UNIVERSIDADE DE BRASÍLIA - UNB

FACULDADE DE DIREITO

DEPARTAMENTO DE PÓS-GRADUAÇÃO

TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO

Laura Schertel Mendes

Brasília, junho de 2008.

LAURA SCHERTEL MENDES

TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de Brasília, para obtenção do grau de Mestre em Direito.

Orientador: Cristiano Paixão Araujo Pinto

Brasília

2008

A candidata foi considerada ..... pela banca examinadora, com a média final igual a (.....) .....

_____

Cristiano Paixão Araujo Pinto
Orientador

_____

_____

_____

_____

Brasília, ... de ..... de 2008.

RESUMO

A utilização massiva de dados pessoais por organismos estatais e privados, a partir de avançadas tecnologias da informação, apresenta novos desafios ao direito à privacidade. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais. A análise do tratamento de dados pessoais no âmbito da relação de consumo deve considerar de forma prioritária a vulnerabilidade do consumidor nesse processo. Dessa forma, tem-se como necessária a ação do Estado para a proteção dos dados pessoais do consumidor, pois o mercado, ao invés de contribuir para a superação da sua vulnerabilidade, na realidade, acaba por reforçá-la. Sob essa ótica e para possibilitar a resposta adequada aos desafios sociais advindos da revolução tecnológica, é fundamental que o direito brasileiro seja reconstruído a ponto de compreender e solucionar os novos problemas enfrentados pelo cidadão na era da informação. A aplicação efetiva do direito individual fundamental à proteção de dados pessoais depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na realização de uma democracia da informação que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados, tanto por meio de uma cultura jurídica apta a compreender a proteção dos dados pessoais como um direito fundamental autônomo quanto por uma arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro setor de políticas públicas.

Palavras-chave: transparência, privacidade, informação pessoal, dados pessoais, sociedade de consumo, consumidor, sociedade da informação, banco de dados, tecnologia, igualdade, liberdade, direitos fundamentais, Constituição federal.

ABSTRACT

The massive employ of personal data by public and private organisms derived from advanced information technologies presents new challenges to the right to privacy. By the combination from multiple automation techniques, one is enabled to obtain sensitive information about citizens, which grounds the process of taking economic, political and social decisions. The analysis of personal data handling in consumption's relation must take into account mainly the consumer's vulnerability. In light of this fact, state intervention is required in order to protect consumer's personal data, since the market actually reinforces his vulnerability instead of overcoming it. Under this point of view and with the aim of offering a proper response to social challenges arising from the technological revolution, it is crucial to reconstruct Brazilian civil law so to perceive and solve new problems facing citizens in information age. An effective enforcement of the fundamental right to personal data protection depends in great measure upon collective responses. For this reason, the commitment to an informational democracy is vital to protect citizen self-determination and freedom from personal data control, as well as to avoid prejudicial employment of these data. Pursuing these purposes, one needs not only a legal culture capable of comprehending personal data protection as an autonomous fundamental right, but also a regulatory architecture able to state personal data protection as an essential theme for public policies.

Key words: transparency, privacy, personal information, personal data, consumer society, consumer, information society, database, technology, equity, freedom, fundamental rights, federal constitution.

AGRADECIMENTOS

Nessas breves palavras, agradeço primeiramente o apoio irrestrito e o incentivo de minha mãe, Rosa, que, com muito amor, dedicou grande parte da sua vida à minha formação. Essa dissertação, como qualquer outra realização minha, é conseqüência direta do seu investimento e esforço.

Agradeço ao meu pai, Gilmar, pelos incansáveis debates, pelo estímulo à leitura e pela forma paciente e sábia com que me escutava e orientava. Agradeço também o incentivo permanente e o auxílio infinito do meu querido irmão Francisco ("Pipo"), sem o quais este trabalho talvez não pudesse ter ocorrido. Sou grata também a todos os familiares, que mesmo à distância, torceram por essa travessia e acreditaram nela.

Devo meus sinceros agradecimentos a meu orientador, Cristiano Paixão, por me acompanhar, desde os tempos de graduação, em minhas empreitadas acadêmicas, sempre com brilhantismo, paciência e muita disposição; agradeço também à Prof. Cláudia Lima Marques, grande referência na luta pela efetivação dos direitos do consumidor, e ao Prof. Menelick de Carvalho Neto, referência nacional na seara do direito constitucional, por se disporem gentilmente a compor minha banca de mestrado.

Agradeço à Faculdade de Direito da Universidade de Brasília como um todo. Qualquer pesquisa é determinada pelo contexto acadêmico em que se insere. Se um homem é, afinal, suas circunstâncias, como disse uma vez Borges, espero que este trabalho possa refletir o ambiente instigante e profícuo existente na Faculdade de Direito da UnB, criado e compartilhado por alunos, professores e funcionários. Tenho que agradecer em particular o interesse que encontrei nos colegas e professores do Curso de Mestrado. Especial atenção também merecem os funcionários, representados por Helena e Lia, sem as quais não teria conseguido vencer prazos e burocracias administrativas.

Agradeço também ao Departamento de Proteção e Defesa do Consumidor, que nos últimos anos se tornou minha segunda casa. Sou enormemente grata aos amigos Ricardo Morishita e Juliana Pereira por me apoiarem de forma incondicional na minha vida profissional e por me incentivarem na minha incursão acadêmica. Não poderia deixar de agradecer também à minha ótima equipe de trabalho e a todos os companheiros da SDE, sem cujo auxílio não teria tempo nem força para concluir essa monografia. Agradeço também ao professor e amigo Leonardo Bessa, pelos incontáveis debates e pela cessão de material importante para a realização da pesquisa.

Agradeço aos meu queridos amigos, pelo apoio irrestrito, sem o qual a realização do trabalho teria sido insustentável: Helena, Cris, Thaís, Érica, Carol e Samú, Fabrício, Carol Amorim e Bruno Varjão.

Ao João, pelo amor e companheirismo, pelo incentivo incondicional, por tudo.

-*“Someone collected my writings, letters, books, sayings, lectures, parabolas, fairy-stories, obiter-dicta and sketches; then deciphered my alleged soul through them, and was arrogant enough to press me to resurrect myself. So, here I am, back, against my wishes, crippled, maimed and functioning counter to my own intentions.”*
(Fala de Si-Tien, na obra de Adam Podgorecki, One Hundred and One Stories of Si-Tien.

SUMÁRIO

Introdução 8

1. Da privacidade à proteção de dados pessoais: entre liberdade e igualdade 14
   1.1. Privacidade: origem e evolução 14
   1.2. Privacidade: conceito e dimensões 18
   1.3. Para além da privacidade: a proteção de dados pessoais entre liberdade e igualdade 24
   1.4. O surgimento da política de proteção de dados e a convergência internacional 29
   1.5. As gerações das leis de proteção de dados pessoais na Europa 33
   1.6. A dimensão da liberdade 40
      1.6.1 O direito à autodeterminação informativa – a decisão da Corte Constitucional alemã 45
      1.6.2 O consentimento na proteção de dados pessoais 49
      1.6.3 Os direitos subjetivos do titular dos dados pessoais 53
      1.6.4 Os princípios da proteção de dados pessoais 56

   1.7 A dimensão da igualdade 57
      1.7.1 Dados sensíveis ou tratamento sensível dos dados? 62

2. Informação pessoal e tecnologia nas relações de consumo 69
   2.1. Dados pessoais e tutela jurídica: conceitos e dimensões 69
   2.2. A utilização de dados pessoais nas relações de consumo 75
      2.2.1 Economia com especialização flexível 77
      2.2.2 A tecnologia e o tratamento de dados pessoais dos consumidores 79
      2.2.3 O imperativo da vigilância: o consumidor de vidro 81
   2.3. Riscos oriundos do tratamento de dados pessoais nas relações de consumo 85
      2.3.1. Fontes, tipos e usos de dados pessoais 87
      2.3.2. Técnicas de processamento de dados 100
      2.3.3. A circulação de dados pessoais: a “indústria” de banco de dados 109
   2.4 A quem pertencem os dados pessoais? 112

3. Tutela jurídica e diálogo das fontes: a proteção de dados pessoais nas relações de consumo 117
   3.1. Constituição Federal 118
   3.2. Código de Defesa do Consumidor 122
   3.3. Regime legal de proteção de dados pessoais 133
      3.3.1 Âmbito de aplicação 135
      3.3.2 O regime de proteção de dados no Brasil 141

4. Conclusão 144

5. Bibliografia 148

INTRODUÇÃO

Com os avanços da tecnologia da informação ocorridos no século XX, fala-se por toda parte sobre a "morte da privacidade"[1], expressão que visa demonstrar a impossibilidade de se preservarem fatos e elementos da esfera privada diante do enorme fluxo informacional proporcionado pelas novas tecnologias.

Sabe-se que há séculos o controle de informações pelas instituições sociais, tais como a Igreja e o Estado, esteve associado ao controle do poder na sociedade. No entanto, a partir de meados do século XX, o desenvolvimento tecnológico acarretou a intensificação dos fluxos de informação de uma forma nunca antes vista, o que levou à denominação da sociedade atual como "sociedade da informação" ou "era da informação".

Manuel Castells defende que está em curso uma verdadeira revolução tecnológica, cujo núcleo se refere às tecnologias da informação, processamento e comunicação[2]. Por tecnologias da informação, entendem-se as tecnologias em microeletrônica, computação, telecomunicações/radiodifusão e optoeletrônica, além da engenharia genética[3]. Segundo ele, a sociedade que emerge dessa revolução tecnológica é a "sociedade em rede", que se

[1] CF: GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. O'Reilly Media: California, 2000; SMITH, Robert Ellis. *Privacy. How to protect. What´s left of it.* Garden City: Anchor Press/Doubleday, 1979; SOLOVE, Daniel J.. *The digital person: technology and privacy in the information age.* New York: New York University Press, 2004.

[2] CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede.* Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, p. 50.

[3] Idem, p.49.

caracteriza não pela centralidade de conhecimentos e informação, mas pela "aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso"[4]. Isso significa que essa nova tecnologia da informação tem uma capacidade ininterrupta de difusão, na medida em que os próprios usuários dela se apropriam, redefinindo-a. A diferença dessa tecnologia é exatamente a possibilidade de que usuários se tornem criadores, podendo assumir o controle da tecnologia, como no caso da internet[5].

A revolução da tecnologia da informação alterou radicalmente a realidade social, penetrando em todas as esferas da atividade humana e, por conseguinte, criando novas relações a serem reguladas pelo sistema jurídico. Juntamente com Castells, é interessante evitar o "lugar-comum" de que a tecnologia determina a sociedade; a tecnologia é a sociedade e essa não pode ser compreendida sem o seu aparato tecnológico – da mesma forma como não há uma tecnologia "fora" da sociedade[6]. Nesse contexto, a indiferença do direito perante o desenvolvimento tecnológico deixa de ser possível, devendo o jurista ou o operador do direito estar preparado para enfrentar as novas situações decorrentes dessa tecnologia informacional inovadora.

O surgimento da internet, como uma estrutura aberta de rede de computadores, constitui um marco no fluxo de informações ao ampliar radicalmente as possibilidades de comunicação. A principal característica da internet é a sua abertura, tanto em sua arquitetura técnica, como em sua organização social/institucional. Castells define a enorme difusão e ampliação da internet a partir de duas características principais: o fato de sua arquitetura de interconexão ser ilimitada, descentralizada, distribuída e multidirecional em sua interatividade; e o fato de todos os protocolos de comunicação e suas implementações serem

[4] Idem, Ibidem.

[5] Idem, p. 51.

[6] Idem, Ibidem, p. 25.

abertos, distribuídos e suscetíveis de modificação, muito embora os criadores de novos protocolos preservem a propriedade de parte de seu software[7]. Essa estrutura aberta da internet, ao mesmo tempo em que possibilitou a sua difusão e o aperfeiçoamento da tecnologia, propiciou também o desenvolvimento de tecnologias de controle, decorrentes do interesse de governos e do comércio e que podem acarretar a restrição da liberdade do usuário.

Interessa-nos analisar os efeitos da inovadora tecnologia da informação sobre a privacidade dos indivíduos no que se refere especificamente às relações de consumo. Isso porque, muito embora esses efeitos possam ser percebidos nos mais diversos setores da sociedade, inclusive no âmbito da relação entre a administração pública e os cidadãos, entendemos que o consumidor, por ser o pólo vulnerável da relação de consumo, possui grande dificuldade de controlar o fluxo de dados e de informações pessoais no mercado de consumo. Nesse contexto, buscar-se-á analisar quais são as conseqüências da conexão entre sociedade de informação e sociedade de consumo, bem como as formas que o direito pode contribuir para proteger a privacidade do consumidor.

São inúmeras as situações em que o consumidor pode ter a sua privacidade violada na sociedade atual, principalmente por meio das formações de arquivos pessoais. Diante da grande massa de consumidores anônimos, as empresas buscam diversas fontes de informação sobre eles para segmentar produtos e serviços, aumentar a eficiência de seu processo produtivo, reduzir as operações de riscos e ampliar a eficácia de seu marketing.

A partir da evolução da tecnologia da informação e das transformações do ordenamento jurídico, a privacidade deixa de ser concebida como o direito do indivíduo a ser deixado só, adquirindo progressivamente um caráter mais positivo, como sendo o direito de se

[7] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 28 e 29.

construir uma esfera privada própria, a partir da idéia de livre desenvolvimento da personalidade.

Além de adquirir esse caráter positivo, é possível perceber que o direito à privacidade se transformou para se adaptar às novas transformações sociais ocasionadas pela revolução da tecnologia da informação, a ponto de ensejar o surgimento da disciplina de proteção de dados pessoais[8]. Assim, os ordenamentos jurídicos de diversos países passaram a tutelar expressamente os dados pessoais de seus cidadãos, por entenderem que tais dados constituem uma projeção da personalidade do individuo, merecendo inclusive uma tutela constitucional.

Nesta pesquisa, trabalha-se com a hipótese de que a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito[9].A proteção de dados passa a ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo igualmente uma tutela jurídica coletiva. Ademais, a disciplina da proteção de dados pessoais envolve outra questão, que em certa medida era ignorada pelo direito à privacidade: o problema da igualdade. Nesse sentido, entende-se fundamental a compreensão da disciplina de proteção de dados pessoais como meio, principalmente, de tutela da liberdade e da igualdade.

Compreende-se que nem todos os problemas advindos do processamento de dados pessoais são passíveis de serem examinados sob a ótica da privacidade, uma vez que esse conceito não é capaz de abordar os problemas individuais e coletivos oriundos dos atuais sistemas de classificação e risco, como por exemplo, a utilização de dados genéticos dos pacientes por planos de saúde ou a discriminação por supermercados em razão do código postal. Desse modo, o vocabulário utilizado para nos referirmos à regulação da economia da

[8] Idem, Ibidem, p. 27.

9 Como afirma Doneda, “a proteção de dados pessoais, em suma, propõe o tema da privacidade, porém modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão”. (DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Op. Cit., p. 205)

informação pessoal deve ser mais amplo e diversificado, ultrapassando o conceito de privacidade e abrangendo idéias como igualdade, mobilidade social, mérito e alocação de riscos.

No primeiro capítulo deste trabalho, serão analisadas a origem e a evolução do conceito de privacidade, desde o seu delineamento no direito americano até a sua transformação na disciplina mais ampla da proteção de dados pessoais, fundada na liberdade e na igualdade. Em seguida, analisar-se-á o contexto do surgimento das primeiras legislações de proteção de dados, na década de 1970, a partir dos planos nacionais de centralização de bancos de dados, bem como a evolução das normas de proteção de dados, a partir de uma perspectiva de gerações. Por fim, examinar-se-á quais os instrumentos jurídicos aptos a proteger a liberdade e a igualdade do titular dos dados pessoais, tais como os direitos subjetivos a ele atribuídos, os princípios gerais da proteção de dados e a restrição ao tratamento de dados sensíveis.

No segundo capítulo, será demonstrado como o tema da proteção de dados, no âmbito da economia da informação pessoal, desloca o seu foco do temor da centralização das informações em um gigantesco banco de dados estatal para o seu oposto: uma constelação vasta e indistinta de redes de tratamento de dados pessoais privadas, composta por milhares de unidades de processamento de dados, com grande capacidade de interconexão. Analisar-se-á o imperativo de vigilância do consumidor nesse contexto, bem como as formas de coleta e as técnicas de processamento de dados pessoais. Por fim, será examinada a problemática a respeito da possibilidade de se atribuir direitos de propriedade ao titular dos dados pessoais.

No terceiro capítulo, objetiva-se estudar a pluralidade de normas que incide sobre o tratamento de dados no âmbito de uma relação de consumo. Para tanto, será utilizado o conceito de diálogo das fontes, a fim de explicar a convivência harmônica de diversas fontes normativas. Ademais, apresentar-se-á a tutela constitucional dos dados pessoais e a proteção jurídica albergada no Código de Proteção e Defesa do Consumidor. Ao final, tentar-se-á

ressaltar a importância da promulgação no Brasil de uma legislação geral de proteção de dados pessoais que institua um verdadeiro sistema de regulação do processamento de dados na sociedade.

1.
DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: ENTRE LIBERDADE E IGUALDADE

1.1. Privacidade: origem e evolução

A origem do direito à privacidade ocorreu em momento diferente de outros direitos de cunho liberal, na medida em que não foi reconhecido nas Constituições, nem nos Códigos Civis do século XIX. Sua origem deu-se inicialmente no contexto doutrinário, tendo sido reconhecido no âmbito legislativo apenas no século XX.

O início dos debates doutrinários sobre o direito à privacidade ocorreu como conseqüência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente impensável. Isso pode ser percebido com o pioneiro artigo sobre privacidade de Warren e Brandeis, publicado na Harvard Law Review e intitulado "The Right to Privacy"[10], no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica.

[10] WARREN e BRANDEIS, The Right to Privacy. In Harvard Law Review, Vol IV, Dezembro 15, 1890, No. 5. Louis Brandeis e Samuel Warren estudaram juntos no curso de direito da Harvard Law School. Quando escreveram o artigo, eram sócios na advocacia. Posteriormente, Brandeis tornou-se ministro da Suprema Corte dos EUA. O referido artigo foi considerado um dos mais citados da história norte-americana. (SHAPIRO, Fred.

Como afirma Doneda, esse artigo não deve ser entendido como uma referência histórica isolada, mas como parte de um contexto mais amplo da história americana, em que o capitalismo estava se desenvolvendo e a expansão para o oeste tinha chegado ao seu fim[11]. A finalidade principal do referido artigo é buscar identificar um direito à privacidade na *common law*, a partir de diversos precedentes jurisprudenciais de tribunais ingleses.

Os autores iniciam a sua reflexão a partir da constatação de que os novos aparatos tecnológicos, como a fotografia e a imprensa, estavam invadindo os domínios da vida privada, ao tornarem públicos até mesmo o que era murmurado nos aposentos[12]. Eles buscam encontrar uma proteção contra esse fato na própria *common law*. Segundo os autores, a *common law* tem a característica de se alterar e ampliar ao longo do tempo para abarcar outros direitos, sendo necessário, em razão das novas invenções tecnológicas, que a *common law* avance mais uma vez no reconhecimento do direito à privacidade, denominado pelo juiz Cooley, de "direito a ser deixado a só" ("*right to be let alone*")[13].

Ao fundamentarem o direito à privacidade, Warren e Brandeis relacionam a sua proteção à inviolabilidade da personalidade, rompendo com uma tradição anterior que associava a proteção da vida privada à propriedade. Nas suas palavras, "o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade"[14].

Nesse sentido, é importante ressaltar que o ineditismo do artigo consistiu, não apenas em identificar um direito à privacidade, mas em fundamentar esse direito na proteção da

---

"The Most-Cited Law Review Articles Revisited", in: 71 Chicago-Kent Law Review 751 (1996) apud DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Rio de Janeiro: Renovar, 2006, p. 137.)

[11] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Rio de Janeiro: Renovar, 2006, p. 136.

[12] WARREN e BRANDEIS, The Right to Privacy. Op. Cit.

[13] É importante se fazer uma ressalva a respeito do "direito a ser deixado só" (right to be let alone), cuja formulação é atribuída muitas vezes na história a Warren e Brandeis, pois, na realidade, tal definição foi dada pela primeira vez pelo Juiz Thomas McIntyre Cooley em seu *Treatise of the law of torts*, Callaghan, 1888.

[14] WARREN e BRANDEIS, The Right to Privacy. Op. Cit.

personalidade, em demonstrar a importância desse direito frente aos avanços da tecnologia e de tornar possível o reconhecimento futuro desse direito como um direito protegido constitucionalmente[15].

Os autores fundamentam a necessidade do reconhecimento do direito à privacidade na própria vida moderna e complexa, que tornou o homem mais sensível à publicidade, de maneira que a solidão e a intimidade passaram a ser mais essenciais ao indivíduo. Dessa forma, extrai-se do artigo uma definição de privacidade relacionada à aversão contra qualquer intromissão não consentida na vida privada. Nesse contexto, o privado é referido como o espaço da vida doméstica e das relações sexuais.

Deve-se ressaltar que Warren e Brandeis, ao identificarem o direito à privacidade, buscam igualmente definir os seus limites, nos seguintes termos: i) o direito à privacidade não impede a publicação do que é publicado ou do que é de interesse geral; ii) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como por exemplo, em um Tribunal ou em uma Assembléia Legislativa, não há violação desse direito; iii) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; iv) o consentimento do afetado exclui a violação do direito; v) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; vi) a ausência de dolo também não exclui a violação desse direito[16].

Como se pode perceber a partir da análise do artigo de Warren e Brandeis, a proteção à privacidade teve um caráter fortemente individualista em seus primórdios, com a sua feição do direito a ser deixado só. É nesse sentido que ela foi considerada por muito tempo como um direito tipicamente burguês, na medida em que sobressaíam as suas características de direito negativo, como a exigência absoluta de abstenção do Estado na esfera privada individual para a sua garantia.

---

[15] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 139.

[16] WARREN e BRANDEIS, The Right to Privacy. Op. Cit.

Como afirma Doneda, o que contribuiu para a associação do sentido de privacidade à imagem de mundo burguesa foi exatamente o contexto de seu surgimento, principalmente, no ambiente judicial. Isso porque os primeiros casos judiciais em que se reconhece a violação à privacidade diziam respeito a grandes celebridades, como o caso Rachel (da famosa atriz Elisa Rachel Félix, na França, em 1858) e o caso de Benito Mussolini e de sua amante Clara Petacci (Itália, 1953)[17].

Importa observar que, no decorrer do século XX, a transformação da função do Estado, aliado à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado como pressuposto para o reconhecimento de outros direitos fundamentais. Nesse contexto, a violação da privacidade deixou de ser um problema apenas de grandes celebridades, passando a atingir a maioria dos cidadãos.

Após a II Guerra Mundial, a proteção à privacidade ganha reconhecimento no âmbito internacional. A Declaração Universal dos Direitos do Homem, de 1948, prevê, em seu art. XII, além do direito à privacidade, também o direito à honra e ao sigilo de correspondência, nos seguintes termos: *"Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques"*[18].

A Convenção Européia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica também previram a proteção da vida privada em termos semelhantes.

A evolução do direito à privacidade prosseguiu para se adaptar às novas transformações sociais ocasionadas pela revolução da tecnologia da informação, que

[17]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 11.

[18] ONU. Declaração Universal dos Direitos do Homem. Resolução no. 217ª (III) da Assembléia Geral das Nações Unidas. 10 de dezembro de 1948.

possibilitou a coleta e o processamento dos dados pessoais dos cidadãos de forma pioneira. Além de adquirir um caráter positivo e de ser reconhecido no âmbito internacional, o direito à privacidade transformou-se para ensejar o nascimento da disciplina de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados[19].

A partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominado privacidade informacional, "proteção de dados pessoais", "autodeterminação informativa", entre outros.

Desse modo, os ordenamentos jurídicos de diversos países passaram a tutelar, não apenas a privacidade, mas expressamente os dados pessoais de seus cidadãos, por entenderem que tais dados constituem uma projeção da personalidade do indivíduo, merecendo inclusive tutela constitucional. Dentre os países que protegem expressamente na Constituição o direito à privacidade informacional estão Espanha, Portugal, Hungria, Eslovênia e Rússia[20] .

1.2. Privacidade: conceito e dimensões

Embora reconhecido por diversos países, o direito à privacidade apresenta variações quanto à nomenclatura, conteúdo e extensão nas diferentes legislações. Com relação à terminologia utilizada para designá-lo, encontram-se no direito americano expressões como *"right to privacy*" e *"right to be let alone"*, enquanto no direito francês, encontram-se as expressões *"droit a la vie privée"* e *"droit a la intimité"*. Na Itália, utilizam-se os termos

[19] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 27.

[20] MALTA, Tatiana. *O Direito à Privacidade na Sociedade da Informação.* Op. Cit., p. 44.

"diritto alla riservatezza", *"diritto alla segretezza"* e *"diritto alla rispetto della vita privatta"*, na Espanha fala-se de "*derecho a la intimidad*" e na Alemanha utiliza-se predominantemente a expressão *"Recht auf informatiolelle Sebstbestimmung"* (direito à autodeterminação informacional)[21].

Também na doutrina brasileira não há consenso sobre a denominação desse direito, pois a própria Constituição Federal propicia o debate terminológico sobre o direito à privacidade, ao determinar em seu artigo 5º, X, que são invioláveis a vida privada e a intimidade. Nesse sentido, a norma suprema suscita a discussão acerca do sentido de cada uma das expressões: designariam "vida privada" e "intimidade" bens jurídicos distintos?

O embasamento da distinção do Constituinte brasileiro pode ser encontrado na teoria das esferas de Heinrich Hubmann, segundo a qual o sentimento de privacidade do indivíduo pode ser compreendido a partir de um esquema de círculos concêntricos, que representam diferentes graus de manifestação da privacidade: no núcleo estaria a esfera da intimidade ou do segredo (*Geheimsphäre*); em torno dela, viria a esfera privada (*Privatsphäre*); e em torno de ambas, em um círculo de maior amplitude, encontrar-se-ia a esfera pessoal (*Öffentlichkentsbereich*), que abrangeria a vida pública do indivíduo.

A teoria das esferas foi utilizada pelo Tribunal Constitucional alemão na decisão sobre a "Lei do Microcenso" de 16 de julho de 1969, em que se declarou que a mais restrita das esferas, a esfera do segredo (*Geheimsphäre*) não poderia ser limitada nem sequer por lei, por se constituir em um âmbito inviolável da vida do individuo. No caso mencionado, o Tribunal declarou a constitucionalidade da referida lei, por compreender que as suas disposições não acarretaram a violação da esfera do segredo. Apesar disso, pode-se dizer que a teoria das esferas foi alvo de inúmeras criticas, tendo sido superada pela própria doutrina alemã, que

[21] CARVALHO, Ana Paula Gambogi. O Consumidor e o Direito à Autodeterminação informacional: considerações sobre os bancos de dados eletônicos. In: *Revista de Direito do Consumidor*. No. 46, Ano 12, abril-junho de 2003, p. 82.

chegou a denominar a teoria de Hubmann como a "teoria da pessoa como uma cebola passiva", conforme menciona Danilo Doneda[22].

Sob essa perspectiva, é importante retomar a distinção conceitual efetuada pela Constituição Federal entre "vida privada" e "intimidade". Muito embora a norma suprema mencione ambos os termos, tal distinção não deve operar efeitos jurídicos na tutela da privacidade pelo direito brasileiro, porque, tanto o seu âmbito de proteção, como as suas limitações, assim como os efeitos de sua violação, independem da distinção entre "vida privada" e "intimidade", razão pela qual se entende que tal distinção não deve ser tratada juridicamente. Isso porque a gravidade da violação ao direito à privacidade não estará relacionada necessariamente ao grau de intimidade ou de segredo de determinada informação armazenada, mas, por exemplo, ao seu potencial discriminatório, como ocorre nos casos de dados sensíveis[23].

Nesse sentido e sob a ótica de que no direito toda distinção conceitual deve se traduzir em uma distinção funcional, entende-se ser mais adequado utilizar-se a expressão "privacidade"[24], o que traduz a existência de um único direito para abranger todos os casos que se trata da proteção do indivíduo em sua esfera privada[25]. Esse posicionamento pode ser reforçado considerando também a extrema subjetividade da distinção entre "vida privada" e "intimidade", o que poderia prejudicar a adequada análise jurídica desse direito, inclusive de suas funções e de sua extensão no ordenamento jurídico brasileiro. Por fim, pode-se dizer que a utilização do termo privacidade é adequada também pelo fato de que possui uma amplitude

---

[22] BURKERT, Herbert. "Privacy-Data Protection – A German/European Perspective", in: *Governance of Global Networks in the Light of Differing Local Values"*. Cristoph Engel; Kenneth Keller (ed.). Baden-Baden: Nomos, 2000, p. 46, *apud* DONEDA, Danilo, *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 108.

[23] Ver Cap. III desta Dissertação.

[24] O vocábulo "privacidade", embora tenha raiz latina (do verbo *privare*), tornou-se amplamente utilizado na língua inglesa, o que fez com que muito autores considerassem a sua tradução para o idioma português como um anglicismo. (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 107)

[25] No mesmo sentido, ver Doneda (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 111). Em sentido diverso, José Adércio Leite Sampaio afirma haver distinção entre os termos "vida privada" e "intimidade" (SAMPAIO, José Adércio Leite. *Direito à Intimidade e à vida privada.* Op Cit.). Já Paulo José da Costa Jr. entende ser a melhor denominação para esse direito "direito à intimidade" (COSTA Jr, Paulo José da. *O direito de estar só: tutela penal da intimidade*. São Paulo: Editora Revista dos Tribunais, 1995, p. 32-36).

incomum, em comparação com os termos anteriormente mencionados, tendo sido denominada inclusive como "palavra-ônibus" e "noção guarda-chuva"[26].

