*) acabou por gerar um aberto conflito de interesses entre países produtores e países consumidores de dados informáticos, pois os países tecnologicamente avançados se achavam no direito de recolher informações, armazená-las e distribui-las, ao passo que aos países subdesenvolvidos restava apenas receber e consumir informações, quando isto era possível, uma vez que às vezes o país nem ao menos detinha os meios técnicos necessários para aproveitá-las.

Tal circunstância ensejou uma tomada de posições bastante diversa. De um lado os países desenvolvidos favoráveis a uma liberdade ilimitada de troca de informações entre todos os países; de outro, os países subdesenvolvidos exigindo que se reconhecesse a faculdade de exercerem um controle sobre os dados recolhidos em seu território.

Assim que em 1973, adeptos da livre circulação de dados se pronunciaram na Convenção Internacional das Telecomunicações em Torremolinos – Málaga, e por sua vez a Suécia, através da Lei denominada *Datalagen* (Lei n. 289), passou a exigir uma autorização especial para a transmissão de dados recolhidos na Suécia para o estrangeiro, dando o primeiro passo para se regulamentar o tratamento informatizado de dados pessoais, prevendo a proteção ao seu titular.

Ainda conforme leciona Perez Luño (1996, p. 36), no mesmo ano de 1973 e depois 1974, o Comitê de Ministros do Conselho da Europa, através de duas

Resoluções[28], a primeira referente à proteção da vida privada das pessoas físicas frente aos bancos de dados eletrônicos no setor privado e a segunda sobre os bancos de dados no setor público, recomendava aos países membros a adoção de medidas legislativas que garantissem determinados princípios.

São exemplos destes princípios o direito dos interessados em conhecer e acessar as informações que lhes digam respeito; a obrigação dos bancos de dados públicos ou privados de corrigir a informação inexata e cancelar a obsoleta, irrelevante ou obtida por procedimentos ilegais; a adoção das garantias correspondentes para impedir que a difusão de dados estatísticos permita a identificação de sujeitos individuais e para evitar a transmissão de dados a pessoas ou entidades não autorizadas.

Nesta época era aprovada nos Estados Unidos a Lei de Privacidade de 1974 (Privacy Act), uma lei bastante direta e simples, que apesar de se aplicar apenas a certos órgãos federais, serve como diretriz para as organizações privadas.

Drummond (2003, p. 50), referindo-se à regulamentação dos países europeus após a lei sueca de 1973, cita alguns países que elaboraram leis referentes à proteção de dados pessoais, como a Alemanha (1977), França (1978), Noruega (1978), Dinamarca (1978), Áustria (1978), Luxemburgo (1978) e Islândia (1979), dentre outros.

Porém, foi a elaboração, pelo Conselho da Europa, do Convênio para a proteção das pessoas com respeito ao tratamento automatizado de dados de

[28] Tais textos foram os primeiros documentos internacionais a se referirem à proteção de dados pessoais.

caráter pessoal, firmado pelos Estados-membros da então Comunidade Econômica Européia em 28.01.1981, que trouxe diretrizes claras a respeito da matéria.

O documento, informa Perez Luño (1996, p. 36/7), trazia certas recomendações, tais como garantir a qualquer pessoa física o respeito de seus direitos e liberdades fundamentais, especialmente seu direito à vida privada no que tange ao tratamento de dados que pudessem afetar-lhe, conciliando os valores fundamentais do respeito às liberdades e da livre circulação de informação entre os povos (*finalidade*); estabelecimento de limites para que os dados de caráter pessoal pudessem ser armazenados, registrados e tratados, bem como a garantia jurídica das pessoas e sua defesa frente aos bancos de dados automatizados públicos e privados e as exceções que pudessem se estabelecer (*estrutura*); acesso aos interessados às informações que lhes dissessem respeito, com a possibilidade de cancelá-las ou corrigi-las quando processadas indevidamente, bem como a faculdade de recorrer diante de qualquer transgressão dos direitos anteriormente assegurados; e por outro lado, a consagração jurídica do princípio da livre circulação de dados (*free flow*) entre os Estados-membros, sendo que aos países signatários era possível estabelecer exceções (*instrumentos*).

Perez Luño (1996, p. 37) ainda relata que, embora este Convênio tenha aberto uma importante perspectiva de colaboração internacional na Europa no que diz respeito à proteção de dados, pecou por sua ambigüidade na regulamentação do fluxo internacional de dados, pela ausência de distinção entre o tratamento de dados pessoais nos setores público e privado e por não prever uma tutela específica do *software*.

A fim de tentar harmonizar a circulação de dados na Europa com a proteção dos dados pessoais foi elaborada, em 1995, a Diretiva 95/46/CE pela União Européia, que na sua exposição de motivos[29] faz constar estas duas antigas ambições do projeto de integração européia, quais sejam, a realização de um mercado interno – auxiliado pela livre circulação de informações pessoais – e a proteção dos direitos e das liberdades fundamentais das pessoas.

Em suas disposições finais a Diretiva estipulou um prazo de três anos, a contar da data de sua adoção, para que os Estados-membros dessem cumprimento à Diretiva, elaborando sua legislação nacional (art. 32), o que foi observado por quase todos os Estados-membros.[30]

Antes mesmo que alguns Estados-membros efetuassem a transposição da Diretiva 95/46/CE para seu direito interno, nova Diretiva foi elaborada pela União Européia em 15 de dezembro de 1997. A Diretiva 97/66/CE - relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações (União Européia, 2003b), tratou de traduzir os princípios dispostos na Diretiva 95/46/CE em regras específicas para o setor das telecomunicações.

Ocorre que, já em 2002 sentiu-se a necessidade da edição de nova Diretiva[31] que abrangesse mais ainda a questão da proteção de dados, tendo sido

[29] Conforme as considerações expostas no item 3 da Diretiva 95/46/CE, "o mercado interno europeu, que tem assegurada a livre circulação de mercadorias, pessoas, serviços e capitais, a teor do art. 7. do Tratado da União Européia, exige não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas também que sejam protegidos os direitos fundamentais das pessoas".

[30] Como a Diretiva entrou em vigor em 1995, o prazo estipulado venceu em 1998. No entanto, de acordo com o relatório elaborado pela Comissão da Comunidade Européia, por ocasião da revisão da Diretiva, ocorrida em 2002, vários países só comunicaram a Comissão da transposição da Diretiva para o direito interno em 2000 e 2001 e a Irlanda ainda não havia comunicado. (UNIÃO EUROPÉIA, 2003a)

[31] Embora a Diretiva 97/66/CE tenha transposto os princípios estabelecidos na Diretiva 95/46/CE em regras específicas para o setor das telecomunicações, tal abrangência não foi total. O desenvolvimento dos mercados e das tecnologias dos serviços de comunicações eletrônicas

editada a Diretiva 2002/58/CE da União Européia, de 12 de Julho de 2002[32], relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, publicada no Jornal Oficial em 31.07.2002, que revogou expressamente a Diretiva 97/66/CE.

Seu objetivo é assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Européia[33], nomeadamente os direitos consignados nos artigos 7º e 8º da citada carta e ainda refletir os desenvolvimentos nos mercados e tecnologias dos serviços de comunicações eletrônicas, como a Internet, de modo a fornecer o mesmo nível de proteção de dados pessoais e de privacidade, independentemente das tecnologias utilizadas.

Diante desse novo cenário que a Internet e outras tecnologias de informação e comunicação oferecem, a Diretiva 2002/58/CE procura atingir, em suma, o setor das telecomunicações (art. 1), sendo que suas disposições especificam e complementam a Diretiva 95/46/CE, além do que asseguram a proteção dos legítimos interesses dos assinantes que sejam pessoas coletivas. É, porém, o item 1 do art. 3º que bem delimita os serviços que são abrangidos pela Diretiva, sendo ela então aplicável ao tratamento de dados pessoais em ligação com a oferta de serviços de telecomunicações acessíveis ao público nas redes públicas de telecomunicações da Comunidade, nomeadamente através da Rede Digital com Integração de Serviços (RDIS) e das redes públicas móveis digitais.

---

passaram a exigir um nível idêntico de proteção dos dados pessoais e da privacidade ao utilizador de serviços de comunicações publicamente disponíveis.

[32] Conforme o art. 17, 1., da Diretiva 2002/58/CE, os Estados-membros deveriam transpor a nova diretiva para o direito nacional até 31 de Outubro de 2003.

[33] A Carta dos Direitos Fundamentais da União Européia, proclamada pelo Parlamento Europeu, o Conselho e a Comissão, em Dezembro de 2000, incorpora em seu artigo 8º o direito à proteção de dados, acrescentando uma ênfase à dimensão que a diretiva atribui aos direitos fundamentais.

2.2 Destaques do direito comparado: especial referência à Diretiva 95/46 da União Européia e à Portugal, Espanha, Alemanha e Estados Unidos

Embora outras Diretivas tenham sucedido à Diretiva 95/46/CE, esta ainda é referência na questão dos dados pessoais, motivo pelo qual merece ser analisada detidamente. Desta mesma forma, países como Portugal, Espanha e Alemanha recebem uma análise diferenciada em razão de sua proximidade e influência no direito nacional e os Estados Unidos, servindo de contra-ponto, como exemplo de desregulamentação da matéria.

Muito embora a Diretiva 95/46/CE tenha se proposto a realizar a harmonização entre a livre circulação de dados e a proteção de dados pessoais, esta não se consolidou. Muitas são as garantias com relação à proteção dos dados pessoais, porém as exceções previstas acabam por deixar certas garantias inoperantes. Assim tem-se como exemplo o contido em seu art. 1º, que determina aos Estados-membros o dever de assegurar, em conformidade com a Diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, especialmente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, porém no mesmo artigo impede que os Estados-membros restrinjam ou proíbam a livre circulação de dados pessoais entre Estados-membros por razões relativas à proteção assegurada.

Da mesma forma encontra-se a previsão do art. 3º. Primeiramente delimita o âmbito de aplicação da Diretiva, devendo sua aplicação se estender ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num

banco de dados ou a ele destinados, para logo em seguida estabelecer algumas ressalvas à aplicação da proteção (ao tratamento de dados pessoais) conferida pela Diretiva, como por exemplo, quando o tratamento de dados tenha como objeto a segurança pública, a defesa, a segurança do Estado, e as atividades do Estado no domínio do direito penal, ou ainda quando o tratamento for realizado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.

Um outro ponto da Diretiva que merece ser abordado é o que trata da transferência de dados pessoais a países terceiros, ou seja, aqueles que não fazem parte da União Européia. No art. 25 há o estabelecimento de seis princípios, aqui nomeados para melhor assimilação, quais sejam:

(1) princípio da proteção adequada - estabelece que os Estados-membros só poderão transferir dados a países terceiros, desde que estes assegurem um nível de proteção adequado;

(2) princípio da garantia da proteção adequada - elenca os fatores que serão analisados a fim de se constatar a adequação do nível de proteção, tais como a natureza dos dados, a finalidade e a duração do tratamento;

(3) princípio da notificação compulsória - tanto os Estados-membros quanto a Comissão têm que se informar mutuamente quando considerarem que um país terceiro não oferece um nível de proteção adequado;

(4) princípio da não-transferência de dados - obriga os Estados-membros a tomar as providências necessárias a fim de impedir a transferência de dados a um país terceiro, sempre que a Comissão verificar que este não garante um nível de proteção adequada;

(5) princípio da negociação - confere à Comissão a incumbência de estabelecer negociações com países terceiros que não garantam o nível de proteção adequada exigido pela Diretiva e constatado pela Comissão ou por um Estado-membro;

(6) princípio da constatação superveniente - admite que a Comissão constate que um país terceiro assegura um nível de proteção adequado em virtude de sua legislação interna ou de seus compromissos internacionais, subscritos na seqüência das negociações.

Ocorre que, no artigo seguinte, em que pese as garantias exigidas pelo art. 25, apresentam-se várias derrogações, que vêm minar as garantias antes tão bem delineadas. A mais preocupante encontra-se no item 2 do art. 26:

> *2. Sem prejuízo do n.1, um Estado-membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro que não assegura um nível de proteção adequado na acepção do n. 2 do art. 25, desde que o responsável pelo tratamento apresente garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respectivos direitos; essas garantias podem, designadamente, resultar de cláusulas contratuais adequadas. (UNIÃO EUROPÉIA, 2003a)*

Em recente revisão da Diretiva 95/46/CE, realizada pela Comissão da União Européia (Comissão Européia, 2004), constatou-se que, apesar de alguns problemas de implementação e execução da Diretiva, a maioria dos consultados se manifestou pela sua manutenção, sem proposta de alteração, seja porque ainda há pouca experiência na execução da Diretiva, seja porque os problemas apontados poderiam ser resolvidos sem alterá-la.

No entanto, sugeriu-se a complementação da alínea b) do n.º 2 do artigo 8º, que permite aos Estados-membros fazer exceções à regra geral de que os dados sensíveis não possam ser tratados; a promoção e o encorajamento das tecnologias que aumentem a privacidade, no sentido de conceber sistemas e tecnologias de informação e de comunicação de maneira a minimizar a recolha e a utilização de dados pessoais e impedir formas ilegais de tratamento[34]; a implementação satisfatória dos artigos 6º e 7º, que tratam respectivamente da qualidade dos dados e dos critérios de legitimidade do tratamento, ressaltando-se a necessidade de se clarificar e uniformizar o entendimento do termo *consentimento inequívoco* (alíena a, art. 7º), especialmente nos casos *on line*; a simplificação e aproximação dos requisitos nos Estados-membros no que respeita à notificação das operações de tratamento por responsáveis pelo tratamento dos dados (arts. 18 e 19); a harmonização na implementação pelos Estados-membros das disposições dos arts. 25 e 26[35].