Como visto, a terminologia para se designar o direito ora estudado carece de consenso na doutrina. Da mesma forma, também o conceito de privacidade é objeto de diversas polêmicas jurídicas. Não obstante a divergência doutrinária, compreende-se que uma adequada definição do direito à privacidade é a de Alan Westin, que constitui uma referência doutrinária nesse tema: "Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros."[27] No mesmo sentido, tem-se uma outra definição interessante de Rohan Samarajiva, segundo o qual, "privacidade é a habilidade, explícita ou implicitamente, de negociar condições de delimitação nas relações sociais."[28] De acordo com esse autor, "tal definição inclui o controle do fluxo de informações que podem ser estratégicas ou de valor estético para a pessoa e do influxo de informações (...). A definição não considera privacidade como uma estado de solidão, conforme sugerido pelo conceito do direito a ser deixado só"[29]

Como se pode perceber, não obstante os diversos conceitos de privacidade, entende-se que a definição mais adequada é a que faz prevalecer a idéia de controle do indivíduo sobre as suas informações, em detrimento da idéia de isolamento do indivíduo. Conceituada dessa forma, a privacidade reflete claramente a existência de uma autonomia do seu titular na conformação desse direito. Isso significa que o titular tem a faculdade de conformar as fronteiras e os limites do exercício de seu direito à privacidade.[30]

Como exemplo desse fenômeno pode-se citar a controvérsia que ocorreu na Alemanha a respeito da possibilidade de se proibirem programas televisivos denominados "*reality*

[26] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. Cit., p. 111.

[27] WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1970, p. 7 (tradução livre).
[28] SAMARAJIVA, Rohan. "Interactivity as though privacy mattered." In: *Technology and Privacy: the New Landscape*, Op. Cit., p. 283 (tradução livre).
[29] Idem, ibidem, p. 283.
[30] PINTO, Paulo Mota. "A Proteção da Vida Privada e a Constituição." In: *Boletim da Faculdade de Direito.* Vol LXXVI, Coimbra: Universidade de Coimbra, 2000, p. 190.

shows", sob o fundamento de renúncia ilegal ao direito à privacidade e da violação da dignidade humana. Nesses programas, um conjunto de concorrentes, que podem revogar o seu consentimento a qualquer momento, permanece dentro de uma casa, na qual eles são filmados diuturnamente, com o objetivo de ganharem prêmios. Muito se questionou sobre se os participantes estariam tendo a sua dignidade violada e se eles teriam renunciado ao seu direito à privacidade. Com base nesses fundamentos, alguns doutrinadores alemães chegaram a defender o controle da programação e a interrupção desse programa por órgãos estatais.

Gomes Canotilho e Jónatas Machado, em estudo específico sobre o tema[31], refutam a tese de que os participantes dos reality shows renunciariam ao seu direito de privacidade ao participar do programa. Isso porque o próprio conceito de direito de privacidade envolve a idéia de autonomia: "o direito à privacidade consiste na possibilidade de a pessoa controlar, tanto quanto possível a massa de informações sobre si mesma a que outros podem ter acesso"[32]. Isso porque o direito à privacidade deve centrar-se na proteção das decisões individuais em matéria de privacidade e não na promoção de uma determinada concepção acerca desse bem. Do contrário, o direito à privacidade tornar-se-ia um dever de privacidade.

Os autores afirmam também que não há como se falar em violação da dignidade da pessoa humana nos programas de *reality shows,* tendo em vista que não há sinais de danos psicológicos ou físicos causados pelo programa aos participantes. Além disso, afirmam eles, seria um equívoco condenar o referido programa à luz de um determinado feixe de valores, pois, em uma ordem constitucional pluralista, deve o conceito de dignidade humana ser compatível com diversas concepções de mundo. Esse conceito não pode servir para limitar liberdades e garantias, como se fazia antes com as cláusulas dos bons costumes e da moral pública. Assim, a dignidade da pessoa humana deve ser concebida, não como um conceito

---

[31] CANOTILHO, Gomes e MACHADO, Jónatas, *Reality Shows e Liberdade de Programação.* Coimbra: Coimbra Editora, 2003.

[32] Idem, Ibidem, p. 55 e 56.

vazio, mas como a afirmação dos indivíduos como sujeitos livres e responsáveis, capazes de autodeterminação[33].

Do caso analisado, pode-se extrair que, em uma sociedade pluralista que não visa impor uma única visão de mundo, nem uma determinada concepção de bem, o titular do direito à privacidade possui um espaço de liberdade na conformação e interpretação de seu direito. Afinal, se o direito à privacidade pretende se constituir como espaço de livre desenvolvimento da personalidade, não se pode impedir o indivíduo de exercer livremente o direito à privacidade do qual é titular, em uma democracia constitucional, baseada na dignidade humana e na autodeterminação do indivíduo. Do contrário, correr-se-ia o risco de se ter a exclusão de direitos, liberdades e garantias em razão de um absolutismo valorativo decorrente da Constituição. O reconhecimento de que o titular do direito fundamental à privacidade tem autonomia para exercê-lo conforme os seus planos de vida e a sua vontade decorre da própria idéia de dignidade humana e do princípio da auto-determinação, que integram e moldam o cerne de todos e de cada um dos direitos fundamentais.[34]

Deve-se ressaltar que o direito à privacidade não constitui um direito absoluto, vez que possui limitações, baseadas em outros direitos individuais ou coletivos, necessários para a vida em sociedade. É o que afirma Alan Westin:

> O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive. O indivíduo o faz em face das pressões da curiosidade dos outros e dos processos de vigilância que toda sociedade necessita para a implementação de normas sociais.[35]

---

[33] Idem, Ibidem, p. 70.

[34] É interessante observar que ao mesmo tempo em que o princípio da dignidade humana é o fundamento da autonomia do titular do direito, é ela também o seu limite. CF: NOVAIS, Jorge Reis. Renúncia a Direitos Fundamentais. In: MIRANDA, Jorge. (org.) *Perspectivas Constitucionais nos 20 anos da Constituição de 1976.* Volume I. Coimbra: Coimbra Editora, 1996, p. 287.

[35] WESTIN, Alan. *Privacy and Freedom*. Op. Cit., p. 7 (tradução livre).

Desse modo, percebe-se que o direito à privacidade deve ser tratado sempre de modo a não ferir outros direitos e princípios do ordenamento jurídico, tais como a liberdade de imprensa, a criação cultural, a segurança dos cidadãos, a autonomia pública, entre outros.[36]

1.3. Para além da privacidade: a proteção de dados pessoais entre liberdade e igualdade

A utilização massiva de dados pessoais, cuja origem remonta ao século XX, pode ser associada a duas características principais do Estado pós-industrial: a burocratização (dos setores público e privado) e o desenvolvimento da tecnologia da informação[37]. Ambos esses fenômenos, que podem ser considerados transnacionais, suscitaram o processamento dos dados pessoais por governos das mais variadas ideologias políticas e por grandes corporações empresarias, com finalidades estatísticas, administrativas, negociais e investigativas[38].

A combinação de diversas técnicas automatizadas permitiu a coleta, o registro, o processamento, o cruzamento, a organização e a transmissão de dados, de uma forma anteriormente inimaginável, possibilitando a obtenção de informações valiosas sobre os cidadãos e auxiliando a tomada de decisões econômicas, políticas e sociais[39].

O valor das informações obtidas não reside apenas na capacidade de armazenamento de grande volume de dados, mas, principalmente, na possibilidade de se obterem novos elementos informativos a respeito dos cidadãos a partir do tratamento desses dados[40].

---

[36] Não constitui objeto deste trabalho analisar os limites do direito à privacidade em relação a outros princípios do ordenamento jurídico. Para tanto, ver: ETZIONI, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999. LOSANO, Mario. "Dos Direitos e dos Deveres: também no direito à privacidade."In: *Verba Júris: anuário da pós-graduação em direito.* Universidade Federal da Paraíba, v. 2 n. 2 janeiro/ dezembro 2003.

[37] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 43.

[38] Idem, Ibidem, p. 44.

[39] ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data em Chile e información comparativa. In: *Anuário de Derecho Constitucional Latioamericano 2005*, Tomo II, Konrad Adenauer Stiftung, p. 449.

[40] DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. In: *Revista de Estudios Políticos* ,104 (Nueva Época), Abril/Junio 1999, Madri, p. 38.

Exemplo disso é a técnica de construção de perfis pessoais em função dos quais podem ser tomadas importantes decisões a respeito dos consumidores, trabalhadores e cidadãos em geral, afetando diretamente a vida das pessoas e influenciando o seu acesso a oportunidades sociais.

Como afirma Perez Luño, na sociedade atual, a informação converte-se em poder a partir do momento em que a informática permite transformar informações parciais e dispersas em informações em massa e organizadas, o que torna imperativa a regulamentação jurídica dessas técnicas para a proteção da privacidade dos cidadãos[41].

A partir dessas constatações, poder-se-ia pensar que se está diante de um *trade-off* entre tecnologia e privacidade: a ampliação da tecnologia reduziria inevitavelmente a privacidade pessoal, que, por sua vez, somente poderia ser preservada com a contenção do desenvolvimento de tecnologias da informação. Juntamente com Simson Garfinkel, entende-se que a melhor forma de se observar a questão não é por meio da dicotomia entre tecnologia e privacidade, mas sim, a partir da concepção de que o desenvolvimento tecnológico deve ser harmonizado com a preservação da privacidade dos cidadãos[42].

O autor faz uma analogia dessa questão com a devastação do meio ambiente pela técnica, que foi tratada nas décadas de 1950 e 1960 como um problema inevitável: sob tal ótica, seria necessário conviver com a destruição das reservas naturais do planeta como condição para o desenvolvimento econômico e o aumento do nível de vida da população. Ocorre, no entanto, que tal visão foi superada a partir da concepção do desenvolvimento sustentável, que propugna conciliar o desenvolvimento econômico com a preservação ambiental[43].

---

[41] PÉREZ LUÑO, Antonio-Enrique. *Manual de Informática e Derecho*. Barcelona: Editorial Ariel, 1996, p. 43.

[42] GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. O'Reilly Media: California, 2000, p. 5.

[43] Idem, Ibidem, p. 5.

De forma semelhante, entende-se que a sociedade somente poderá obter as vantagens do desenvolvimento tecnológico se esse for acompanhado da tutela jurídica da personalidade, nas suas dimensões de privacidade, liberdade e igualdade.

Ao se analisar o tema da proteção de dados pessoais na sociedade da informação, é fundamental compreender que o cerne do problema não está situado na tecnologia[44]. Afinal, a tecnologia não se encontra em um vácuo, devendo ser compreendida a partir do meio social, econômico e político em que está inserida. Isso porque a própria tecnologia é criada pela sociedade para atingir determinados fins e o grau de sua regulação é estabelecido pela sociedade que a criou. Nesse sentido, é fundamental que o debate sobre a proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a idéia de que ela é a responsável pela perda de privacidade pessoal da sociedade contemporânea. Isto é, não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia.

Sob essa ótica e para possibilitar a resposta adequada aos desafios sociais advindos da revolução tecnológica, é fundamental que a teoria do direito se reconstrua a ponto de compreender e solucionar os novos problemas enfrentados pelo homem na era da informação[45]. Nesse sentido, é importante que os juristas adquiram a capacidade de refletir de forma crítica e responsável perante as dificuldades decorrentes da tecnologia,o que Vittorio Frosini denominou de "consciência tecnológica"[46].

Nesse contexto de desenvolvimento da tecnologia de informação, o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos desafios impostos pelo avanço da técnica. Naturalmente, tanto o direito à privacidade, como a proteção de dados pessoais, fundamentam-se, em última medida, na

[44] LYON, David. Surveillance as social sorting. Computer codes and mobile bodies. In: *Surveillance as Social Sorting. Privacy, risk and digital discrimination.* Ed. LYON, David. Londres: Routledge, 2003, p. 14. No mesmo sentido: GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. Op. Cit., p. 6.

[45] PÉREZ LUÑO, Antonio-Enrique. *Manual de Informática e Derecho*, Op. Cit., p. 10.

[46] FROSINI, Vittorio, apud PÉREZ LUÑO, Antonio-Enrique. *Manual de Informática e Derecho* Op. Cit., p. 10.

proteção da personalidade e da dignidade do indivíduo. Pode-se dizer, no entanto, que a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito[47].

É de se notar, inclusive, que a proteção de dados pessoais deu origem a um setor de política pública autônomo, dada a importância de se controlar o fluxo de informações pessoais na sociedade atual[48]. Essa autonomia pode ser percebida a partir da constatação de que a proteção de dados pessoais desenvolveu "instrumentos legais próprios, organismos regulatórios específicos, uma rede de especialistas e juristas, um robusto grupo de jornalistas e ativistas dispostos a demonstrar todo tipo de abuso e violações, uma crescente comunidade acadêmica especializada no tema, bem como uma rede internacional, pela qual se realiza o intercâmbio de experiências e idéias"[49].

Sob essa perspectiva, pode-se compreender que a proteção de dados pessoais adquire um âmbito mais abrangente. Primeiramente, ela passa a ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo igualmente uma tutela jurídica coletiva. Diferentemente, a privacidade sempre foi tratada sob um viés mais individualista, sendo os danos ao direito à privacidade tratados majoritariamente de forma individual[50].

Ademais, a disciplina da proteção de dados pessoais envolve outra questão, que em certa medida era ignorada pelo direito à privacidade: o problema da igualdade. A igualdade se apresenta como um tema para essa disciplina, na medida em que a vigilância realizada por organismos privados ou estatais, a partir de informações obtidas em bancos de dados, pode

47 Como afirma Doneda, "a proteção de dados pessoais, em suma, propõe o tema da privacidade, porém modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão". (DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Op. Cit., p. 205)

48 BENNET, Colin e RAAB, Charles. *The Governance of Privacy*: policy instruments in global perspective. Cambridge: The MIT Press, 2006, p. XXI.

49 Idem, Ibidem, p. XXI e XXII.

50 ARGENTINA: Protección de Datos Personales. In: Investigaciones 1 (1998), p. 121, Secretaria de Investigaión de Derecho Comparado, Corte Suprema de Justicia de La Nación, República Argentina.

acarretar a seleção e a classificação dos indivíduos, de modo a afetar expressivamente as suas oportunidades de vida na sociedade[51]. Desse modo, a tutela jurídica dos dados pessoais tem como uma de suas funções combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados, buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias.

Como afirma David Lyon, o direito à privacidade tem uma importância limitada nos contextos em que vigilância constante está implicada nos modos de reprodução social, determinando a classificação da população e efetuando a discriminação de cidadãos[52] Tal constatação adquire ainda maior importância quando se considera que, na sociedade atual, caracterizada pelas relações remotas, os dados pessoais acabam por se constituir na única forma de representação das pessoas perante as mais diversas organizações estatais e privadas, sendo determinantes para "abrir ou fechar as portas de oportunidades e acessos"[53].

Nesse sentido, entende-se fundamental a compreensão da disciplina de proteção de dados pessoais como meio, principalmente, de tutela da liberdade e da igualdade. Como se verá, nos itens subseqüentes, a tutela da privacidade foi associada historicamente ao princípio da liberdade e à autonomia individual, como o controle do indivíduo sobre as suas próprias informações. Ocorre, no entanto, que outro aspecto essencial diz respeito à não discriminação do cidadão em razão das informações armazenadas a seu respeito em bancos de dados. Para tanto, é fundamental apreender a dupla dimensão da disciplina de proteção de dados pessoais, fundada na liberdade e na igualdade.

Analisar-se-á primeiramente, as gerações de leis de proteção de dados pessoais para que se perceba de que modo esse tema foi sendo tratado gradativamente pela legislação dos

[51] LYON, David. Surveillance as social sorting. Computer codes and mobile bodies, Op. Cit., p. 1.

[52] Idem, Ibidem, p. 19.

[53] LYON, David. Surveillance as social sorting. Computer codes and mobile bodies, Op. Cit., p. 27.

países europeus. Em seguida, será examinada a articulação da proteção de dados pessoais com os princípios da liberdade e da igualdade.

1.4. O surgimento da política de proteção de dados e a convergência internacional

O início do debate público acerca da necessidade de proteção de dados pessoais está relacionado à tentativa de alguns governos, nas décadas de 1960 e 1970, de efetuarem a centralização de diversos bancos de dados automatizados em um gigantesco banco de dados nacional, o que ensejou a reação da população e, conseqüentemente, influenciou a aprovação da primeira geração das normas de proteção de dados pessoais, tanto nos EUA como na Europa.

Exemplo disso foi o caso do "National Data Center", nos EUA, projeto que nunca saiu do papel naqueles moldes, dada à grande reação da população. De acordo com Simson Garfinkel, o "National Data Center" foi proposto em 1965 pelo "Bureau of Budget", órgão competente para administrar o orçamento, e visava à redução de custos pelo Estado[54]. Sua idéia era a de que um único centro de dados nacional eximiria os demais órgãos do governo de investirem em informática e em tecnologia de armazenamento. No entanto, logo se percebeu que o centro traria inúmeras outra vantagens, tais como a possibilidade de se extraírem estatísticas de forma precisa e ágil, de se rastrearem e corrigirem inúmeros dados equivocados dos cidadãos e de utilizarem com grande eficiência os dados pessoais para as inúmeras atividades estatais, facilitando a tomada de decisões e o planejamento de ações[55].

À medida que o projeto evoluiu, chegou-se à idéia de que o centro deveria conter dados de todos os cidadãos americanos em relação à data de nascimento, cidadania, registros escolares, serviço militar, registros de impostos, benefícios da previdência social, registro do espólio e, eventualmente, registros criminais. Procederam-se a inúmeras discussões nos meios

[54] GARFINKEL, Simson. *Database Nation.* Op. Cit., p. 13.

[55] Idem, Ibidem, p. 13.

de comunicação e a diversas audiências no Congresso. Esses debates culminaram em um senso comum acerca dos potenciais danos que tal centralização de dados poderia causar, principalmente em razão do grande poder que ele conferia ao Estado sobre a vida de todos os cidadãos, ameaçando gravemente a tradição liberal americana[56]. Com essa repercussão, o "National Data Center" nunca chegou a ser construído.

É interessante mencionar que também na Europa ocorreu um caso semelhante, que consistiu no projeto francês SAFARI (Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus), apresentado em 1970 pelo Instituto Nacional de Estatística[57]. A partir desse projeto, cada indivíduo passaria a ser identificado por um número. Tendo em vista a má repercussão que o projeto teve na esfera pública, sob a alegação da violação da privacidade dos cidadãos, o governo francês decidiu não levá-lo adiante. O debate causado pelo projeto influenciou a posterior aprovação da lei francesa de proteção de dados pessoais, de 1978.

Esses projetos para a construção de grandes bancos de dados nacionais não lograram êxito, não apenas em razão da sua rejeição pelos cidadãos, mas principalmente, porque a tecnologia desenvolveu-se por outro caminho. Ao invés da criação de um único banco de dados, foram desenvolvidas técnicas para permitir o processamento de dados de forma descentralizada, como os "minicomputers", o que transformou completamente o debate sobre a proteção de dados pessoais.

Juntamente com os planos de construir bancos de dados centralizados, os governos também buscaram desenvolver números de identificação pessoal para cada cidadão, o que também foi motivo de forte reação dos cidadãos americanos e dos paises europeus. Esses números universais serviriam para ampliar a eficiência da Administração Pública, facilitar a comunicação, ampliar a conectividade com outros bancos de dados e aumentar a acuidade das

[56] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Op. Cit., p. 189.

[57] Idem, Ibidem, p. 191.

informações dos cidadãos armazenadas pelo Estado.[58] Diversas foram as tentativas de se reunir em um único número de identificação todas as informações pessoais dos cidadãos, mas, conforme afirma Colin Bennett, nenhum país logrou atingir essa meta, nos moldes planejados. Na realidade, o que se viu foram inúmeros números de identificação criados em cada país, referentes a áreas específicas do governo, como, por exemplo, o *Social Security Number*, dos EUA, o *National Health Service Number*, da Inglaterra, e o *Social Insurance Number*, do Canadá.[59]

Ao lado dos bancos de dados centralizados e dos números universais de identificação, na década de 70, a preocupação da população a respeito da violação da privacidade voltou-se também contra a realização de censos populacionais. Em 1970, o censo realizado na Suécia foi duramente questionado pela imprensa, principalmente em razão das especificidades das perguntas do questionário e do potencial risco de comercialização dessas informações para as empresas de marketing direto. Em 1971, o censo da Inglaterra gerou a maior discussão já vista no país a respeito do tema da privacidade. A sociedade civil em geral e a imprensa criticou duramente as perguntas referentes à origem étnica e qualificação profissional. Protestos semelhantes ocorreram na Alemanha, na ocasião dos censos de 1983 e 1987.

Evidências de convergência internacional

Como resultado desses processos acima mencionados, surgiu a necessidade de regulamentação do tema da proteção de dados pessoais nos mais diversos países. Ao se analisar o tratamento jurídico desses países à temática da proteção de dados pessoais, é possível perceberem-se mais semelhanças do que diferenças, conforme compreende Colin Bennett, o que foi denominado de tese da convergência.[60]. Segundo o autor, se por um lado,

[58] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Cornell University Press, 1992, p. 49.
[59] Idem, Ibidem, p. 50 e 51.

[60] Idem, Ibidem, p. 95 a 115.

existem diferenças entre as legislações dos diversos países europeus acerca do tema, por outro, a proteção dos dados pessoais pode ser compreendida, para além das particularidades nacionais, como um processo internacional informalmente coordenado no qual as legislações em estágios diversos não podem sucumbir à evolução geral da matéria. De acordo com Bennett:

> Convergência significa mais que similaridade. Denota um padrão que ultrapassa o tempo, um processo dinâmico, ao invés de uma condição estática. (…). Deste modo, a partir de uma posição em que os Estados não tinham nenhuma ou muito pouca legislação de proteção de dados e, por isso, havia diversos tipos de estratégia para o tema, um consenso emergiu durante a década de 1970, em volta de Princípios. Podemos concluir, portanto, que a convergência ocorreu.[61]

Para uma ilustração a respeito das datas das primeiras legislações de proteção de dados no mundo, é interessante analisar o quadro abaixo[62], que demonstra o período no qual as respectivas leis foram promulgadas:

A difusão da legislação de proteção de dados por região

	Década de 1970	Década de 1980	Década de 1990	Década de 2000
Europa Ocidental	Suécia (1973) Alemanha Ocidental (1978) Dinamarca (1978) Áustria (1978) França (1978) Noruega (1978) Luxemburgo (1978)	Islândia (1981) Reino Unido (1984) Finlândia (1987) Irlanda (1988) Holanda (1988)	Portugal (1991) Espanha (1992) Suíça (1992) Bélgica (1992) Mônaco (1993) Itália (1996) Grécia (1997)	
Europa Oriental e Central			Eslovênia (1990) Hungria (1992) República Tcheca (1992) Rússia (1995) Estônia (1996) Lituânia (1996) Polônia (1997) Eslováquia (1998) Letônia (2000)	
América do Norte	Estados Unidos (1974)	Canadá (1982)		Canadá (2000)
América do Sul			Chile (1999)	Argentina (2000)

[61] Idem, Ibidem, p. 111 e 112.

[62] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*, Op. Cit., p. 127.

Australásia		Nova Zelândia (1982) Austrália (1988)	Austrália (1997)	
Oriente Médio e Ásia		Israel (1981) Japão (1988)	Coréia do Sul (1994) Hong Kong (1995) Taiwan (1995) Tailândia (1998)	Japão (2004)

1.5. As gerações das leis de proteção de dados pessoais na Europa

A proteção de dados pessoais constitui um tema de grande relevância no contexto europeu, tendo sido acolhido pela maioria dos ordenamentos jurídicos dos Países-Membros desde a década de 1970. Apesar disso, ainda é bastante complexo conceituar exatamente o significado da proteção de dados pessoais, já que tal tema passou por uma forte evolução, à medida que ia sendo regulamentado por diversas legislações em diferentes períodos. A evolução do tema pode ser atribuída também às transformações tecnológicas que exigiram uma adaptação do tratamento legal do assunto.

Sob uma perspectiva histórico-evolutiva de gerações, proceder-se-á à analise geral do contexto europeu relativo à proteção de dados pessoais, conforme descrita por Mayer-Schönberger[63].

A primeira geração das normas de proteção de dados pessoais surgiu, na década de 70, como reação ao processamento eletrônico de dados nas Administrações Públicas e nas Empresas Privadas, bem como às idéias de centralização dos bancos de dados em gigantes bancos de dados nacionais. São exemplos de normas da primeira geração as seguintes: as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados

[63] MAYER-SCHÖNBERGER, Generational Development of Data Protection in Europe. Op. Cit., p. 219.

da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração pela sua estrutura e linguagem[64].

O impulso para o surgimento dessas normas foi o contexto generalizado do Estado Social, que requeria, para o funcionamento de sua burocracia, de planejamento sofisticado, o que, por sua vez, somente poderia ser alcançado por meio da coleta e do processamento dos dados dos cidadãos. Como exemplos do grande interesse das burocracias governamentais pela coleta desses dados nesse período, podem-se citar a proposta feito pelo Paramento da Suécia, em 1960, de fundir todas as informações fiscais e os registros civis e aos dados do censo, bem como o Comitê criado pelo governo alemão para viabilizar a conexão entre os bancos de dados municipais, estaduais e federal[65].

A reação dos cidadãos contra as tentativas dos governos de utilizar a tecnologia existente para ampliar a coleta e o processamento dos dados foi extremamente forte, pois esses temiam o poder absoluto de controle de uma burocracia automatizada e desumanizada. Assim, a crítica da sociedade voltou-se exatamente no sentido de se controlar a tecnologia, crítica essa que também se fez presente na primeira geração das normas de proteção de dados pessoais.

Sob essa ótica, é possível perceber que grande parte das normas de proteção de dados pessoais da década de 1970 tem uma perspectiva funcional e busca controlar os bancos de dados de forma *ex ante*, condicionando o seu funcionamento à licença prévia ou ao registro nos órgãos competentes[66].

Outra característica interessante das normas de primeira geração consiste no fato de que, ao priorizar o controle rígido dos procedimentos, elas deixavam para segundo plano a

[64] Idem, Ibidem, 221.

[65] Idem, Ibidem, p. 222.

[66] Idem, Ibidem, p. 223.

garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado nas normas.

De acordo com Mayer-Schönberger, os planos estatais ambiciosos de construção de um banco de dados centralizado não se concretizaram. Isso, no entanto, aconteceu não apenas em razão das reivindicações dos cidadãos, mas em razão da transformação tecnológica que possibilitou que unidades organizacionais pequenas do governo e da iniciativa privada utilizassem processamento de dados eletrônicos de forma descentralizada[67]. Tal fato ocasionou a proliferação da quantidade de bancos de dados existentes e, conseqüentemente, expôs a fragilidade da regulamentação das normas de primeira geração que estabeleciam procedimentos em detrimento de direito.

Desse modo, surgiu a necessidade de alteração legislativa e abriu-se espaço para a segunda geração das normas de proteção de dados pessoais. Tais normas buscavam tratar prioritariamente do direito à privacidade, ao invés de procedimentos. A temática da proteção de dados pessoais passa a se associar diretamente ao direito à privacidade, às liberdades negativas e à liberdade individual em geral. Como conseqüência, a privacidade informacional é inserida nos textos das Constituições da Áustria, Espanha e Portugal.

O temor por um banco de dados único e centralizado foi substituído pelo temor da existência de milhares de bancos de dados espalhados pelo mundo, conectados em rede. Nesse contexto, entendeu-se que o melhor seria que os cidadãos lutassem pela preservação de sua privacidade a partir de direitos fortes, inclusive, protegidos constitucionalmente, em alguns casos. São exemplos de normas da segunda geração as leis da Áustria, da Franca, da Dinamarca e da Noruega.

A característica principal das normas de segunda geração reside na possibilidade de participação do individuo no processo de coleta e de processamento de dados, por meio de seu

[67] Idem, Ibidem, p. 225.

consentimento. Assim, dá-se ao cidadão um poder de decisão para interferir no âmbito de sua própria privacidade informacional[68].

Outra mudança significativa dá-se no âmbito institucional, com a ampliação dos poderes das autoridades administrativas encarregadas da proteção de dados, com intuito de garantir o direito à privacidade. Como afirma Mayer-Schönberger:

> Primeiramente, algumas das instituições de segunda geração não apenas investigavam as ofensas à proteção de dados pessoais, mas também se tornaram uma espécie de ombudsman da proteção de dados pessoais para os cidadãos. Quando os direitos individuais eram violados, os cidadãos deveriam poder se reportar a alguma instituição – uma instituição que de algum modo poderia ajudá-los a reforçar o direito individual à proteção de dados pessoais. Segundo, algumas das instituições de segunda geração transformaram-se em órgãos adjudicatórios que concediam opiniões de como a burocracia poderia ou não interpretar as normas de proteção de dados pessoais[69].

A segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social. Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca do cadastro de suas informações pessoais.

Mayer-Schönberger observa de forma crítica e precisa o custo social que o indivíduo tem de pagar para exercer o seu direito à privacidade e à proteção dos dados pessoais:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do individuo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados

[68] Idem, Ibidem, p. 227.

[69] Idem, Ibidem, p. 228.

> pessoais possa ser exercida apenas por eremitas? Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?[70]

A terceira geração de normas de proteção de dados pessoais é marcada pela decisão do Tribunal Constitucional alemão[71], de 1983, no sentido de declarar a inconstitucionalidade da "Lei do Censo", que previa a obrigatoriedade dos indivíduos de fornecerem inúmeros dados pessoais, sem a adequada garantia da proteção desses dados. Na ocasião, o Tribunal reinterpretou a Lei federal de proteção de dados pessoais alemã à luz da Lei Fundamental de Bonn e declarou que os cidadãos possuem o direito à autodeterminação informativa, radicalizando a idéia do consentimento do indivíduo no processamento de seus dados.

Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecida pelas interpretações das normas de proteção de dados pessoais em períodos anteriores. A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre "tudo ou nada".

Também o contexto tecnológico sofreu alteração na década de 80, na medida em que novas tecnologias de rede e de telecomunicações ampliaram a capacidade e a velocidade de transmissão de dados. Nesse sentido, não é mais possível localizar fisicamente os bancos de dados, pois esses estão armazenados em redes e não mais em uma central identificável de processamento, podendo ser transferidos em segundos[72].

São exemplos dessa fase as leis dos Estados alemães após a decisão do Tribunal Constitucional, a emenda à lei federal de proteção de dados pessoais alemã de 1990, a emenda

[70] MAYER-SCHÖNBERGER, Generational Development of Data Protection in Europe. Op. Cit., p.228.

[71] BVERGE 65, 1 - grifo nosso. Ver MARTINS, Leonardo. (org.) Cinqüenta anos de Jurisprudência doTribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 233 a 245.

[72] MAYER-SCHÖNBERGER, Generational Development of Data Protection in Europe. Op. Cit, p. 230.

da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda.

No entanto, mais uma vez, pode-se dizer que ideal participativo dos cidadãos no controle das informações pessoais, consubstanciado na idéia de autodeterminação informativa, provou-se não ser factível no mundo real. Isso porque, semelhante ao que ocorreu com a segunda geração das normas de proteção de dados pessoais, os cidadãos não estavam dispostos a arcar com os altos custos monetários e sociais de exercer o seu direito e, por conseqüência, ser privado do acesso a bens e serviços ou a benefícios[73].

Ademais, tendo em vista que o consenso do indivíduo autorizava o processamento dos dados pessoais, em caso de violação ao seu direito à privacidade, não teria ele condições de lutar pela reparação daquela violação, na medida em que tinha consentido para o tratamento de seus dados.

A quarta geração de normas buscou resolver esses problemas apresentadas nos períodos anteriores por meio de duas soluções.

Primeiramente, algumas das normas, visaram fortalecer a posição dos indivíduos, tornando mais efetivo o seu auto-controle sobre os dados pessoais. Isso foi possível, por exemplo, a partir da previsão de "*no fault compensation*" para reclamações individuais a respeito da violação à proteção de dados pessoais, que se deu na Alemanha, com a emenda à Lei Federal de Proteção de Dados alemã, sendo que norma semelhante já existia na legislação da Noruega em menor extensão.

Em outros casos, as normas retiraram da esfera do controle do individuo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o cidadão, que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. Tal pode ser observado na proibição, total ou parcial, imposta para o tratamento dos dados pessoais considerados sensíveis, que são aqueles cujo tratamento

[73] Idem, Ibidem, p. 232.

tem grade potencial de acarretar discriminação, tais como os dados relativos à etnia, opção sexual, opinião política e religião.

A proibição total do tratamento desses dados deu-se nas legislações da Noruega, da Finlândia, da Dinamarca, da França e da Grã-Bretanha. Já as legislações da Suíça e da Alemanha, assim como a Diretiva Européia sobre proteção de dados pessoais de 1995, restringem o processamento de dados sensíveis, sem determinar, no entanto, a sua proibição total[74].

Outra característica bastante interessante da quarta geração de normas de proteção de dados pessoais consiste no fato de que, em diversos países, normas gerais sobre a proteção de dados são complementadas com normas setoriais. Tal fato tem como finalidade ampliar a proteção do individuo nos diversos setores em que é possível o tratamento dos seus dados pessoais, de modo que a legislação possa contemplar as diversas especificidades setoriais existentes. Assim, na maioria dos países europeus, percebe-se a existência de uma regulamentação geral sobre proteção de dados, mas com códigos de conduta setoriais suplementares.

Conforme afirma Mayer-Schönberg, a Diretiva Européia sobre proteção de dados pessoais de 1995 reflete a evolução geracional, pela qual passou a disciplina da proteção de dados pessoais na Europa[75]. Isso porque está no seu cerne a participação do individuo no processo de tratamento dos dados pessoais. Alem disso, em caso de tratamento de dados sensíveis, a Diretiva determina que esse está condicionado ao consenso expresso e informado do individuo. Com relação ao uso dos dados pessoais para a realização de marketing direto, a Diretiva possibilita que os cidadãos proíbam a utilização de seus dados para tal fim.

Como se pôde perceber a partir dessa análise evolutiva das normas de proteção de dados na Europa, tal disciplina passou por uma transformação dinâmica e significativa no

[74] Idem, Ibidem, p. 233.

[75] Idem, Ibidem, p. 233.

período das ultimas três décadas, principalmente em razão das modificações tecnológicas. Ademais, é notável como, aos poucos, o regime de proteção de dados pessoais possibilitou tanto a proteção da liberdade, consubstanciado na idéia de autodeterminação informativa, como da igualdade, concretizada na proibição ou na restrição de tratamento de dados sensíveis.

É bastante provável que as normas de proteção de dados pessoais continuem a se transformar e a se adaptar às novas realidades sociais. Assim, é possível se fazer algumas previsões[76]. Cada vez mais é provável que todas as legislações na Europa se tornem mais homogêneas, sempre com uma alto nível de proteção individual, principalmente em razão do intenso fluxo transfronteiriço de informações e das exigências econômicas globais. Ademais, os direitos de participação tendem a ser ampliados, na medida em que novas tecnologias de comunicação permitem cada vez mais a participação do individuo no momento do processamento de seus dados pessoais. Por fim, é provável que diante do fluxo de informações pessoais entre países, as normas nacionais de proteção de dados pessoais sejam enfraquecidas, ampliando a forca de regulamentações regionais.

1.6. A dimensão da liberdade

A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais a partir da moderna tecnologia da informação. Como visto, a sua função não é a de proteger os dados *per se*, mas a pessoa que é titular desses dados.

[76] MAYER-SCHÖNBERGER, Generational Development of Data Protection in Europe. Op. Cit., p. 235.

Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito[77]. Nessa hipótese, tem-se a violação também da autodeterminação e da liberdade do indivíduo, na medida em que ele deixa de ter controle sobre as suas próprias informações, ficando eventualmente sujeito ao poder de organismos privados ou públicos.

Nesse sentido, a proteção de dados pessoais tem como uma das suas finalidades principais prover o indivíduo de poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de autodeterminação e de livre desenvolvimento de sua personalidade[78].

Por se constituir como um direito sobre as informações pessoais, a proteção de dados pessoais tem um forte componente de autodeterminação e de autoconformação, tendo em vista que somente o indivíduo pode determinar o âmbito da própria privacidade, isto é, em que medida as suas informações pessoais podem ou não ser coletadas e transmitidas e até que ponto isso não viola a sua personalidade. Nesse aspecto, nota-se que a proteção de dados pessoais, à semelhança do direito que lhe deu origem, o direito à privacidade, é marcado por esse acentuado viés de autocontrole e de liberdade do seu titular.

Cabe ao Estado, por meio de legislação, prover os mecanismos necessários para que o cidadão possa exercer o controle do fluxo de informações a seu respeito na sociedade.

Tais constatações pressupõem que o discurso de direitos fundamentais, em uma sociedade pluralista, deve prezar antes de mais nada por um discurso da liberdade e da igualdade. Ele não pode visar impor uma única visão do mundo, nem uma determinada

[77] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Op. Cit.

[78] MURILLO, Pablo Lucas. *El Derecho a la autodeterminación informativa*. Op. Cit., p. 174.

concepção de bem. No Estado democrático de direito[79], que se baseia na dignidade humana e na autodeterminação da pessoa, é fundamental que o indivíduo possa exercer livremente o controle de seus dados pessoais na sociedade, cabendo a ele a conformação e a interpretação do seu direito à privacidade informacional.

É de se ressaltar que a liberdade, no sentido aqui pretendido, não se constitui como princípio absoluto: ela articula-se de forma permanente ao princípio da igualdade e ambas compõe em conjunto o preceito da dignidade humana. Como afirma Gomes Canotiho, "a dignidade da pessoa humana deve ser vista, em primeira linha, como fundamento de um direito geral de liberdade e de um direito geral de igualdade, concretizados através de múltiplos direitos especiais de igual liberdade". Assim, a liberdade passa a se conformar, no Estado Democrático de Direito, à justiça social e às exigências igualitárias da sociedade. Como se verá, no próximo tópico, o risco de violação ao princípio da igualdade, por meio de um tratamento de dados pessoais potencialmente discriminatório, poderá limitar a própria liberdade do indivíduo. Assim, liberdade e igualdade conformam-se mutuamente e definem o seu significado, alcance e limites de forma recíproca.

Diferentemente da concepção liberal, entende-se que a privacidade, na sua vertente de proteção de dados pessoais, ultrapassa a dimensão de um direito individual fundamental[80]. Isso porque a privacidade informacional, além de visar à proteção do indivíduo e de sua personalidade, exerce um importante papel perante a sociedade, atingindo também propósitos coletivos, como a preservação da democracia[81]. Ademais, a concepção desse direito, nos moldes aqui pretendidos, exige a superação do paradigma liberal, também na medida em que

[79] Compartilhamos da concepção desenvolvida por Habermas acerca do Estado democrático de direito, fundado na co-originalidade da autonomia privada e da autonomia pública.Ver: HABERMAS, Jürgen. *Direito e Democracia: entre Facticidade e Validade*, vol I e II. Op. Cit.

[80] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*, Op. Cit., p. 24.

[81] WESTIN, Alan. *Privacy and Freedom*. Op. Cit., p. 24.

compreende como necessária para a proteção de dados pessoais a institucionalização pelo Estado de mecanismos que possibilitem o exercício da autonomia do indivíduo[82].

O desenvolvimento da proteção de dados pessoais como um setor de política pública autônomo, dotado de instrumentos legais próprios e de organismos regulatórios específicos, demonstra como tal temática vai além da sua caracterização como direito fundamental[83].

É interessante observar que a dimensão da liberdade na disciplina de proteção de dados pessoais, consubstanciada na garantia de controle do indivíduo sobre as próprias informações, é uma característica generalizada das diversas legislações nacionais e regionais sobre o tema. As expressões "autodeterminação informativa", consolidada no direito alemão, e "liberdade informática", utilizada no direito espanhol, expressam com exatidão a importância que a dimensão da liberdade alcançou na temática da proteção de dados pessoais.

De modo semelhante, tal fato também pode ser constatado na principiologia desenvolvida nos EUA, que ressalta de forma significativa a dimensão da liberdade na temática da proteção de dados pessoais. Em 1972, no âmbito do "*Department of Health, Education, and Welfare"*, deu-se a primeira ação do Poder Executivo americano em relação ao problema dos dados pessoais[84]. Neste ano, foi designado pelo então Secretário desse departamento, um comitê consultivo de sistemas automatizados de dados pessoais ("*Advisory Committee on Automated Personal Data Systems"*), para o estudo da questão. Em 1973, o comitê emitiu um relatório sobre "Registros, Computadores e Direitos do Cidadão", que propunha alguns princípios fundamentais, cujo objetivo era "assegurar ao indivíduo o direito de participar de forma significativa das decisões sobre o que é inserido em registros sobre ele

[82] SCHWARTZ, Paul. "Privacy and Democracy in Cyberspace". In: *Vanderbilt Law* Review 52: 1609 – 1702, p. 1662.

[83] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*, Op. Cit., p. XXI e XXII.

[84] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 70 e 71.

e como aquela informação é usada"[85]. Assim, resta clara a dimensão de controle do cidadão sobre os dados pessoais também na tradição americana.

Colin Bennett demonstra que existe uma convergência das legislações entres os diversos países que regulamentaram a matéria, especialmente, no que diz respeito aos princípios básicos da proteção de dados pessoais[86]. O autor afirma que a regulamentação do tema nesses países visou, majoritariamente, atribuir aos indivíduos maior liberdade de controle sobre a informação coletada, armazenada, processada e disseminada[87]. Isso ocorreu, em razão da predominância do paradigma, segundo o qual, as leis e as políticas públicas somente poderiam estabelecer regras, princípios e procedimentos pelos quais os dados pessoais seriam tratados, devendo o conteúdo desse direito ser estabelecido pelo titular dos dados pessoais[88].

A análise das gerações das leis de proteção de dados pessoais na Europa demonstra em que momento o tema passou a ser tratado como uma liberdade individual dos cidadãos. Segundo Mayer-Schönberger, a segunda geração dessas normas já evidencia o tratamento da proteção de dados pessoais como um direito do indivíduo de controlar livremente o fluxo de seus dados, em contraste com a primeira geração de normas, que tinham como foco, não o indivíduo, mas o processamento dos dados em si[89].

O exercício dessa liberdade de controle de dados pessoais baseia-se no consentimento do titular, que possibilita à pessoa, em tese, determinar o nível de proteção dos dados a ela referentes. Exige-se que o consentimento seja consciente e informado. Conforme se verá

---

[85] U.S. HEW, *Records, Computers and the Right of Citizens*, p. 41 *apud* BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 70 e 71 (tradução livre). Segundo o autor, a importância do referido relatório foi bastante expressiva, chegando até mesmo a influenciar *Privacy Act* de 1974.

[86] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 95. A análise comparativa realizada por Bennett envolve os seguintes países: Estados Unidos, Alemanha, Grã-bretanhae Suécia.

[87] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*, Op. Cit., p. 8.

[88] Idem, Ibidem, p. 8 e 9.

[89] Mayer-Schönberger, Generational Development of Data Protection in Europe. Op. Cit, p. 227. Para a análise da evolução das gerações das leis de proteção de dados pessoais na Europa, ver item 2.2. desta Dissertação.

adiante, o tema do consentimento é repleto de minúcias e dificuldades que devem ser analisadas com cautelas.

Para possibilitar o controle do titular acerca dos seus dados, foram estabelecidos, na maioria das legislações sobre o tema, direitos subjetivos, tais como os direitos de informação, acesso, retificação e cancelamento. Sua função principal era a de tornar efetivo o exercício dos princípios previstos nas normas. Embora esses direitos configurem significativo empoderamento do indivíduo, ver-se-á que o seu estabelecimento nem sempre é suficiente para garantir a adequada proteção de dados na sociedade da informação.

O exercício do direito de controle do indivíduo sobre as suas informações consiste em uma dimensão importante da disciplina de proteção de dados pessoais. Ocorre, no entanto, que a forma de sua implementação é bastante complexa, num contexto, caracterizado pela sociedade de massas, pelo enorme fluxo de informações e pela predominância de grandes burocracias ávidas por informação, tanto no setor público, como no setor privado. A evolução das gerações de normas de proteção de dados pessoais reflete a tentativa de se buscar, cada vez mais, um modelo que garantisse efetivamente a autodeterminação do indivíduo, não obstante as diversas dificuldades encontradas para tanto.

Ver-se-á adiante as possibilidades e os limites do efetivo controle do cidadão sobre os seus dados pessoais, bem como os mecanismos estabelecidos legalmente para o exercício dessa liberdade.

1.6.1. O direito à autodeterminação informativa – a decisão da Corte Constitucional alemã

O conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade foi radicalizado com a decisão do Tribunal Constitucional Federal alemão, ao julgar a “Lei do Recenseamento de População, Profissão, Moradia e Trabalho” de 25 de março de 1982. O Tribunal decidiu pela inconstitucionalidade parcial da referida lei, ao argumentar a

existência de um direito à "autordeterminação informativa", com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade, respectivamente, Art. 1 I GG e Art. 2 I GG.

A referida lei visava à coleta dos dados dos cidadãos referentes à profissão, moradia e local de trabalho, com intuito de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas realizadas no país. Os dados a serem coletados por pesquisadores estavam listados na lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. Ademais, o §9 da norma determinava que os dados poderiam ser comparados àqueles presentes em registros públicos, com a finalidade de averiguar a veracidade das informações fornecidas, além de possibilitar a sua transmissão na forma anônima a órgãos públicos federais.

À época da lei do recenseamento, estava em vigor a Lei Federal de Proteção de Dados alemã, de 1977 (Bundesdatenschutgesetz – BDSG). Esta, no entanto, não foi capaz de fornecer os fundamentos jurídicos aptos a solucionar o descontentamento da população em relação à norma[90]. Isso pode ser demonstrado, pelo fato de que, quando confrontada com a lei do recenseamento, foi decidido por um juiz administrativo, em 1978, que as leis referentes à coleta de dados para fins estatísticos prevaleceriam sobre a lei federal[91].

Foram ajuizadas diretamente diversas reclamações constitucionais contra a Lei do recenseamento, com fundamento na violação direta ao Art. 2 I GG, que protege o livre desenvolvimento da personalidade. O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração.

---

[90] DONEDA,Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Op. Cit., p. 195.

[91] Idem, Ibidem, p. 195.

A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento. Nesse contexto, argumentou que a Constituição alemã protege o indivíduo contra o indevido tratamento de dados pessoais, por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual, o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade:

> O livre desenvolvimento da personalidade pressupõe, sob as modernas condições de processamento de dados, a proteção do indivíduo contra levantamento, armazenagem uso e transmissão irrestritos de seus dados pessoais. Essa proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c.c. Art 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais.[92] (BVERGE 65, 1, Volkszählung)

O Tribunal afirmou que a autodeterminação informativa não é um direito absoluto, podendo ser restringido em razão de interesse público predominante. Isso pode ocorrer, na medida em que a informação representa um recorte da realidade social, da qual o próprio indivíduo faz parte e é interdependente:

> Esse "direito à autodeterminação sobre a informação" não é garantido ilimitadamente. O indivíduo não tem um direito no sentido de uma domínio absoluto, ilimitado, sobre os seus dados; ele é muito mas uma personalidade em desenvolvimento, dependente da comunicação, dentro da comunidade social. A informação, também quando ela é relativa à pessoa, representa um recorte da realidade social que não poder ser associado exclusivamente ao indivíduo atingido (...). Por isso, em princípio o indivíduo tem que aceitar limitações de seu direito à autodeterminação à informação em favor do interesse geral predominante. (BVERGE 65, 1, Volkszählung) [93]

Pode-se dizer que a Corte avançou, também, ao reconhecer constitucionalmente os princípios da exatidão dos dados e da finalidade do uso dos dados pessoais, bem como o princípio de que devem ser coletados o mínimo possível de dados, necessários para se atingir a finalidade legal.

---

[92] MARTINS, Leonardo. (org.) Cinqüenta anos de Jurisprudência doTribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 238.

[93] MARTINS, Leonardo. (org.) Cinqüenta anos de Jurisprudência doTribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 238.

Outro aspecto levantado pelo Tribunal Constitucional diz respeito à indistinção, presente na lei do recenseamento, entre os dados coletados para serem manipulados individualmente e os que seriam usados para fins estatísticos. A Corte entendeu que não se pode exigir que a coleta e o uso dos dados para fins estatísticos estejam restritos a uma única finalidade, na medida em que, pela sua natureza, a estatística é multifuncional. Em razão disso, afirmou que, para a preservação da autodeterminação individual, seria necessária a criação de condições de manipulação claramente definidas: "se a diversidade das possibilidades de uso e associação de dados não é determinável antecipadamente, pela natureza da estatística, são necessários limites compensatórios no levantamento e no uso da informação dentro do sistema de informação"[94]. Exigiu, por fim, que fossem incluídas na lei mecanismos procedimentais de precaução, dada à ameaça inerente que o censo representa à personalidade.

A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subseqüentes leis sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo como o protagonista no processo de tratamento de seus dados. O reconhecimento desse direito pela Corte como um direito fundamental implica a limitação do legislador, que passa a ter o dever de concretizar na norma infralegal o preceito constitucional. Desse modo, a formulação de um direito à autodeterminação informativa delimitou os parâmetros legais para o tratamento em geral de dados pessoais na Alemanha.

De fato, a lei de 1985, que estabeleceu as normas para a realização do censo de 1987 abarcou diversos preceitos estabelecidos pela decisão da Corte, tais como a separação entre os dados coletados para fins estatísticos e os dados individualizados, a determinação de que o

[94] BVERGE 65, 1, Volkszählung. In: MARTINS, Leonardo. (org.) Cinqüenta anos de Jurisprudência doTribunal Constitucional Federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 241.

cidadão fosse informado sobre as finalidades da coleta de dados e sobre a sua obrigação de fornecê-las, bem como a vedação da transferência de dados pessoais entre órgãos públicos[95].

Dessa forma, o grande mérito do julgamento, e o que explica em parte a sua repercussão nos países da União Européia, reside na consolidação da idéia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação. Cabe destacar também o fato da sentença ter vinculado expressamente a temática da proteção de dados pessoais ao livre desenvolvimento da personalidade e ao princípio da dignidade humana. Por fim, pode-se dizer que a decisão logrou demonstrar a fragilidade dos sistemas de proteção de dados pessoais baseados apenas em normas infraconstitucionais, evidenciando a importância do reconhecimento constitucional de um direito subjetivo fundamental do cidadão, cujos dados pessoais são objeto de tratamento.

1.6.2. O consentimento na proteção de dados pessoais

Para que o indivíduo possa exercer o seu poder de autodeterminação informativa, faz-se necessário um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão.

Na Diretiva Européia 95/46/CE, é possível perceber a importância dada ao consentimento do titular dos dados pessoais. Conforme estabelecido em seu art. 7º, o consentimento inequívoco do titular constitui pressuposto para o tratamento de dados

[95] DONEDA,Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Op. Cit., p. 196.

pessoais, salvo na hipótese de previsão contratual ou legal. Por sua vez, o seu art. 2º, c, define consentimento como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento".

Sabe-se, contudo, que o consentimento, aplicado ao tema da proteção de dados pessoais, apresenta diversas dificuldades, devendo ser tratado com cautela em razão dos seguintes aspectos: i) o problema da eficácia do consentimento no tratamento de dados pessoais, em face da possibilidade do não consentimento do indivíduo acarretar a sua exclusão do mercado de consumo e da sociedade; ii) o problema da violação da proteção de dados pessoais, após o tratamento ter sido consentido pelo titular dos dados; iii) a questão do consentimento aplicado ao tratamento dos dados sensíveis.

Assim, deve-se evitar a mera transposição do consentimento negocial ao âmbito da proteção de dados, buscando as suas características próprias.

Como visto, a partir da análise das gerações das leis de proteção de dados pessoais, tanto a segunda, quanto a terceira geração de normas buscou estabelecer a participação do indivíduo no processo de tratamento de dados. Ocorreu, no entanto, que os altos custos monetários e sociais que os cidadãos deveriam suportar para exercer o seu direito tornaram essa participação ilusória[96]. Mayer-Schönberger questiona-se acerca do custo social que o indivíduo tem de pagar para exercer o seu direito à privacidade e à proteção dos dados pessoais: "Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?"[97].

O autor menciona outro problema relevante a respeito do consentimento no âmbito da proteção de dados pessoais: na medida em que consentimento do indivíduo permite o

[96] Mayer-Schönberger, Generational Development of Data Protection in Europe. Op. Cit, p. 232.

[97] Mayer-Schönberger, Generational Development of Data Protection in Europe. Op. Cit, p. 228.

processamento dos seus dados, na eventual hipótese de violação ao seu direito à privacidade, como poderia ele reivindicar a reparação daquela violação, se tinha autorizado o tratamento de seus dados pessoais?[98] É o que Doneda designa como paradoxo da privacidade, pois a estrutura desse direito exige, primeiramente, que o indivíduo autorize o processamento de seus dados, para apenas depois buscar a tutela jurídica[99]. Para se resolver essa questão, é fundamental compreender que o consentimento não representa a ausência de interesse do indivíduo na tutela dos dados pessoais, mas, constitui um ato de escolha no âmbito da autodeterminação individual[100].

Por fim, o consentimento pode gerar também um problema quando se está a tratar de dados sensíveis, isto é, dados cujo tratamento pode ser potencialmente discriminatório. Para a solução dessa questão, muitas das normas nacionais retiraram da esfera do controle do individuo esses assuntos, por compreenderem que são tão relevantes para o cidadão, que não podem estar na esfera de disposição individual. Por outro lado, algumas legislações exigiram para a coleta e o processamento desses dados o consentimento de forma expressa e escrita, como é o caso da lei espanhola de dados pessoais (LORTAD, Art. 7º)[101].

Em razão das dificuldades acima mencionadas, entende-se melhor evitar a transposição do consentimento negocial, aplicado aos mecanismos contratuais tradicionais, à disciplina da proteção de dados[102]. Tal constatação fundamenta-se no fato de que a proteção de dados pessoais envolve diretamente a dimensão da personalidade do indivíduo, fator que não pode ser ignorado em uma análise mais aprofundada.

Nesse sentido, o consentimento pode ser compreendido como um ato unilateral, que visa autorizar o tratamento dos dados pessoais, sem que isso implique uma estrutura

[98] Idem, Ibidem, p.233.

[99] DONEDA,Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Op. Cit., p. 196, p. 375

[100] Idem, Ibidem, p. 378.

[101] O problema do consentimento no tratamento dos dados sensíveis será analisado de forma minuciosa no item 2.4.2.

[102] DONEDA,Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Op. Cit., p. 376.

contratual[103]. É fundamental distinguir o consentimento em relação ao processamento de dados pessoais em dois momentos: i) o consentimento para a autorização da coleta e processamento dos dados, isto é, para o acesso à esfera privada do indivíduo; e ii) o consentimento para a autorização da transferência dos dados[104]. A mesma distinção pode ser encontrada na lei espanhola de proteção de dados pessoais (LORTAD), que exige o consentimento do titular tanto para o tratamento dos dados, como para a sua cessão.

Sob essa ótica, adquire grande relevância a possibilidade de revogação do consentimento. Tal prerrogativa é fundamental para fazer valer a autodeterminação do indivíduo e o livre desenvolvimento de sua personalidade. Vale dizer que a revogação é possível de acontecer tanto em relação à autorização para o tratamento, quanto em relação à circulação dos dados.

É o que determina os art. 6º, 3, e 11º, 4 da lei espanhola[105]. De acordo com tal lei, a revogação do consentimento para o tratamento dos dados pessoais exige uma causa justificada, além de não poder acarretar efeitos retroativos. Como causa justificada pode-se compreender qualquer descumprimento das obrigações por parte do responsável pelo tratamento dos dados pessoais. Já com relação à cessão dos dados, o direito do indivíduo de revogar o seu consentimento não está condicionado a esses pressupostos. Isso porque a circulação dos dados pessoais pode se caracterizar em uma ameaça maior à personalidade do cidadão, e, portanto, a lei autoriza a revogação do consentimento sem qualquer justificativa.

[103] Idem, Ibidem, p. 378.

[104] Idem, Ibidem, p. 379.

[105] "Art. 6º. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos."

"Art. 11º. 4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable."

Deve-se ressaltar que a eventual conduta abusiva do indivíduo que revogue o consentimento não estará isenta de reparação, na hipótese de serem causados danos ao legítimos interesses do responsável pelo tratamento dos dados pessoais[106].

Por fim, pode-se dizer que os pressupostos de um consentimento válido, no âmbito da proteção de dados pessoais, são os seguintes: i) que o titular dos dados que emita o consentimento o faça por sua livre vontade; ii) que o consentimento seja voltado a uma finalidade específica; iii) que o titular seja informado acerca do objetivo da coleta, do processamento e do uso dos dados, assim como das conseqüências de não consentir com o tratamento[107].

1.6.3. Os direitos subjetivos do titular dos dados pessoais

O pressuposto de que o indivíduo deve ter o poder de controlar o fluxo de seus dados pessoais requer que lhe sejam atribuídos determinados direitos subjetivos em face dos responsáveis pelo controle dos bancos de dados. Esses direitos, presentes na maioria das legislações sobre o tema, geralmente, podem ser resumidos aos seguintes: i) direito geral de informação; ii) direito de acesso e iii) direito de notificação; iv) direito de retificação, cancelamento e bloqueio dos dados; v) direito de não se ficar sujeito a uma decisão individual automatizada.

O direito geral de informação consiste no direito que as pessoas têm de conhecer sobre a existência dos bancos de dados, bem como dos seus objetivos e de seu conteúdo. Ele baseia-se na idéia de que a transparência é uma das principais formas de se combaterem os abusos[108].

---

[106] DONEDA,Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Op. Cit., p. 381.

[107] É o que prescreve a lei de proteção de dados alemã (BDSG), em sua seção 4a, (1): "Consent shall be effective only when based on the data subject's free decision. He shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or at his request, of the consequences of withholding consent. (…)"

[108] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 156.

Em contrapartida a esse direito de informação, surge para o banco de dados o dever publicar seu nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia desse direito[109].

Outro viés do direito à informação consiste no direito do indivíduo cujos dados são coletados de conhecer a identidade do responsável pelo tratamento, o objetivo do tratamento e os destinatários dos dados em caso de transferência[110]. Esse direito manifesta-se nos casos em que os dados pessoais são colhidos diretamente do seu titular.

O direito de acesso refere-se ao direito do indivíduo de receber a informação acerca dos dados registrados sobre ele, quando assim o requisitar[111]. Essa faculdade compreende o conhecimento sobre os dados armazenados, incluindo informações acerca da sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento. A freqüência desse acesso varia de acordo com as diversas legislações, assim como a sua gratuidade ou onerosidade. Entende-se que para a garantia da efetividade do referido direito, seria fundamental garantir a gratuidade do acesso a essas informações, conforme estabelece, por exemplo, a Lei Federal de Proteção de Dados alemã, de 2006 (BDSG), em sua seção 19, (7) e 35, (5)[112]. Não sendo possível estabelecer tal gratuidade, é fundamental garantir-se que a cobrança de taxa não torne ineficaz tal direito.

O direito de acesso compreende também o direito do indivíduo de conhecer, na hipótese da existência de uma rede de bancos de dados, em qual banco de dados estão armazenadas as suas informações. Nesse caso, pode o cidadão procurar qualquer um desses

[109] Idem, Ibidem, p. 157.

[110] Lei de Proteção de Dados Pessoais de Portugal, art, 10º, 1. (Lei no. 67/98 de 26 de outubro)

[111] MURILLO, Pablo Lucas. *El Derecho a la Autodeterminación Informativa*, Op. Cit., p. 187.

[112] A BDSG permite a cobrança de taxa, que não exceda os custos necessários para a realização do acesso, somente quando o tratamento de dados pessoais é feito por organismo privado para fins de transferência e o indivíduo puder auferir algum valor daquela informação – Seção 35, (5).

bancos, que terá a obrigação de encaminhar a sua solicitação ao organismo responsável pelo armazenamento, bem como de comunicar tal informação ao cidadão[113].

O direito de notificação está relacionado aos direitos anteriores e surge para o indivíduo sempre quando os seus dados forem coletados sem o seu conhecimento[114]. Nessa hipótese, deve o indivíduo ser informado sobre o armazenamento, a identidade do responsável pelo banco de dados e o objetivo do tratamento[115]. O indivíduo deve ser notificado também em caso de transferência de seus dados, devendo constar da notificação os organismos receptores. A notificação é dispensada caso o indivíduo tenha conhecimento do armazenamento ou da transferência por outros meios ou quando esses atos tiverem fundamento legal[116].

Os direitos de retificação, cancelamento e bloqueio dos dados visam assegurar o princípio da qualidade dos dados pessoais, de modo a corrigi-los em caso de equívoco, cancelá-los, caso estejam obsoletos ou tenham sido indevidamente armazenados e bloqueá-los, na hipótese do cancelamento não ser possível faticamente ou não ser permitido por lei. Os dados devem ser bloqueados também na hipótese de haver uma controvérsia sobre a sua veracidade e não houver sido apresentada prova para confirmá-la.