O relatório ainda concluiu que o nível de insatisfação dos europeus com relação à implementação e à execução da Diretiva é relativamente alto, o que não deixa de ser preocupante, tendo em vista a amplitude da regulamentação européia.[36] Diante desse quadro a Comissão concluiu que os recursos que vêm

[34] No Canadá, o governo federal foi o primeiro governo nacional a tornar obrigatórias as avaliações do impacto na privacidade (*Privacy Impact Assessments* - PIA) para todos os departamentos e agências federais relativamente a todos os programas e serviços onde as questões da privacidade pudessem ser inerentes.

[35] Nesse sentido é preocupante a constatação do relatório de que desde 1998 o número de notificações à Comissão, no que tange ao n.2 do art. 26, foi irrisório, sugerindo a realização de muitas transferências não autorizadas e possivelmente ilegais para destinos ou destinatários que não garantem uma proteção adequada.

[36] A Comissão colocou dois questionários no seu *website* e convidou titulares de dados (consulta pública) e responsáveis pelo tratamento dos dados (grupo-alvo) a darem as suas opiniões sobre vários aspectos da proteção de dados. Quando os questionários foram encerrados, tinham respondido 9156 pessoas e 982 entidades responsáveis pelo tratamento dos dados. Embora estes resultados não possam ser considerados tão representativos como os resultados de inquéritos baseados em amostras cientificamente selecionadas, 44,9% das pessoas disseram considerar mínimo o nível de proteção, 81% indicaram que o nível de sensibilização sobre a proteção de dados

sendo atribuídos ao controle da execução da diretiva estão sendo insuficientes e não vem sendo dada prioridade, pelas autoridades de controle, às ações coercitivas.

Para tanto, a Comissão previu para os anos de 2003 e 2004 um plano de ação, que se preocupa basicamente com o fato de detectar as causas do nível insatisfatório de cumprimento, execução e sensibilização da Diretiva, bem como definir soluções exeqüíveis para melhorar este quadro. Ainda previu um incentivo para que organizações apresentem códigos de conduta setoriais para aplicação a nível comunitário[37], de forma que desempenhem um papel importante no desenvolvimento futuro da proteção de dados na União Européia e no exterior, e também para evitar uma legislação excessivamente pormenorizada.

Seguindo a orientação do Parlamento e do Conselho da União Européia, todos os seus Estados-membros cuidaram de elaborar sua legislação nacional acerca da proteção dos dados pessoais. No entanto, destaque especial será dado a Portugal, Espanha e Alemanha, em virtude da semelhança do direito, de origem latina. Estados Unidos também, em razão da peculiaridade de sua (não) regulamentação, tudo a fim de contribuir com a formação de uma sólida doutrina pátria, ainda bastante incipiente.

Além do Brasil manter estreita relação com Portugal, por motivos históricos e culturais, a doutrina jurídica pátria também se espelha muito na lusitana,

---

é insuficiente, ruim ou muito ruim, sendo que entre os responsáveis pelo tratamento dos dados a opinião foi quase igualmente negativa (30%), 69,1% dos responsáveis pelo tratamento de dados aceitam as regras de proteção de dados, considerando que os requisitos para sua implementação são necessários, e 62,1% dos responsáveis pelo tratamento de dados não consideraram que responder aos pedidos de acesso das pessoas aos seus dados pessoais envolva um grande esforço para sua empresa, mesmo porque o número de pedidos se mostrou ínfimo no ano de 2001 ou não tinham os números disponíveis.

[37] O Grupo de Trabalho do artigo 29.º está considerando atualmente as seguintes contribuições: código de conduta sobre marketing direto; código de conduta sobre o tratamento de dados pessoais por empresas de pesquisa de executivos (*head-hunters*) e código de conduta sobre a identificação pan-europeia da linha de chamada.

especialmente no que tange ao Direito Constitucional. Portugal foi um dos primeiros países a inserir em seu texto constitucional a previsão de direitos em face da utilização da informática.

A Constituição de Portugal, em vigor desde 25 de abril de 1976[38], estabelece em sua primeira parte os *Direitos e deveres fundamentais*, que englobam os *Direitos, liberdades e garantias pessoais* previstos no Capítulo I, do Título II, que por sua vez, estatuem no art. 35 a utilização da informática, assim expressa:

> *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. (PORTUGAL, 2004)*

Acerca do artigo 35 da Constituição Portuguesa, que trata da utilização da informática, o Tribunal Constitucional de Portugal já se pronunciou em diversas ocasiões, sendo tais pronunciamentos de capital importância para a

[38] A Constituição da República Portuguesa entrou em vigor em 25 de Abril de 1976, tendo a Assembléia já aprovado cinco Leis constitucionais de Revisão (1982, 1989, 1992, 1997 e 2001).

solidificação do direito lusitano quanto à proteção de dados pessoais, bem como para a construção de uma doutrina geral acerca de tais direitos *universais*.

Em acórdão prolatado em 07 de junho de 1997, sob nº 355, o Tribunal Constitucional (2003), apreciando preventivamente a constitucionalidade do decreto do Governo nº 110/97, com fundamento em eventual violação da reserva relativa da competência legislativa da Assembléia da República, decidiu pela inconstitucionalidade do decreto por violação do disposto na alínea "b" do n. 1 do artigo 168, com referência ao artigo 35, ambos da Constituição da República, ou seja, reconheceu que a constituição de bancos de dados informatizados contendo dados relativos ao estado de saúde de pacientes com doenças oncológicas violava a garantia ao direito à vida privada[39], previsto no mencionado artigo 35 da Constituição Portuguesa.

A importância desse pronunciamento centra-se, nem tanto na decisão acerca da inconstitucionalidade do decreto, mas sim na sua fundamentação, pois a constatação de que a Constituição portuguesa consagra em seu art. 35 o chamado *direito fundamental à autodeterminação informacional*, não podendo, portanto, a informática ser utilizada indiscriminadamente[40] para tratamento de dados referentes à vida privada (estado de saúde), reforça a tese de que a legislação sobre bancos de dados automatizados no domínio da saúde sempre se relacionará,

[39] Devido à ausência de definição legal e à polêmica da conceituação do termo *vida privada*, o próprio Tribunal recorreu às suas jurisprudências (acórdãos 128/92 e 319/95) para consigná-lo como "o direito a uma esfera própria inviolável, onde ninguém deve poder penetrar sem autorização do respectivo titular, constitucionalmente consagrado no n.1 do artigo 26 da CR". Engloba nesta esfera própria inviolável a vida pessoal, a vida familiar, a relação com outras esferas de privacidade, como a amizade, o lugar próprio da vida pessoal e familiar, assim entendido o lar ou domicílio e os meios de expressão e de comunicação privados, como a correspondência, o telefone, etc.

[40] O Tribunal reconheceu que por se tratar o termo *vida privada* de uma conceituação aberta, exige concretização e implica um grau diferenciado de proteção e inviolabilidade, não significando, porém, uma proibição total, permanente e absoluta de tratamento automatizado de quaisquer dados pessoais relacionados com a vida privada (e o estado de saúde).

direta ou indiretamente, com o direito à vida privada, previsto de forma ampla no art. 26 e de forma mais específica no art. 35 da Constituição.

No caso do tratamento automatizado de dados relativos a doenças oncológicas reconheceu o Tribunal que se viola a esfera de privacidade dos doentes, impedindo sobre eles qualquer tratamento informatizado, sobre o qual não tenha o legislador se manifestado através de lei da Assembléia da República ou de decreto-lei por esta autorizado.

Em 1998, Portugal, através da Lei 67, de 26 de outubro, transpôs para sua ordem jurídica a Diretiva 95/46/CE, regulamentando assim o art. 35 da Constituição. Em linhas gerais, adotou a mesma redação dada pela Diretiva.

Da mesma forma que Portugal, a Espanha exerce certa influência sobre o direito brasileiro, tanto que Sarlet (1998, p. 24), ao tratar dos direitos fundamentais, faz clara opção pela incursão no direito lusitano e espanhol, que por sua vez, é fortemente influenciado pelo direito alemão.

A Constituição espanhola de 1978 (España, 2004), no capítulo[41] que trata dos direitos fundamentais e das liberdades públicas, prevê no artigo 18 a garantia do direito à honra, à intimidade pessoal e familiar e à própria imagem (item 1), e de forma específica a garantia da intimidade informática ao estabelecer que a lei[42] limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos (item 4).

[41] Capítulo Segundo, Seção 1., do Título I.
[42] A expressão "ley" é utilizada no sentido de "ley orgánica", o que equivaleria à lei complementar no ordenamento jurídico brasileiro.

É, portanto, com base constitucional que o sistema jurídico espanhol fundamenta a proteção da privacidade relativa aos dados pessoais, notadamente pelo art. 18.4. da Constituição da Espanha. Sua lei de proteção aos dados pessoais é conhecida como LOTAD (Ley Orgânica de Tratamiento Automatizado de los Datos), Lei 15/1999.

O direito alemão, diferentemente do direito português e do direito espanhol, não prevê expressamente na Constituição Federal o direito à intimidade informática. Porém, como leciona Sousa (1986, p. 71) é da conjugação de dois preceitos da Lei Fundamental de Bonn, a saber, a inviolabilidade da dignidade humana (1.1) e o direito à livre ostentação da personalidade[43] (2.1), que a doutrina e a jurisprudência alemãs retiram um direito jurídico-fundamental a favor dos cidadãos quanto à recolha, tratamento e transmissão de dados pessoais. Esse posicionamento foi fixado pela jurisprudência constitucional alemã em três decisões[44] do Tribunal Constitucional Federal (Bundesverfassungsgerich), sendo que a mais conhecida delas é a decisão sobre o senso populacional (Volkszählungsurteil), emitida em 15.12.1983, onde foi construído o direito à autodeterminação informacional, adiante tratado de forma pormenorizada.

A Alemanha foi um dos primeiros países a elaborar uma lei nacional a respeito da proteção aos dados pessoais, em 27.01.77. Atualmente vige a Lei federal de proteção de dados (Bundesdatenschutzgesetz), de 20.12.1990.

[43] "Jeder ha das Recht auf freie Entfaltung seiner Persönlichkeit, sowie er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmässige Ordnung oder das Sittengesetz verstösst". Cada um tem o direito ao livre desenvolvimento de sua personalidade, a medida que não prejudique os direitos alheios e não infrinja a ordem constitucional e a moral. (trad. aut.)

[44] "Mikrozensusentscheidung" (BverfGE 27, 1 ss.); "Scheidungsaktenbeschluss" (BverfGE 27, 344) e "Volkszählungsurteil" (NJW, 1984, 419 ss.)

Tendo entrado em vigor na União Européia, em 25 de outubro de 1998, a Diretiva relativa à proteção de dados pessoais, que constitui a legislação geral da União Européia no domínio da vida privada, os Estados Unidos, segundo a Comissão Européia (2003), embora abordem a questão da proteção da vida privada em face do tratamento de dados de forma diversa, recorrendo a uma abordagem setorial com base numa mescla de legislação, regulamentação e auto-regulamentação, não puderam ficar alheios à exigência da Diretiva de constatação de um nível adequado de proteção, sem o qual não seria possível a transferência de dados pessoais da União Européia para os Estados Unidos.

Sendo assim, o *Department of Commerce* dos EUA emitiu, em 21 de julho de 2000 um documento contendo *os princípios de porto seguro* – proteção da vida privada - e as FAQ (Frequently Asked Questions - Questões mais Freqüentes), de modo a incentivar, promover e desenvolver o comércio internacional. Segundo consta de decisão da Comissão Européia (2003), esse documento destina-se a ser utilizado exclusivamente por organizações dos Estados Unidos que recebam dados pessoais da União Européia para efeitos de reconhecimento como *porto seguro* e para a presunção de *adequação* implicada no processo. A organização que deseje usufruir dos benefícios de *porto seguro* tem que apresentar uma autocertificação ao *Department of Commerce* (ou a um seu representante), de acordo com o estabelecido na FAQ sobre autocertificação.

São princípios de porto seguro:

a) aviso – a organização tem o dever de informar os cidadãos quanto aos fins a que se destinam a recolha e utilização dos dados, bem como quanto aos meios que a organização coloca à disposição dos cidadãos para

limitarem a utilização e comunicação desses dados. Este aviso deve ser formulado em linguagem clara e de forma bem visível no momento em que se solicita pela primeira vez qualquer informação pessoal aos cidadãos;

b) escolha – possibilidade dos cidadãos escolherem se os seus dados pessoais podem ser divulgados a terceiros ou ser utilizados para fins incompatíveis com os que presidiram à recolha inicial ou com os que foram subsequentemente autorizados pela pessoa em causa;

c) retransferência – ocorre nos casos em que a organização que recolheu os dados pessoais divulgue essas informações a terceiros, quando, então, deverão aplicar os princípios de aviso e escolha;

d) segurança - as organizações que criam, mantêm, utilizam ou divulgam bancos de informações pessoais devem tomar precauções razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados;

e) integridade dos dados – as organizações devem tomar providências razoáveis para assegurar que os dados recolhidos são fiáveis para os fins de sua utilização, exatos, completos e atuais;

f) acesso - os cidadãos devem poder ter acesso às informações pessoais que lhes dizem respeito e que estejam na posse de uma organização; devem poder retificar, alterar ou eliminar informações inexatas, salvo se os encargos ou as despesas para facultar esse acesso forem desproporcionados em relação aos riscos para a vida privada da pessoa em causa, ou sempre que os legítimos direitos de terceiros incorram em risco de violação;

g) aplicação - a proteção efetiva da vida privada deve incluir mecanismos que garantam o cumprimento dos princípios de *porto seguro*. Estes mecanismos devem incluir, no mínimo: g.1) mecanismos de recurso independentes, imediatamente disponíveis e pouco onerosos através dos quais as queixas e os litígios dos cidadãos possam ser investigados e resolvidos e os danos reparados sempre que a lei aplicável ou as iniciativas privadas o prevejam; g.2) procedimentos de acompanhamento para indagar da veracidade das atestações e alegações das empresas em relação às suas práticas em matéria de proteção da vida privada e para verificar se essas práticas relativas à vida privada foram executadas da forma apresentada; e g.3) a obrigação de solucionar problemas decorrentes do descumprimento dos princípios por organizações que tenham anunciado a sua adesão e conseqüências para essas organizações. As sanções devem ser suficientemente rigorosas de modo a garantirem o cumprimento por parte das organizações.