Em caso de correção, bloqueio ou cancelamento dos dados, é direito do indivíduo que todos os organismos que receberam por transferência os seus dados sejam notificados para tomarem as devidas providências. Nesse sentido, têm-se, por exemplo, a Lei Federal de Proteção de Dados portuguesa (Art. 11º, e), a Lei Federal de Proteção de Dados alemã (seção 20, (2) 8).

---

[113] BDSG, Seção 6, (2).

[114] Ver "considerando" 39 da Diretiva Européia 95/46/CE: "Considerando que por vezes se tratam dados que não foram recolhidos directamente pelo responsável junto da pessoa em causa; que, além disso, os dados podem ser legitimamente comunicados a um terceiro sem que essa comunicação estivesse prevista na altura da recolha dos dados junto da pessoa em causa; que, em todos estes casos, a pessoa em causa deve ser informada no momento do registo dos dados ou, o mais tardar, quando os dados são comunicados pela primeira vez a um terceiro".

[115] BDSG, 19a (1).

[116] BDSG, 19a (2)

O direito de não se ficar sujeito a uma decisão individual automatizada consiste no direito do cidadão de não ficar submetido a decisões que influenciem significativamente a sua posição jurídica, tomadas exclusivamente com base no tratamento automatizado de dados.[117] Desse modo, tal regra constitui uma proibição geral referente a decisões automatizadas, podendo ocorrer apenas em duas hipóteses, conforme a Diretiva: desde que existam medidas adequadas que garantam a representação e expressão do titular dos dados para a sua defesa ou que ocorra no âmbito da celebração ou execução de contratos.

Tal direito consiste, na realidade, em uma regra de justiça, que visa assegurar a possibilidade de defesa do titular e a mínima participação do titular em um processo de decisão tomado com base em seus dados e que afetará de forma significativa as suas oportunidades de vida.

1.6.4. Os princípios da proteção de dados pessoais

Para que o indivíduo possa exercer o seu poder de autodeterminação informativa, existem importantes princípios que devem nortear a atividade de tratamento de dados pessoais. Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados.

O primeiro princípio que todas as atividades de processamento de dados devem seguir é o princípio da publicidade. Também chamado de princípio da transparência, ele exige que a existência de um banco de dados pessoais seja de conhecimento público. Este princípio pode ser atendido por meio da exigência de autorização estatal prévia para a criação de um banco de dados pessoais ou pela necessidade de divulgação periódica de relatórios sobre o seu funcionamento.

[117] Esse direito está previsto no art. 15 da Diretiva Européia 95/46/CE.

Outro princípio relevante é o da exatidão. Ele se refere à exigência de que os dados constantes de um banco reflitam a realidade. Além de requerer cuidado na formação do banco de dados, ele também demanda a sua constante atualização, de forma a impedir que os dados contidos restem ultrapassados com o passar do tempo.

O princípio da finalidade indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Esse princípio é essencial para se justificar a limitação do acesso de terceiros ao banco de dados. De forma semelhante, ele também serve como parâmetro para se julgar se determinado uso dos dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado.

O princípio do livre acesso demanda que um banco de dados pessoais esteja sempre disponível ao interessado que possui seus dados ali armazenados. Além de garantir a obtenção de cópias dos registros dos bancos de dados, este princípio também assegura o direito do interessado em retificar as informações incorretas ou atrasadas.

O princípio da segurança, por fim, refere-se à exigência básica de que qualquer banco de dados pessoais esteja protegido contra extravios, destruições, modificações e desvios não autorizados pelos interessados.

1.7. A dimensão da igualdade

Como foi demonstrado no tópico anterior, o intenso processamento de dados pelos setores público e privado, a partir de meados do século XX, suscitou o problema da violação à dignidade humana e à liberdade individual. Afinal, o indivíduo passa a ter cerceada a sua autodeterminação, quando deixa de ter controle sobre as suas próprias informações, podendo ficar sujeito ao poder de organismos privados ou públicos.

Ocorre, no entanto, que o processamento de dados pessoais por grandes burocracias, a partir da moderna tecnologia da informação, tem o potencial de violar a dignidade do indivíduo também em uma outra dimensão, pouco explorada pela teoria da proteção de dados pessoais: a dimensão da igualdade.

A igualdade se apresenta como um princípio ameaçado, na medida em que a vigilância realizada por organismos privados e estatais, a partir de informações obtidas em bancos de dados, pode acarretar a classificação e a discriminação dos indivíduos, afetando expressivamente as suas oportunidades sociais. Sob essa perspectiva, David Lyon, evidencia como a idéia de privacidade se mostra limitada para se compreender o atual fenômeno da vigilância:

> Antigamente, as preocupações referentes à vigilância eram expressas na linguagem da privacidade e, possivelmente, da liberdade. (...) Embora essas questões ainda sejam importantes, está ficando muito claro para muitos que eles não contam a história toda. A vigilância hoje classifica as pessoas em categorias, atribuindo valor ou risco, de forma a afetar realmente as suas chances de vida. Profundas discriminações ocorrem, tornando a vigilância não uma questão meramente de privacidade pessoal, mas de justiça social[118].

É importante esclarecer que a categoria "vigilância" tem sido estudada principalmente por uma tradição sociológica para analisar o fenômeno do intenso monitoramento e controle aos quais estão submetidos o indivíduo na sociedade contemporânea. Essa corrente defende que o conceito de privacidade não funciona mais como uma solução para os problemas relativos à seleção, classificação e discriminação do fluxo de informações na sociedade e argumenta em favor da análise do fenômeno a partir categoria da "vigilância". Tal concepção é fundamental para o presente trabalho, na medida em que permite evidenciar o problema da discriminação realizada a partir dos dados pessoais, possibilitando a busca por instrumentos jurídicos que coíbam tal violação à igualdade.

[118] LYON, David. Surveillance as social sorting: privacy, risk and social discrimination, Op. Cit., p. 1.

Sabe-se que os sistemas de vigilância não foram inventados na era da informática, mas existem há séculos, categorizando pessoas, lugares e situações com base em seu risco e valor. A vigilância na sociedade da informação, no entanto, adquire características e contornos próprios. Primeiramente, ela passa a ser realizada, não mais apenas pelo Estado, mas diversos organismos privados, atingindo consumidores, trabalhadores e cidadãos em geral. Segundo, ela utiliza-se de tecnologias extremamente modernas, como as diversas técnicas para tratamento de dados pessoais, que permitem a consolidação de um quadro da personalidade do indivíduo relativamente completo. Por fim, ressalta-se que a principal característica da nova vigilância, concretizada por meio da coleta e do processamento de dados pessoais, é a sua ocorrência cotidiana, tanto local quanto globalmente. Isto é, tornou-se uma vigilância do dia-a-dia e de todos os aspectos corriqueiros da vida: do trabalho, da casa, do consumo[119].

Pode-se dizer que os objetivos dessa vigilância residem no planejamento, na possibilidade de prognósticos, e na prevenção dos riscos das atividades administrativas e empresariais, por meio da classificação e da avaliação dos perfis pessoais. Para tanto, são manipulados os mais variados dados referentes a pessoas, como dados de vídeo, dados biométricos, dados genéticos e arquivos administrativos[120].

Sob essa ótica, nota-se a necessidade de que a tutela jurídica dos dados pessoais abranja também a proteção da igualdade dos cidadãos e não apenas a sua liberdade, como ocorreu majoritariamente nas primeiras normas de proteção de dados. Para tanto, a proteção de dados pessoais deve ser apta a combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados, buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias.

Desse modo, entende-se fundamental compreender que a disciplina de proteção de dados pessoais possui uma dupla dimensão, fundada na liberdade e na igualdade, devendo-se

[119] LYON, David. Surveillance as social sorting. Computer codes and mobile bodies, Op. Cit., p. 13 e 14.

[120] Idem, Ibidem, p. 13.

refletir sobre o modo como ambos os princípios se conformam e se concretizam na prática da tutela jurídica das informações pessoais.

A idéia da igualdade, conforme aqui defendida, constitui um princípio fundamental de qualquer sociedade democrática e um pressuposto para o governo legítimo. Para que a igualdade seja efetivada, é necessário que o governo "demonstre igual consideração pelo destino de todos os cidadãos"[121]. Isto é, a igualdade pressupõe que, em uma sociedade, sejam implementadas normas e ações "que garantam que o destino de seus cidadãos (...) não dependa de quem eles sejam – seu histórico econômico, sexo, raça ou determinado conjunto de especializações ou deficiências"[122]. Sob essa perspectiva, a igualdade de todos os indivíduos não se fundamenta nas características da pessoa, mas na importância de que a sua vida tenha algum resultado.

No entanto, a realização da igual consideração, somente pode ser adequadamente alcançada, se aliada a outro princípio fundamental, o princípio da liberdade: que toda pessoa tem responsabilidade especial e final pela sua vida, embora se reconheça a igual importância objetiva de que todas as vidas tenham êxito. Isso significa que, na perspectiva ora adotada, liberdade e igualdade são constituintes do mesmo ideal político, não podendo ser compreendias isoladas uma da outra. Resta clara a interdependência entre liberdade e igualdade, nas palavras de Dworkin:

> A liberdade e a igualdade não podem entrar em conflito como duas virtudes políticas fundamentais, pois a igualdade só pode ser definida quando se presume a liberdade em vigor, e não pode ser aprimorada, nem no mundo real, por políticas que comprometam o valor da liberdade. (...)
> A estratégia da ponte presume que a liberdade e a igualdade são aspectos de uma só virtude política, pois a estratégia emprega a liberdade para ajudar a definir a igualdade e, em nível mais abstrato, utiliza a igualdade para ajudar a definir a liberdade.

[121] DWORKIN, Ronald. *A virtude soberana: a teoria e a prática da igualdade*. São Paulo: Martins Fontes, 2005, p. IX.

[122] Idem, Ibidem, p. XVII.

A referida concepção difere significativamente das teorias tradicionais sobre igualdade e liberdade, que costumavam compreender tais princípios como inconciliáveis, atribuindo predominância a algum deles. Por um lado, os igualitaristas compreendiam que a comunidade política deveria demonstrar igual consideração por todos os cidadãos, sem, no entanto, atentar para a importância de se atribuir também responsabilidade pessoal a cada um deles. Por outro, os conservadores tenderam a priorizar a responsabilidade individual, ignorando a necessidade de tratamento igualitário dos cidadãos pela comunidade[123].

No contexto da sociedade da informação, em que os dados pessoais do indivíduo passam a se constituir como intermediário entre a sua personalidade e a sociedade, a tutela da igualdade constitui-se como um importante mecanismo para evitar que as oportunidades de vida dos indivíduos sejam limitadas em razão de suas características pessoais, retratadas em bancos de dados. Assim, se no primeiro momento pode parecer estranho aliar o tema da proteção de dados pessoais ao princípio da igualdade, na prática, é fácil perceber essa vinculação; esta se baseia tão somente no antigo ideal contrário à discriminação, segundo o qual as características naturais das pessoas não podem ser utilizadas para lhe negar oportunidades e acesso a recursos sociais.

Desse modo, argumenta-se que a proteção de dados somente pode ser compreendida em toda a sua complexidade se vista sob o ponto de vista da igualdade e da liberdade. Isso porque ambas se conformam e se limitam reciprocamente. A mera proteção da liberdade sem a equivalente proteção da igualdade impossibilita a realização do ideal liberal. Isso significa que a lei que protege meramente um ato livre, que tenha conseqüências potencialmente discriminatórias, não está sequer protegendo a liberdade do cidadão.

Sob tal ótica, entende-se que a proteção de dados pessoais, se limitada à sua dimensão de liberdade, pode acabar traindo a sua própria concepção de liberdade. Isto é, se compreendida apenas na sua dimensão de liberdade, a disciplina de proteção de dados

[123] Idem, Ibidem, p. XVII e XVIII.

pessoais não logrará o êxito de proteger o cidadão, na medida em que de nada adianta a comunidade atribuir responsabilidade pessoal a todos, se não demonstra igual preocupação com o destino de cada um. Afinal, liberdade que possibilita discriminação não é liberdade, em uma sociedade democrática.

Nos tópicos seguintes desta seção, ver-se-á como a igualdade e a liberdade se articulam na problemática dos dados sensíveis (2.5.1), bem como na questão sobre a classificação e a discriminação dos indivíduos (2.5.2), realizada a partir de modernas técnicas de tratamento de dados pessoais, afetando expressivamente as suas oportunidades sociais.

1.7.1. Dados sensíveis ou tratamento sensível dos dados?

A categoria dos dados sensíveis foi desenvolvida a partir da percepção de que o armazenamento, processamento e circulação de alguns tipos de dados podem se constituir em uma ameaça maior à personalidade individual, especialmente, se utilizados para condutas discriminatórias. Os dados referentes à raça, opção sexual, saúde e religião, são exemplos desse tipo.

Tal perspectiva permite realçar as discussões acerca da violação da igualdade material em um terreno anteriormente dominado por concepções liberais. Desse modo, passa-se a considerar também os abusos decorrentes do tratamento dos dados pessoais como um problema de igualdade, sempre que sua inadequada utilização acarretar ações potencialmente discriminatórias.

A diferenciação da categoria dos dados sensíveis foi consagrada pelo Convênio 108, editado pelo Conselho da Europa, em 1981, em seu art. 6. O Convênio previu a proibição de tratamento dos dados sensíveis, ao menos que o direito interno previsse as garantias adequadas para o seu processamento[124].

[124] HIGUERAS, Manuel Heredero. *La Directiva Comunitaria de Protección de los datos de carater personal.* Aranzadi Editorial, 1997, p. 116 e 117.

O estabelecimento de um regime especial para os dados sensíveis está presente na legislação da maioria dos países europeus e na Diretiva Européia 95/46/CE, de forma a proibir ou limitar o seu processamento. A proibição total do tratamento desses dados deu-se nas legislações da Noruega, da Finlândia, da Dinamarca, da França e da Grã-Bretanha. Já as legislações da Suíça e da Alemanha, assim como a Diretiva Européia, restringem o processamento de dados sensíveis, sem determinar, no entanto, a sua proibição total[125].

A referida Diretiva prescreve, em seu art. 8º, que "os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde ou à vida sexual". Em seguida, estabelece as hipóteses possíveis de tratamento de dados sensíveis, que são, entre outras, quando a pessoa tiver dado o seu consentimento explícito e quando o tratamento dos dados for necessário para o cumprimento de obrigações e de direitos do responsável pelo tratamento, quando for necessário para a proteção dos interesses vitais da pessoa.

A inclusão da categoria dos dados sensíveis nas leis de proteção de dados pessoais veio acompanhada de disposições normativas mais severas, visando à maior proteção do cidadão e da sociedade. O aumento do rigor das normas nesse âmbito reflete-se nos seguintes aspectos: i) ampliação das exigências legais para o consentimento do indivíduo sobre a disposição de seus dados pessoais; ii) ampliação das exigências legais para o tratamento desses dados pelo responsável, como, por exemplo, a intensificação de medidas de segurança, em alguns casos; e iii) pelo aumento do controle pela autoridade administrativa para a autorização de armazenamento, processamento e circulação dos dados sensíveis.

Ressalta-se que a restrição ao tratamento desses dados não significa uma completa vedação, podendo a autoridade administrativa autorizar o seu tratamento quando for comprovada a ausência de potencial lesivo. Nesse sentido, vale mencionar decisão da

[125] Mayer-Schönberger, Generational Development of Data Protection in Europe. Op. Cit., p. 233.

Comissão Nacional de Proteção de Dados de Portugal, que autorizou o processamento de dados raciais, cuja finalidade era a promoção de pessoas que trabalham ou se propõe a trabalhar como modelos fotográficos ou como atores de cinema, televisão, publicidade, teatro e outros eventos (autorização no. 192/2002, da CNPD). [126]

Deve-se destacar que, além da proteção especial reservada aos dados definidos expressamente na Diretiva 95/46/CE como sensíveis, é fundamental proteger também outros dados que, embora aparentemente insignificantes, podem vir a se tornar sensíveis, a depender do tipo de tratamento a que são submetidos. Trata-se na realidade, de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias. Conforme afirmou o Tribunal Constitucional alemão no julgamento sobre a lei do recenseamento, a partir das possibilidades de ligação e processamento da tecnologia da informação, "um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados".[127]

São exemplos de técnicas que podem acarretar riscos à igualdade material dos cidadãos a mineração de dados (*datamining*), o sistema de avaliação de riscos *(Scoring- ou Rating- System)* e a construção de perfis (*profiling*), que serão estudados no capítulo 2.

Vejamos em seguida algumas formas de tratamento de dados pessoais que possuem um potencial discriminatório e que, portanto, devem ser vedadas ou realizadas de forma a assegurar a privacidade dos cidadãos.

Dados médicos e genéticos

A prática da medicina, bem como dos planos e seguros de saúde, alterou-se fortemente a partir da informatização dos arquivos médicos, uma vez que possibilitou a ampliação da

[126] CASTRO, Catarina Sarmento e. *Direito da Informática, Privacidade e Dados Pessoais.* Coimbra: Almedina, 2005, p. 98.
[127]MARTINS, Leonardo. (org.) *Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão.* Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.

coleta, do armazenamento e da cessão das informações do paciente, desde a seqüência de seus genes até os prontuários do paciente.[128]

A preservação da privacidade na área médica tem uma enorme relevância na sociedade, na medida em que o paciente relata os sintomas da sua doença a um médico, em quem ele confia, com a finalidade de receber um diagnóstico e um tratamento adequado. Nesse sentido, percebe-se que a relação médico-paciente é caracterizada por um relevante grau de confiança. Caso os dados sensíveis do prontuário do paciente passem a circular e a lhe causar danos em potencial, a sua expectativa de confiança e de sigilo é violada, iniciando-se um ciclo de desconfiança que tende a incentivar atitudes prejudiciais do paciente, como por exemplo, de não mais relatar com detalhes os seus sintomas ou buscar formas alternativas de tratamento.

Dentre diversos assuntos preocupantes relativos à privacidade médica, um dos mais sensíveis é certamente o de armazenamento e circulação de dados genéticos do paciente. Isso porque, embora esses dados sejam visados por empresas de seguro de vida, a sua circulação na sociedade pode acarretar graves danos a seu titular.

Não é fácil definir o conceito de dados genéticos. Esses são considerados os dados oriundos de testes e análises genéticas, mas também podem compreender informações sobre o histórico familiar e eventualmente informações sobre o grupo étnico do paciente. De toda forma, os dados genéticos são sempre informações baseadas na probabilidade, o que significa que a constatação de uma propensão genética a uma determinada doença não significa que ela realmente ira se manifestar no paciente, nem em que período isso ocorrerá.

A partir desse contexto, e sob o ponto de vista de que os dados genéticos podem embasar decisões discriminatórias e prejudiciais ao paciente, entende-se ser necessário assegurar padrões altos de sigilo e proteção para esse tipo de dado. Ademais, pode-se inferir que a falta de proteção adequada desses dados, no contexto de planos e seguros de saúde,

[128] ALPERT, Sheri. Protecting medical privacy: challenges in the age of genetic information. In: *Journal of Social Issues.* Vol. 59. No. 2, 2003, p. 301.

levará à contraditória conclusão de que somente terão direito ao seguro aqueles que não precisam, enquanto os que precisam ficarão excluídos desse acesso.

Desse modo, entende-se que a proteção dos dados genéticos é essencial não apenas para a proteção dos direitos fundamentais do indivíduo, como também de grupos sociais e étnicos, na medida em que o conceito de privacidade pode ultrapassar a esfera do indivíduo, abrangendo também interesses coletivos. Portanto, é fundamental que a legislação assegure a proteção e o sigilo dos dados genéticos, vez que a sua circulação pode gerar uma fonte de informações inconclusivas e discriminatórias.

No Brasil, o sigilo médico é protegido, além da Constituição Federal, em seu art. 5º, X, também pelo Código de Ética Médica, aprovado pela Resolução de Conselho Federal de Medicina nº 1.246/88, que determina, entre outros: i) a vedação ao médico de revelar fato que tenha conhecimento em virtude da profissão; ii) vedação de facilitar o manuseio do prontuário do paciente e de outras observações a terceiros; iii) obrigação do médico de conceder acesso ao paciente de seu prontuário e demais informações médicas e iv) a vedação de encaminhamento do prontuário e demais dados sem o expresso consentimento do paciente.[129] Ademais, a revelação de sigilo profissional é tipificado como crime com base no art. 159 do Código Penal.

Como visto, a problemática sobre a privacidade dos dados genéticos é bastante complexa, havendo diversas questões que ainda não foram totalmente solucionadas, como: será que a privacidade abrange o círculo da família? Se os testes genéticos envolvem

[129] A Resolução da Agencia Nacional de Saúde Suplementar (ANS) nº 153/07, que instituiu a Troca de Informações de Saúde Suplementar (TISS), suscitou a temática da violação do sigilo dos dados Por meio dessa Resolução, a ANS determinou a implantação de um novo sistema que permitirá aos planos de saúde o acesso a dados sigilosos dos pacientes que sejam a estes credenciados, a partir da padronização do modelo de guias de consultas e exames. Segundo a norma, os médicos deverão inserir, na nova guia, além dos rotineiros e usuais dados do paciente e dos exames necessários ao diagnóstico (ou ao seu aperfeiçoamento) – imprescindível para a determinação do tratamento e busca da cura, também o tipo de doença acometida, que, burocraticamente, vem traduzido pelo código CID (Classificação Internacional de Doenças). Consoante a ANS, o objetivo desta nova metodologia seria nortear o intercâmbio de dados entre os planos de saúde e os prestadores de serviços, ensejando a melhora na qualidade de gestão, além de propiciar a coleta de dados epidemiológicos, importantes para a definição e planejamento de políticas de saúde. Certamente, haverá ainda grande polêmica sobre o assunto.

diretamente outros membros da família, quando os resultados dos testes forem conhecidos, a quem pertencem? Ao indivíduo? Ao indivíduo e ao cônjuge? A toda a família? Mesmo estando em risco de desenvolver no futuro uma doença genética, não deveria ser possível obter um seguro de vida ou um empréstimo bancário a um custo aceitável? E se a longo prazo for descoberta uma cura? Seria aceitável penalizar a pessoa antes disso? Não temos todos o direito a igual nível de proteção?

"Listas negras" de trabalhadores

No ambiente de trabalho, que é um contexto sujeito a inúmeras discriminações, o processamento e o fluxo de dados pessoais devem ser restringidos sempre que violarem o direito à privacidade, à liberdade e à igualdade do trabalhador. Exemplo disso são as listas negras, que constituem registros criados pelos empregadores para agregar o nome dos trabalhadores que acionaram a Justiça do Trabalho, serviram como testemunhas ou que por qualquer outro motivo não sejam bem vistos por algumas empresas.

Tais listas, que são utilizadas com a finalidade de dificultar o acesso ao mercado de trabalho das pessoas cujo nome estava registrado, têm um caráter discriminatório evidente, uma vez que visam impedir o trabalhador de obter um emprego pelo simples fato de ter exercido o seu direito constitucional à ação.[130] Nesse sentido, tem sido reconhecido reiteradamente pelo Tribunal Superior do Trabalho o direito à indenização por dano moral em razão de inserção do nome do trabalhador em "listas negras"[131].

[130] Anteriormente, havia maior facilidade de elaboração das "listas negras", tendo em vista que a Justiça do Trabalho possibilitava a pesquisa de processos a partir dos nomes dos trabalhadores. Desde que essa pesquisa foi proibida, tem havido diminuição na quantidade dessas listas.

[131] Ementa: RECURSO DE REVISTA. DANO MORAL. -LISTAS NEGRAS-. OFENSA AO PRINCÍPIO QUE PROTEGE A DIGNIDADE DA PESSOA HUMANA (ARTIGO 1º, INCISO III, DA CONSTITUIÇÃO FEDERAL). PROVIMENTO. A inclusão dos nomes de Empregados nas chamadas -listas negras-, por si só enseja o pagamento de indenização por dano moral, tendo em vista que a prática constitui ofensa ao princípio constitucional que protege a dignidade da pessoa humana (artigo 1º, inciso III, da Constituição Federal), ainda que não haja comprovação no sentido de ter o Autor sofrido prejuízo concreto, no que se refere à conquista de nova colocação no mercado de trabalho. Recurso conhecido e provido para que sejam restabelecidos os comandos da sentença quanto ao deferimento da indenização por dano moral requerida. (Processo: RR -

Listas de suspeitos

Outro caso que pode ser enquadrado no tratamento sensível de dados é a divulgação de lista de suspeitos de criminosos. Um caso emblemático ocorreu em novembro de 2002, quando agentes do FBI confirmaram, em declarações à imprensa, que uma lista de nomes, preparada logo após os atentados de 11 de setembro, foi reproduzida em páginas da internet e distribuída para os mais diversos atores, públicos e privados, uma vez que teria fugida ao controle.[132] Ocorre, no entanto, que a lista, ao invés de conter nomes de suspeitos de ação terrorista, continha o nome de pessoas que foram procuradas, logo após os atentados, para fornecer informações aos órgãos de investigação. Essa lista revela-se nitidamente ilegal, por lesar a privacidade e a dignidade das pessoas cujos nomes constavam na lista, sem jamais ter tido qualquer relação com o evento terrorista.

325/2004-091-09-00.7 Data de Julgamento: 02/04/2008, Relatora Ministra: Maria de Assis Calsing, 4ª Turma, Data de Publicação: DJ 18/04/2008.)

Ementa: RECURSO DE REVISTA. DANO MORAL. -LISTAS NEGRAS-. OFENSA AO PRINCÍPIO QUE PROTEGE A DIGNIDADE DA PESSOA HUMANA (ARTIGO 1º, INCISO III, DA CONSTITUIÇÃO FEDERAL). PROVIMENTO. A inclusão dos nomes de Empregados nas chamadas -listas negras-, por si só enseja o pagamento de indenização por dano moral, tendo em vista que a prática constitui ofensa ao princípio constitucional que protege a dignidade da pessoa humana (artigo 1º, inciso III, da Constituição Federal), ainda que não haja comprovação no sentido de ter o Autor sofrido prejuízo concreto, no que se refere à conquista de nova colocação no mercado de trabalho. Recurso conhecido e provido para que sejam restabelecidos os comandos da sentença quanto ao deferimento da indenização por dano moral requerida. (Processo: RR - 532/2003-091-09-00.0 Data de Julgamento: 02/04/2008, Relatora Ministra: Maria de Assis Calsing, 4ª Turma, Data de Publicação: DJ 18/04/2008.)

[132] PINTO, Cristiano. *A reação norte-americana aos atentados de 11 de setembro de 2001 e seu impacto no constitucionalismo contemporâneo: um estudo a partir da teoria da diferenciação do direito.* Tese defendida na Faculdade de Direito da Universidade Federal de Minas Gerais, inédita, p. 239.

2.

INFORMAÇÃO PESSOAL E TECNOLOGIA NAS RELAÇÕES DE CONSUMO

2.1. Dados pessoais e tutela jurídica: conceitos e dimensões

A importância da tutela jurídica dos dados pessoais reside no fato de que esses dados, assim como as demais informações extraídas a partir deles, podem se constituir em uma representação virtual da pessoa perante a sociedade. Os organismos sociais, tanto estatais quanto privados, conhecem os indivíduos por meio de uma seqüência de códigos e números computadorizados, situação que poderia se adequar à afirmação de Vladimir Medem, desde que atualizada, segundo a qual "Um indivíduo na Rússia era composto por três partes: corpo, alma e passaporte"[133]. Tal afirmação ajuda a demonstrar como os dados pessoais passam a ser constituintes da própria personalidade do indivíduo, dada a sua importância para a representação das pessoas na sociedade complexa contemporânea.

Por diversas razões, tais como a ampliação da complexidade do sistema industrial, a burocratização dos setores público e privado e a transformação das ciências sociais, o certo é que nos tornamos a sociedade que mais gerou dados pessoais na história da humanidade, o que pode ser demonstrado pelas dezenas de bancos de dados nos mais variados setores: registros de nascimento e casamento, registros escolares, dados do censo, registros militares,

[133] MEDEM, Vladimir apud LYON, David. *The Electronic Eye*. Minneapolis: Minnesota Press, 1994, p. 3.

dados de passaporte, registros de empregados e de servidores públicos, registros do serviço de saúde, registros da defesa civil, registros de seguros, registros financeiros, registros de dados telefônicos, dentre outros[134].

Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade. Sob essa perspectiva, faz-se necessário compreender o conceito jurídico de "dado" e "informação". Muito embora ambos sejam utilizados na maioria das vezes de forma idêntica, pode ser útil distinguir o seu significado.

Segundo Raymond Wacks, "dado" pode ser compreendido como a informação em potencial, isto é, ele pode se transformar em informação se for comunicado, recebido e compreendido[135]. De acordo com o autor, "se o 'dado' assume a forma de uma palavra impressa ele é imediatamente compreendido como informação pelo leitor. Se, no entanto, o dado consiste em atos ou sinas que requeiram a interpretação antes de adquirirem qualquer sentido, ele permanece no estado de pré-informação até poder ser efetivamente compreendido por alguém"[136]. A informação pode apresentar-se em diversas formas, como a gráfica, fotográfica e acústica[137]. Apesar dessa diferença sutil de significados, sabe-se que geralmente a doutrina, ao utilizar esses vocábulos, não realiza ta distinção.

Com relação ao conceito de dados pessoais, pode-se dizer que são os fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável[138]. Nesse sentido, cabe mencionar a definição presente na Diretiva Européia 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao

---

[134] WESTIN, Alan. *Privacy and Freedom.* Nova York: Atheneum, 1970, p. 158 e 159.

[135] WACKS, Raymond. *Personal Information: Privacy and the Law.* Oxford, Clarendon Press, 1989, p. 25.

[136] Idem, Ibidem, p. 25, tradução livre.

[137] MALTA, Tatiana. *O Direito à Privacidade na Sociedade da Informação.* Op. Cit., p. 252.

[138] Seção 3, (1), da Lei de Proteção de dados da Alemanha, de 15 de novembro de 2006 (Bundesdatenschutzgesetz – BDSG). Vale mencionar também a definição de Wacks: "'Personal information' consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation (WACKS, Raymond. *Personal Information.* Op. Cit., p. 26).

tratamento de dados pessoais e à livre circulação desses dados. De acordo com o seu art. 2º, dados pessoais constituem "qualquer informação relativa a uma pessoa singular identificado ou identificável". O dispositivo prescreve que "é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

A informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por revelar aspectos que lhe dizem respeito[139]. Desse modo, resta claro que tais informações merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade[140]. Fundamental é esclarecer que, na realidade, tal tutela visa à proteção da pessoa e de sua personalidade e não dos dados *per se*[141].

É possível também que os dados se refiram a pessoas indeterminadas. Nessa hipótese, são considerados dados anônimos e podem ser utilizados para fins estatísticos. O anonimato dos dados é uma forma de proteger a pessoa que teve os seus dados coletados e armazenados. Nesse sentido, vale mencionar a decisão da Corte Constitucional alemã de 15 de dezembro de 1983, ao julgar a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho", em que se determinou que os dados pessoais coletados para o censo somente poderiam ser transferidos a outros órgão da Administração Pública se fossem tornados anônimos ou após o seu processamento estatístico:

> Uma eventual transmissão (entrega) dos dados que não sejam anônimos nem tenham sido processados estatisticamente – portanto, que sejam ainda pessoais – encerra problemas especiais. Os levantamentos de dados para fins estatísticos abrangem também dados individualizados de cada cidadão, que não são necessários para os fins estatísticos e que (...) servem apenas como auxiliares no processo de pesquisa. Todos esses dados podem até ser transmitidos a terceiros por força de expressa autorização legal, se e na medida em que isso aconteça para o processamento estatístico por parte de outras autoridades, e para que as medidas prescritas em prol da proteção do direito e personalidade, principalmente **o sigilo estatístico e o princípio do anonimato**

[139] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Op. Cit., p.157.

[140] CATALA, Pierre, *apud* DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Op. Cit., p.157.

[141] ARGENTINA: Protección de Datos Personales. Op. Cit., p. 121.

> sejam, tão logo possível, garantidas de maneira confiável, tanto na organização e procedimento quanto nos órgãos estatísticos federais e estaduais. A transmissão a terceiros dos dados levantados para fins estatísticos, não anônimos nem processados estatisticamente para fins de execução administrativa, pode, ao contrário, intervir de forma inadmissível o direito de autodeterminação sobre a informação.[142] (BVERGE 65, 1, Volkszählung - grifo nosso)

De modo semelhante, a Lei de Proteção de dados da Alemanha, de 15 de novembro de 2006 (Bundesdatenschutzgesetz – BDSG), estabeleceu o princípio pelo qual o processamento de dados pessoais deve ocorrer de forma a utilizar o mínimo possível de dados e, principalmente, buscando sempre conferir a tais dados o caráter de anônimos ou de pseudônimos[143]. O mesmo preceito foi estabelecido pela Diretiva Européia 2002/58/CE, em seu art. 6º, I.

Deve-se ressaltar que após adquirirem a característica de anônimos, os dados não estão mais sujeitos à disciplina da proteção de dados pessoais, se tiverem sido tratados de modo a impossibilitar toda e qualquer identificação pessoal. Isso porque a tutela jurídica abrange apenas aqueles dados que se refiram à pessoa identificada ou identificável[144].

Utiliza-se a expressão "Tratamento de dados pessoais" para designar as operações técnicas que podem ser efetuadas sobre os dados pessoais, de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa ou útil. São formas de

---

[142] MARTINS, Leonardo. (org.) *Cinqüenta anos de Jurisprudência doTribunal Constitucional federal Alemão.* Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.

[143] Section 3.

(6) "Rendering anonymous" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch einKennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Section 3a. Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.

[144] Ver preâmbulo, da Diretiva Européia 95/46/CE, segundo o qual não se aplica o regime de proteção de dados pessoais aos dados anônimos, já que não possibilitam a identificação da pessoa: "Preâmbulo (...) 26) É o que prevê o "Considerando" no. 26, da Diretiva Européia 95/46/CE, segundo o qual "os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável;" No mesmo sentido, ORTIZ, Ana Isabel Herrán. La Violación de la Intimidad en la Protección de Dados Personales. Madri: Dykinson, 1999, p. 223.

tratamento definidas pela Diretiva Européia 95/46/CE, a coleta, o registro, a organização, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, o apagamento ou a destruição.

Assim, o tratamento de dados pessoais tem um viés marcadamente dinâmico, pois consiste na ação de manejar a informação, relacionando e reelaborando dados, com intuito de se obterem conclusões a partir da aplicação de critérios[145].

Para que o tratamento de dados pessoais atinja a sua finalidade, os dados geralmente são organizados na forma de "banco de dados". Este se caracteriza por ser um conjunto organizado e lógico de dados, de fácil utilização e acesso. Conforme definição da Diretiva Européia 95/46/CE, banco de dados constitui "qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico".

Os bancos de dados podem ser manuais, na forma de dossiês e fichários organizados, ou automatizados. Embora ambos apresentem riscos à violação da privacidade do individuo, não se pode negar que a maior ameaça reside naturalmente na informatização do tratamento dos dados pessoais. Nesse sentido, é clara a sentença do Tribunal Constitucional alemão ao afirmar que o poder de autodeterminação do individuo em relação ao livre desenvolvimento da personalidade encontra-se ameaçado frente às inúmeras possibilidades de processamento dos dados pessoais pelos meios automatizados:

> Esse poder necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Ele está ameaçado, sobretudo, porque em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostos manualmente. Hoje, com a ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (...) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distancia e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa

[145] Idem, Ibidem, p. 214.

> controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação publica em suas informações privadas (BVERGE 65, 1, Volkszählung)[146].

Desse modo, percebe-se que a informatização dos meios para o tratamento de dados pessoais afetou o direito à privacidade do individuo principalmente por duas razões: i) ao ampliar a possibilidade de armazenamento, tornando-a praticamente ilimitada; ii) ao possibilitar a obtenção de novos elementos informativos por meio da combinação de dados em estado bruto, a princípio, desprovidos de importância, a partir da utilização de novas técnicas, tais como o "*profiling*", "*data mining*", "*data warehousing*", "*scoring-system*", dentre outros, conforme se explicará com detalhes no item 2.2.2..

Como visto no capítulo 1, a figura do "banco de dados" esteve no centro das discussões iniciais sobre a proteção de dados pessoais, como nos casos do *National Data Center*, nos EUA, e Safári, na França, nos quais havia o temor da população em relação à construção de um banco de dados nacional, gigante e centralizado. Posteriormente, esse cenário sofreu alterações, em razão do desenvolvimento de avançada tecnologia da informação, que deslocou o foco dos riscos à personalidade dos grandes bancos de dados centralizados pelos governos para as infinitas formas descentralizadas de tratamento de dados pessoais e pelas redes que permitem o envio em tempo real de informação. Assim, o tema da proteção de dados deixa de se preocupar prioritariamente com os bancos de dados para abordar as dinâmicas formas de tratamento de dados pessoais e, principalmente, os direitos dos cidadãos cujos dados são processados[147].

Conforme afirma Mayer-Schönberger, de forma bastante curiosa, a ameaça se transformou: se antes a violação da privacidade residia na centralização das informações em

[146] MARTINS, Leonardo. (org.) *Cinqüenta anos de Jurisprudência doTribunal Constitucional federal Alemão.* Montevidéu: Fundação Konrad Adenauer, 2005, p. 237.

[147] Mayer-Schönberger, Generational Development of Data Protection in Europe. Op. Cit., p. 225.

um colossal banco de dados, ela se transmuta em exatamente seu oposto: torna-se uma "constelação vasta e indistinta" de redes de tratamento de dados pessoais, composta por milhares de unidades de processamento de dados, com grande capacidade de interconexão, ampliando os riscos de ofensa à privacidade dos cidadãos[148].

2.2. A utilização dos dados pessoais nas relações de consumo

Em razão de modificações sociais e da evolução tecnológica, a discussão sobre os danos causados pelo processamento e fluxo de dados na sociedade não se restringe mais à ameaça do enorme poder do Estado, expresso na figura do "Big Brother" de Orwell, mas abrange hoje também o setor privado, que utiliza massivamente dados pessoais para atingir os seus objetivos econômicos. Assim, a ameaça passa a ser representada pelos "pequenos irmãos"[149], isto é, pelas milhares de empresas que coletam, armazenam e processam dados de seus clientes, consumidores finais ou não. Conforme afirma Hassemer: "o Estado ainda aparece em algumas áreas... em outras, o tema se desloca para distintos demônios, que são muito piores que ele: por meio de uma potente tecnologia da informação nas mãos de qualquer um, essa força se desloca (...) de forma ágil, oculta, voraz e por toda a Terra, coletando, classificando, repreendendo, reunindo, comercializando e utilizando dados pessoais."[150]

Vivemos em uma economia da informação pessoal desde a década de 70, na qual a informação constitui-se como a fonte motriz. Tal fenômeno ultrapassa as áreas de proteção ao crédito e marketing direto, pois atualmente grandes empresas de varejo tomam as suas

[148] "The image of a monolitic Big Brother who could be fairly easily regulated through stringent technology-based procedures gave way to a broad, blurry picture of a constellation of distinctive and novel potential data-protection offenders. This led to a shift in the data-protection discussion". (Mayer-Schönberger, Generational Development of Data Protection in Europe. In: Technology and Privacy: The New Landscape. The MIT Press: Massachusetts, 2001, p. 225).

[149] BUCHNER, Benedikt. *Informationelle Sebstbestimmung in Privatrecht*. Op. cit., p. 26.

[150] HASSEMER, Winfried. "Datenschutz: Die Aufgaben der nächsten Jahre." *Apud* BUCHNER, Benedikt. *Informationelle Sebstbestimmung in Privatrecht*. Op. cit., p. 26 (tradução livre).

decisões de investimento referentes a estratégias, produtos e locação de pontos de venda baseadas em refinadas análises a respeito da renda, preferências e comportamento.dos seus clientes.[151] Assim, diversamente das pesquisas no Brasil que estudam a temática dos dados pessoais sob o foco a proteção ao crédito, este trabalho visa ampliar o foco de análise e demonstrar que a problemática é mais vasta e complexa, abrangendo diversos setores da economia[152], na medida em que os dados pessoais constituem-se em condição *sine qua non* para essa nova configuração econômica.

A utilização de dados pessoais pelo setor privado não é uma novidade, remontando ao século XIX. Nesse período, sabe-se que as instituições financeiras já faziam uso da estratégia de coletar e armazenar informações sobre os seus clientes, de forma manual, para controlar riscos e minimizar custos.

No início do século XX, em 1920, sabe-se que informações dos consumidores foram utilizadas para a realização de marketing direto, pela General Motors, a partir da constatação de que os consumidores que adquiriam um Ford não compravam outro Ford como o seu próximo veículo. Para buscar fidelizar os seus clientes, a empresa passou a encaminhar aos proprietários de um Ford com dois anos de uso, publicidade a respeito da marca.[153]

Alan Westin, no relatório de sua pesquisa sobre bancos de dados computadorizados, realizada de 1970 a 1972, estudou e visitou quatro ramos empresariais que utilizavam bancos de dados para os seus negócios (bancos, empresas de seguro, de proteção ao crédito e de marketing direto), com a finalidade de compreender o impacto da informatização sobre as atividades de processamento de dados pessoais. [154] Com essa pesquisa, Westin foi capaz de

---

[151] 6, Perry. The Personal Information economy: trends and prospects for consumers. In: LACE, Susane. The *Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005, p. 17.

[152] Por exemplo: empresas de telefone, bancos, financeiras, associações de empregadores, sindicatos de trabalhadores, empresas de transporte, diversas empresas varejistas, armazéns, farmácias, empresas de marketing direto, serviços e proteção ao crédito, companhias de seguro, profissionais liberais, como advogados e psicólogos, agências de viagem, organizações de caridade, hotéis.

[153] SOLOVE, Daniel. *The Digital Person.* Op. Cit., p. 16.

[154] WESTIN, Alan. *Databanks in a Free Society: Computers, Record-keeping and Privacy. A Project of the Computer Science & Engineering Board National Academy of Sciences.* Nova York: Quadrangle/ The New York Times Book Company, 1972, p.

mostrar que esses setores informatizaram as suas bases de dados, a partir da década de 50, mas que já utilizavam a coleta e o processamento manual de dados pessoais antes mesmo do fenômeno da informatização, tendo sido essa atividade incrementada com a informática.

2.2.1. Economia com especialização flexível

Pode-se dizer que é a partir da década de 70 que o processamento de dados pessoais pelo setor privado adquire a importância e visibilidade na sociedade da forma que acontece atualmente. Tal fenômeno pode ser explicado com a transformação da economia de produção em massa em uma economia com estratégia de especialização flexível, que se caracteriza pela diversificação da produção para diferentes produtos e diferentes clientes. [155] Esta nova configuração econômica, que se desenvolve a partir da década de 70, surge em razão da internacionalização do mercado de produtos, da introdução de novas tecnologias de produção e informação, bem como em razão de novas técnicas de gerenciamento.

A denominação para essa economia emergente varia entre os autores, embora as características atribuídas sejam as mesmas. Perry 6 utiliza a expressão "economia da informação pessoal"[156]. Rohan Samarajiva utiliza o termo "economia de massa customizada" - *mass customization model*[157]. Ronaldo Porto Macedo e David Lyon utilizam o termo "economia de produção flexível"[158]. Neste trabalho utilizaremos essas expressões para nos

[155] MACEDO Jr, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor*. 2ª. Ed. São Paulo: Editora Revista dos Tribunais, 2006, p. 103. O autor demonstra como o surgimento de uma economia voltada para a flexibilidade da produção propicia a transformação do direito contratual neoclássico em uma teoria dos contratos relacionais. Para fins didáticos, o autor distingue em três tipos de produção: a produção manufatureira (1840-1890), a produção de massa (1890-1975) e a especialização flexível (a partir de 1975). Naturalmente, embora cada um desses tipos de produção tenha predominado em determinado período, isso não significa que eles não coexistiram. Pelo contrário, sabe-se que até hoje os três tipos de produção podem existir concomitantemente no mesmo espaço.

[156] 6, Perry. The Personal Information economy: trends and prospects for consumers. In: LACE, Susane. The *Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005, p. 17.

[157] SAMARAJIVA. Rohan. "Interactivity as though privacy mattered." In: *Technology and Privacy: the New Landscape*, Op. Cit., p. 277.

[158] LYON, David. *The Electronic Eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 1994.

referirmos ao mesmo fenômeno, isto é, à nova forma econômica flexível, especializada e diversificada, que emerge a partir da década de 70.

Enquanto a economia de produção de massa consistiu em uma estratégia de fornecer grandes quantidades de bens padronizados por baixos custos, o modelo econômico baseado na individualização e flexibilização em massa caracteriza-se pela oferta de volumes menores de produtos especializados, singularizados e altamente qualificados, em função do mercado e do consumidor.

O modo de produção de massa mostrou-se instável diante de variações abruptas do mercado, pois, em razão do grande investimento inicial necessário, quaisquer interrupções ou diminuições bruscas na produção poderiam causar grande prejuízo. O modelo flexível, por outro lado, mesmo em contextos instáveis, permite a manutenção do nicho produtivo, a adaptabilidade às demandas e às variações do mercado e a utilização plena da linha de produção implantada, em razão de sua produção flexível. Como afirma Ronaldo Porto Macedo Jr.:

> A estratégia de especialização flexível visa fundamentalmente obter vantagens de mercado, oferecendo um produto com tecnologia única, qualidade única ou apoiada por serviço único. A oferta de um bem único permite a criação de um nicho, o que, por sua vez, permite a manutenção de alto grau de lucratividade e estabilidade comercial. Isto, entretanto, requer a constante mudança do produto, a combinação de inovação com formas flexíveis de produção.[159]

Nesse sentido, o modelo flexível de economia apresenta uma tendência à "customização". Tal expressão, que constitui um anglicismo, denota a flexibilidade e a suscetibilidade desse modelo de produção de fornecer bens e serviços com uma variedade suficiente para criar e fidelizar diferentes segmentos de consumidores.[160] Assim, a tendência é de se fornecerem cada vez mais complexos integrados de bens e serviços, voltados para a criação de nichos distintos de consumidores.

---

[159] Idem, Ibidem, p. 103.
[160] SAMARAJIVA. Rohan. "Interactivity as though privacy mattered." In: *Technology and Privacy: the New Landscape*, Op. Cit., p. 278.

Diferentemente da produção de massa, o modelo flexível compreende que as empresas devem investir na diferenciação dos produtos e serviços para adquirir vantagens competitivas e aumentar a lucratividade. Por conseqüência, tal concepção de produção exige uma alteração também da forma de realização do marketing. Afinal, o marketing de massa convinha para uma produção em massa. Já uma produção diferenciada e segmentada pressupõe igualmente um marketing diferenciado e segmentado.

As principais diferenças entre o marketing de massa e o marketing individualizado e, por conseqüência, entre a economia de massa e a economia de produção flexível, podem ser observadas de forma clara no quadro abaixo[161]:

Marketing de massa	**Marketing individualizado**
Consumidor médio	Consumidor individual
Consumidor anônimo	Consumidor com perfil armazenado
Produto padronizado	Produto individualizado
Produção massificada	Prestação de serviços personificada/singularizada
Propaganda massificada	Comunicação individual
Fomento da venda massificada	Estímulos pessoais
Comunicação de uma via só	Comunicação por várias vias
Economias de Escala (redução dos custos por meio da produção massificada)	Economia flexível
Fatia de mercado	Fatia de Consumidores (*share of customer*)
Todos os consumidores	Consumidores que podem gerar lucros
Atração de consumidores	Fidelização de clientes

2.2.2. A tecnologia e o tratamento de dados pessoais dos consumidores

Para se atingir tanto a diferenciação da produção, quanto a diferenciação do marketing, faz-se necessária a coleta massiva de informações sobre os consumidores, seus hábitos e comportamentos. Assim, as empresas adquirem a capacidade de ofertar produtos

[161] SCHWENKE, Mathias. *Individualierung und Datenschutz*. Wiesbaden: Deutscher Universitäts-Verlag, 2006, p. 44 (tradução livre).

especializados, singularizados e altamente qualificados, em função do mercado e do consumidor, bem como de direcionar-lhe a sua publicidade.

Essa coleta imensa de informações sobre o mercado e os consumidores passou a ser possível com o desenvolvimento de tecnologias de informação e comunicação. Tais tecnologias permitem não apenas o armazenamento de todas essas informações em bancos de dados de consumo, como também possibilitam o refinamento desses dados e a sua rápida circulação na sociedade.

Nesse sentido, observa-se que existe uma convergência entre a sociedade da informação e a sociedade contemporânea de consumo[162], na medida em que a economia passa a exigir, para o seu complexo funcionamento, uma quantidade enorme de dados pessoais, possíveis de serem armazenados, processados e transmitidos por meio da tecnologia da informação.

Pode-se dizer que o tratamento de dados pessoais pelas empresas privadas objetiva atingir, principalmente, as seguintes finalidades no mercado: i) previsibilidade e diminuição de riscos, ii) interação com o consumidor (p.ex. marketing direto), iii) diferenciação de produtos e iv) diferenciação de serviços.[163]

Em uma economia de produção flexível, no contexto de uma sociedade de risco, a vigilância sobre os consumidores e a captação de seus dados pessoais constitui-se em uma forma de gerenciar riscos e distribuí-los socialmente, acarretando um ciclo ininterrupto de obtenção de informações, que gera mais insegurança e a necessidade de vigilância, conforme afirma Priscilla Regan:

> Em uma sociedade de risco, qualquer instituição que lida com um indivíduo coleta informações desse indivíduo e sobre as suas atividades. (...) A sociedade de risco requer a vigilância como forma de gerenciar o risco. Mas a vigilância gera uma insaciável sede de mais e mais informações sobre riscos que existem e que são gerados pelos indivíduos em particular. O conhecimento gerado pelo sistema de

[162] Ressalta-se que aqui não estamos nos referindo ao conceito sociológico de "sociedade de consumo", desenvolvido por Jean Baudrillard, mas ao sentido mais corriqueiro da expressão.
[163] SCHWENKE, Mathias. *Individualierung und Datenschutz*. Wiesbaden: Deutscher Universitäts-Verlag, 2006, p. 58.

> vigilância não gera uma sensação de segurança e de confiança, mas produz, ao invés, novas incertezas, acarretando mais vigilância e coleta de informações.[164]

A economia customizada exige, para a obtenção de vantagens no mercado, que a comunicação da empresa se individualize, criando e fidelizando nichos de consumo. Nessa perspectiva, a interação direta com o consumidor e a segmentação do marketing passam a ser bastante valorizadas, ganhando relevo a concepção do marketing "one-to-one". Esse conceito foi desenvolvido pelos americanos Pepper e Roger, que propagaram a necessidade de utilização de bancos de dados de consumidores e de meios interativos para oferecer ao consumidor o máximo de produtos e serviços possíveis, em substituição à antiga máxima de oferecer o mesmo produto à maior quantidade de clientes possíveis.[165] O marketing "one-to-one" insere-se em uma estratégia mais ampla de relacionamento entre a empresa e o cliente, conhecida como *customer relation management – CRM* (gerenciamento da relação com o cliente).

Por fim, na economia customizada, a obtenção de informações sobre os consumidores é pressuposto para a adaptação e diversificação dos produtos e serviços para diferentes segmentos de clientes. Assim, a oferta de volumes menores de produtos especializados, altamente qualificados e segmentados permite a manutenção de alto grau de lucratividade e estabilidade comercial.

2.2.3. O imperativo de vigilância: o consumidor de vidro

Ao constatar-se a relação inerente entre a economia de produção flexível e a coleta de dados dos consumidores, cabe examinar também os seus efeitos.

---

[164] REGAN, Priscilla M. (2002) 'Privacy as a Common Good in the Digital World', In: *Information, Communication & Society*, 5:3, p. 387 (tradução livre).
[165] SCHWENKE, Matthias. *Individualisierung und Datenschutz.*Wiesbaden: Deutscher Universitäts-Verlag 2006, p. 42.

Como visto, a estratégia de especialização flexível exige a formação de distintos públicos para a comunicação do marketing, a fidelização do cliente e a diversificação da produção. Isso somente é possível com o armazenamento e processamento de grande quantidade de informação quase cotidiana dos consumidores e de seus hábitos de consumo, por meio da mais moderna tecnologia da informação. Percebe-se, assim, que a informação transformou-se em insumo da produção, possuindo um papel tão importante quanto a força de trabalho e o capital. A partir dessa constatação, pode-se concluir que existe na economia atual um imperativo de vigilância dos consumidores, conforme afirma Samarajiva:

> Marketing efetivo para um grande número de consumidores dispersos no espaço requer a habilidade de diferenciar o consumidor em perspectiva e de formar distintas audiências para as mensagens de marketing; para alcançar essas audiências com diferentes mensagens persuasivas sobre bens, serviços e compactos; (...). Mais do que no passado, a lealdade do cliente tem de ser preservada, porque a movimentação do cliente (entrada e saída) aumenta os custos do marketing. Todas essas ações requerem a utilização de tecnologias da informação. (...) Em suma, a customização da massa exige a vigilância em relação ao espaço disperso, mercados com alvos dinâmicos e a construção de relações com os clientes. Produção customizada relaciona-se ao marketing customizado, que, por sua vez, relaciona-se à vigilância do cliente. Esse é o imperativo da vigilância.[166] (grifo nosso)

Antigamente, o termo vigilância era utilizado para se referir a fenômenos específicos de controle, relacionados a investigações policiais e a serviços de inteligência governamentais. Atualmente, com o enorme processamento de dados pessoais pelas empresas para a análise detalhada e tomada de decisão, a vigilância tornou-se uma característica do cotidiano na sociedade contemporânea. Os mais diversos tipos de entidades realizam a vigilância de cidadãos, consumidores e empregados no dia-a-dia. A conseqüência disso é a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços, de modo a afetar significativamente as suas chance de vida.

Sob essa perspectiva, ficam nítidos os riscos aos quais os consumidores e a sociedade democrática estão submetidos. Afinal, se por um lado, há um ganho para as empresas em

[166] Idem, Ibidem, p. 279 (tradução livre).

termos de custos e de diminuição de concorrência, por outro, há uma ameaça patente à liberdade e à igualdade do sujeito consumidor, bem como do equilíbrio do mercado de consumo como um todo, se o fluxo de dados pessoais for utilizado para limitar indevidamente o acesso dos consumidores a bens e serviços ou para selecioná-los e classificá-los de forma discriminatória.

Entende-se que esses riscos podem ser compreendidos sob a perspectiva da violação da igualdade e da liberdade do cidadão-consumidor.[167] O risco de ter reduzida a sua liberdade ocorre na medida em que a vigilância de todos os seus comportamentos pelas empresas enseja a perda de controle sobre as suas informações que circulam na sociedade e gera uma pressão causada pela participação social em informações privadas. Ademais, se o consumidor não consegue determinar quais informações sobre si são conhecidas na sociedade e podem ser utilizadas para a tomada de decisões que influenciem a sua vida, ele terá a sua capacidade de autodeterminação reduzida. Afinal, nos termos de Philip Agre, "o controle da informação pessoal é o controle sobre o aspecto da identidade do seu próprio projeto de mundo, e o direito à privacidade é a liberdade de que a construção da própria identidade não sofrerá coação injustamente."[168]

Segundo, o consumidor está sujeito ao risco de ter reduzido o seu direito à igualdade, caso tenha negado acesso a bens e serviços do mercado de consumo ou tenha as suas chances de vida diminuídas, em razão das informações armazenadas em bancos de dados e utilizadas de forma discriminatória.

Por conseqüência, o "imperativo da vigilância" imposto por esse modelo econômico afeta também a própria sociedade democrática como um todo, pois a vigilância, mesmo exercida pelo setor privado, enseja a inibição da expressão da individualidade e as aspirações a ela, da liberdade de escolha e da autodeterminação.

---

[167] Essa questão será mais aprofundada no tópico 3.4.
[168] AGRE, Philip. Introduction. In: AGRE, Philip e ROTENBERG, Marc (Ed). *Techonology and Privacy: The New Landscape*. Op. Cit., p. 7 (tradução livre).

Ao se analisarem esses riscos, é importante levar em consideração que eles estão distribuídos desigualmente na sociedade entre os diversos grupos sociais, pois isso depende do seu poder em relação aos serviços e produtos que deseja consumir, à sua habilidade de pleitear indenização e à sua relação com pessoas em situações semelhantes.[169] No entanto, é extremamente difícil quantificar a exposição dos consumidores a essas questões.

A economia emergente necessita, nesse contexto, da construção de relacionamentos, tanto na própria cadeia produtiva, como entre produtores e consumidores. Ocorre que relacionamentos exigem que cada parte tenha conhecimento sobre a outra, o que passa a ser possível a partir da moderna tecnologia da informação.[170] Naturalmente, aqui vale a crítica de que tal conhecimento é extremamente assimétrico: a empresa conhece o consumidor, mas esse não conhece a empresa. Ademais, há outro fator relevante: muitas vezes, esse conhecimento da empresa advém da coleta de dados do consumidor, sem sequer que ele saiba dessa coleta ou dê o seu consentimento para tanto.

A vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão "consumidor de vidro"[171] para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras burocracias privadas que tomam decisões e influenciam as suas chances de vida, a partir das informações pessoais armazenadas em bancos de dados.

Diversos são os atores que participam desse processo de coleta, tratamento e circulação de dados pessoais dos consumidores, podendo acarretar riscos à sua personalidade e privacidade. Uma interessante pesquisa publicada por Oscar Gandy Jr. identifica quais são os atores, que na opinião das empresas questionadas são os principais responsáveis pelo crescimento da importância do problema sobre a informação do consumidor. Conforme tabela

[169] Perry. The Personal Information economy: trends and prospects for consumers. Op. Cit., p. 22.
[170] SAMARAJIVA. Rohan. "Interactivity as though privacy mattered". Op. Cit., p. 279.
[171] LACE, Susane. The *Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005.

abaixo[172], pode-se perceber que em primeiro lugar estão os fornecedores de listas, isto é, as empresas que trabalham unicamente com a coleta, a compilação e a comercialização dos dados pessoais dos cidadãos. Em seguida, estão os responsáveis pelo telemarketing, as empresas não respeitáveis, os consumidores reclamantes, os órgãos reguladores fiscais, o Congresso, entre outros:

Atores vistos como sendo responsáveis pelo crescimento da importância da questão da informação pessoal do consumidor

Fornecedores de listas	62,6
Responsáveis pelo telemarketing	57,6
Empresas não respeitáveis	56,1
Consumidores que reclamam	54,0
Reguladores federais	48,9
Congresso	46,8
Legisladores estaduais	43,9
Competidores agressivos	23,0
Ativistas contra o comércio	27,3

Se, por um lado, a transformação da economia amplia a tendência de se intensificar o relacionamento entre empresa e cliente, por outro, a forma que se dará esse relacionamento ainda não está definida. Isso significa que cabe à sociedade e ao Estado determinar em que termos poderá se dar esse estreitamento entre empresas e clientes, se baseado na confiança, na proteção da privacidade e no consenso ou se será uma relação patológica, baseada na desconfiança, no temor e na coerção.[173]

Veremos ao longo desse capítulo quais as medidas, no âmbito estatal e privado, que podem ser tomadas para que essa relação entre empresa e consumidor seja estabelecida, respeitando os direitos fundamentais e os princípios da sociedade democrática.

2.3. Riscos oriundos do tratamento de dados pessoais nas relações de consumo

[172] GANDY, Oscar. *The Panoptic Sort. A Political Economy of Personal Information.* Boulder: Westview Press, 1993, p. 114 (tradução livre).

[173] SAMARAJIVA. Rohan. "Interactivity as though privacy mattered". Op. Cit., p. 300.

Sob a perspectiva de que o fluxo de dados pessoais constitui um imperativo de vigilância da nossa sociedade, é fundamental compreender-se o processo de tratamento de dados realizado pelas inúmeras empresas dos mais diversos setores econômicos, bem como analisar os riscos que ameaçam a personalidade do consumidor-cidadão. Assim, é fundamental entender-se o modo como é realizado tal tratamento para que se distingam as práticas legítimas das ilegítimas, visando à preservação dos direitos fundamentais e à consolidação de um mercado saudável e equilibrado.

O tratamento de dados pessoais, conforme visto no início deste capítulo, é um processo dinâmico, que compreende todas as operações técnicas que podem ser efetuadas sobre os dados pessoais, de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa ou útil. O tratamento abarca, portanto, a realização de inúmeras atividades, como a coleta, o registro, a organização, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, o apagamento ou a destruição.