O documento que trata das FAQ contempla várias questões, dentre elas perguntas sobre *dados sensíveis*, *exceções jornalísticas*, *responsabilidade subsidiária*, *bancos de investimentos e auditorias*, *papel das autoridades responsáveis pela proteção dos dados*, *autocertificação*, *verificação*, *acesso*, *recursos humanos*, *resolução de litígios e aplicação*, *prazo de opção de não participação*, *informação relacionada com viagens*, *produtos farmacêuticos e medicinais*, *registros públicos e informação disponível ao público*.

2.3 A via dupla do modelo europeu

O controle acerca da proteção de dados pessoais nos países membros da União Européia se faz em dois sentidos, o controle administrativo e o controle judiciário ou normativo, exercendo o primeiro um papel mais preventivo e o segundo atuando mais de forma repressiva.

Assim é que a Diretiva 95/46/CE determina que cada Estado-membro tenha uma ou mais autoridades públicas responsáveis pela fiscalização da aplicação da sua legislação acerca da proteção de dados pessoais (via administrativa). Essa autoridade, por sua vez, deverá ser dotada de certos poderes, como

a) *o poder de inquérito*, pelo qual pode a autoridade recolher todas as informações necessárias ao desempenho de sua fiscalização, bem como acessar aos dados objeto de tratamento;

b) *o poder de intervenção administrativa*, podendo ordenar o bloqueio, a exclusão e a destruição de dados; proibir temporária ou definitivamente o tratamento; dirigir advertência ou censura ao responsável pelo tratamento; e ainda enviar a questão para o parlamento ou outra instituição política;

c) *o poder de intervenção judicial*, quando violadas as disposições acerca da proteção de dados ou mediante comunicação de infrações à autoridade judiciária.

No exercício de suas atribuições a autoridade de controle deverá ter total independência, competindo-lhe, no entanto, a elaboração periódica de um relatório sobre sua atividade, que deverá, ao menos, ser publicado.

Dentre suas atribuições encontram-se a elaboração de pareceres prévios à elaboração de medidas regulamentares ou administrativas relativas ao tratamento de dados pessoais e à proteção dos direitos e liberdades das pessoas e a verificação da licitude de tratamento de dados.

Na Alemanha a Lei federal de proteção de dados (Bundesdatenschutzgesetz), de 20.12.1990, prevê a existência de uma pessoa responsável pela proteção de dados, em âmbito federal, chamado de responsável/delegado federal pela proteção de dados (Bundesbeauftragte für den Datenschutz), que é eleito pelo Parlamento Alemão para um mandato de cinco anos, permitida uma reeleição. Essa pessoa ocupa posição de destaque, sendo autoridade independente, que só deve respeito à lei. Suas principais atribuições são aconselhamento do Parlamento Federal, do Governo e de todos os organismos públicos federais, assim como de outros organismos e a realização de controle.

Na França, como relata Castro (2004), a Lei Informática e Liberdades, de 06.01.1978, criou a CNIL - Comissão Nacional de Informática e Liberdades, que é uma autoridade independente, formada por 17 personalidades, dos quais seis parlamentares, seis representantes das cortes superiores e cinco personalidades designadas pelo presidente da Assembléia Nacional.

Esses integrantes são eleitos pelos órgãos de que se originam e conjuntamente elegem o presidente da CNIL. Não estão funcionalmente subordinados a nenhum órgão ou autoridade, porém, anualmente, a CNIL apresenta um relatório ao Presidente da República e ao parlamento.

Dentre suas várias missões destacam-se a função de conselho e a de harmonização de condutas, bem como a promoção de códigos deontológicos de

boa conduta em vários setores profissionais. Emite ainda relatórios e pareceres e propõe projetos de lei ou de normativas e atua como órgão fiscalizador, possuindo poder de controle e de verificação *in loco*, podendo emitir advertências aos responsáveis por infrações, além de provocar o Ministério Público, no caso de vir a ter conhecimento de infrações.

Em Portugal, segundo informa Drummond (2003, p. 51/2), a Lei 67/98, criou a Comissão Nacional de Proteção, entidade administrativa independente com poderes de autoridade, que funciona junto da Assembléia da República portuguesa.

A Comissão, além de controlar o tratamento dos dados e proteger os cidadãos contra atos ofensivos à sua privacidade, que ocorram através do tratamento lesivo dos dados pessoais, ainda controla e fiscaliza o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais; emite parecer prévio sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos comunitários ou internacionais relativos ao tratamento de dados pessoais; exerce poderes de investigação e inquérito, podendo para tal acessar aos dados objeto de tratamento; exerce poderes de autoridade, designadamente o de ordenar o bloqueio, o apagamento ou destruição de dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais; pode advertir ou censurar publicamente o responsável do tratamento dos dados, pelo não cumprimento das disposições legais nesta matéria; intervém em processos judiciais no caso de violação da lei de proteção de dados; e formula denúncia ao Ministério Público sobre infrações penais nesta matéria, bem como pratica os atos cautelares necessários e urgentes para assegurar os meios de provas.

Não obstante o controle exercido no âmbito administrativo pela autoridade de controle, qualquer pessoa poderá recorrer à via judicial em caso de violação de seus direitos em relação ao tratamento de dados pessoais e ainda, em caso de prejuízo devido ao tratamento ilícito ou incompatível com a regulamentação vigente, obter do responsável a reparação pelo prejuízo sofrido, bem como as devidas sanções.

Desta forma, a via normativa se caracteriza por ser aquela prevista nos ordenamentos jurídicos. Na Europa, a regulamentação da proteção dos dados pessoais teve início com a lei sueca, denominada *Datalagen*, de 11 de maio de 1973. Desde então outros países europeus elaboraram leis específicas, mesmo antes do Convênio 108/80 e da Diretiva 95/46/CE.

Drummond (2003, p.51) arremata concluindo que a "via normativa é a que pretende o controle através da aplicação de princípios previstos no ordenamento legal".

2.4 O direito alemão à autodeterminação informacional

O direito à autodeterminação informacional (Recht auf informationelle Selbstbestimmung) foi reconhecido pela primeira vez pelo Tribunal Constitucional Alemão na decisão conhecida por *decisão sobre o senso populacional* (Volkszählungsurteil), emitida no dia 15 de dezembro de 1983. Nela aquele Tribunal declarou a inconstitucionalidade (parcial) da Lei de Senso de População da Alemanha, especificamente no que dizia respeito à exigibilidade de fornecimento de dados pessoais, por parte dos cidadãos alemães, para fins de estatística.

Restou consignado nesta decisão que “o direito fundamental garante, não obstante, o poder do indivíduo, determinar, ele próprio, a princípio, sobre o abandono ou utilização de seus dados pessoais”[45].

Como leciona Sousa (1986, p. 71) é da conjugação de dois preceitos da Lei Fundamental de Bonn, a saber, a inviolabilidade da dignidade humana (1.1) e o direito à livre ostentação da personalidade[46] (2.1), que a doutrina e a jurisprudência alemãs retiram um direito jurídico-fundamental a favor dos cidadãos quanto à recolha, tratamento e transmissão de dados pessoais, conferindo-lhes o direito a controlar sua utilização. O escritório alemão para proteção de dados da Alemanha (Informationelle, 2004) mantém em sua página na internet a seguinte definição para o direito a autodeterminação informacional: “cada um tem o direito de saber quem sabe o que e quando sobre si”[47].

Conforme as explanações do responsável/delegado federal pela proteção de dados pessoais na Alemanha, esse direito

> *deve possibilitar ao indivíduo conservar sua esfera privada e impedir que ele, por isso, caia numa dependência crescente de organismos estatais e econômicos, porque estes sempre querem saber mais sobre ele*[48]*. (DEUTSCHLAND, 2003, p. 12)*

Porém, como o moderno Estado Social e de Direito também precisa de um grande volume de dados pessoais, a fim de poder cumprir suas múltiplas

[45] Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

[46] Jeder ha das Recht auf freie Entfaltung seiner Persönlichkeit, sowie er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmässige Ordnung oder das Sittengesetz verstösst. Cada um tem o direito ao livre desenvolvimento de sua personalidade, a medida que não prejudique os direitos alheios e não infrinja a ordem constitucional e a moral.

[47] Jeder hat das Recht zu wissen, wer was wann über ihn weiß.

[48] Das Recht auf informationelle Selbstbestimmung soll es dem Einzelnen ermöglichen, sich seine Privatsphäre zu erhalten, und verhindern, dass er deshalb in zunehmende Abhängigkeit von Stellen in Staat und Wirtschaft gerät, weil diese immer mehr von ihm wissen.

incumbências de forma correta e justa, não pode ficar à mercê da colaboração voluntária das pessoas. O direito à autodeterminação informacional não pode, por isso, ser ilimitado, absoluto.

Assim se manifestou a Corte Constitucional Alemã ainda na decisão *Volkszählungsurteil*, impondo, no entanto, limitações a essas limitações. “Limitações a esse direito a autodeterminação informacional apenas são admissíveis em favor do interesse geral preponderante”[49], tendo a mesma Corte ainda fixado a necessidade da existência de um lei limitadora.

Esta lei, por sua vez, deve

> *ser indispensável ao interesse geral preponderante, regular as hipóteses de limitações dos direitos fundamentais e o volume reconhecível aos cidadãos, enfim, a que preceitos corresponde a clareza da norma e considerar o princípio da proporcionalidade. (DEUTSCHLAND, 2003, p. 12)*

Nessa esteira, Sousa (1986, p. 73) sustenta que o direito à autodeterminação informacional tem seu conteúdo garantido através da proteção da essência dos direitos fundamentais e do princípio da proporcionalidade. A proteção da essência dos direitos fundamentais encontra guarida no art. 19, II, da Lei Fundamental de Bonn, que consagra que em caso algum um direito fundamental pode ser afastado na sua essência.

Desse modo só poderá limitar o direito à autodeterminação informacional à medida que não penetre no núcleo absolutamente protegido da vida do particular. Já o princípio da proporcionalidade[50] resulta do Estado de Direito e tem

[49] Einschränkungen dieses Rechts auf ‘informationelle Selbstbestimmung’ sind nur im überwiegenden Allgemeininteresse zulässig.

[50] O princípio da proporcionalidade não consta formalmente do texto da Lei Fundamental de Bonn, mas se tornou um dos princípios cardeais do Direito Constitucional da Alemanha. Constitui-se de

status constitucional, segundo decisão do Tribunal Constitucional Alemão e deve ser respeitado pela lei que trata do tratamento automatizado de dados, eis que esta subordina-se à proibição do desproporcional, aos princípios da propriedade e da exigibilidade, assim como da proporcionalidade em sentido estrito.

Cabe, nesse ponto, uma breve transposição para o direito pátrio, embora no Brasil a proporcionalidade não exista enquanto norma geral de direito escrito. Existe, entretanto, como norma esparsa no texto constitucional, a teor dos incisos V, X e XXV do art. 5º; incisos IV, V e XXI do art. 7º; inciso IX do art. 37.

Segundo sustenta Bonavides (2001, p. 396) é na qualidade de princípio constitucional ou princípio geral de direito que se torna necessário reconhecê-lo, apto a acautelar o cidadão e toda a sociedade do arbítrio do poder. Embora ainda não haja sido formulado expressamente, flui do espírito do § 2º do art. 5º, o qual abrange a parte não escrita ou não expressa dos direitos e garantias da Constituição, a saber, aqueles direitos e garantias cujo fundamento decorre da natureza do regime, da essência do Estado de Direito e dos princípios que este consagra e que fazem inviolável a unidade da Constituição.

Referido autor conclui seu pensamento incitando os aplicadores do direito a dar corpo a esse princípio, asseverando

> *Em nosso ordenamento constitucional não deve a proporcionalidade permanecer encoberta. Em se tratando de princípio vivo, elástico, prestante, protege ele o cidadão contra os excessos do Estado e serve de escudo à defesa dos direitos e liberdades constitucionais. De tal sorte que urge, quanto antes, extrai-lo da doutrina, da reflexão,*

---

três elementos básicos, quais sejam, da pertinência ou adequação (com o auxílio de determinada medida se pode alcançar o resultado desejado, baseado no interesse público), da necessidade (a medida não há de exceder os limites indispensáveis à conservação do fim legítimo que se almeja, ou uma medida para ser admissível deve ser necessária); e da proporcionalidade *strictu sensu* – a escolha recai sobre o meio ou os meios que, no caso específico, levarem mais em conta o conjunto de interesses em jogo (vedação quanto ao uso de meios desproporcionados).

> *dos próprios fundamentos da Constituição, em ordem a introduzi-lo, com todo o vigor no uso jurisprudencial (BONAVIDES, 2001, p. 394-395)*

Não deixa de ter razão o mestre constitucionalista, haja vista a dificuldade encontrada em se proteger direito que, invariavelmente, estará colidindo com outro de igual natureza e valor.

2.5 A inviolabilidade do sigilo da comunicação de dados

Antes, porém, de trilhar o caminho do direito à privacidade, cumpre destacar que o ordenamento pátrio contempla algumas previsões capazes de tutelar os dados pessoais, como a previsão constitucional da inviolabilidade do sigilo de comunicação de dados e do *habeas data* e, infraconstitucional, referente aos bancos de dados no Código de Defesa do Consumidor. Infelizmente o Brasil ainda não conta com uma legislação acerca da proteção dos dados pessoais, como a União Européia e diversos países.