Para fins didáticos, optou-se por estudar três momentos específicos no âmbito do tratamento de dados pessoais - a coleta, o processamento e a difusão de dados – visto que esses podem acarretar mais riscos à personalidade e à privacidade do consumidor. A legitimidade dos instrumentos de cada uma dessas fases será avaliada à luz dos princípios básicos de proteção de dados pessoais, já analisados no capítulo 2. Sempre que houver normas brasileiras, essas também serão utilizadas como parâmetro de análise.

O momento da coleta pode ser considerado a primeira fase do tratamento dos dados, no qual a empresa ou o controlador do banco de dados necessita obter as informações pessoais do consumidor, o que pode ser realizado a partir do próprio consumidor ou de outras fontes, como se verá em seguida. Nesse tópico, serão vistas as fontes nas quais se podem obter dados dos consumidores, bem como a legitimidade de cada uma delas.

O processamento de dados constitui a segunda fase do tratamento, na qual os dados são submetidos a diversas técnicas necessárias para lapidá-los e transformá-los em informações úteis para a empresa. Serão explicadas as principais técnicas utilizadas para processar dados pessoais, bem como os riscos que cada uma oferece aos direitos dos consumidores.

Por fim, será vista o terceiro momento de tratamento de dados, que corresponde à sua difusão ou cessão. Nesse tópico, será observado como essa difusão de dados ocorre e em que hipóteses ela pode ser tida como legítima.

2.3.1. Fontes, tipos e usos de dados pessoais

Na economia moderna, as empresas não têm a possibilidade de coletar informações de seus clientes de modo pessoal, como ocorria há tempos atrás, quando a vida, os gostos e os hábitos dos consumidores eram facilmente conhecidos pelos vendedores por meio do contato pessoal cotidiano. Diante da grande massa de consumidores anônimos, as empresas buscam diversas fontes de informação sobre eles, para ampliar a sua base de clientes, oferecer novos serviços aos clientes antigos, tomar decisões a respeito de seus ambientes competitivos, aumentar a eficiência de seu processo produtivo, bem como para diminuir as operações de riscos.

Os dados dos consumidores nem sempre são obtidos por meios secretos, sem que ele tenha conhecimento da coleta. Ao contrário, muitas vezes, o consumidor participa ativamente no processo de concessão de suas informações à empresa, ainda que muitas vezes não tenha consciência sobre as conseqüências de sua ação. Isso pode ocorrer quando utilizamos cotidianamente diversos aparatos tecnológicos, como o telefone, o cartão de crédito, caminhando por vias monitoradas por câmaras de vídeo, entre outros.

As principais fontes de dados dos consumidores são as seguintes: i) transações comerciais, ii) censos e registros públicos; iii) pesquisas de mercado e de estilo de vida e; iv)

sorteios e concursos; v) comercialização e cessão de dados; vi) tecnologias de controle na internet; e vii) facilitadores tecnológicos.[174]

Na exposição de cada uma dessas fontes, serão apresentados exemplos de alguns países, especialmente dos EUA e do Brasil, bem como serão examinadas as hipóteses de legitimidade da coleta dos dados à luz dos princípios gerais do regime de proteção de dados pessoais.

A princípio, é fundamental destacar que a legitimidade da coleta dos dados pessoais está condicionada ao consentimento do consumidor ou ao seu conhecimento, a menos que a atividade de coleta esteja prevista legalmente. Além disso, a finalidade pela qual os dados pessoais foram coletados deve sempre ser respeitada, não podendo os dados ser utilizados para finalidade diversa, sem o expresso consentimento do consumidor. Por fim, a utilização de dados pessoais para fins de marketing direto deve ser sempre precedida de consentimento expresso do consumidor.

Transações comerciais

Os dados de transações comerciais podem ser facilmente obtidos pela empresa por meio da realização de cadastros dos consumidores no momento da compra do produto ou da realização de serviço. Geralmente, na primeira transação comercial, a empresa solicita a realização do cadastro do consumidor, para maior segurança, em caso de pagamento com cartão de crédito ou cheque, ou simplesmente para o registro dos dados dos clientes. Nesses registros, é comum constar não apenas os dados do consumidor, mas também os seus hábitos de consumo, possibilitando que posteriormente a empresa possa ofertar-lhe produtos específicos. Grandes lojas de departamento, como C&A e Sears, possuem enormes cadastros com dados de milhares de consumidores. Amex, que é uma empresa americana que oferece serviços financeiros e de viagens (*traveler cheques*) em todo o mundo, possui mais de trinta e

[174] EVANS, Martin. The data-informed marketing model and its social responsibility. In: LACE, Susan (Ed.) *The Glass Consumer.* Op. Cit., p. 103 e 104.

quatro milhões de nomes no seu cadastro de consumidores internacional, no qual estão registrados dados sobre o que os seus clientes compram, para onde viajam e onde comem.[175]

Os dados de transações comerciais também podem ser obtidos por meio dos cartões de fidelidade, que hoje se multiplicam em supermercados, farmácias e lojas diversas, possibilitando cada vez mais o conhecimento do comportamento do consumidor. Como exemplo, os dados armazenados nesse tipo de cartão ao se comprar em um supermercado permitem conhecer o seu endereço e perceber a freqüência com que o consumidor faz compras, em que dia ele prefere fazê-lo, se tem crianças ou não, quais os seus produtos e marcas preferidos. Nesse sentido, fica claro que com essas informações, o supermercado poderá segmentar a sua oferta, enquanto o consumidor poderá receber ofertas e promoções de seu interesse.

Ademais, a partir desses dados de transações comerciais, que são dados comportamentais, a empresa pode avaliar e classificar o consumidor em relação à sua freqüência, à última vez que esteve na loja e ao seu valor monetário (recency, frequency and monetary value – RFMV). As conseqüências dessa classificação podem ser indesejáveis, tais como a possibilidade de exclusão do consumidor de menor capacidade financeira.

Tanto na coleta de dados a partir de transações comerciais, como de cartões de fidelidade, o consentimento do consumidor é essencial para que a obtenção de dados pessoais seja legítima. Assim, não é o consumidor obrigado a fornecer os seus dados pessoais, a menos que a transação econômica escolhida requeira, para a sua segurança, tais informações. Com relação ao cartão de fidelidade, a questão é um pouco mais complexa, pois nem sempre o consumidor percebe que por trás dessa fidelização estão, na realidade, o monitoramento e o armazenamento dos dados referentes ao seu comportamento de consumo. Assim, a legitimidade dessa coleta dependerá do consentimento do consumidor em ceder esses dados, bem como da explicitação da finalidade da coleta.

[175] GANDY, Oscar. *The Panoptic Sort. A Political Economy of Personal Information.* Boulder: Westview Press, 1993, p. 66.

Censo e registros públicos

O governo teve um papel importante para o desenvolvimento da economia da informação ao criar a cultura de estatística e de pesquisa de informações dos cidadãos, bem como ao transferir para o setor privado essas informações coletadas oficialmente, ainda que de forma anônima. Conforme afirma Daniel Solove, na década de 70, o governo americano comercializou fitas magnéticas com dados do censo, que continham informações sobre idade, nível de renda, raça, etnia, gênero e localização geográfica, sem se referir aos nomes das pessoas.[176] Tal fato possibilitou o mapeamento demográfico dos cidadãos, que passam a ser identificados e classificados pelas empresas, com base no seu local de domicílio, para a realização de geomarketing e outras técnicas.[177]

A partir desses dados, a CACI e a Experian[178], empresas americanas do ramo de análise de risco, crédito e marketing direto, desenvolveram programas específicos (ACORN e MOSAIC, respectivamente) para o mapeamento demográfico das pessoas.[179] Esse fato nos leva a refletir sobre alguns problemas. Primeiramente, constata-se que esses programas que tendem a classificar as pessoas pelo local onde residem uniformizam o tratamento para todos os moradores de determinada região, deixando de considerar a real situação de cada indivíduo. Além disso, é bastante questionável que os dados pessoais que foram coletados com o propósito de servirem ao censo demográfico possam ser utilizados para fins de marketing direto ou avaliação de risco, uma vez que viola o princípio da finalidade da proteção de dados pessoais.

[176] SOLOVE, Daniel. *The Digital Person.* Op. Cit., p.18.
[177] Importa mencionar que a divulgação pelo governo de todos esses dados do censo de forma anônima em nada protegeu, de fato, o cidadão, na medida em que a divulgação do endereço permitia a qualquer um associar o domicílio da pessoa ao nome dos moradores, a partir de informações presentes no registro eleitoral. (EVANS, Martin. The data-informed marketing model and its social responsibility. Op. Cit., p. 106.)
[178] A Experian atua no Brasil, com sua sede em São Paulo, e em mais de 65 países, oferecendo cerca de dez serviços, relacionados a marketing e estratégias de tomada de decisão.
[179] EVANS, Martin. The data-informed marketing model and its social responsibility. Op. Cit., p. 106.

Pesquisas de mercado e de estilo de vida

A forma mais fácil de obter dados sobre o gosto e comportamento dos consumidores é perguntar-lhes diretamente por meio de pesquisas de mercado.[180] Essas pesquisas podem ser feitas pessoalmente, por telefone, ou respondidas por meio de questionários. Os dados oriundos de pesquisas de mercado não se referem a indivíduos específicos, mas constituem informações relevantes sobre o campo de atuação da empresa, seu negócio, sua concorrência e especialmente seus clientes. As empresas necessitam das pesquisas de mercado para conhecer o que os consumidores desejam e quanto estão dispostos a pagar, buscando obter uma vantagem competitiva. Apesar da importância desse tipo de pesquisa, as empresas têm preferido os dados de oriundos de transações comerciais que retratam o perfil do consumidor e que são mais abrangentes.[181]

As pesquisas de estilo de vida, diferentemente das pesquisas de mercado, não são anônimas e, portanto, referem-se aos consumidores de forma individualizada.[182] Atualmente, são realizadas pelas mesmas empresas que se utilizam do geomarketing, que é o marketing segmentado geograficamente, para complementar os dados dos consumidores com informações sobre os seus hábitos de consumo de produtos e serviços. De acordo com Martin Evans, mais de 16 milhões de indivíduos já completaram questionários sobre estilo de vida, mas a precisão e retidão desses dados são questionados por especialistas em marketing.[183]

Por constituírem um meio direto de obtenção de dados dos consumidores, as pesquisas de mercado e de estilo de vida tornam-se um meio legítimo de coleta de dados, desde que se apresente ao consumidor claramente a finalidade da coleta. Ademais, é necessário que a empresa obtenha o consentimento expresso do consumidor, caso tenha interesse em compartilhar ou ceder tais dados a terceiros ou de utilizá-los com a finalidade de marketing direto.

---

[180] GANDY, Oscar. *The Panoptic Sort.* Op. Cit., p. 64.
[181] EVANS, Martin. The data-informed marketing model and its social responsibility. Op. Cit., p. 112.
[182] Idem, Ibidem, p. 108.
[183] Idem, Ibidem.

Sorteios e concursos

Os sorteios e concursos são uma forma bastante utilizada pelas empresas para obter dados pessoais de potenciais clientes ou para aumentar o registros de antigos clientes. Para as empresas, muitas vezes, o preenchimento dos questionários que acompanham os sorteios é a única finalidade de sua realização, muito embora a maioria dos consumidores não o percebam. A empresa Reader's Digest há décadas promove concursos e sorteios de prêmios, por meio de sua revista Seleções, e constitui-se em uma das primeiras empresas nos EUA a coletar massivamente dados dos consumidores, visando à sua comercialização e à realização de marketing direto.

Essa fonte de coleta de dados é bastante problemática, na medida em que o consumidor , geralmente, não tem o conhecimento de que a finalidade da realização dos sorteio e do concurso de prêmios é a obtenção de seus dados pessoais. Nesse sentido, é fundamental que fique claro ao consumidor que os dados apresentados por ele voluntariamente na inscrição para o sorteio estão sendo coletados para determinada finalidade. Além disso, qualquer cessão de dados ou utilização para fins de marketing deve ser precedida de consentimento expresso pelo consumidor. Somente assim essa fonte de coleta poderá ser considerada legítima sob a perspectiva do regime de proteção de dados pessoais e da legislação de defesa do consumidor.

Compartilhamento e cessão de dados

Outra fonte de dados pessoais pelas empresas é o compartilhamento de dados com outras empresas de ramos semelhantes ou complementares, por meio da formação estratégica de consórcios. Assim, por exemplo, é possível um consórcio entre uma empresa de seguros, uma empresa especializada em serviços de automóveis acidentados e uma companhia de TV satélite. Um consórcio para o compartilhamento de dados, nesses moldes, foi estabelecido

entre Unilever, Kimberley Clark e Cadbury, com a finalidade de reduzir custos de bancos de dados e denominado JIGSAW.[184] Outro consórcio formado com esse objetivo, denominado TANK!, foi o realizado entre o Banco Royal da Escócia, o Instituto de Marketing Direto e a Associação de Marketing Direto.

O compartilhamento de dados também é bastante comum nos serviços de proteção ao crédito no Brasil. Conforme afirma Leonardo Bessa, em 2002, foi formada a Rede de Informações e Proteção ao Crédito (RIPC), composta pela Confederação Nacional de Lojistas, Associação Comercial de São Paulo, Clube de Diretores Lojistas do Rio de Janeiro e Associação Comercial do Paraná.[185] A Rede centraliza um banco de dados comum, acessível a todos os participantes, e que é responsável por mais de 40 milhões de registros ativos e pela movimentação de cerca de 20 milhões de informações de concessão de crédito ao mês.[186]

Outra forma de obtenção de dados dos consumidores é por meio da aquisição ou do aluguel de dados de empresas que têm como único objetivo a comercialização[187] de dados pessoais de consumidores para diversos setores.

Tecnologias de controle na internet

A coleta de dados pessoais e a interação entre consumidor e fornecedor no momento pré-contratual podem ser realizados por meio de tecnologias de controle na internet, tais como *cookies* e criptografia.

A internet, que é uma estrutura aberta de rede de computadores, é um marco no fluxo de informações ao ampliar radicalmente as possibilidades de comunicação. A sua principal característica é a abertura, tanto em sua arquitetura técnica como em sua organização social/institucional; é a flexibilidade dos protocolos de comunicação que possibilita a conexão

[184] Idem, Ibidem, p. 109.
[185] BESSA, Leonardo. *O Consumidor e os Limites dos Bancos de Dados de Protecao ao Crédito*. São Paulo: RT, 2003. p. 35.
[186] Idem, Ibidem, p. 36.
[187] SOLOVE, Daniel. *The Digital Person. Technology and Privacy in the Information Age.* New York: New York University Press, 2004, p. 19.

entre milhares de redes locais. A abertura dessa rede é a sua principal força, na medida em que possibilitou o seu desenvolvimento autônomo por meio dos seus próprios usuários que tornaram produtores da tecnologia e artífices de toda a rede.[188]

Se por um lado a estrutura aberta da internet possibilitou a sua difusão e o aperfeiçoamento da tecnologia, por outro, também estimulou o desenvolvimento de inúmeras tecnologias de controle, decorrentes do interesse de governos e do comércio, que podem acarretar a restrição da liberdade do usuário. A partir de aplicações de software que são superpostas em camadas a protocolos da internet, torna-se possível identificar rotas de comunicação e conteúdo. Segundo Lawrence Lessig[189], "com o uso dessas tecnologias, é possível violar a privacidade, e uma vez que se torna possível relacionar indivíduos com processos específicos de comunicação em contextos institucionais específicos, todas as formas tradicionais de controle político e organizacional podem ser lançadas sobre o indivíduo em rede"[190].

É interessante observar como o ambiente virtual é propenso às violações da privacidade, de uma forma mais imperceptível e silenciosa que o ambiente físico. Isso porque o espaço físico possibilita a constatação mais nítida do nível de privacidade disponível e permite que a pessoa tome as decisões a fim de aumentar ou diminuir a sua privacidade, o que nem sempre é possível no espaço virtual, vez que não se sabe quais informações estão sendo capturadas, nem o momento em que esse controle é realizado. Priscilla Regan constata a diferença entre a percepção da privacidade que se tem no ambiente físico e no ambiente virtual:

> O mundo físico permite que se construa uma extensão mais clara dos espaços públicos e privados: ruas cheias de pessoas, centros comerciais fechados, carros com películas

[188] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 141 e 142.

[189] LESSIG; Lawrence. *Code and Other Laws os Cyberspace* **apud** CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Op. Cit., p. 140.

[190] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Op. Cit., p. 141 e 142.

> escuras, apartamentos com paredes finas, mansões cercadas. A extensão é intuitivamente familiar a todos. Pessoas que vivem em apartamentos pequenos com vizinhos próximos sabem que a sua capacidade de estabelecer uma fronteira entre si e os outros (...) é fisicamente limitada. Eles conseguem ver concretamente tais limitações. Ao ver essas limitações, eles podem agir de acordo. No cyberespaço, não há claramente indícios visuais sobre o nível de privacidade disponível. De fato, os novos usuários da internet pensam inicialmente que todas as atividades no cyberespaço são privadas se ninguém no espaço físico os estiver observando ao usar o computador.[191]

De tal forma, são diversos os riscos à privacidade a que os internautas estão sujeitos, em razão das inúmeras tecnologias de controle existentes e, principalmente, pela facilidade de camuflagem dessas tecnologias.[192] As tecnologias de controle disponíveis no meio da Internet podem ser classificadas em três tipos, quais sejam, de identificação, de vigilância e de investigação.[193]

As tecnologias de identificação constituem aquelas que permitem a localização do usuário, bem como a verificação de todos os seus movimentos *on line*. São exemplos dessas tecnologias o *cookie*, o *web bug* e os procedimentos de verificação com tecnologia de criptografia.

Os *cookies* são marcadores digitais que são automaticamente inseridos por websites visitados, nos discos rígidos do computador do consumidor, em sua casa ou no seu local de trabalho, para possibilitar a sua identificação e a memorização de todos os seus movimentos.[194] Agem quase sempre sem que o internauta tenha conhecimento, podendo trazer benefícios ou malefícios, conforme o caso. Por um lado, são os cookies que permitem aos internautas a memorização de senhas e a personalização de serviços. Por outro, quando o computador é associado aos dados do internauta, a partir de seus dados pessoais fornecidos a

---

[191] REGAN, Priscilla M. (2002) 'Privacy as a Common Good in the Digital World', In: *Information, Communication & Society*, 5:3, p. 348 (tradução livre).

[192] Para se verificar o potencial de coleta de dados da internet, basta que se insira o próprio nome em sites de busca, o que permitirá perceber a quantidade de informações pessoais que são facilmente acessíveis nessa rede, tais como, nome completo, data e local de nascimento, telefone e endereço, local de trabalho, fotos, entre outros.

[193] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Op. Cit., p. 141 e 142.

[194] BELLEIL, Arnaud. *@ privacidade. O mercado de dados pessoais: proteção da vida privada na idade da internet.* Trad: Paula Rocha Vidalinc. Lisboa: Instituto Piaget, 2002, p. 65.

um determinado site, esses marcadores tornam-se ameaçadores à privacidade.[195] Ademais, quando inseridos por um longo período, os cookies possibilitam o rastreamento do comportamento do usuário em diversos *sites*.

Vale mencionar, com relação à legalidade da utilização de cookie, que a Diretiva Européia 2002/58/CE, referente ao tratamento de dados pessoais e à proteção à privacidade nas comunicações eletrônicas, prescreve que ele somente pode ser usado quando os seus fins forem legítimos e quando houver consenso do usuário da máquina.[196]

Outra tecnologia de identificação de endereços é o *web bug*. Este é uma imagem, muito pequena e praticamente invisível, que pode compor um sítio eletrônico ou uma mensagem de e-mail, com a finalidade de monitorar quem está acessando este sítio ou mensagem de e-mail.[197] Ao ser visualizado, o *web bug* possibilita que diversas informações seja armazenadas no servidor onde esta hospedados, como, por exemplo, endereço IP do computador, o horário em que foi visualizado, entre outros.

Já as tecnologias de vigilância são as que permitem a interceptação de mensagens, o rastreamento dos fluxos de comunicação e o monitoramento ininterrupto das atividades da

---

[195] Idem, Ibidem, p. 67.

[196] É o que afirma o seu "Considerando 25": Todavia, esses dispositivos, por exemplo os denominados testemunhos de conexão («cookies»), podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transacções em linha. Sempre que esses dispositivos, por exemplo os testemunhos de conexão («cookies»), se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Directiva 95/46/CE, acerca da finalidade dos testemunhos de conexão («cookies») ou dos dispositivos análogos por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam. Os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal.Tal é particularmente importante nos casos em que outros utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento. A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio web específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão («cookie») ou dispositivo análogo, caso seja utilizado para um fim legítimo.

[197] REGAN, Priscilla M. (2002) 'Privacy as a Common Good in the Digital World', In: *Information, Communication & Society*, 5:3, p. 388.

máquina, tais como o *spyware*. Este é um tipo de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, podendo comprometer a privacidade do usuário e a segurança do computador.[198] Algumas de suas funções são, por exemplo, o monitoramento de URLs acessadas enquanto o usuário navega na Internet e captura de senhas bancárias e números de cartões de credito.

A Diretiva Européia 2002/58/CE refere-se aos web bugs e spywares, proibindo-os sempre que utilizados para fins não legítimos e sem o conhecimento do usuário. É o que afirma o Considerando 24:

> (24) O equipamento terminal dos utilizadores de redes de comunicações electrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais. Os denominados «gráficos espiões», «programas-espiões», («spyware»), «gráficos-espiões» («web bugs») e «identificadores ocultos» («hidden identifiers») e outros dispositivos análogos podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das actividades do utilizador e podem constituir uma grave intrusão na privacidade desses utilizadores. A utilização desses dispositivos deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa.

As tecnologias de investigação dizem respeito à construção de banco de dados a partir dos resultados obtidos pelas ações de vigilância e monitoramento. Conforme afirma Castells, "no ambiente tecnológico atual, toda informação eletronicamente transmitida é gravada, podendo vir a ser processada, identificada e combinada numa unidade de análise coletiva ou individual."[199]

Se por um lado o ambiente da internet é propício para o desenvolvimento de inúmeras tecnologias de controle, ele também estimula a criação de tecnologias de liberdade, que visam proteger a identidade e a privacidade do internauta, também chamadas de tecnologias de

[198] Idem, Ibidem.
[199] CASTELLS, Manuel. *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Op. Cit., p. 141 e 142.

proteção à privacidade, conhecidas pela sigla PET - *Privacy Enhancing Tecnologies*.[200] Uma das mais conhecidas tecnologias desse tipo é a criptografia, que protege a identidade dos internautas e possibilita a realização de transações anônimas na internet. A criptografia possibilita o envio de mensagens em forma cifrada ou em código, podendo ser utilizada para autenticar a identidade de usuários, para proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias, e para assegurar o anonimato do emissor de uma mensagem, entre outras finalidades.[201]

Não obstante a importância da criação da criptografia para a proteção dos dados pessoais do internauta, deve-se ressaltar que esse instrumento sofreu resistência do governo durante o seu desenvolvimento, na década de 90.[202] Compreendeu-se que a criptografia poderia ameaçar a sociedade e o próprio Estado, na medida em que o nível de confidencialidade proporcionado pela mensagem criptografada poderia facilitar não apenas a proteção da privacidade, como também a realização de crimes na internet, como a pedofilia e a pirataria informática, entre outros. Desse modo, o incentivo e a restrição ao desenvolvimento da criptografia variou entre os países, mas os seus benefícios foram reconhecidos inclusive pela OCDE, em suas diretrizes para a política de criptografia, de 27 de março de 1997.

Dentre as tecnologias de liberdade, é importante mencionar o instrumento denominado Plataforma para as Preferências relativas à Privacidade (*Platform for Privacy Preferences* – P3P). Conforme afirma Belleil, o P3P tem como objetivo o seguinte:

> Cada internauta predefine o que está disposto a aceitar por parte dos sítios da web em matéria de coleta e de utilização de seus dados pessoais. Em seguida, à medida que vai surfando, instaura-se automaticamente um diálogo entre o navegador do internauta e o sítio web visitado. Efectua-se uma comparação automática entre as práticas do sítio

[200] BENNETT, Colin e RAAB, Charles. *The Governance of Privacy.* Op. Cit., p. 180 e 181. Para esse assunto, Ver também: BELLEIL, Arnaud. *@ privacidade. O mercado de dados pessoais: proteção da vida privada na idade da internet.* Op. Cit., p. 157 a 170. BORKING, John. The use and value of privacy-ehancing technologies. In: LACE, Susanne (Ed). *The Glass Consumer.* Op. Cit., p. 69 a 95.

[201] Cartilha de Segurança para Internet, versão 3.1 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2006. Acessível em: http://cartilha.cert.br/livro/

[202] BENNETT, Colin e RAAB, Charles. *The Governance of Privacy.* Op. Cit., p. 201.

> web, ou seja, a sua política de dados pessoais e os desejos do internauta. Se as práticas do sítio web excederem os limites fixados pelo utilizador ou se ele não reunir condições para acitar a plataforma P3P, então o utilizador é automaticamente prevenido. Cabe-lhe a ele prosseguir ou interromper a sua visita, sabendo que a solução não prevê um bloqueio automático de conexão.[203]

A tecnologia P3P foi incorporada à ultima geração dos navegadores de internet da Microsoft, podendo os usuários estabelecer o seu grau de privacidade de 1 a 6.[204] Esse mecanismo, assim como a criptografia, constituem exemplos de como a tecnologia pode também atuar em prol do aumento da privacidade pessoal.

A análise das tecnologias de liberdade requer uma reflexão acerca de seu papel de atuação juntamente com outros instrumentos de política pública aptos a realizarem a proteção da privacidade, tais como lei e regulamentos estatais, bem como instrumentos de auto-regulação. Entende-se que essas tecnologias defensivas são complementares às medidas legislativas estatais e auto-regulamentares das empresas, formando um complexo regime de proteção à privacidade.[205] Conforme afirma Philip Agre, "a tecnologia não pode, obviamente, garantir a justiça nas relações humanas, mas pode criar as condições sob as quais a justiça é ao menos possível; ela pode também arruinar as condições de justiça".[206]

Assim, os PETs podem ser considerados condição necessária, mas não suficiente para uma política de privacidade adequada, sempre que utilizados em conjunto com a legislação nacional e uma ação pró-ativa dos consumidores.

Facilitadores tecnológicos

Como visto, o advento da internet possibilitou o desenvolvimento de inúmeras tecnologias invasivas à privacidade, ao mesmo tempo em que incentivou a criação de tecnologias de liberdade. No entanto, é importante não perder de vista também o papel de

[203] BELLEIL, Arnaud. *@ privacidade. O mercado de dados pessoais: proteção da vida privada na idade da internet.* Op. Cit., p. 164.
[204] BENNETT, Colin e RAAB, Charles. *The Governance of Privacy.* Op. Cit., p. 196.
[205] Idem, Ibidem, p. 198.
[206] AGRE, Philip. Introduction. In: AGRE, Philip e ROTENBERG, Marc (Ed). *Techonology and Privacy: The New Landscape*. Op. Cit., p. 8 (tradução livre).

outros instrumentos tecnológicos, que ampliam a possibilidade de vigilância e violação à privacidade, tais como o GPS, tecnologia de impressão digital, TV interativa, telefone celular, sistemas eletrônicos de rastreamento de veículos, entre outros, que podem facilitar a coleta dos dados dos consumidores.

2.3.2. Técnicas de processamento de dados

No item anterior, analisou-se o primeiro momento do tratamento de dados pessoais, que é o momento da coleta dos dados dos consumidores. Foram vistas as fontes de coleta de dados, bem como as hipóteses de sua legitimidade ou ilegitimidade. Passar-se-á, agora, para a análise do segundo momento, que é o do processamento desses dados por meio de modernas tecnologias para o refinamento da informação.

Conforme visto, na sociedade atual, diversas são as fontes de coleta de dados dos consumidores, como as transações comerciais, os censos e registros públicos, bem como as tecnologias disponíveis na internet. Ocorre, no entanto, que para o fornecimento de produtos e serviços diversificados e para a diminuição dos riscos do negócio, as empresas necessitam refinar as informações coletadas. Isso torna-se possível com a submissão dos dados coletados a processos técnicos de lapidação da informação, a fim de buscar informações mais completas sobre os hábitos e o comportamento dos consumidores ou clientes em potencial.

Sofisticadas tecnologias de análise de dados permitem às empresas implementar uma complexa estratégia de relacionamento com os seus clientes, utilizando as informações armazenadas em bancos de dados. A partir desses instrumentos tecnológicos, a empresa pode lograr a classificação de seus clientes e a sua segmentação em grupos diversos, diferenciando entre os consumidores de maior valor para a companhia e os de menor valor. Com isso, a empresa objetiva obter previsibilidade de variações no mercado e na demanda, de modo a

reduzir seus riscos, bem como conhecer os diferentes segmentos para direcionar-lhes a sua publicidade.

Diversas são as técnicas que possibilitam a extração de valiosas informações a partir dos dados coletados, como a *Datawarehousing*, *Data Mining*, *On-Line Analyticial Processing (OLAP)*, Construção de Perfil (*Profiling*) e Sistema de avaliaçao *(Scoring- ou Rating-System)*. Essas técnicas trazem benefícios e desafios ao consumidor. De um lado, a personalização de produtos e serviços e a possibilidade de diminuição de publicidade importuna; de outro, riscos à privacidade, à discriminação do consumidor e à sua exclusão do mercado de consumo. Vejamos cada uma dessas técnicas, bem como os riscos que elas podem acarretar ao cidadão-consumidor.

Datawarehousing

Um *data warehouse*, que significa depósito de dados, é um sistema informatizado que armazena enorme quantidade de informações e está organizado de tal modo a facilitar a extração de relatórios, o exame de grandes volumes de dados, bem como a tomada de decisão.[207] É, em suma, uma grande base de dados, integrada, orientada pelo sujeito, com dimensão temporal, e não volátil. A orientação pelo sujeito é fundamental para que se possam obter informações sobre uma pessoa em particular, ao invés de informações sobre operações de determinada empresa. Ele não é volátil, na medida em que os dados armazenados não sofrem alteração, nem podem ser cancelados.

A expressão *datawarehousing* denota a atividade de organizar dados de inúmeros sistemas operativos e heterogêneos de acordo com sua relevância, transformando-os e selecionando-os, com vistas a possibilitar a tomada de decisão estratégica. Com essa técnica, as empresas podem armazenar os dados coletados de consumidores de acordo com critérios específicos, para a sua utilização futura.

[207] SCHWENKE, Matthias. *Individualisierung und Datenschutz.* Op. Cit., p. 115 a 117.

Tendo em vista a variedade de finalidades futuras para as quais o *data warehouse* pode servir, poder-se-ia questionar a legitimidade de sua utilização pelas empresas, em face do princípio da finalidade, que deve ser explícito e concreto, no momento da coleta dos dados. Sob essa ótica, pode-se compreender que a utilização de um *data warehouse* somente é legitima se a sua finalidade concreta puder ser compreendida de forma expressa e clara pelo consumidor, de modo a não frustrar as suas legítimas expectativas.[208]

A exploração do *data warehouse* pode ser feita por inúmeras técnicas, como o *On-Line Analytical Processing* (OLAP), o *data mining* e a construção de perfis. Uma vez que os seus efeitos são mais aparentes quando está associada a essas outras técnicas, entende-se que é melhor que a análise sobre a legitimidade do armazenamento de dados pessoais seja realizada em conjunto com elas.[209] A seguir explicar-se-á o significado de cada uma dessas técnicas.

Data Mining

Data mining, ou mineração de dados, é o processo pelo qual dados de difícil compreensão são transformados em informações úteis e valiosas para a empresa, por meio de técnica informática de combinação de dados e de estatística. Isso significa que por meio de uma única tecla, empresas são capazes, a partir do *data mining*, de unir e combinar dados primitivos de uma pessoa, formando novos elementos informativos.

A mineração de dados, como uma ferramenta para a descoberta de padrões significativos de informações, é o produto de rápido desenvolvimento no domínio das técnicas aplicadas à análise estatística. A crescente sofisticação dos pacotes de software que operam a mineração de dados, bem como o rápido declínio de seus preços, permite crer que essa técnica tem um grande potencial de expansão para todos os setores do mercado.[210]

---

[208] Idem, Ibidem.
[209] Idem, Ibidem.
[210] GANDY, Oscar e SCHILLER, Herbert. Data mining and surveillance in the post-9.11 environment. For presentation to the Political Economy Section, IAMCR. Barcelona, July, 2002, p. 3.

O objetivo da mineração de dados é a extração de inteligência significativa e de padrões de conhecimento, partindo de um banco de dados, por meio de sua ordenação e transformação. Geralmente, a mineração de dados tem como finalidade gerar regras para a classificação de pessoas ou objetos. Nesse sentido, pode-se inferir que aí reside um risco dessa técnica, uma vez que ao facilitar a classificação e a segmentação, ela pode gerar análises discriminatórias, negando o direito constitucional à igualdade de todos os cidadãos.

Sob essa perspectiva, Oscar Gandy compreende que a obtenção de informações a partir da técnica de mineração de dados é tão prejudicial à sociedade como o é a técnica de extração de minerais preciosos do solo:

> As rotinas que fazem parte do esforço mineração de dados são, em alguns aspectos, semelhantes às técnicas que são utilizadas para extrair minerais preciosos do solo. No entanto, enquanto a extração de metais preciosos constitui freqüentemente um trabalho intensivo, e representa riscos tanto para os trabalhadores como para o ambiente, a extração de inteligência da bases de dados é cada vez mais automatizada, de modo a reduzir os riscos diretos para o trabalho, embora ampliando os riscos da sociedade em geral. Na verdade, como espero demonstrar, o impacto desta tecnologia no ambiente social a longo prazo pode ser tão destrutivo como a mineração a céu aberto.[211]

Desse modo, pode-se perceber que a técnica de mineração de dados constitui uma tecnologia potencialmente discriminatória, na medida em que propicia a classificação de pessoas a partir de dados pessoais armazenados, o que pode acarretar práticas que violam o princípio fundamental da igualdade. Naturalmente, compreende-se que não é tal técnica em si que propicia a discriminação, mas sim o seu modo de utilização e as decisões que serão tomadas com base nas informações extraídas.

A análise da legitimidade da mineração de dados, à luz do regime de proteção de dados pessoais, deve considerar não apenas o seu uso potencial, mas sim as hipóteses em que ela será legítima e as hipótese em que seu uso será ilegítimo. De antemão, pode-se ressaltar que sempre que o seu uso causar discriminação, esse será considerado ilegal, por ferir o direito fundamental à igualdade de todos cidadãos.

[211] Idem, Ibidem, p. 4.

Para além do problema da discriminação, dois outros problemas podem aparecer com o *data mining*, à luz da teoria da proteção de dados pessoais. O primeiro deles diz respeito ao descumprimento do princípio da finalidade, na hipótese em que a finalidade da mineração de dados não tenha ficada clara para o consumidor ou não tenha sido apresentada pela empresa. O segundo diz respeito à possibilidade de que essa técnica de mineração de dados possa transformar dados, à primeira vista inofensivos, em informações sensíveis, que revelem informações do consumidor sobre as quais ele esperava sigilo. Conforme afirmou a Corte alemã no julgamento sobre a lei do recenseamento, a partir das possibilidades de ligação e processamento da tecnologia da informação, "um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados".[212]

Desse modo, fica claro que a utilização da técnica de mineração de dados somente será legítima se a relação entre o consumidor e a empresa for transparente a ponto de ele ser informado sobre a finalidade da coleta e do processamento de seus dados por meio dessa técnica. Ademais, a sua legitimidade depende também que o uso das informações oriundas da mineração de dados seja legal e que não seja discriminatório.

On-Line Analytical Processing (OLAP)

O OLAP é uma técnica desenvolvida em 1993, como um aperfeiçoamento da mineração de dados. De forma semelhante à mineração, o OLAP possibilita a análise de dados a partir dos dados presentes em um *data warehouse*, possuindo uma estrutura adequada tanto para a realização de pesquisas como para a apresentação de informações.[213] Com essa técnica, as empresas são capazes de realizar uma análise de dados de forma dinâmica e multidimensional, obtendo novas relações entre os dados e diferentes variáveis. A sua

[212]MARTINS, Leonardo. (org.) *Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão.* Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.
[213] SCHWENKE, Matthias. *Individualisierung und Datenschutz.* Op. Cit., p. 124.

principal vantagem é possibilitar a previsão de tendências e prognósticos, a partir da análise de uma determinada base de dados.

Para se analisar os aspectos relevantes em relação à proteção de dados pessoais do OLAP, é mais adequado examiná-lo em conjunto com outras técnicas, como a mineração de dados e a construção de perfis.

Construção de Perfil (Profiling)

O perfil pode ser considerado um registro sobre uma pessoa que expressa uma completa e abrangente imagem sobre a sua personalidade. Assim, a construção de perfis compreende a reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter um imagem detalhada e confiável sobre o pessoa, visando, geralmente, à previsibilidade de padrões de comportamento do consumidor, de gostos, hábitos de consumo e preferências do consumidor.

Sabe-se que essa técnica de construção de perfis pessoais possibilita a tomada de importantes decisões a respeito dos consumidores, trabalhadores e cidadãos em geral, afetando diretamente a vida das pessoas e influenciando o seu acesso a oportunidades sociais.

Os riscos da técnica de construção de perfis não residem na sua grande capacidade de junção de dados; na realidade, a ameaça consiste exatamente na sua enorme capacidade de combinar diversos dados de forma inteligente, formando novos elementos informativos. Nesse sentido, é o entendimento de Matthias Schwenke, que afirma como a construção de perfis pode ser ameaçadora à personalidade e integridade do cidadão-consumidor:

> A criação de perfis dos consumidores é problemática em diversos aspectos: perfis apresentam riscos à esfera privada e íntima, uma vez que possibilitam a manipulação relativa à sua vontade, bem como ensejam o mau uso dos dados no perfil. Problemático é também que o perfil seja criado sem o conhecimento e o consentimento do consumidor, sem que sejam asseguradas adquada proteção do sujeito submetido a essa técnica.[214]

[214] Idem, Ibidem, p. 127 e 128.

Não obstante o perigo que essa técnica pode representar, pode-se dizer que esses perfis não constituem por si só uma ameaça à personalidade, pois o que determinará a sua legitimidade ou ilegitimidade é o uso que dele se fará, bem como o consentimento e o conhecimento do consumidor a respeito da criação de perfis relativos à sua pessoa.

Sistema de avaliação ou medição (Scoring- ou Rating- System)

O sistema de avaliação objetiva identificar os consumidores que têm maior valor para a empresa, para que esses sejam os alvos de promoções e estratégias de fidelização de clientes. Isto é, a empresa tem interesse em identificar os "melhores consumidores" para que possa construir com eles uma relação mais duradoura, garantindo vantagens competitivas e manutenção dos níveis de lucratividade.

Como é de se esperar, a identificação dos melhores também pressupõe a identificação daqueles considerados os "piores consumidores". Esses são aqueles que as empresas têm interesse de oferecer as piores ofertas. Ademais, esses podem ter o seu acesso a bens e serviços negado, em razão da sua classificação como um consumidor "ruim". Exemplos de empresas que oferecem esse serviço no Brasil são a SERASA[215] e a Experian Brazil[216].

Esse tema é bastante preocupante à luz do regime de proteção de dados pessoais, pois a inadequação desses sistemas pode causar graves danos aos consumidores, especialmente à sua dignidade e personalidade. Por isso, aplica-se a esse sistema de avaliação ou medição a proibição de que o cidadão fique sujeito a uma decisão individual automatizada que influencie

[215] A SERASA oferece o serviço de *credit rating*, que consiste, de acordo com o seu site, em um "avançado sistema de classificação de risco de crédito de pessoas jurídicas que organiza as empresas em classes homogêneas de risco e mede a probabilidade de a empresa se tornar inadimplente em um determinado horizonte de tempo". (Fonte: http://www.serasa.com.br/solucoes/creditrating/index.htm)

[216] No site da Experian consta a oferta do serviço "*Connect+*", que consiste em um conjunto de soluções de gerenciamento de risco e de serviços de informação, com o objetivo de revelar a inteligência contida na informação. Dentre as ferramentas do *Connect+*, está o *scoring*, sistema de avaliação, que busca agregar valor aos dados, de modo a maiximizar a informação oriunda dos dados e facilitando a tomada de decisões. (fonte: http://www.experian-scorex.com/Web/Solutions/DC/Intro.html)

significativamente a sua esfera jurídica, prevista.[217] Tal proibição geral suporta apenas duas exceções: i) que existam medidas adequadas que garantam a representação e expressão do titular dos dados para a sua defesa; e ii) que a decisão ocorra no âmbito da celebração ou execução de um contrato. Como visto, no Capítulo 2, essa norma visa assegurar uma regra de justiça, que possibilite o mínimo de controle e de participação do titular em um processo de decisão tomado com base em seus dados pessoais e que afetará de forma significativa as suas oportunidades de vida.

Como afirma Catarina Sarmento e Castro, o *Scoring- ou Rating- System* não são válidos, se por si só, forem utilizados para referendar uma decisão. Eles somente podem ser utilizados para auxiliar a tomada de decisão e desde que os seus critérios sejam claros e transparentes:

> A previsão do art. 13º, no. 1, da Lei de Protecção de Dados, que segue de perto a redacção da Diretiva 95/46/CE, teve como um dos seus objectivos a proibição do *credit scoring* que consiste na 'atribuição ou denegação automática de crédito pessoal, consoante a pessoa que solicita esse crédito responde ou não a certas características pessoais ou profissionais, previamente definidas no programa de computador.' (...)
> Esse art. 13º, no. 1, da Lei de Protecção de Dados não impede, de modo absoluto, a utilização de operações de triagem e selecção realizadas a partir de um tratamento automatizado de dados pessoais. Admite-se que os dados armazenados de forma automatizada possam ser utilizados para ajudar uma tomada de decisão, *v.g.* fornecendo mais informação, ou seguindo a actuação apropriada, mas os computadores e os dados que armazenam não devem ser utilizados como único meio para encontrar a solução.[218]

Percebe-se, portanto, que a transparência e a objetividade são características essenciais para assegurar a legitimidade do sistema de avaliação dos consumidores. Por conseqüência, compreende-se que caso o consumidor tenha excluído o seu acesso a determinados bens e produtos no mercado de consumo em razão desse sistema de avaliação, é fundamental que os critérios desse sistema sejam transparentes e publicizados. Ademais, a sua utilização deve estar prevista contratualmente e o consumidor deve ter sido previamente informado sobre a

[217] Essa proibição está prevista no art. 15 da Diretiva Européia 95/46/CE.
[218] CASTRO, Catarina Sarmento e. *Direito da Informática, Privacidade e Dados Pessoais.* Coimbra: Almedina, 2005, p. 252.

sua realização, os critérios e os seus efeitos. Do contrário, ele será contrário aos princípios da proteção de dados pessoais e, portanto, ilegítimo.

Finalidades comerciais das técnicas de processamento de dados

É interessante observar que cada uma dessas técnicas acima estudadas é utilizada para atingir fins comerciais específicos, quais sejam, i) previsibilidade e diminuição de riscos, ii) interação com o consumidor e iii) diferenciação de produtos e iv) diferenciação de serviços, conforme mencionado no tópico 2.2.2. deste capítulo[219]. Para atingir a meta de diminuição de riscos, as empresas utilizam, principalmente, as técnicas de *Data Warehousing*, avaliação e mineração de dados. Para ampliar a interação com o consumidor e a realização de técnicas de marketing direto, é utilizada a técnica de mineração de dados. Quando o objetivo é a segmentação de produtos, as empresas utilizam a técnica de construção de perfis e quando se visa a segmentação da prestação de serviços, utiliza-se, além da construção de perfis, técnicas de localização.

O quadro abaixo[220], elaborado por Mathias Schwenke, expressa a finalidade comercial em razão da qual cada uma dessas técnicas é utilizada e a relação em que são preponderantemente empregadas, isto é, se no âmbito da relação entre empresas ou no âmbito de uma relação de consumo:

Medidas de individualização

Grupo de individualização	1	2	3	4
Nome do grupo	Minimização de risco	Marketing	Mercadorias e Produtos	Prestação de Serviços
Métodos de individualização tipicamente utilizados	Data Warehousing, Scoring, Data Mining	Data Mining	Construção de perfis	Construção de perfis, Localização, etc.
Relação, na qual a	B2B[221]	B2B, B2C[222]	B2C	B2C

[219] SCHWENKE, Mathias. *Individualierung und Datenschutz*. Wiesbaden: Deutscher Universitäts-Verlag, 2006, p. 58.
[220] Idem Ibidem, p. 58 (tradução livre).
[221] Significa "Business to Business", isto é, a relação entre duas ou mais empresas.

individualizacao é preponderantemente utilizada				

2.3.3 A circulação de dados pessoais: a "indústria" de bancos de dados

Nos tópicos anteriores, foram analisadas duas fases do tratamento de dados pessoais que podem constituir graves ameaças ao consumidor-cidadão: a fase da coleta dos dados e a de seu processamento e refinamento por meio de modernas tecnologias da informação. Passaremos agora a analisar o terceiro momento desse tratamento, que se refere à fase de circulação dos dados pessoais na sociedade.

Diante da importância que o conhecimento sobre os consumidores adquiriu na economia atual, os dados pessoais tornaram-se capital essencial para o sucesso de inúmeros negócios. Assim, no contexto da economia de produção flexível, emerge uma verdadeira "indústria de bancos de dados"[223], nos termos de Daniel Solove, cuja finalidade principal é a de propiciar aos setores interessados os dados pessoais de categorias de consumidores, por meio da comercialização ou cessão. O resultado é a ampla circulação das informações pessoais na sociedade, gerando benefícios aos setores envolvidos, mas também grandes riscos aos consumidores, cujos dados são coletados, processados e transferidos.

A comercialização dos dados pessoais não é a única forma de ensejar a circulação desses dados na sociedade. Também o compartilhamento de bancos de dados constitui uma prática comum entre empresas do mesmo grupo empresarial ou que possuam atividades complementares. É o que ocorre com a Rede de Informações e Proteção ao Crédito (RIPC), composta pela Confederação Nacional de Lojistas, Associação Comercial de São Paulo,

[222] Significa "Business to Consumer", ou seja, a relação entre uma empresa e o um consumidor (relação de consumo).
[223] SOLOVE, Daniel. *The Digital Person. Technology and Privacy in the Information Age.* New York: New York University Press, 2004, p. 19.

Clube de Diretores Lojistas do Rio de Janeiro e Associação Comercial do Paraná, para o compartilhamento de dados sobre consumidores inadimplentes.

Pode-se dizer que processamento de dados pessoais é realizado por quase todos setores da economia, como empresas de telefone, bancos, financeiras, associações de empregadores, sindicatos de trabalhadores, empresas de transporte, diversas empresas varejistas, armazéns, farmácias, empresas de marketing direto e de telemarketing, serviços e proteção ao crédito, companhias de seguro, profissionais liberais, como advogados e psicólogos, agências de viagem, organizações de caridade, hotéis, entre outros.[224]

Assim, ao lado das empresas que coletam dados dos seus clientes em razão da necessidade dos serviços oferecidos, surgem também empresas cuja única finalidade é a coleta e o armazenamento da maior quantidade possível de dados pessoais para a sua comercialização e cessão. ChoicePoint, Acxiom e LexisNexis são três das maiores empresas, nos EUA, cuja única finalidade é a comercialização de dados. Existem muitas outras empresas que compõem esta indústria. A base de dados da indústria fornece dados às empresas de marketing, ao governo, ao setor privado, aos credores para verificações de crédito, e aos empregadores para controle sobre os antecedentes.

O tema da transferência, cessão, comercialização ou compartilhamento de dados pessoais é complexo e polêmico à luz dos princípios da proteção de dados e do regime de proteção e defesa do consumidor. Isso ocorre porque os riscos advindos da coleta e do processamento de dados indevidos podem se multiplicar infinitamente, caso essas informações sejam repassadas a terceiros. Afinal, se essas informações circulam na sociedade, de forma equivocada, sem se constituir em uma representação fidedigna do consumidor, a sua liberdade e a igualdade de acesso aos bens de consumo estarão sendo gravemente violadas.

Nesse sentido, compreende-se da mesma forma como Philip Agre que "a extrema falta de transparência da transferência de dados pessoais na sociedade enseja à questão um caráter

[224] FLAHERTY, David. "Visions of Privacy: past, present and future." In: BENNETT, Colin. *Visions of Privacy*. Op. Cit., p. 33.

nebuloso. Os cidadãos sabem que a circulação de informações computadorizadas sobre eles, mas geralmente não conseguem reconstruir as conexões de causa e efeito."[225]

A complexidade da questão reside também na necessidade de se equilibrar tanto a proteção adequada à privacidade, liberdade e igualdade do consumidor, como também a livre iniciativa das empresas e o desenvolvimento dos setores empresariais, que dependem, em uma sociedade com economia flexível, da informação como um dos principais insumos da produção. Nesse sentido, prevê o Código de Defesa do Consumidor, em seu art. 4º, III, a necessidade de "(...) harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico (...)".

No mesmo sentido, a Diretiva Européia 95/46/CE busca harmonizar ambos os aspectos e prevê a livre circulação dos dados pessoais entre órgãos do governo e entre empresas, localizados nos países da União Européia, bem como entre aqueles que assegurem um grau de proteção à privacidade semelhante ao da União Européia. A equivalência de proteção assegurada por um país terceiro deve ser aferida caso a caso, pela Comissão, conforme determina o seu art. 25. Desse modo, a Diretiva determina que a livre circulação dos dados pessoais deve estar condicionada à garantia da proteção da privacidade e da personalidade.

Sob a perspectiva da harmonização, é fundamental estabelecer as hipóteses em que a transferência de dados pessoais será legítima, à luz dos princípios da proteção de dados pessoais. Entende-se que um parâmetro adequado para analisar quando tal transferência será legítima é o estabelecido pela Lei de Proteção de Dados da Espanha (LORTAD), em seu art. 11. A regra geral é de que os dados pessoais somente poderão ser transferidos para o cumprimento de fins diretamente relacionados as funções legítimas da empresa que transfere e da empresa para a qual os dados são transferidos, com o prévio consentimento do

[225] AGRE, Philip. Introduction. In: AGRE, Philip e ROTENBERG, Marc (Ed). *Techonology and Privacy: The New Landscape*. Op. Cit., p. 6 (tradução livre).

consumidor. Tal consentimento prévio somente será dispensado se determinado por lei, se os dados forem acessíveis ao público, se a transferência for realizada com base em uma relação jurídica ou se o seu objeto for relativo à saúde e a situação for urgente. O consentimento, que é revogável, somente será válido se a empresa para a qual forem transferidos os dados for determinada ou determinável e se a finalidade da transferência estiver expressa. Caso contrário, ela será nula. É importante que nas hipóteses de dispensa do consentimento, o consumidor seja notificado da cessão.[226]

Conclui-se, portanto, que a cessão de dados pessoais entre empresas somente será válida na hipótese de plena transparência do processo de cessão de dados pessoais e consentimento expresso e válido do consumidor para a sua realização.

2.4. A quem pertencem os dados pessoais?

[226] Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal - ley 5/1992
Artículo 11. Cesión de datos
1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.
2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando una Ley prevea otra cosa.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas.
e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.
3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.
4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.
5. El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.
6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

"A quem pertencem os dados pessoais?"[227] – é a pergunta de Simson Garfinkel com a qual nos ocuparemos neste tópico. Na economia global, a informação torna-se capital essencial e adquire um expressivo valor no mercado. Nesse contexto, sabe-se que os dados pessoais tornaram-se objeto de valor na sociedade, existindo um verdadeiro mercado para as informações pessoais.

Garfinkel narra um interessante caso, ocorrido em 1995 nos EUA, de uma pessoa que, ao receber um marketing direto, via correspondência, questiona a empresa sobre como ela tinha conhecimento de seu endereço, vez que nunca havia firmado qualquer contrato com ela. Em resposta, a empresa afirmou que havia alugado as suas informações pessoais de uma revista e que, por isso, teria adquirido o direito de usá-las uma única vez[228].

Diante do fato de que as informações pessoais são comercializadas em grande escala no mercado, desenvolveu-se um debate na doutrina acerca da possibilidade de se garantir um direito de propriedade sobre os dados pessoais, sob o pretexto de que o direito tem de se adequar à realidade e ao fato social[229]. Naturalmente, o que está em jogo não é a discussão sobre "se o direito deve se adequar ao mercado ou se este deve se adequar ao direito". Ao contrário, entende-se que o cerne do debate reside nos potenciais danos que a comercialização dos direitos da personalidade, em especial o da privacidade, podem acarretar aos princípios fundamentais do direito, como a dignidade humana e a proteção da personalidade[230].

O fundamento da concepção proprietária do direito à privacidade reside no pragmatismo da teoria conhecida como *Law and Economics*, cujo expoente é Richard Posner. Tal teoria consiste no estudo das dimensões econômicas de problemas jurídicos e tem como

---

[227] Expressão utilizada por GARFINKEL, Simson, *Database Nation* Op. Cit., p. 177.

[228] GARFINKEL, Simson, *Database Nation* Op. Cit., p. 177.

[229] CF: POSNER, R. (1978). An Economic Theory of Privacy. Regulation(May/June), 19-26 e POSNER, R. (1978). The Right of Privacy. Georgia Law Review, 12, 393-422.

[230] BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Tübingen: Mohr Siebeck, 2006, p. 187.

característica o fato de privilegiar o ponto de vista da maximizacão da riqueza da sociedade.[231]

Lawrence Lessig, um dos conhecidos defensores de um direito de propriedade sobre os dados pessoais, argumenta que, em razão do alto valor desses dados, há um grande incentivo para que eles sejam comercializados no mercado. No entanto, essa comercialização acarreta custos decorrentes de externalidades negativas, isto é, a violação ao direito à privacidade das pessoas que não consentiram na transmissão de seus dados. Para minimizar esses danos, ele defende que tal custo seja internalizado por quem usa o dado, exigindo que ele pague por isso[232].

No entanto, deve-se atentar para os reais efeitos de se conceber o direito à proteção de dados pessoais como um direito de propriedade. Compreende-se que tal fato acarretaria três graves problemas.

Primeiramente, entende-se que esse modelo de mercado violaria o princípio da igualdade, entendido, em termos formais, como a distribuição de iguais liberdades a todos os cidadãos. Na hipótese de existir um direito de propriedade sobre os dados pessoais, poder-se-ia inferir que apenas parte da população usufruiria desse direito, provavelmente a parcela mais abastada da sociedade, ou no mínimo, a que tenha condições de optar pela proteção dos seus dados pessoais em detrimento da remuneração a ser paga pelo interessado em utilizá-lo.

---

[231] DWORKIN, Ronald. *Uma questão de princípio.* São Paulo: Martins Fontes, 2000, p. 352.

[232] "The intuition is this: Data is an asset. It is a resource which has become extremely valuable. And as it has become extremely valuable, commerce has tried to exploit it. This use has a cost — an externality born by those who would rather this data not be used. So the trick is to construct a regime where those who would use the data internalize this cost. A regime to assure that they pay for this cost. The laws of property are one such regime. If individuals can be given the rights to control their data, or more precisely, if those who would use data had first to secure the right to use it, then a negotiation could occur over whether, and how much, data should be used. The market, that is, could negotiate these rights, if a market in these rights could be constructed." (LESSIG, Lawrence. The Architecture of Privacy, Draft 2, p. 17, Artigo apresentado na Conferência Taiwan Net '98, Taipei, Março de1998. Acessível em http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf , acessado em 16/01/2008, 20:40)

O segundo argumento diz respeito à supressão da individualidade e o surgimento de indivíduos direcionados ao mercado ("*market-oriented*")[233]. Isso poderia ocorrer na medida em que a procura pelas empresas por dados pessoais com determinadas características poderia induzir os indivíduos a forjarem a sua personalidade e a realizar determinados tipos de atividades de modo a se conformar ao que o mercado deseja. Isto é, as pessoas poderiam moldar a sua personalidade para moldar os seus dados, e assim conseguir melhores condições de comercialização de suas informações pessoais, acarretando, ao final, um nivelamento da individualidade[234].

O terceiro argumento está relacionado aos anteriores e diz respeito à ameaça ao princípio da democracia que o desenvolvimento de um direito de propriedade sobre os dados pessoais poderia acarretar. Tal afirmação baseia-se na idéia de que a efetividade da democracia constitucional tem como fundamento a proteção da liberdade e da igualdade dos cidadãos, bem como de sua personalidade, que seriam afetados, caso essa hipótese fosse implementada, conforme demonstrado nos argumentos anteriores. A partir do momento em que a proteção dos dados pessoais passa a ser substituída por um modelo de mercado, nem todos os cidadãos teriam mais a garantia de proteção de sua personalidade e privacidade, ameaçando o próprio funcionamento da democracia como um todo. Afinal, em uma sociedade em que nem todos os cidadãos têm controle sobre as suas informações pessoais conhecidas por outras pessoas, o exercício da democracia poderia ficar ameaçado, em razão do estado de vigilância e de medo trazido por essa situação[235].

Percebe-se, portanto, que ao se tratar o direito à privacidade e aos dados pessoais sob a perspectiva do direito de propriedade, poder-se-ia provocar sérios riscos à dignidade humana, à personalidade e, por fim, ao próprio Estado democrático de direito.

---

[233] PEIFER, Karl Nikolaus, *Individualität im* Zivilrecht. Tübingen, 2001, apud BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Op. Cit., 188.

[234] BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Op. Cit., 190.

[235] Idem, Ibidem, p.192.

Sabe-se, no entanto, que a polêmica acima mencionada deve ser observada com bastante cautela. Afinal, o que ocorre atualmente, no setor privado, mesmo sob a perspectiva de um direito de personalidade, é que as empresas oferecem facilidades de consumo, somente em troca do cadastro das informações pessoais dos consumidores. Assim, percebe-se que, em alguma medida, os dados pessoais já são negociados indiretamente no mercado de consumo e que o exercício da liberdade de escolha do consumidor, muitas vezes, pode gerar o não recebimento de benefícios e, inclusive, a dificuldade de acesso a determinadas facilidades do mercado, como promoções e descontos.

3.
TUTELA JURÍDICA E DIÁLOGO DAS FONTES: A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO

Como visto, na economia atual, caracterizada pela flexibilidade e customização da produção, bem como pela avidez das empresas por informações pessoais, inúmeras são as ameaças à privacidade nas relações de consumo. Nesse sentido, diante do processamento de dados pessoais dos consumidores pelas empresas, é fundamental analisar quais os mecanismos jurídicos necessários para o estabelecimento do equilíbrio entre ambos.

O tratamento de dados pessoais no âmbito do relacionamento entre o consumidor e a empresa consiste numa relação de direito privado, mais especificamente, uma relação de consumo, sujeita a uma pluralidade de normas do ordenamento jurídico, como a Constituição federal, o código de defesa do consumidor e o regime legal de proteção de dados pessoais. Essas normas, aplicáveis concomitantemente, devem ser interpretadas de forma harmônica e dialógica, buscando a convivência entre esses paradigmas.

Trata-se do diálogo das fontes, que constitui um modelo de aplicação simultânea de fontes normativas diversas, adequado aos atuais fenômenos jurídicos complexos, não mais passíveis de serem resolvidos à luz da regras de conflitos de leis no tempo (ab-rogação, derrogação e revogação). Conforme explicado por Cláudia Lima Marques, o diálogo das fontes é "a atual aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o CDC, a lei de seguro-saúde) e gerais (como o CC/2002), com campos de aplicação convergentes, mas não mais iguais."[236]

Este capítulo tem como finalidade examinar quais os mecanismos jurídicos existentes para proteger o consumidor cujos dados pessoais são coletados e processados. Objetiva-se analisar, portanto, quais normas incidem sobre a atividade de processamento de dados pessoais realizada no âmbito de uma relação de consumo. Primeiramente, ver-se-á, de que forma a Constituição federal se aplica a essa relação. Em seguida, será analisado o Código de Defesa do Consumidor e as suas normas referentes à privacidade. Por fim, será examinado o modo como o regime legal de proteção de dados pessoais se aplica ao caso e como ele se articula com as demais legislações.

3.1. Constituição federal

Cabe analisar, primeiramente, a incidência da Constituição federal sobre o processo de tratamento de dados pessoais pelas empresas. Isto é, examinaremos as normas e princípios constitucionais que dizem respeito aos direitos fundamentais, como privacidade, liberdade, igualdade e dignidade humana, e aos princípios que asseguram uma ordem econômica justa e equilibrada.