A atual Constituição brasileira, promulgada em outubro de 1988, trouxe grata inovação ao tutelar a inviolabilidade do sigilo da comunicação de dados, prevista no art. 5º, inc. XII:

> *é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.*

Muito embora o legislador constituinte não tenha sido claro o bastante ao prever a inviolabilidade do sigilo da comunicação de *dados*, não há que se entender ou se interpretar de forma restrita esta previsão, uma vez que tal interpretação, neste caso específico, atenta contra a finalidade da norma. Bastos, ao comentar o inciso supra citado, parece não ter entendido o alcance da previsão constitucional, especialmente da expressão *dados*:

> *Mas pela inserção da palavra no inciso vê-se que não se trata propriamente do objeto da comunicação, mas sim de uma modalidade tecnológica recente que consiste na possibilidade das empresas, sobretudo financeiras, fazerem uso de satélites artificiais para comunicação de dados contábeis. (BASTOS, 1988-1989, p. 73)*

Efetivamente a expressão *dados* quer significar muito mais, pois abrange, sem distinção, todos os dados informáticos, mediante os quais se realizam as comunicações de informática e telemática. Assim, a proteção conferida ao indivíduo pela norma constitucional é ampla, protegendo-o de qualquer forma de intromissão na sua esfera de comunicação.

Aliás, esta parece ter sido a intenção do legislador ao incluir a inviolabilidade do sigilo da comunicação de dados na redação do inciso XII. Com o desenvolvimento de sistemas de informática e telemática e a crescente penetração desses sistemas na vida do indivíduo, este passou a ser extremamente vulnerável à violação de sua esfera de comunicação e de privacidade.

A edição da Lei 9.296/96, que regulamentou o mencionado inciso XII, gerou muita polêmica ao estender a possibilidade de interceptação ao fluxo de comunicações em sistemas de informática e telemática (art. 1, parágrafo único), quando a norma constitucional é clara ao ressalvar apenas essa possibilidade às comunicações telefônicas.

Sustentando a inconstitucionalidade do referido parágrafo único, Vicente Greco Filho assim se posiciona:

> *Em nosso entendimento, é inconstitucional o parágrafo único do art. 1. da lei comentada, porque não poderia estender a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática. Não se trata aqui de aventar a possível conveniência de fazer interceptação nesses sistemas, mas sim de interpretar a Constituição e os limites por ela estabelecidos à quebra do sigilo. (GRECO FILHO, 1996, p. 12)*

Assim como Greco Filho, outros juristas também sustentam a inconstitucionalidade da interceptação das comunicações de dados, como Ada Pellegrini Grinover e José Afonso da Silva.

No entanto, o entendimento de Alexandre de Morais parece mais acertado. O ilustre jurista discorda do posicionamento de Greco Filho apontando os seguintes argumentos:

> *1°) A interpretação das normas constitucionais exige que a uma norma constitucional seja atribuído o sentido que maior eficácia lhe conceda (Canotilho), sendo vedada a interpretação que lhe suprima ou diminua a finalidade (Jorge Miranda);*
> *2°) Assim, apesar de a exceção constitucional (CF, art. 5°, XII, in fine) expressamente referir-se somente à interceptação telefônica, nada impede que nas outras espécies de inviolabildidades haja possibilidade de relativização da norma constitucional, como por exemplo, na permissão da gravação clandestina com autorização judicial (RT, 692/370), pois entende-se que nenhuma liberdade individual é absoluta, sendo possível, respeitados certos parâmetros, a interceptação das correspondências, das comunicações e de dados, sempre que essas liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas, pois como salienta o Tribunal de Justiça do Estado de São Paulo, "afirmar que um direito é absoluto significa que ele é inviolável pelos limites que lhe são assinalados pelos motivos que o justificam" (TJSP - Cam. Esp. MS 13.176-0/2-SP - rel. Des. Denio Garcia);*
> *3°) Finalmente, o fato da ementa da lei afirmar que "Regulamenta o Inciso XII, Parte Final, do art. 5° da Constituição Federal", de forma alguma impede que o texto legal discipline outros assuntos, uma vez que a lei que veicula matéria estranha ao enunciado constante de sua ementa, por só esse motivo, não ofende qualquer postulado constitucional, não vulnerando tampouco as regras de processo legislativo constitucional, pelo que excluída da possibilidade de*

> *declaração de inconstitucionalidade (STF - Pleno - Adin n° 1.096-4 - medida liminar - rel. Min. Celso de Mello, Diário da Justiça, Seção I, 22 SET 1995, p. 30589), pois inexistente no vigente sistema de direito Constitucional brasileiro regra idêntica à prevista pelo art. 49 da Constituição Federal de 1934 ("Os projectos de lei serão apresentados com a respectiva ementa, enunciando, de fórma succinta, o seu objectivo, e não poderão conter matéria estranha ao seu enunciado"). (MORAES, 2002, p.151/152)*

Ademais, é preciso se atentar para o fato de que a possibilidade de quebra do sigilo da comunicação de dados apenas se concretiza se atendidos os requisitos previstos em lei, quais sejam, para subsidiar investigação ou instrução criminal e existindo indícios razoáveis da autoria ou participação em infração penal. Além do mais, se a prova puder ser feita por outros meios, ou se o fato investigado constituir infração penal punida, no máximo, com pena de detenção, a interceptação não será admitida.

Portanto, ultrapassada a questão da constitucionalidade ou não do parágrafo único do art. 1° da Lei n° 9.296, basta zelar pela observância dos limites impostos na lei para a interceptação da comunicação de dados. Assim se coíbe a prática abusiva e invasiva desse instituto, permitindo, no entanto, a investigação e apuração de ilícitos realizados através de sistemas de informática e telemática.

2.6 *Habeas data*

Outra previsão constitucional inovadora foi o *habeas data*, que insere-se no texto da Constituição Federal de 1988 mais como uma garantia em face do antigo regime ditatorial do que como instrumento efetivo de proteção à violação dos dados pessoais. Essa conclusão é inevitável quando se observa a redação do art. 5º, inciso 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;"*

Como se constata do inciso LXXII o remédio processual do *habeas data* será concedido apenas em duas circunstâncias específicas, quais sejam, para possibilitar ao impetrante o conhecimento de informações relativas a sua pessoa que estejam armazenadas em registros ou bancos de dados apenas de entidades governamentais ou de caráter público[51] e para a correção de dados constantes destes mesmos registros ou bancos de dados.

Resta claro que o constituinte de 88, ao estabelecer a previsão do *habeas data,* ainda guardava as lembranças do período ditatorial[52] e ocorreu-lhe apenas garantir o cidadão contra as arbitrariedades do governo, razão pela qual não existe a possibilidade, pela atual redação, de impetração de *habeas data* em face de entidade privada.

Bonavides (2001, p. 362) sintetiza de forma apropriada o objeto do *habeas data* consignando que "é o asseguramento do acesso às informações pessoais do impetrante constantes de registros ou bancos de dados de entidades governamentais ou de caráter público com o fim de retificação".

Não bastasse a timidez constitucional, a lei que regulamenta o acesso a informações e disciplina o rito processual do *habeas data* (Lei 9.507/97) demorou quase dez anos para ser promulgada e tem nítido caráter sancionatório,

[51] De natureza privada, mas com repercussões públicas em decorrência do modo de sua atuação.
[52] "O instituto cristaliza historicamente na consciência da sociedade brasileira uma reação jurídica do constituinte a violações, manipulações e excessos perpetrados em matéria informativa pessoal pelas entidades governamentais da ditadura ao longo de duas décadas de exercício do poder autoritário sem limites." (BONAVIDES, 2001, p. 507).

não prevendo mecanismos de controle prévio, ou medidas preventivas.

Ademais, o fato do *habeas data* ter por pressuposto a prévia negativa de prestação da informação, ou da retificação da informação[53], pelo órgão da administração, reduz sua aplicabilidade.

2.7 Código de Defesa do Consumidor

No campo da legislação infraconstitucional, o Código de Defesa do Consumidor garante ao indivíduo, na qualidade de consumidor, efetiva proteção contra a violação de seus dados pessoais constantes em bancos de dados e cadastros de consumidores.

Recolher o máximo de dados pessoais, em especial de consumidores, é um dos fundamentos da nova economia e a tecnologia vem possibilitar essa recolha de forma bastante eficiente.

Ao mercado interessa não apenas a recolha desses dados e sim todo o potencial que eles oferecem quando tratados, possibilitando verdadeira devassa na vida do seu titular.

A fim de coibir tal devassa ou ao menos minimizá-la é que o Código de Defesa do Consumidor, na Seção VI do Capítulo V, que trata dos *bancos de dados e cadastros de consumidores*, prevê a devida proteção ao titular-consumidor, estabelecendo em seu art. 43:

[53] Neste sentido a Súmula 02 do Superior Tribunal de Justiça: "Não cabe o *habeas data* (CF, art. 5º LXXII, letra a) se não houve recusa de informações por parte da autoridade administrativa".

> *Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*
> *Parágrafo 1. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*
> *Parágrafo 2. A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
> *Parágrafo 3. O consumidor, sempre que encontrar inexatidão em seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.*
> *Parágrafo 4. Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*
> *Parágrafo 5. Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.*

Embora tenha o legislador utilizado as expressões banco de dados e cadastros de consumo, indicando sua intenção em diferenciá-las, acabou por não o fazer, deixando esta tarefa para a doutrina[54]. No entanto, segundo os esclarecimentos do professor Antônio Herman V. Benjamin, um dos autores do anteprojeto do Código, citado por Efing (2002, p. 35), a intenção foi abarcar todas as modalidades de armazenamento de informações sobre consumidores, sejam elas privadas ou públicas, de uso pessoal do fornecedor ou abertas a terceiros, informatizadas ou manuais, setoriais ou abrangentes, de tal forma que a proteção ao consumidor fosse a mais abrangente possível.

[54] Embora a diferenciação entre os dois termos não seja relevante no presente trabalho, cumpre conhecê-los. Efing define *banco de dados de consumidores* como "sistemas de coleta aleatória de informações, normalmente arquivadas sem requerimento do consumidor, que dispõem de organização mediata, a atender necessidades latentes através da divulgação permanente de dados obrigatoriamente objetivos e não-valorativos, utilizando-se de divulgação a terceiros por motivos exclusivamente econômicos, e *cadastros de consumidores* como "sistemas de coleta individualizada de dados objetivos, sejam de consumo ou juízos de valor, obtidos normalmente por informação do próprio consumidor e com objetivo imediato relativo a operações de consumo presentes ou futuras, tendo provisoriedade subordinada aos interesses comerciais subjetivos do arquivista, e divulgação interna, o que demonstra a função secundária de seus arquivos". (EFING, 2002, p. 35/36)

No âmbito dessa proteção conferida pelo Código de Defesa do Consumidor, serviços de proteção ao crédito como o SCPC (Serviço Central de Proteção ao Crédito) devem observar as determinações do art. 43, sob pena de responderem por eventuais prejuízos materiais e morais.

Além disso, o próprio comércio eletrônico, modalidade que a cada ano cada mais espaço entre os consumidores,

Como observado, o ordenamento pátrio oferece algumas saídas para a proteção do titular de dados pessoais, porém ainda não a proteção jurídica esperada. Por esta razão e ante a falta de uma legislação que regulamente o tratamento informatizado de dados pessoais é que o direito à privacidade, previsto constitucionalmente, assume papel crucial nesse embate, merecendo ser devidamente analisado.

3 O DIREITO À PRIVACIDADE E O DESAFIO DA PROTEÇÃO AOS DADOS PESSOAIS

Torna-se cada vez mais difícil garantir ao titular de dados a devida proteção contra as mais variadas ameaças de violação. No entanto, como é inerente ao Direito, a busca pela solução dos conflitos e mesmo a luta por sua prevenção, impulsiona os estudiosos a encontrar possíveis caminhos a serem trilhados. Um desses caminhos conduz à previsão constitucional do direito à privacidade que, na sua condição de direito fundamental, tem a real possibilidade de garantir sua observância em face de outros direitos, ainda que fundamentais.

3.1 Evolução conceitual do direito à privacidade face às inovações tecnológicas

Talvez o ser humano nunca tenha dado tanta importância à sua privacidade quanto nos dias atuais, quando se encontra submetido a constante exposição de sua pessoa e extremamente vulnerável a perder sua privacidade.

Mas, afinal, o que se entende por privacidade? É comum a utilização dos termos vida privada, privacidade e intimidade como sinônimos. Muito embora no

campo prático a precisão técnica de cada termo não faça qualquer diferença quanto à proteção que deve ser conferida à pessoa, importa destacar suas peculiaridades e justificar o porquê da escolha do termo *privacidade*.

Em visão mais técnica, e segundo o ensinamento dos juristas alemães, conforme relata Jabur (2000, p. 257), a vida privada (entendo-a em termos amplos como o resguardo do ser humano) posiciona-se como gênero, do qual fazem parte a privacidade, a intimidade e o segredo, que se relacionam sob a forma de círculos concêntricos.

O primeiro, de maior latitude, representa a esfera privada (*Privatsphare)*, excluindo-se do conhecimento de terceiros aspectos *específicos* da pessoa; o segundo, a esfera íntima (*Intimsphare*), representa os valores atinentes ao âmbito determinado da intimidade ou esfera confidencial cujo acesso passa a ser mais restrito, somente permitido àqueles indivíduos com quem a relação pessoal se desenvolve de forma mais intensa, mas não absoluta; e por fim o terceiro, a esfera do segredo, da reserva (*Geheimsphare)*, que representa as mais profundas manifestações espirituais da pessoa, caracterizadoras da vida íntima, *stricto sensu*.

Assim, uma vez delimitado o alcance de cada expressão, parece mais oportuna a utilização do termo privacidade para se referir ao completo resguardo da pessoa, haja vista a necessidade de sua proteção integral.

Antes, contudo, de adentrar aos meandros que a privacidade encerra, compete registrar sua procedência imediata, ou seja, reconhecer que a privacidade só é efetiva se exercida em liberdade. Aliás, Jabur (2000, p. 140) leciona que “a liberdade é o primeiro atributo da vida humana. Os demais predicados

inerentes ao indivíduo e inseparáveis de sua condição humana a partir dela se amoldam e se desenvolvem".

É a liberdade, pois, pressuposto essencial ao pleno desenvolvimento da pessoa e, por via de conseqüência, à garantia de sua privacidade. A real possibilidade do indivíduo determinar o que ou quem participa de sua vida privada, reflete um exercício pleno de sua liberdade. No entanto, é sabido que na vida em sociedade a liberdade é limitada pela liberdade do outro e pelo interesse comum.

Silva sintetiza bem o problema ao asseverar que

> *a questão fundamental, contudo, é saber se, feita a escolha, é possível determinar-se em função dela. Isto é, se se têm condições objetivas para atuar no sentido da escolha feita, e, aí, se põe a questão da liberdade externa. (SILVA, 2003, p. 230/232).*

Portanto, existindo condições favoráveis ao atuar da liberdade externa, o homem seria livre para realizar todas as suas vontades. Ocorre que uma liberdade assim colocaria em risco o atuar livre de outros, pois não teria medida. Daí porque a necessidade de se limitar a liberdade, sem que com isso o homem seja menos livre. Isso se explica pelo fato da liberdade conviver pacificamente com a autoridade e dela depender.

Silva ainda explica que liberdade e autoridade se complementam e que um mínimo de coação sempre há que existir, devendo, no entanto, tratar-se de autoridade legítima, que provém do exercício da liberdade mediante o consentimento popular.

Neste sentido, Jabur afirma que o direito à liberdade consiste em:

> *poder satisfazer um interesse jurídico de natureza econômica ou espiritual munido de proteção jurídica (direito subjetivo), ou seja, conforme o querer do titular desse direito, mas também de acordo com a* voluntas legis *que estabelece eventual contrapeso a tal prerrogativa. É o modo de ser da pessoa encontrando temperamentos no sistema que deve privilegiar o conjunto de princípios fundamentais cuja predominância interessa ao Estado e à sociedade. (JABUR, 2000, p. 144)*

A Declaração francesa de 1789, intitulada de Declaração dos Direitos do Homem e do Cidadão, de inspiração iluminista, ao definir a liberdade, acabou por consagrar o direito à liberdade como "aquele que termina onde começa o direito do outro"[55].

Ocorre que esse princípio do Iluminismo já vem sendo revisto diante das inovações tecnológicas, em especial da revolução das tecnologias da informação e comunicação, como noticia Ferraz Júnior:

> *é uma alteração no antigo princípio do Iluminismo, segundo o qual a dignidade humana está centrada na liberdade individual e a liberdade de um termina onde começa a liberdade do outro. Com efeito, o que está sendo proposto é que a dignidade humana deve estar centrada no viver em livre comunicação um com o outro. Na verdade, hoje, o que deveria ser dito é que 'a liberdade de um começa onde começa a liberdade do outro'. (FERRAZ JÚNIOR, 2001, p. 245)*

Em que pese as novas nuances do conceito de liberdade, que com certeza irão influenciar o alcance do direito à privacidade, estas ainda precisam de certo espaço de tempo para serem absorvidas pela sociedade e reguladas pelo direito, uma vez que se está diante de verdadeira mudança comportamental.

---

[55] É preciso deixar registrado o posicionamento inovador de Ferraz Júnior (2001, p. 241/7) que, em sintonia com a moderna doutrina alemã, propõe, em recente artigo, um repensar do tema *liberdade* diante das profundas mudanças pelas quais a sociedade vem passando. Cita Wolfgang Hoffmann-Riem que trata do *exercício da liberdade em reciprocidade* em face das modernas relações de comunicação, onde liberdade não é ser livre *dos* outros, mas liberdade *por* intermédio dos outros, uma vez que a liberdade em rede informatizada se manifesta sempre em reciprocidade, pois a informação posta individualmente em rede é, simultaneamente, para os outros.

Portanto, é ainda seguindo a velha orientação iluminista que o homem vem se comportando e elaborando as leis que norteiam a vida em sociedade, estabelecendo limites ao exercício da liberdade natural. Assim é que o indivíduo é livre para fazer ou não o que bem entender, desde que a lei não preveja o contrário (art. 5, II, da Constituição Federal); a manifestação do pensamento é livre, desde que não acobertada pelo anonimato (art. 5, IV, da Constituição Federal).

Neste campo conceitual da privacidade, que tem a liberdade como pressuposto, tem se vislumbrado a necessidade de se atualizar o conceito de privacidade e o âmbito de sua proteção legal. Em virtude do advento das tecnologias da informação e comunicação, um outro tipo de necessidade relacionada à privacidade tem se manifestado. Trata-se da necessidade do indivíduo resguardar seus dados pessoais.

Em face do valor adquirido pela informação, obtê-la tornou-se verdadeira obcessão, pouco importando se de forma lícita ou não. O fato é que a tecnologia tem possibilitado um acesso aos dados pessoais como nunca antes, tornando possível a descoberta de aspectos relevantes da intimidade das pessoas, sem que elas ao menos se dêem conta, diante da naturalidade de se preencher uma ficha cadastral em qualquer estabelecimento médico, escolar ou comercial.

Ante esta realidade assustadora, que pode servir tanto a uma causa nobre, como por exemplo, a tecnologia do anjo digital (digital angel)[56] e do cartão

[56] Um chip de computador do tamanho de uma moeda de 1 centavo, que chegou ao mercado americano no começo de 2001. Ele pode ser embutido num relógio de pulso ou até mesmo implantado sob a pele e enviar e receber sinais eletrônicos que podem ser captados por um satélite. Assim, pode tanto rastrear um indivíduo e localizá-lo em qualquer lugar do planeta, quanto enviar sinais, por exemplo, a um centro médico, avisando que a pessoa sofreu um acidente ou teve um ataque cardíaco (com consentimento do usuário). (LEPIANI, 2001, p. 77 e 78).

inteligente (smart card)[57], quanto a um governo totalitário[58] ou a um empregador inescrupuloso[59], tornou-se imperativo repensar a extensão do conceito de *privacidade*.

Assim é que pensar em privacidade como aquele direito do indivíduo *ser deixado em paz*[60] já não mais satisfaz as exigências do homem atual. À época do surgimento do direito à privacidade, este pretendia ser o mais abrangente dos direitos do homem. Doneda (2004) explica que esse direito era estritamente ligado ao espaço físico privado do homem, tanto que já no século XVII, na Inglaterra, se estabelecia o princípio da inviolabilidade do domicílio - *man´s house is his castle.* Daí então a identificação da doutrina do *right to privacy* com o direito ao isolamento.

As tecnologias evoluíram e com elas o homem, de forma que hoje já não é mais possível se identificar o direito à privacidade apenas com o sentido de isolamento. A fim de se garantir a privacidade do indivíduo urge reconhecer-lhe a capacidade de controlar suas informações pessoais, pois estas, sem dúvida, são seu maior patrimônio, são a garantia de sua individualidade e assim de sua identidade.

---

[57] Cartão de crédito que contém um circuito integrado que lhe dá uma quantidade limitada de inteligência e memória e que são usados para identificação e codificação de determinadas informações, tais como o histórico médico de uma pessoa. (GATES, 1999, p. 423)

[58] Na Itália, em 1954, o Conselho Ministerial decidiu iniciar uma política de discriminação contra os comunistas e seus aliados, com base em informações colhidas sobre a fé política dos italianos. (BELLAVISTA apud DONEDA, 2003)

[59] É o caso do fabricante de automóveis FIAT que, conforme posteriormente divulgado, selecionou 350.000 dos seus empregados entre 1948 e 1971 com base em dados sigilosos do SIFAR (antigo serviço secreto militar italiano), evitando a contratação de pessoas com tendências políticas de esquerda. (BELLAVISTA apud DONEDA, 2003)

[60] Segundo Efing (2003, p. 51) data de 1890 o famoso artigo de Warren e Brandeis, denominado “The right to privacy”, onde os autores norte-americanos, utilizando-se da definição atribuída ao juiz norte-americano Cooley, criada em 1873 e considerada o mais expressivo conceito de privacidade, qual seja, “o direito de ser deixado em paz” (the right to be let alone), reivindicaram o nascimento de um novo direito que tutelasse a esfera privada do ser humano, o direito à privacidade.

Com Doneda (2003) pode-se falar em uma evolução do conceito de *ser deixado em paz* para abarcar também *o exercício do controle dos dados que lhe digam respeito*.

A própria doutrina pátria, municiada pela estrangeira, já começa a refletir essa evolução conceitual. Neste sentido Silva, que utiliza a expressão privacidade para abarcar todas as manifestações da esfera íntima, privada e da personalidade, utilizando-se da definição fornecida por Matos Pereira, define o direito à privacidade como

> *o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controlo, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. (PEREIRA apud SILVA, 2003, p. 202)*

Também acompanhando a evolução conceitual, Bastos afirma que este direito

> *consiste na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano. (BASTOS,1988-1989, p. 63)*

É, portanto, evidente a influência da sociedade informacional na atual esfera protetiva da privacidade. O indivíduo precisa, de alguma forma, encontrar guarida no direito à privacidade para proteger seus dados pessoais, de forma que mantenha o controle sobre informações a seu respeito que considera essenciais ao pleno desenvolvimento de sua personalidade.

É interessante anotar, na esteira do posicionamento sustentado, que o novo Código Civil brasileiro prevê os direitos da personalidade, o que demonstra

uma grata afinação no quadro positivo brasileiro e aumenta as possibilidades de efetividade do direito à privacidade.

3.2 Invocação do direito à privacidade

O Brasil faz parte do rol de países que não disciplinam a proteção dos dados pessoais a nível constitucional e nem infraconstitucional. Não obstante a ausência de disciplina específica, o ordenamento jurídico pátrio prevê o direito fundamental à privacidade, estatuído no art. 5º, inciso X, da Constituição Federal, a saber:

> *Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
> *X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas[61], assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

Constando, pois, o direito à privacidade, do rol dos direitos fundamentais[62], o cidadão brasileiro não se encontra totalmente desprotegido contra a violação de seus dados pessoais. Tal afirmação se justifica em dois sentidos, um positivo e outro negativo.

[61] Como se percebe, o constituinte de 88 optou por diferenciar o direito à intimidade do direito à vida privada, à honra e à imagem, distinção esta desnecessária para os fins da presente discussão, uma vez que a proteção que ora se discute para os dados pessoais requer uma noção ampla e genérica do direito à privacidade, englobando os conceitos de intimidade, privacidade, honra e imagem.

[62] Assim, segundo Sarlet (1998, p. 31) tem-se como fundamentais "aqueles direitos do ser humano reconhecidos e positivados na esfera do direito constitucional positivo de determinado Estado"

Positivamente justifica-se pela vanguarda de certos magistrados que, em sintonia com a moderna doutrina e com os avanços tecnológicos, não deixam o titular de dados pessoais sem proteção jurídica e, para tanto, utilizam-se do direito à privacidade, previsto constitucionalmente, para salvaguardar o direito à proteção de dados pessoais.

Nesse sentido a posição[63] do Ministro Ruy Rosado de Aguiar, do Superior Tribunal de Justiça, ao votar em Recurso Especial acerca do cancelamento de registro de nome em arquivos do SCPC, exemplifica bem a orientação de lúcidos membros do Judiciário pátrio. Dentre outras palavras consigna:

> *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 da vida, permite 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. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do ombudsman, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação (Hassemer, Proteção de dados, palestra proferida na Faculdade de Direito da UFRGS, 22.11.1993). No Brasil, a regra do art. 5, inc. X, da Constituição de 1988, é um avanço significativo: 'São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à*

[63] Decisão proferida no Recurso Especial n. 22.337/RS, publicada no DJ de 20.03.1995.

indenização pelo dano material ou moral decorrente de sua violação´. (SUPERIOR TRIBUNAL DE JUSTIÇA, 2003)

Verifica-se, portanto, que a ausência de norma que discipline a proteção de dados pessoais não tem sido obstáculo à efetiva proteção do titular de dados, quando estes se encontrem violados ou em vias de sofrer violação. É evidente que a regulamentação acerca do tratamento de dados pessoais conferiria ao seu titular uma esfera protetiva muito mais abrangente e específica.

Da forma como se encontra hoje (ou melhor dizendo, não se encontra), o direito pátrio pode garantir ao titular a proteção de seus dados pessoais, invocando-se o direito à privacidade, previsto no art. 5º, X, da Constituição Federal[64] – contando com o bom senso do magistrado -, e em determinados casos específicos o direito à privacidade nas comunicações, previsto no art. 5. XII, e o *habeas data*, ambos também previstos na Constituição Federal.

De outro modo, justifica-se negativamente face a ausência de regulamentação da matéria. É extremamente temerária essa lacuna na legislação brasileira, pois permite que o tratamento informatizado de dados pessoais ocorra sem um mínimo de controle. Ademais, aquele que sinta lesado em virtude de violação de seus dados pessoais não tem segurança e nem certeza de ver seus direitos assegurados por meio do Judiciário.

É inadmissível que o Brasil, através de seus legisladores, venha dispensando tão pouca atenção a tema tão relevante quanto a proteção de dados pessoais. Enquanto o país parece *dormir*, outros já estão na estrada há muito tempo

[64] No tocante ao direito à privacidade, pela primeira vez previsto expressamente na Constituição pátria, importa destacar que até então este poderia ser deduzido do direito à propriedade ou à liberdade. Atualmente, porém, é possível enquadrá-lo, com maior propriedade, como manifestação do direito à vida, presente no caput do art. 5º.

e continuam a aprimorar seu sistema de proteção, pois a evolução tecnológica não pára.

Além dos enormes prejuízos que o titular possa vir a sofrer com o tratamento de seus dados, o país também não é visto com bons olhos por aqueles que prezam pela segurança de suas relações comerciais e pela segurança de seus cidadãos.

É preciso ainda que se registre, além da natureza de direito fundamental do direito à privacidade, sua natureza de direito personalíssimo[65] e nesse sentido a existência de normas infraconstitucionais a também assegurá-lo.

Jabur, a esse respeito, esclarece que

> *alguns autores afirmam a identidade entre os direitos do homem ou direitos fundamentais (liberdades públicas ou civis, para alguns) e os direitos da personalidade. Destaca-se a essencialidade que predomina em ambos, embora os primeiros sejam concernentes ao direito público - vocacionados, pois, à proteção do indivíduo contra o arbítrio do Estado -, enquanto os últimos, pertencentes ao direito privado, voltam-se às relações entre particulares. (JABUR, 2000, p. 30)*

Serve a aludida diferenciação apenas para reforçar o âmbito de proteção aos dados pessoais, pois em se tratando de violação perpetrada por particular cabe a invocação também do direito à privacidade, como espécie dos direitos personalíssimos.

[65] Jabur (2000, p. 32-40) esclarece que os direitos da personalidade, embora reconhecidos desde a antiguidade, apenas afirmaram-se no século passado, quando superou-se a concepção defendida por Savigny, que inadmitia a existência de direitos originários subjetivos, repelindo a idéia de direitos do homem sobre ele próprio. Na França, a noção de direitos da personalidade apareceu pela primeira vez no julgamento Lecoq, em 25.06.1902, tendo evoluído de forma lenta, mas ricamente interpretada pela doutrina e jurisprudência que se formaram. No Brasil, apesar da parcial constitucionalização dos direitos personalíssimos (CF, art. 5, caput, IV, V, XI, XII, v.g.), a exemplo do que vem ocorrendo em grande parte das nações, o novo Código Civil cuidou de dedicar capítulo especial aos direitos da personalidade.

Jabur (2000, p. 39/74) elenca as qualidades dos direitos personalíssimos, que se reunidas integralmente são capazes de garantir o pleno desenvolvimento da personalidade do ser humano. Esses direitos, e conseqüentemente o direito à privacidade, são *inatos*, pois surgem com o primeiro respiro pulmonar humano, momento em que também aflora a personalidade para a maioria dos ordenamentos jurídicos, entre eles o brasileiro; *essenciais ou vitalícios*, porque não podem faltar durante toda a vida[66]; *extrapatrimoniais*, porque não encontram, pura e simplesmente, estimativa em dinheiro – senão diante da lesão, para efeito de compensação -, mas apresentam nítido influxo pecuniário; *relativamente indisponíveis*, na medida que seu titular fruir e explorar algumas de suas faculdades, por não ofenderem a preservação do direito de que emanam[67]; *irrenunciáveis*, devido a ausência de poder pleno de disposição.

Em vigor desde janeiro de 2003, o novo Código Civil brasileiro inovou ao dedicar um Capítulo aos direitos da personalidade, entendidos estes como direitos subjetivos da pessoa que visam defender o que lhe é próprio, ou seja, a vida, a integridade, a liberdade, a sociabilidade, a reputação ou honra, a imagem, a privacidade, a autoria, etc.

Introduz assim, no ordenamento pátrio, mais uma forma de proteção à privacidade constitucional pela garantia da dignidade humana. O art. 11 do Código Civil assim estatui:

---

[66] Jabur (2000, p. 44) A fruição da vida, em sua mais ampla acepção, o desfrute da integridade física incólume, assim como, e ainda exemplificativamente, o respeito devido à honra e à privacidade constituem expressões das quais não pode o ser humano, em princípio, abrir mão. Porque é o desenvolvimento da personalidade que estaria comprometido, se fossem tais direitos tomados como prescindíveis.

[67] É o caso da utilização e publicação consentida do retrato, da divulgação autorizada de aspectos íntimos e da tolerância da ofensa à honra. O direito permanece intacto, apenas suas potencialidades são cedidas temporariamente.

> *Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.*

E em caso de violação desses direitos o legislador cuidou de garantir sua observância através da atuação do magistrado, deixando bem claro que compete ao Judiciário zelar pela inviolabilidade da vida privada, ao determinar no art. 21:

> *A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.*

À primeira vista pode parecer desnecessária esta previsão, já que a Constituição Federal garante o direito à privacidade como direito individual fundamental e como tal tem aplicação imediata, a teor do parágrafo 1, de seu art. 5. Porém, embora tenha aplicação imediata a previsão constitucional, o legislador infraconstitucional quis torná-la plenamente efetiva, atribuindo ao juiz a adoção das providências necessárias para impedir ou fazer cessar qualquer ato contrário.

Em acurada análise do art. 21 do ainda então Projeto do Código Civil, Jabur (2000, p. 304) expressa sua quase decepção com a redação do mencionado dispositivo, que na sua opinião foi extremamente tímida ao nem sequer ventilar o que se depreende da expressão “vida privada”. Não que o legislador infraconstitucional devesse se preocupar em conceituar o termo, porém, que apresentasse, ao menos, um rol exemplificativo de ações consideradas atentatórias, o que, sem dúvida, diminuiria o arbítrio e facilitaria o exercício do direito ora protegido.

Não deixa de ser uma observação bastante interessante, haja vista que a lei ordinária poderia ter dado maior contribuição à proteção da vida privada se ousasse transpor os lindes principiológicos que caracterizam a Constituição de um país.

> *Conveniente seria, assim, e pelo menos, dispor para proteger sobre: (i) os aspectos fundamentais que integram a noção da vida privada, como a mera tranqüilidade, ou ausência de turbação, bem ainda a compreensão de outras manifestações personalíssimas, bastante afeitas ao direito em estudo (palavras, escritos pessoais, manuscritos e correspondências etc); (ii) os meios e instrumentos aptos à freqüente intromissão, tais como interceptação de comunicações telemáticas ou informatizadas, transmissão de dados pessoais, familiares ou profissionais; captação de imagens, filmes, fotos etc. (JABUR, 2000, p. 305)*

De qualquer forma, o direito à vida privada é protegido em nível constitucional, por se tratar de direito fundamental, o que, de certa forma, ameniza a ausência de comando na lei ordinária em comento.

3.3 A eficácia dos direitos fundamentais

Muito se tem escrito a respeito dos direitos fundamentais[68], sem contudo haver uma convergência a respeito do prisma pelo qual estes devem ser analisados. Sarlet (1998, p.22), na esteira do jurista lusitano Vieira de Andrade, consigna que os direitos fundamentais podem ser abordados sob uma *perspectiva filosófica (ou jusnaturalista)*, entendidos como direitos de todos os homens, em todos os tempos e lugares; sob uma *perspectiva universalista (ou internacionalista)*,

[68] Sarlet (1998, p. 29) opta pela terminologia "Direitos Fundamentais", inobstante outras expressões sejam largamente utilizadas pela doutrina, como direitos humanos, direitos do homem, direitos subjetivos públicos, liberdades públicas, direitos individuais, liberdades fundamentais, direitos humanos fundamentais. A nossa própria Constituição Federal de 1988 se caracteriza por sua diversidade semântica, a saber: art. 4º, II – direitos humanos; epígrafe do Título II e art. 5º, § 1º - direitos e garantias fundamentais; art. 5º, LXXI – direitos e liberdades constitucionais; art. 60, § 4º, IV – direitos e garantias individuais.

entendidos como direitos de todos os homens (ou categorias de homens) em todos os lugares, num certo tempo; e sob uma *perspectiva estatal (ou constitucional)*, analisados na qualidade de direitos dos homens, num determinado tempo e lugar.

Assim não há que se rotular essa ou aquela perspectiva como certa ou errada e sim escolher uma ótica para centrar o estudo e a partir daí aprofundar a análise. Desta forma, optou-se pela perspectiva do direito constitucional positivo (estatal), enfatizando-se o Direito pátrio. Porém, é necessário que se registre a ocorrência de um processo de aproximação e harmonização, especialmente entre os direitos humanos e os direitos fundamentais, visando a concretização de um direito constitucional internacional[69].

Mas, em conformidade com a opção acima revelada, esclarecedor é o conceito de direitos fundamentais apresentado por Sarlet:

> *o termo 'direitos fundamentais' se aplica para aqueles direitos do ser humano reconhecidos e positivados na esfera do direito constitucional positivo de determinado Estado, ao passo que a expressão 'direitos humanos' guardaria relação com os documentos de direito internacional, por referir-se àquelas posições jurídicas que se reconhecem ao ser humano como tal, independentemente de sua vinculação com determinada ordem constitucional, e que, portanto, aspiram à validade universal, para todos os povos e tempos, de tal sorte que revelam um inequívoco caráter supranacional (internacional). (SARLET, 1998, p. 31)*

[69] Bastos (2000, p. 174) registra a prática da proclamação de direitos de âmbito transnacional, como por exemplo, as feita por meio de "Declarações", que procuram respondem à necessidade de conferir uma proteção ao estrangeiro em face das autoridades do Estado sob cujo território ele se encontre, à preocupação de assegurar uma defesa de cada nacional contra eventual opressão de seu próprio Estado, e ao desejo de se levar a efeito uma consagração internacional de uma concepção universalista dos direitos do homem. Porém, a escolha de quais direitos devam ser protegidos, aliado ao fato do indivíduo ainda encontrar resistência em ser reconhecido como pessoa juridicamente relevante perante a ordem internacional, tem trazido dificuldades à implementação dessa ordem internacional. O mais importante dos documentos dessa natureza é a Declaração Universal dos Direitos do Homem, que foi votado pela Assembléia Geral da ONU, em dezembro de 1948. Em 2000, a União Européia editou a Carta dos Direitos Fundamentais.

Seguindo esse raciocínio, o caminho lógico para se chegar aos direitos fundamentais é descobrir de que forma estes foram sendo inseridos nos textos constitucionais. Essa inserção ocorreu de maneira gradativa, mediante o reconhecimento de determinado grupo de direitos fundamentais em dado momento da história. Assim se convencionou denominar de geração de direitos fundamentais a certo grupo de direitos reconhecidos e positivados por determinada ordem estatal em determinado tempo, ou no dizer de Sarlet, *dimensão*, e não geração, de direitos fundamentais, a fim de evidenciar o caráter evolutivo e complementar das várias fases de reconhecimento desses direitos.

Em apertada síntese pode-se registrar que a primeira geração de direitos fundamentais foi aquela que marcou o reconhecimento de seu *status* constitucional material e formal, através da inserção dos primeiros direitos em texto constitucional, representados pelos direitos civis e políticos, em nítida resistência e oposição ao Estado.

Sarlet (1998, 44) esclarece, a despeito do dissídio doutrinário sobre a paternidade dos direitos fundamentais, disputada entre a Declaração de Direitos do povo da Virgínia, de 1776, e a Declaração Francesa, de 1789, que é a primeira que efetivamente "marca a transição dos direitos de liberdade legais dos ingleses[70] para os direitos fundamentais constitucionais", ressaltando ainda que pela primeira vez esses direitos foram reconhecidos na ordem constitucional:

> *Com a nota distintiva da supremacia normativa e a posterior garantia de sua justiciabilidade por intermédio da Suprema Corte e do controle judicial da constitucionalidade, pela primeira vez os direitos naturais do homem foram acolhidos e positivados como direitos fundamentais constitucionais, ainda que este status constitucional da*

[70] São antecedentes dos direitos fundamentais a *Magna Carta* (1215-1225), a *Petition of Rights* (1628), o *Habeas Corpus Amendment Act* (1679) e o *Bill of Rights* (1688) do direito inglês.

> *fundamentalidade em sentido formal tenha sido definitivamente consagrado somente a partir da incorporação de uma declaração de direitos à Constituição de 1791, mais exatamente, a partir do momento em que foi afirmada na prática da Suprema Corte a sua supremacia normativa. (SARLET, 1998, p. 45)*

A segunda geração de direitos fundamentais ampara-se no princípio da igualdade, refletindo-se nos chamados direitos sociais, culturais, econômicos e coletivos. Perpassa praticamente todo o século XX sob a égide do Estado Social.

A respeito, Bastos complementa:

> *De outro lado, e essa talvez seja a alteração mais profunda, surgiram os direitos cujo conteúdo consiste na possibilidade de o indivíduo receber alguma prestação do Estado. Este não permanece neutro diante das disparidades sociais. O princípio da igualdade, muito provavelmente o mais importante dos direitos clássicos, tornou-se um irrisão. Como alguém observou, consistia em dizer que a lei assegurava igual direito de pobres e ricos dormirem debaixo da ponte. Esta igualdade perante a lei passou a chamar-se formal para opor-se a uma outra que se denominou material. Na elaboração desta última teve importância decisiva o pensamento marxista ao demonstrar que o exercício dos direitos depende de meios. Por exemplo, a liberdade de escolher o domicílio está na dependência de ter-se o dinheiro para pagar o aluguel. (BASTOS, 2000, p.172/173)*

A terceira geração é edificada sobre o princípio da fraternidade ou solidariedade, nas palavras de Bonavides (2001, p. 523), dotada “de altíssimo teor de humanismo e universalidade”. À medida que não se destinam à proteção de interesses de um indivíduo ou de um grupo ou Estado determinado, materializam-se no direito ao desenvolvimento, no direito à paz, no direito ao meio ambiente, no direito de propriedade sobre o patrimônio comum da humanidade e no direito de comunicação.

Por fim, pode-se falar numa quarta geração de direitos, ainda em fase de desenvolvimento, tendo em vista o processo de globalização política em andamento no mundo. Tal processo conduz à globalização dos direitos

fundamentais, ou seja, a sua universalização no campo institucional. Assim, o direito à democracia, o direito à informação e o direito ao pluralismo são exemplos de direitos essenciais à concretização da sociedade que se almeja.

Da forma como se encontram positivados, em especial no direito pátrio, os direitos fundamentais têm garantia de aplicabilidade imediata, a teor do § 1º do art. 5º da Constituição Federal. Isso importa dizer que um direito fundamental será plenamente eficaz e aplicável, apenas podendo sofrer certa restrição em sua eficácia diante da aplicação de outro direito fundamental, quando então se instala possível colisão de direitos fundamentais.

3.4 A possível colisão entre direitos fundamentais

Como já ressaltado, a contemplação, pelo Código Civil, dos direitos da personalidade, apenas reforçou a proteção que se conferia antes à privacidade por meio de previsão constitucional, com *status* de direito fundamental. Sendo assim, a invocação da tutela constitucional é indispensável.

No entanto, ao se invocar o direito à privacidade para proteger o titular da violação de seus dados pessoais, outros direitos, também fundamentais, podem ser invocados pelo responsável pelo tratamento desses dados, haja vista a previsão constitucional de direitos, verdadeiros princípios, que abrangem os mais diversos interesses e que foram gradativamente incorporados à Constituição, como já analisado.

Assim, o choque entre direitos fundamentais é inevitável. Ocorre que a solução do conflito entre esses direitos não se resolve simplesmente excluindo-se

um dos direitos em prol do outro. A questão se coloca no nível dos princípios, de acordo com a moderna doutrina[71], que agora lhes confere normatividade[72], de forma que eventual colisão deve se resolver no plano dos princípios.

Alexy, eminente jurista alemão, ao estudar uma teoria material dos direitos fundamentais em bases normativas, instituiu a distinção entre regras e princípios, conjugando ambos debaixo do conceito de normas, no que, em essência, também sustenta Ronald Dworkin.

Canotilho (1998, p. 1034), na esteira de Alexy e Dworkin, também defende a normatividade dos princípios, consignando que regras e princípios são duas espécies de normas e que a distinção entre elas é uma distinção entre duas espécies de normas. Esse também é o entendimento de Paulo Bonavides:

> *Não há distinção entre princípios e normas, os princípios são dotados de normatividade, as normas compreendem regras, a distinção relevante não é, como nos primórdios da doutrina, entre princípios e normas, mas entre regras e princípios, sendo as normas o gênero e as regras e os princípios a espécie. (BONAVIDES, 2001, p. 259)*

Assim, há a necessidade de se diferenciar regras de princípios, uma vez que a solução dos conflitos ocorre de modo diferente. Canotilho bem trabalha essas diferenças, afirmando que, qualitativamente, se distinguem nos seguintes aspectos:

---

[71] Friedrich Müller (com sua teoria estruturante do direito – fazendo contraponto com a teoria de Kelsen), Alexy (com a análise dos direitos fundamentais) e Dworkin (estabelecendo a conexidade entre Direito e Moral – fazendo contraponto com a teoria de Hart e assim entre as universidades de Harvard e Oxford).

[72] Na fase jusnaturalista, a mais antiga, a normatividade era nula, preocupando-se os jusnaturalistas mais com seu ideal de justiça. Os princípios gerais de direito são concebidos em forma de axiomas jurídicos ou normas estabelecidas pela razão, são princípios de justiça, constitutivos de um Direito ideal. Essa corrente ressurge no século XX, embora com menos força. A fase seguinte é a positivista, contrapondo-se ao jusnaturalismo. Ocorre a teorização dos princípios, integrando estes os Códigos, como fonte normativa subsidiária. Sustenta-se que os princípios já estão dentro do Direito Positivo e, por ser este um sistema coerente, podem ser inferidos do mesmo. O valor dos princípios deriva das próprias leis e não em razão de um Direito natural ou ideal, ou de certa forma ditados pela razão.

> *Em primeiro lugar, os princípios são normas jurídicas impositivas de uma optimização, compatíveis com vários graus de concretização, consoante os condicionalismos fácticos e jurídicos; as regras são normas que prescrevem imperativamente uma exigência (impõem, permitem ou proíbem) que é ou não cumprida (nos termos de Dworkin: applicable in all-or-nothing): A convivência dos princípios é conflitual (Zagrebelsky), a convivência de regras é antinómica; os princípios coexistem, as regras antinómicas excluem-se. Conseqüentemente, os princípios, ao constituírem exigências de optimização, permitem o balanceamento de valores e interesses (não obedecem, como as regras, à 'lógica do tudo ou nada'), consoante o seu peso e a ponderação de outros princípios eventualmente conflitantes; as regras não deixam espaço para qualquer outra solução, pois se uma regra vale (tem validade) deve cumprir-se na exacta medida das suas prescrições, nem mais nem menos. Como se verá mais adiante, em caso de conflito entre princípios, estes podem ser objecto de ponderação, de harmonização, pois eles contêm apenas 'exigências' ou 'standards' que, em 'primeira linha' (prima facie), devem ser realizados; as regras contêm 'fixações normativas' definitivas, sendo insuscentável a validade simultânea de regras contraditórias. Realça-se também que os princípios suscitam problemas de validade e peso (importância, ponderação, valia); as regras colocam apenas questões de validade (se elas não são correctas devem ser alteradas)." (CANOTILHO, 1998, p. 1035-1036)*

Portanto, em se tratando de colisão entre direitos fundamentais, verdadeiros princípios, não há que se falar em antinomia de regras jurídicas, de forma que sua solução também não poderá ser na forma do tudo ou nada. Isso porque no moderno Estado Democrático de Direito tem-se uma Constituição pluralista, que reúne interesse de toda uma sociedade pluralista, interesses muitas vezes antagônicos e conflitantes, de forma que não é possível simplesmente excluir um princípio em prol de outro, aceitando que um é válido e outro não.

Bonavides (2001, p. 251) analisando a questão do conflito de regras e a colisão de princípios e citando Alexy conclui afirmando que "um conflito entre regras somente pode ser resolvido se uma cláusula de exceção, que remova o conflito, for introduzida numa regra ou pelo menos se uma das regras for declarada nula".

Já com os princípios isto não ocorre. Quando há colisão não existe necessidade que seja declarado nulo ou que uma cláusula de exceção seja introduzida no ordenamento jurídico, bastando que um princípio recue. Nos casos concretos os princípios têm um peso diferente, então prepondera aquele de maior peso.

Logo, colidindo o direito à privacidade com o direito à informação ou à liberdade de expressão, por exemplo, um princípio não pode simplesmente ser considerado inválido, justamente por se tratar de um direito fundamental. Nesse caso a solução que melhor parece resolver a controvérsia é a aplicação do juízo de ponderação e concordância prática (Canotilho).

O juízo de ponderação propõe uma harmonização, no caso concreto, dos direitos fundamentais em colisão, por meio de juízo de ponderação que vise preservar e concretizar ao máximo os direitos e bens constitucionais protegidos.[73]

Canotilho, ao propor o juízo de ponderação, alerta que

> *a pretensão de validade absoluta de certos princípios com sacrifício de outros originaria a criação de princípios reciprocamente incompatíveis, com a consequente destruição da tendencial unidade*

[73] Conforme relata Lima (2003), na Alemanha, em um caso famoso, um sujeito foi preso, por estar sendo acusado de inúmeros crimes de grande repercussão social. Logicamente, a imprensa local pretendia divulgar amplamente a matéria, tendo, inclusive, uma emissora editado um documentário, o qual seria transmitido em horário nobre. Diante desses fatos, o sujeito que havia sido preso aforou uma ação pretendendo impedir os intentos da imprensa sob a alegação de que a divulgação da matéria feriria o seu direito à intimidade e à privacidade, sendo certo que, após a divulgação, seria impossível ao sujeito tornar a ter uma vida normal. Estaríamos, assim, diante de uma colisão de dois princípios constitucionais: a liberdade de expressão e o direito à intimidade. O fato foi posto a julgamento, e a Justiça Alemã, utilizando o princípio da concordância prática, assim decidiu: a imprensa poderá, em nome da liberdade de expressão, exibir a matéria. No entanto, visando preservar o direito à intimidade do indivíduo, não poderá citar seu nome completo (mas somente as iniciais), nem mostrar seu rosto (deverá utilizar mecanismos eletrônicos para desfigurá-lo). Conciliou-se, dessa forma, os princípios da liberdade de expressão e da privacidade. É a concordância prática.

> *axiológica-normativa da lei fundamental. (CANOTILHO, 1998, p. 1056)*

Daí porque os princípios serem “objecto de ponderação e concordância pratica, consoante o seu ‘peso’ e as circunstancias do caso”.

Luis Roberto Barroso, nesta linha de harmonização, alerta que o operador do direito terá ainda que respeitar o núcleo essencial dos direitos fundamentais, nos seguintes termos:

> *Trata-se de uma linha de raciocínio que procura identificar o bem jurídico tutelado por cada uma delas, associá-lo a um determinado valor, isto é, ao princípio constitucional ao qual se reconduz, para, então, traçar o âmbito de incidência de cada norma, sempre tendo como referência máxima as decisões fundamentais do constituinte. (BARROSO, 1996, p. 185).*

Nesse sentido, o princípio da dignidade da pessoa humana, expresso no artigo 1º, inciso III, da Constituição Federal de 1988, mostra-se como o princípio central da ordem constitucional, tanto que José Afonso da Silva afirma que este princípio é “um valor supremo que atrai o conteúdo de todos os direitos fundamentais do homem” e que em decorrência dele

> *a ordem econômica há de ter por fim assegurar a todos existência digna (art. 170), a ordem social visará a realização da justiça social (art. 193), a educação, o desenvolvimento da pessoa e seu preparo para o exercício da cidadania (art. 205) etc., não como meros enunciados formais, mas como indicadores do conteúdo normativo eficaz da dignidade da pessoa humana”. (SILVA, 2003, p. 109)*

Essa orientação, portanto, deve ser clara ao operador do direito, a fim de respeitar a vontade original da Constituição e harmonizar da melhor maneira possível os direitos colidentes. No caso específico do tratamento informatizado de dados pessoais e a possível ocorrência de dano à privacidade do

titular desses dados, é preciso primar pela dignidade da pessoa humana, de modo que, toda vez que o tratamento de dados implicar em violação à dignidade do titular dos dados, sua privacidade deverá ter primazia, sob pena de violação a sua dignidade.

Por fim, há que se registrar que, ao se propor a harmonização dos direitos fundamentais colidentes, mediante o respeito à essência do núcleo dos direitos fundamentais – consubstanciado no direito à dignidade humana -, está a se propor também a observância do princípio da proporcionalidade, que tem a finalidade de garantir que, em cada caso, a composição que se efetue não enseje o sacrifício unilateral de um princípio em relação aos outros, mas sim a harmonização dos mesmos, de modo a obter-se a máxima efetividade de todos eles.

Aliás, este é o grande desafio da sociedade brasileira, à medida que carece de regras jurídicas específicas ao tratamento informatizado de dados pessoais. Se as mesmas existissem, eventual conflito se resolveria no plano da regras, quando uma teria de ceder em favor da outra, ou na melhor lição de Dworkin, na forma do tudo ou nada.

Não existindo tais regras, são os princípios que oferecem ao titular de dados a proteção almejada, em especial o princípio da dignidade humana, consubstanciado no direito à privacidade, que deve prevalecer ante a qualquer outro direito fundamental que, diante do caso concreto, se mostre contrário à dignidade humana.

3.5 O direito do titular de dados pessoais a caminho da regulamentação

Mesmo diante da constatação de que o titular de dados pessoais encontra proteção jurídica no ordenamento brasileiro em face de violação à seus dados - conseqüentemente à sua privacidade -, por meio da previsão constitucional do direito à privacidade, a necessidade em se elaborar leis que tratem do tema de forma detalhada é premente.

O próprio legislador já se despertou para esta necessidade, porém ainda falta vontade política para a aprovação de alguns bons projetos de lei que tramitam no Congresso Nacional[74].

Esse é o caso, por exemplo, do PL 6891/2002, que estabelece regras para a proteção e tratamento de dados pessoais, atualmente tramitando em conjunto com o PL 3494/2000, de 22.08.2000, de autoria do Senado Federal (PLS-268/1999), que dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do *habeas data*.

Na exposição de motivos do PL 6981/2002 é considerado o crescente número de bancos de dados pessoais e proposto a formulação de regras de preservação do direito à privacidade. Baseando-se basicamente na legislação

[74] Dentre outros, atualmente tramitam na Câmara dos Deputados o *PL 3360/2000*, que dispõe sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas, encontra-se, desde 10.04.2003 na Comissão de Ciência e Tecnologia, Comunicação e Informática; o *PL 4249/2001*, que acrescenta dispositivo à Lei nº 8.078/90, para estabelecer a inviolabilidade de informações pessoais e patrimoniais em posse de fornecedor, e dá outras providências, encontra-se desde 01.08.2003 na CCJR; o *PL 6541/2002*, que acrescenta o art. 153-A ao Código Penal - Decreto-Lei nº 2.848/40, a fim de incluindo como crime passível de pena a divulgação ou comercialização de endereços e dados pessoais sem a devida autorização, encontra-se desde 13.08.2003 na CCJR; o *PL 123/2003*, que veda a transmissão a terceiros de dados relativos a pessoas naturais e jurídicas, encontra-se desde 13.01.2004 aguardando designação de Relator na CCJR. Já no Senado tramitam o *PL 95/2003*, que dispõe sobre a privacidade na Internet, encontra-se na CCJC desde 31.10.2003; o *PL 135/2003*, que dispõe sobre os crimes contra a intimidade e a vida privada das pessoas, acrescentando artigo ao Código Penal, em conformidade com o inciso X do artigo 5. da CF, encontra-se na CCJC desde 22.05.2003; o *PL 292/2003*, que disciplina a formação de banco de dados pessoais e respectivo uso das informações cadastradas, encontra-se na CCJC desde 12.06.2003; e o *PL 508/2003*, que acrescenta dispositivo ao Decreto-Lei nº 2848/40 - Código Penal - para considerar crime a prática dos atos nele indicados como a utilização indevida de dados e informações cadastrais alheias, encontra-se na CCJC desde 17.02.2004.

européia sobre o tema, o mencionado projeto de lei cuida de identificar os sujeitos dos tratamentos de dados, estabelecendo suas obrigações quanto à coleta, destinação, informação, retificação e armazenagem de dados, bem como regras para o tratamento de dados pessoais sensíveis e para o fluxo transfronteiriço de dados.

Ainda faculta ao Poder Executivo a criação de órgão técnico permanente com competência para fiscalizar e acompanhar o funcionamento de bancos de dados, e com poder de orientar e dar pareceres sobre a organização de novos tratamentos dessa natureza, à semelhança dos modelos francês e português.

Embora seja de reconhecida importância a aprovação desse Projeto de lei, parece não haver pressa na sua tramitação, pois encontra-se na Comissão de Constituição e Justiça e de Redação desde 01.08.2003.

CONCLUSÃO

1) As tecnologias da informação, em que pese não serem o único fator, provocaram uma revolução na vida da sociedade atual, tanto que adotou-se a denominação de *sociedade informacional.* Sua estrutura básica é apresentada em redes e a informação gera conhecimento, que por sua vez gera informação, num processo informacional onde o homem é parte essencial;

2) na sociedade informacional a informação assume papel de suma importância, tornando-se mercadoria de valor, e sendo constantemente disputada pelo poder público e privado;

3) informação é um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor do fato em si, sendo que o fato, gerador da informação, nada mais é que um dado, uma indicação;

4) prover os interessados do maior número de dados possíveis, tornou-se a grande obcessão da economia mundial, pois o tratamento desses dados gera informação valiosa;

5) a preocupação do direito se volta aos dados pessoais e à inviolabilidade da vida privada. Consideram-se dados pessoais todo tipo de informação, independentemente de sua natureza e do suporte mediante o qual é coletada, de caráter personalíssimo e passível de identificar o titular dos dados;

6) cresce a preocupação à medida que o processo de informatização atinge tanto o setor público quanto privado, automatizando todo tipo de prestação de serviço e formando enormes bancos de dados, além de possibilitar a recolha de dados sem o consentimento do titular;

7) a falta de regulamentação quanto ao tratamento desses dados pessoais gera insegurança e deixa vulnerável a esfera privada do indivíduo. Por tratamento informatizado de dados pessoais entende-se a recolha, arquivamento, tratamento e transmissão de dados, bem como qualquer operação efetuada sobre dados pessoais;

8) a Europa, de forma especial, é referência na questão do tratamento de dados pessoais e sua proteção, tendo a Suécia elaborado a primeira lei concernente à proteção de dados pessoais em 1973. De lá para cá, houve uma evolução significativa, existindo atualmente na União Européia a Diretiva 95/46/CE, que regulamenta a proteção de dados pessoais, entre outras Diretivas, bem como leis nacionais de cada Estado-membro;

9) a Diretiva 95/46/CE, muito embora tenha se proposto a realizar a harmonização entre a livre circulação de dados e a proteção de dados pessoais, não alcançou plenamente seu objetivo. Muitas são as garantias com relação à proteção dos dados pessoais, porém as exceções previstas acabam por deixar certas garantias inoperantes;

10) países como Portugal, Espanha e Alemanha, integrantes da União Européia, e Estados Unidos, foram analisados a fim de contribuírem com a formação da doutrina pátria, sendo os primeiros modelo de países onde impera a regulamentação e o segundo exemplo da não-regulamentação, cada qual com um enquadramento legal do direito à privacidade;

11) no sistema europeu identificam-se duas vias de controle da proteção dos dados pessoais, uma administrativa e outra normativa, sendo a primeira exercida por órgãos de controle independentes e a segunda através do Judiciário;

12) no Brasil, a ausência de regulamentação específica não obsta a garantia de proteção aos dados pessoais, porém esta proteção pode não ser eficaz, pois depende da atuação do Judiciário através da invocação do direito à privacidade, previsto constitucionalmente e como direito personalíssimo, no Código Civil, além da invocação, em casos específicos, do direito à inviolabilidade do sigilo de dados, do *habeas data* e do Código de Defesa do Consumidor;

13) diante da evolução tecnológica também o conceito de privacidade sofreu transformação, evoluindo do clássico *direito a ser deixado em paz* para o *direito de controlar as informações pessoais;*

14) a invocação do direito à privacidade pode gerar colisão de direitos, haja vista tratar-se a Constituição brasileira de documento pluralista e se sustentar a inexistência de direitos absolutos;

14) face a colisão de direitos se propõe a solução defendida por Canotilho, na esteira de Hesse e Dworkin: o juízo de ponderação ou concordância

prática, respeitando-se sempre o núcleo essencial dos direitos fundamentais, consubstanciado no princípio da dignidade humana. Busca-se uma harmonização entre os direitos colidentes, sendo ponderado pelo operador do direito, no caso concreto, qual direito deverá prevalecer face a circunstância posta;

15) a fim de conferir maior segurança ao titular de dados pessoais, principalmente, nas relações em rede, faz-se mister a regulamentação do direito à proteção dos dados pessoais. No entanto, embora existam projetos de lei em tramitação no Congresso Nacional, parece não haver vontade política nem mobilização popular.

REFERÊNCIAS

BARROSO, Luis Roberto. *Interpretação e Aplicação da Constituição*. Renovar: Rio de Janeiro, 1996.

BASTOS, Celso Ribeiro. *Curso de Direito Constitucional*. 21.ed. São Paulo: Saraiva, 2000.

_____; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. v. 2. São Paulo: Saraiva, 1988-1989.

BONAVIDES, Paulo. *Curso de Direito Constitucional*. 11. ed. São Paulo: Malheiros, 2001.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF, 2004.

_____. Superior Tribunal de Justiça. *Voto do ministro Ruy Rosado de Aguiar*. Disponível em:<http//:www.stj.gov.br> Acesso em: 29 dez. 2003.

CANOTILHO, J.J. Gomes. *Direito Constitucional e Teoria da Constituição*. Coimbra: Almedina, 1998.

CANOTILHO; VITAL MOREIRA. *Constituição da República portuguesa anotada*. 3.ed. Coimbra Editora, 1993.

CARVALHO, Luis Gustavo Grandinetti Castanho de. *Direito de informação e liberdade de expressão*. Rio de Janeiro: Renovar, 1999.

CASTELLS, Manuel. *Sociedade em Rede: A Era da Informação – Economia, Sociedade e Cultura*. v. 1. Rio de Janeiro: Paz e Terra, 2001.

CASTRO, Luiz Fernando Martins. *Proteção de dados pessoais – Panorama Internacional e Brasileiro*. Disponível em: <http://www.cjf.gov.br/pages/sem/eventos/dinformacao/textos/LuizCastro.doc>. Acesso em: 05 fev. 2004.

COMISSÃO EUROPÉIA. *Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de <<porto seguro>> e pelas respectivas questões mais freqüentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América*. Jornal Oficial n. L215 de 25/08/2000 p. 0007 – 0047. Bruxelas, 2000. Disponível em: http://europa.eu.int/eur-lex/search/search_oj.html>. Acesso em: 30 set. 2003.

_____. *Primeiro relatório sobre a implementação da diretiva relativa à protecção de dados (95/46/CE)*. Bruxelas, 2003. Disponível em: <http://europa.eu.int/eur-lex/pt/com/rpt/pt_rpt_month_2003_05.html>. Acesso em: 25 jan. 2004.

DEUTSCHLAND. *Der Bundesbeuftragte für Datenschutz. Bundesdatenschutzgesetz – Text ud Erläuterung*. Bonn, 2003.

_____. *Grundgesetz für die Bundesrepublik Deutschland*. Berlin: Deutscher Bundestag, 2003.

DONEDA, Danilo César Maganhoto. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: <http://www.mundojuridico.adv.br/documtos/artigos/texto433.doc>. Acesso em 12 dez. 2003.

DRUCKER, Peter. *O melhor de Peter Drucker: a sociedade.* Trad. De Edite Sciulli. São Paulo: Nobel, 2001.

DRUMMOND, Victor. *Internet, privacidade e dados pessoais.* Rio de Janeiro: Lúmen Júris, 2003.

DWORKIN, Ronald. *Uma questão de princípio*. São Paulo: Martins Fontes, 2001.

EFING, Antônio Carlos. *Banco de dados e cadastro de consumidores*. São Paulo: Revista dos Tribunais, 2002.

ESPAÑA. *Constitución Española (1978)*. Disponível em: <http://www.congreso.es/funciones/constitucion/indice.htm>. Acesso em: 12 fev. 2004.

FERRAZ JÚNIOR, Tércio Sampaio. A liberdade como autonomia recíproca de acesso à informação. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Coord.). *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo: Revista dos Tribunais, 2001.

GATES, Bill. *A empresa na velocidade do pensamento: com um sistema nervoso digital*. Trad. Pedro Maia Soares, Gabriel Tranjan Neto. São Paulo: Companhia das Letras, 1999.

GRECO FILHO, Vicente. *Inteceptação Telefônica*. São Paulo: Saraiva, 1996.

INFORMATIONELLE Datenschutz. Disponível em: <http://www.datenschutz.de/recht/grundlagen/>. Acesso em 05 jan. 2004.

JABUR, Gilberto Haddad. *Liberdade de Pensamento e Direito à Vida Privada: Conflitos entre Direitos da Personalidade*. São Paulo: Revista dos Tribunais, 2000.

KAMINSKI, Omar. *Privacidade na Internet.* Disponível em: <http://www.cyberlaws.com.br>. Acesso em: 19 set. 2003.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 3. ed. rev. ampl. São Paulo: Atlas, 1993.

LEPIANI, Giancarlo. *Estão de olho em você*. Revista Veja. Edição 1702, ano 34, n. 21, de 30 de maio de 2001.

LIMA, George Marmelstein. *A hierarquia entre princípios e a colisão de normas constitucionais*. Disponível em: <http://www.georgemarmelstein.com.br>. Acesso em: 10 nov. 2003.

MIGUEL, Carlos Ruiz. *El Derecho a la intimidad informática en el ordenamiento español*. Disponível em: <http://www.web.usc.es/~ruizmi/pdf/intiminf.pdf>. Acesso em: 18 abr. 2004.

MORAES, Alexandre de. *Direitos Humanos fundamentais: teoria geral, comentários aos arts. 1 a 5 da Constituição da República Federativa do Brasil, doutrina e jurisprudência.* 4.ed. São Paulo: Atlas, 2002.

OLIVEIRA, Olga Maria Boschi Aguiar de. *Monografia jurídica: orientações metodológicas para o trabalho de conclusão de curso*. Porto Alegre: Síntese, 2000.

PAESANI, Liliana Minardi. *Direito e Internet: liberdade de informação, privacidade e responsabilidade civil*. São Paulo: Atlas, 2000.

PEREIRA, Marcelo Cardoso. *O sistema de proteção de dados pessoais frente ao uso da informática e o papel do direito de autodeterminação informativa. Especial referência ao ordenamento jurídico espanhol*. Disponível em: <http://www.direitonaweb.adv.br/doutrina/dinfo/Marcelo_C_Pereira_(DINFO_0003).htm>. Acesso em: 14 jan. 2003.

PEREZ LUÑO, Antonio-Enrique. *Ensayos de Informática Jurídica*. México: Biblioteca de Ética, Filosofia del Derecho y Política, 1996.

_____. *Impactos sociales y jurídicos de internet*. Disponível em: <http://www.argumentos.us.es/numero1/bluno.htm>. Acesso em: 20 jul. 2003.

PORTUGAL. *Constituição da República Portuguesa (1976)*. Disponível em: <http://www.parlamento.pt/const_leg/crp_port/>. Acesso em: 13 jan. 2004.

_____. Tribunal Constitucional de Portugal. *Acórdão n. 355/97, de 7 de junho de 1997*. Disponível em: <http://www.tribunalconstitucional.pt/jurisprudencia.htm>. Acesso em: 05 set. 2003.

ROVER, Aires José. Sistemas especialistas legais: uma solução inteligente para o Direito. In: ROVER, Aires José (org.). *Direito, Sociedade e Informática: limites e perspectivas da vida digital*. Florianópolis, Fundação Boiteux, 2000.

_____. O direito e o governo frente o desenvolvimento do comércio eletrônico. In: PIMENTEL, Luiz Otávio (org). *Mercosul, alca e integração euro-latina-americana*. Vol. I. Curitiba: Juruá, 2001, pags. 43-56.

SAMPAIO, José Adércio. *Direito à Intimidade e à Vida Privada*. Belo Horizonte: Del Rey, 1998.

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

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 22.ed. São Paulo: Malheiros, 2003.

SOUSA, Antônio Francisco de. *Consentimento do particular em matéria de tratamento de dados pela autoridade administrativa*. In: Revista de Direito Público n. 77, 1986, p. 69-77.

STAIR, Ralph M. *Princípios de Sistemas de Informação: uma abordagem gerencial*. Trad. Maria Lúcia Iecker Vieira e Dalton Conde de Alencar. 2.ed. Rio de Janeiro: LTC Editora, 1998.

UNIÃO EUROPÉIA. *Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial n. L 281 de 23/11/1995 p. 0031-0050. Bruxelas, 1995. Disponível em: <http://europa.eu.int/eur-lex/pt/search/search_oj.html>. Acesso em: 10 jan. 2003.

_____. *Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações*. Jornal Oficial n. L 024 de 30/01/1998 p. 0001-0008. Bruxelas, 1998. Disponível em: <http://europa.eu.int/eur-lex/pt/search/search_oj.html>. Acesso em: 21 jan. 2003.

_____. *Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas*. Jornal Oficial n. L 201 de 31/07/2002 p. 0037-0047. Bruxelas, 2002. Disponível em: <http://europa.eu.int/eur-lex/pt/search/search_oj.html>. Acesso em: 23 jan. 2003.

_____. *Carta dos Direitos Fundamentais da União Européia. Jornal Oficial n. L 364 de 18/12/2000*. Bruxelas, 2002. Disponível em: <http://europarl.eu.int/charter/pdf/tex_pt.pdf>. Acesso em: 23 jan. 2004.