[236] MARQUES, Cláudia (et al). Manual de Direito do Consumidor. São Paulo: Ed. Revista dos Tribunais, p. 85. A autora explica a razão do termo diálogo: "'Diálogo' porque há influencias recíprocas, 'diálogo' porque há aplicação conjunta de duas normas ao mesmo tempo e ao mesmo caso, seja complementarmente, seja subsidiariamente, seja permitindo a opção pela fonte prevalente ou mesmo permitindo uma opção das leis em conflito abstrato – uma solução flexível e aberta, de interpenetração, ou mesmo a solução mais favorável ao mais fraco da relação (tratamento diferente dos diferentes)" - p. 87 e 88.

A Constituição é o ordenamento jurídico fundamental do Estado e da sociedade, que constitui e limita os processos de poder.[237] A partir de suas características procedimentais, ela configura um sistema de direitos fundamentais que institucionaliza os pressupostos de comunicação necessários à autodeterminação democrática dos cidadãos. [238] Segundo uma compreensão dinâmica da Constituição, esta constitui um projeto inacabado, sempre sujeito a alterações interpretativas, que refletem um processo de aprendizagem falível.

A Constituição prevê diversas disposições que se relacionam à proteção da privacidade e dos dados pessoais, como a inviolabilidade da vida privada e da intimidade (art. 5º, X), a proibição da interceptação de comunicações telefônicas, telegráficas ou de dados (art 5º, XII), a vedação da invasão de domicílio (art. 5º, XI) e de correspondência (art. 5º, XII) e a possibilidade de impetração do *habeas data* (art. 5º, LXXII).

Além desses direitos, a proteção de dados pessoais envolve também os direitos fundamentais à liberdade e à igualdade, que estão previstos constitucionalmente e são de extrema relevância para essa temática. Como visto, os maiores riscos do tratamento de dados dos consumidores pelas empresas são a violação da igualdade, como a discriminação do consumidor no mercado em razão de dados sensíveis e da liberdade, como, por exemplo, quando ocorre a limitação de seu acesso a bens e serviços a partir de informações incorretas.

Historicamente, a Constituição do paradigma liberal regulava as relações entre o Estado e os cidadãos, abstendo-se de regulamentar as questões relativas ao mercado. No entanto, esse quadro é alterado com o advento do Estado Social, no qual a Constituição passa a ser vista como um instrumento de regulação de toda a sociedade, inclusive da economia. Seguindo esse conceito, é promulgada a Constituição federal de 1988, que, em razão de seu caráter social, ampliou o conceito e o alcance da idéia de Constituição no Brasil.

---

[237] HÄBERLE, Peter. Incursus. Perspectiva de uma doctrina constitucional del marcado: siete tesis de trabajo. In: HÄBERLE, Peter. *Nueve ensayos constitucionales y na lección jubilar.* Trad.: Luciano Parejo Alfonso e outros. Lima: Palestra Editores, 2004, p. 103.

[238] HABERMAS, Jürgen. *Direito e democracia: entre facticidade e validade.* Vol. II. Trad. Flávio beno Siebeneichler. Rio de Janeiro: Tempo Brasileiro, 1997, p. 119.

Nesse contexto, uma mudança importante diz respeito à eficácia dos direitos fundamentais, que passa a compreender, além da eficácia sobre a relação entre os cidadãos e o Estado, uma eficácia também relativa a entes privados. Isso significa que os direitos fundamentais, antes aplicáveis apenas contra órgãos do governo ou de seus representantes, passam a ser compreendidos como direito de eficácia privada, incidentes até mesmo sobre relações entre particulares. É o caso dos direitos à privacidade, à liberdade e à igualdade, que são de extrema relevância para o estudo da violação dos dados pessoais.

O direito à privacidade, como uma espécie de direito à personalidade, constitui um direito tanto de caráter negativo (direito de defesa), como de caráter positivo (direito à prestação). Negativo, por delimitar uma esfera de proteção, que não pode sofrer intervenção do poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito. Positivo, por ensejar também a obrigatoriedade de uma ação do Estado para garantir tal proteção. Assim, por exemplo, exige-se a intervenção estatal ao determinar a obrigatoriedade de prestar informações pelos órgãos que realizam o tratamento dos dados pessoais.

Tendo em vista que o direito à proteção de dados pessoais deriva do direito à privacidade, previsto na Constituição federal, infere-se que a proteção de dados decorre da Constituição brasileira. Isso significa, sob o ponto de vista de seu caráter negativo, que nenhuma lei poderá ser promulgada de modo a eliminar esse direito fundamental, sob pena de vir a ser considerada inconstitucional e ser declarada nula. Ademais, à luz do seu caráter positivo, o direito fundamental à proteção de dados pessoais, reconhecido indiretamente pela Constituição, enseja a obrigatoriedade de ação do Estado para proteger a personalidade, tal como a edição de lei que regulamente o assunto. Nesse caso, compreende-se que o direito é garantido constitucionalmente, mas a sua densificação e conformação dependem da ação estatal.

A Constituição Federal prevê também, além do direito material à privacidade, um direito fundamental processual para o conhecimento e correção de dados pessoais, que é o

habeas data. Este constitui uma ação constitucional, prevista no art. 5º, LXXII, que pode ser impetrada por pessoa física ou jurídica, com a finalidade de assegurar o conhecimento ou a retificação de informações referentes a si própria, presentes nos registros e bancos de dados de entidades governamentais ou de caráter público. A Lei nº. 9.507/97 regulamentou o direito ao *habeas data* no Brasil e estabeleceu o seu procedimento.

O *habeas data* foi concebido como intrumento para possibilitar às vítimas do regime militar conhecerem arquivos e registros a seu respeito. Esse objetivo restrito que permeou o surgimento e o desenvolvimento do *habeas data* talvez tenha contribuido para a sua reduzida eficácia e utilização no ordenamento juridico brasileiro.[239] Ademais, outros fatores podem explicar a sua pouca utilização no país. Primeiramente, a sua redação nao impõe qualquer limite ao armazenamento e ao tratamento de dados, pressupondo, portanto, que tais processos são legítimos *per se*. Segundo, tendo em vista que ele nao prevê a possibilidade de exclusão de dados em bancos de dados, ele corrobora com o entendimento de que qualquer armazenamento e tratamento de dados é sempre legítimo.[240] Pode-se dizer também que o seu caráter remedial, possibilitando o acesso aos dados apenas em caso da recusa do banco de dados em fazê-lo, relaciona-se a uma concepção muito liberal de privacidade, pouco condizente com a principiologia da Constituição federal.[241]

Por fim, a reduzida eficácia desse remédio, bem como os poucos julgamentos dessa ação na Justiça brasileira, podem ser explicados a partir do caráter simbólico exercido pela simples previsão da possibilidade de impetração do *habeas data*, sem uma efetiva regulamentação, o que pode ter ofuscado a sua eficácia.[242] Isto é, a força simbólica do direito ao *habeas data* pode ter acarretado uma sensação de que o problema da proteção de dados pessoais no Brasil estivesse resolvido, de modo a desincentivar o seu desenvolvimento e a sua real aplicação em concreto. Assim, concordamos com Danilo Doneda ao afirmar que "o

[239] MENDES, Gilmar (et al). *Curso de Direito Constitucional.* São Paulo: Ed. Saraiva, 2008, p. 543.
[240] Idem, Ibidem, p. 544.
[241] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Op. Cit., p.358.
[242] Idem, Ibidem, p.357.

legislador brasileiro, após a primazia da criação de um modelo que cativa por sua simplicidade, é hoje, em certa medida, seu prisioneiro."[243]

3.2. Código de Defesa do Consumidor

Ao se estudar a proteção de dados pessoais nas relações de consumo, é fundamental examinar, além da Constituição Federal, também a legislação de defesa do consumidor. Afinal, sobre a relação de consumo em que ocorre o tratamento de dados pessoais incide também a legislação infraconstitucional de proteção e defesa do consumidor. Essa legislação, no Brasil, consiste no Código de Defesa do Consumidor – Lei 8.078/90, cujas características e importância para essa temática devem ser analisadas.

O direito do consumidor pode ser compreendido como uma área de saber jurídico que visa disciplinar a ordem econômica.[244] O nascimento desse ramo do direito foi ensejado pelas mudanças sócio-econômicas nos mercados de produção, distribuição e de consumo, especialmente a partir da segunda metade do século XX, com a massificação e despersonalização das contratações.[245] Esse período é identificado com a segunda revolução industrial e constitui-se o momento de apogeu do taylorismo e do fordismo.[246] É nesse período que se amplia, radicalmente, a figura do intermediário entre o fabricante e o comprador. Surge, portanto, de forma generalizada nos países capitalistas avançados, a sociedade de consumo propriamente dita e emerge o conflito entre fornecedor-consumidor,

[243] Idem, Ibidem, p. 360.
[244] JR MACEDO, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor*. São Paulo: Ed. Revista dos Tribunais, 2006, p. 207.
[245] MARQUES, Cláudia Lima (et al). *Manual de Directo do Consumidor*. Op. Cit., p. 34.
[246] Conforme afirma Cláudia Lima Marques, a primeira revolução industrial (do carvão e do aço) caracterizou-se pela massificação da produção e pelo conflito entre capitalista-trabalhador. A segunda revolução industrial é marcada pela evolução da produção e distribuição em massa e os trabalhadores passam a ser considerados também consumidores, pois melhor pagos passam a consumir o que produzem. Já a terceira revolução industrial é considerada a revolução causada pela informática e globalização. (MARQUES, Cláudia Lima (et al). *Manual de Directo do Consumidor*. Op. Cit., p. 37.)

marcado pela desigualdade de posições e informações sobre o produto ou serviço comercializado.[247]

Uma das primeiras evidências de reconhecimento da necessidade de proteção ao consumidor veio na Inglaterra, no período do pós-guerra, com a criação do *Molony Committee on Consumer Protection*, em 1959.[248] A função desse comitê era a de avaliar se era necessário e desejável a alteração do direito para ampliar a proteção ao consumidor. O comitê, embora reconhecesse que a estrutura do mercado poderia causar ameaças ao consumidor, fundava-se na premissa de que todas as soluções deveriam ser buscadas no próprio mercado, sob o fundamento de que a concorrência era uma das melhores formas de se proteger o consumidor.

Percebe-se, nesse contexto, o surgimento de uma das concepções de defesa do consumidor mais influentes até hoje, denominada consumerismo econômico[249], que visualiza as demandas dos consumidores sob uma perspectiva meramente econômica. Essa corrente ainda é bastante influente e é vista por alguns como uma forma de conciliar interesses dos consumidores com fornecedores. Conforme afirma Ronaldo Porto Macedo, em alguns países, essa concepção teria sido uma das responsáveis para a expansão do direito do consumidor, por buscar a conciliação de interesses, ao invés do conflito.

A partir dos anos 60, essa concepção econômica do direito do consumidor sofre algumas alterações, na medida em que a economia massificada começa a demonstrar os potenciais riscos à saúde e à segurança do consumidor que ela pode acarretar, como no caso da tragédia da Talidomida[250]. Assim, outras questões, como a ameaça à saúde, também são incluídas na agenda do movimento de defesa do consumidor. Como afirma Porto Macedo:

---

[247] JR MACEDO, Ronaldo Porto. *Contratos R*[247] JR MACEDO, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor.* Op. Cit., p. 207.

[248] Idem, Ibidem, p. 208.
[249] Idem, Ibidem, p. 208.
[250] A Talidomida foi associada a um dos mais horríveis acidentes de consumo da história. Ela chegou ao mercado pela primeira vez na Alemanha em 1957 e foi comercializada como um sedativo e hipnótico com poucos efeitos colaterais. A indústria farmacêutica que a desenvolveu acreditou que o medicamento era tão seguro que era propício para prescrever a mulheres grávidas, para combater enjôos matinais. Foi rapidamente prescrito a milhares de mulheres e espalhado para diversos países. Os procedimentos de testes da substância não

> A questão da defesa do consumidor passava a paulatinamente associar-se direta e intimamente com valores e interesses não exclusivamente econômicos do consumidor. A saúde é, provavelmente, o mais notável destes interesses, mas não será o único, conforme ficará patente nas legislações de proteção e controle da publicidade enganosa e ofensiva a valores educativos, morais, meio ambiente, etc.[251]

Na década de 70, vê-se o apogeu do desenvolvimento das leis de proteção ao consumidor nos países com economias capitalistas avançadas, juntamente com o desenvolvimento de medidas de regulação econômica em outras áreas, como o meio ambiente, a saúde e a antitruste.[252] Entre as medidas adotadas, no âmbito da defesa do consumidor, podem-se citar a criação de leis que ampliam o limite da responsabilidade criminal e civil do fornecedor, a formação de uma burocracia especializada na defesa do consumidor e a ampliação do papel da justiça de primeira instância para a implementação da legislação de defesa do consumidor. Nesse sentido, percebe-se como o direito do consumidor constitui-se em uma das vertentes do direito social e do processo de intervenção estatal na economia.

No fim da década de 70, com a crise econômica mundial, altera-se o contexto da defesa do consumidor em razão da ascensão da ideologia neoliberal, de mínima intervenção estatal na economia. Esse é o cenário que predomina nas décadas de 80 e 90, com uma forte reação à regulação do mercado e à intervenção do Estado.

Não obstante essas alterações nas concepções da defesa do consumidor a partir das transformações sócio-econômicas, podem-se identificar alguns traços comuns e fundamentos nos movimentos de defesa do consumidor, o chamado consumerismo, *lato sensu*. O consumidor é reconhecido como um sujeito universal de direitos a partir da constatação de um traço comum entre eles, qual seja, a sua vulnerabilidade em face aos produtores. Assim, apesar das diferentes formas de contratação e dos mais variados tipos de ambientes em que os consumidores podem estar inseridos, a vulnerabilidade do consumidor pode ser observada a

---

revelaram seus efeitos teratogênicos. No final dos anos 1960, foram descritos na Alemanha, Reino Unido e Austrália os primeiros casos de malformações congênitas. Somente quando já havia milhares de casos de defeitos congênitos a ela associados em todo o mundo, a Talidomida foi removida da lista de remédios indicados.

[251] JR MACEDO, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor*. Op. Cit., p. 209.

[252] Idem Ibidem, p. 208.

partir da diferença de poder entre consumidores e produtores. Desse modo, a legislação de proteção ao consumidor emerge como o instrumento para contrabalancear o poder dos produtores e dos consumidores, reequilibrando a relação, ao reforçar a posição do consumidor ou limitar determinadas condutas do fornecedor.

A necessidade da tutela jurídica e da intervenção do Estado para a proteção do consumidor reside no fato de que o mercado, ao invés de contribuir para a superação da vulnerabilidade do consumidor, na realidade, acaba por fazer o contrário: reforça a sua vulnerabilidade e o desequilíbrio em face dos fornecedores. O mercado propicia o acesso desigual à informação, que implica relações de poder no seu interior e que reflete, por conseqüência, as relações de poder na sociedade. Assim, ele deve ser visto não como um espaço naturalizado e neutro para escolhas voluntárias e livres, mas como uma ordem de poder e riqueza, moldada a partir dos mecanismos legais e regulatórios instituídos.[253]

Nessa ótica, o mito do *"laissez faire"*, isto é, a concepção de que uma economia de livre mercado não necessita de qualquer intervenção estatal para o seu funcionamento, na medida em que a oferta e a demanda seriam capazes de regular o mercado, não subsiste. O livre mercado requer, para a sua existência, mais do que tal noção aparenta: ele exige, por exemplo, uma legislação que proteja a propriedade e que estabeleça sanções para invasões, bem como normas que prevejam a liberdade de contratar e a vinculação do contrato, etc. Nesse sentido, concordamos com Cass Sunstein:

> A noção de 'laissez-faire'é uma descrição grotesca e errônea do que realmente o livre mercado necessita e requer. O livre mercado depende da existência de normas. Não há como se ter propriedade privada sem regras legais, dizendo às pessoas quem é proprietário, impondo penalidades para a transgressão e dizendo quem pode fazer o que a quem. Sem a norma que estabelece o contrato, a liberdade contratual, do modo como conhecemos, seria impossível. (...) Ademais, a legislação que fundamenta o livre mercado é coercitiva no sentido de que, além de facilitar as transações

[253] É o que afirma Ronaldo Porto Macedo, "(...) os mecanismos legais que atuam no mercado de trocas acabam de uma maneira ou de outra por impor um determinado resultado distributivo, o qual variará significativamente conforme o arranjo institucional e jurídico que moldar este mercado. (...) As ordens de mercado variam conforme as diversas estratégias regulatórias, restrições ao comércio de ações, estímulos a poupanças internas e investimentos diretos, salário mínimo e direitos trabalhistas mais ou menos ampliados, garantias ao direito do consumidor (...) orientação para o mercado externo global ou mercado nacional etc." (JR MACEDO, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor.* Op. Cit., p. 49.)

> individuais, ela impede as pessoas de realizarem diversas ações que gostariam de realizar. Esse ponto não é uma crítica ao livre mercado. Mas sugere que os mercados devem ser entendidos como uma construção legal, a serem compreendidos como promotores de interesses humanos e não como partes da ordem natural ou da natureza, ou como um meio simples de possibilitar ações voluntárias.[254]

O sistema de livre mercado é visto, muitas vezes, como um sistema que promove tanto liberdade, como igualdade: liberdade de contratar e igualdade de oportunidades. Ocorre, no entanto, que o livre mercado pode acarretar exatamente o contrário. As mesmas normas que estabelecem a liberdade de agir sob algumas esferas, determinam também, de forma coercitiva, a limitação da liberdade em outros âmbitos, como a sanção à invasão da propriedade ou a impossibilidade de apropriação em diversas circunstâncias. Do mesmo modo, a igualdade pode ser seriamente afetada pelo livre mercado, principalmente quando há fortes incentivos econômicos voltados para a discriminação dos trabalhadores e de consumidores, em razão de raça ou gênero. Por exemplo, no mercado de consumo, em que se limita a entrada de consumidores negros em lojas de varejo, quando os clientes da loja não gostam de freqüentá-la com outros clientes negros; ou na hipótese do mercado de trabalho, em que hospitais não contratam médicas mulheres, pelo fato de seus pacientes preferirem ser atendidos por médicos homens. Nessas hipóteses, a pressão do mercado, ao invés de eliminar a discriminação, irá ampliá-la; e os fornecedores ou empregadores que optarem por agir de forma não discriminatória sofrerão prejuízos, ao invés de receber recompensa.[255]

Segundo Sunstein:

> (...) Diversos estudos demonstraram que o mercado, muitas vezes, desvaloriza os produtos e os empreendimentos de ambos, negros e mulheres. Isso não deveria surpreender. Em um sistema com um significativo preconceito contra negros e mulheres, oculto e manifesto, consciente e inconsciente, o critério 'a vontade de pagar' – do modo como se reflete nas decisões de compra e venda de empregadores, empregados, consumidores e outros – irá assegurar que aqueles que estão sujeitos a atitudes discriminatórias estejam em desvantagem comparativa no mercado. (...) Nesse contexto, a constatação inicial é de que quando a discriminação é o problema, o mercado raramente é a solução.[256]

[254] SUNSTEIN, Cass. *Free Markets and Social Justice.* New York: Oxford University Press, 1997, p. 5.
[255] Idem, Ibidem, p. 153.
[256] Idem, Ibidem, p. 152.

Desse modo, o autor argumenta como os mercados podem criar incentivos econômicos para a discriminação, tornando difícil a garantia da igualdade unicamente pelo próprio mercado. É em razão disso, que se faz necessária a regulação estatal para combater a discriminação e promover a igualdade entre os agentes do mercado.

Assim, constata-se a necessidade de intervenção estatal até mesmo para a manutenção da liberdade e igualdade no mercado de consumo, ao contrário do que proclamado pela doutrina do "laissez-faire". Após essa breve análise da importância da regulação do Estado sobre a economia, é relevante examinar de que forma essas questões foram enfrentadas no mercado de consumo do Brasil, a partir do Código de Defesa do Consumidor.

Sob a ótica da necessidade de regulação do mercado, foi promulgado o Código de Defesa do Consumidor brasileiro - Lei 8.078/90 - com o intuito de equilibrar a relação entre fornecedores e consumidores, estabelecendo um regime civil diferenciado para as relações de consumo e buscando assegurar tanto a liberdade, quanto a igualdade no mercado de consumo. A partir do amplo debate durante o período de redemocratização, o fundamento para a aprovação do Código restou estabelecido na própria Constituição federal de 1988, que em seu Ato das Disposições Transitórias, art. 48, determinou que o Código de Defesa do Consumidor seria elaborado no período de 120 dias da promulgação da Constituição. Ademais, a Constituição identificou o consumidor como sujeito de direitos a ser protegido de forma especial pela ação estatal, ao estabelecer um direito fundamental positivo de que "o Estado promoverá, na forma da lei, a defesa do consumidor" (art. 5º, XXXII). A Carta fundamental previu também a defesa do consumidor como um dos princípios da ordem econômica livre e justa (art, 170, V).

O anteprojeto do Código de Defesa do Consumidor foi o resultado do trabalho do Conselho Nacional de Defesa do Consumidor – CNDC, junto ao Ministério da Justiça, criado em 24 de julho de 1985, que reuniu diversos especialistas no período de redemocratização do

país.[257] A principal influência para a sua elaboração foi o Projeto Calais-Auloy de Código de Consumo (*Projet de Code de la Consommation*), mas outras influências residem nas leis de gerais de proteção ao consumidor da Espanha, de Portugal, do México e do Québec, além de normas dos EUA. Enfim, como afirma Cláudia Lima Marques, o Código de Defesa do Consumidor "apresenta-se como uma obra comparatista, atualizada para o século XXI, com permeabilidade e criatividade. Adaptou conceitos indeterminado, incluiu normas narrativas e cláusulas gerais, e assim permitiu um desenvolvimento jurídico original (*Rechtsforbildung*) do direito privado brasileiro."[258]

Embora se possa afirmar que o Código de Defesa do Consumidor tenha sido o resultado de um "compromisso possível" [259] entre interesses políticos divergentes, como é o caso da maioria das leis, pode-se extrair dele uma proteção ao consumidor bastante forte e consistente, baseada em princípios e direitos básicos, que protegem além da esfera econômica, a esfera da personalidade do consumidor.

Assim, o Código estabelece um regime de proteção integral do consumidor, por meio do estabelecimento da Política Nacional de Relações de Consumo, pautada no atendimento das necessidades dos consumidores, na proteção de sua dignidade, na defesa de seus interesses econômicos, na melhoria da sua qualidade de vida, bem como na harmonia e na transparência das relações de consumo (art. 4º, caput).

Ademais, o Código estabelece princípios fundamentais que devem nortear as ações de todos os atores das relações de consumo, tais como o reconhecimento da vulnerabilidade do consumidor (art. 4º, I), a garantia de serviços e produtos com padrões com qualidade,

[257] MARQUES, Cláudia Lima. (*et. al.*) *Manual de Direito do Consumidor.* Op. Cit. p. 48.
[258] Idem, Ibidem, p. 49.
[259] Como afirma Ronaldo Porto Macedo, "De um modo geral, portanto, ainda que se reconheça a existência de diferenças ideológicas não apenas entre os grupos de defesa do consumidor, como também entre as diversas legislações protetivas do consumidor, a versão dominante da legislação de proteção ao consumidor acabou por ser aquela resultante de um certo compromisso "possível"entre interesses politicamente representados preocupados primordialmente com o estabelecimento de regras para o melhor funcionamento do mercado i.e. a imposição de 'boas maneiras ao mercado'. Esta acabou sendo a linha de menor resistência para a implementação da defesa do consumidor na maioria dos países capitalistas e o Brasil, neste aspecto, não parece ter sido exceção." (JR MACEDO, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor.* Op. Cit., p. 216.)

segurança, durabilidade e desempenho (art. 4º, II, d) e o incentivo à criação pelos fornecedores de meios eficientes de solução de conflitos (art. 4º, V). Podem-se citar também os importantes direitos básicos previstos no Código, como a proteção da vida, saúde e segurança (art. 6º, I), a proteção contra práticas abusivas (art. 6º, IV), a efetiva prevenção e reparação de danos morais (art. 6º, VI), o acesso aos órgãos judiciários e administrativos (art. 6º, VII), bem como a inversão do ônus da prova pelo juiz em alguns casos (art. 6º, VIII).

O princípio da vulnerabilidade é um dos mais relevantes consagrados pelo Código, na medida em que consiste no reconhecimento do estado de risco e fragilidade do sujeito de direitos inserido no mercado de consumo.[260] É a partir desse reconhecimento que o Código de Defesa do Consumidor é capaz de estabelecer um regime diferenciado para reequilibrar os poderes na relação de consumo. Nos termos de Cláudia Lima Marques, "a igualdade perante a lei e a igualdade na lei só podem realiza-se hoje, no direito privado brasileiro, se existir a distinção entre fracos e fortes, entre consumidor e fornecedor (...)".[261]

Ao se examinar o tratamento de dados pessoais realizado no âmbito da relação de consumo, é fundamental se considerar a vulnerabilidade do consumidor nesse processo. Isso porque, os dados pessoais, assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização. O risco ao consumidor que tem os seus dados coletados e processados ocorre, principalmente, quando o tratamento dos dados é realizado de forma equivocada ou discriminatória, acarretando a sua classificação e discriminação no mercado de consumo. Isso acaba por afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais.

Nesse contexto, é fundamental levar-se em conta a vulnerabilidade do consumidor, tanto técnica, por possuir menos informações que o fornecedor a respeito do fluxo de seus

[260] MARQUES, Cláudia Lima. (*et. al.*) Comentários ao Código de Defesa do Consumidor. São Paulo: Ed. Revista dos Tribunais, 2006, p. 144.
[261] Idem, Ibidem, p. 33.

dados, como fática, por possuir menos recursos intelectuais e econômicos para a reparação de prejuízos advindos do tratamento de dados.[262] Tal vulnerabilidade é patente, principalmente se contrastada com outras hipóteses de tratamento de dados pessoais no setor privado, por exemplo, quando ele ocorre em uma relação entre empresas (*business to business*). Essa situação de empresas buscarem dados de outras empresas é bastante comum no mercado, tendo em vista a busca constante pela diminuição de riscos. Nesses casos, naturalmente, trata-se de uma relação civil, entre iguais, e não de uma relação de consumo.

Assim, tendo em vista a desigualdade das partes no âmbito da relação de consumo, e a patente vulnerabilidade do consumidor, é fundamental que se assegurem tanto no âmbito administrativo, quanto no judicial, mecanismos de proteção especial ao consumidor cujos dados pessoais são objeto de coleta, processamento e transferência.

Como se pode perceber, o Código de Defesa do Consumidor permite, a partir dos princípios e direitos nele consagrados, uma interpretação da defesa do consumidor em termos mais protetivos e não baseada apenas no funcionamento adequado do mercado. Além da tutela econômica, o Código prevê uma tutela da personalidade do consumidor. Como afirma Eduardo Bittar:

> (...) deve-se dizer que os direitos do consumidor albergam, em sua textura, direitos da personalidade. São, mais propriamente, em parte, e não em sua totalidade, concretização de direitos da personalidade. Prova disto é a extensa previsão legal existente, que garante ao consumidor a salvaguarda dos valores que o cercam na situação de consumo todos protegidos legalmente (direito à vida, à saúde, à higidez física, à honra) e devidamente instrumentalizados (ação de reparação por danos materiais e morais, ações coletivas para proteção de direitos difusos, procedimentos administrativos...)[263]

[262] Cláudia Lima Marques descreve três tipos de vulnerabilidades: técnica, fática e jurídica. (MARQUES, Cláudia Lima. (*et. al.*) *Comentários ao Código de Defesa do Consumidor*. Op. Cit., p. 144.)
[263] BITTAR, Eduardo C. B, Direitos do consumidor e direitos da personalidade: limites, intersecções, relações. In: *Revista de Direito do Consumidor*, 37, ano 10, janeiro-março de 2001, p. 198 e 199.

Desse modo, pode-se perceber como a arquitetura do Código de Defesa do Consumidor propicia, a partir dos direitos nele consagrados, um amplo espaço de respeito à pessoa humana, no âmbito da relação de consumo.[264]

Além dos direitos à personalidade citados por Bittar, o consumidor também possui, o direito à privacidade, consubstanciado na norma do art. 43, referente aos bancos de dados e cadastros de consumidores. O referido artigo tem o seguinte teor:

> 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.
>
> § 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.
>
> § 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.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 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.

Da leitura do dispositivo, depreende-se que ele autoriza o funcionamento dos bancos de dados e cadastros de consumidores, mas impõe limites à sua existência. Esses limites são os seguintes: necessidade de comunicação da abertura de cadastro ou registro de dados pessoais de consumo (princípio da transparência); obrigação de banco de dados corrigir os dados presentes de forma imediata (direito de acesso e correção), limite temporal para o armazenamento de dados pessoais (direito ao esquecimento). Como se pode perceber, esse artigo, inspirado no *National Consumer Act* e no *Fair Credit Reporting Act*[265], ambos dos Estados Unidos, está em consonância com importantes princípios do regime de proteção de dados pessoais, vistos no capítulo 2.

---

[264] BERTI, Silma Mendes, O Código de Defesa do Consumidor e a protecao dos direitos da personalidade. In: *Revista de Direito do Consumidor*, 23-24, julho-dezembro de 1997, p. 157.

[265] GRINOVER, Ada Pellegrinni. *Código de Defesa do Consumidor comentado pelos autores do anteprojeto.* Rio de Janeiro, Forense Universitária, 2005, p. 400.

Ademais, tal dispositivo prescreve uma importante norma, segundo a qual os bancos de dados e cadastros relativos a consumidores são considerados públicos, com intuito de possibilitar a impetração da ação de *habeas data* e de submeter qualquer registro de dados pessoais ao crivo de legalidade. Esse inteligente dispositivo acarreta, ao final, a impossibilidade de se argumentar que determinada coleta de dados será utilizada para fins estritamente particulares, não estando submetida à legislação; pelo contrário, qualquer armazenamento de dados pessoais, por se referir à personalidade do consumidor, não diz respeito à esfera privada ou empresarial apenas, mas sim ao público e, portanto, a ele se aplica o regime constitucional e legal.

A regulamentação dos limites para o funcionamento de bancos de dados de consumo, prevista no Código de Defesa do Consumidor, é muito relevante, por coibir o mau uso dos arquivos de consumo, que, nos termos de Herman Benjamin, acarreta a violação da privacidade do consumidor, do seu direito à imagem, da sua liberdade de contratar:

> De modo direto, o mau funcionamento dos arquivos de consumo ameaça, primeiramente, o direito à privacidade, por que cada indivíduo pode clamar na esteira da elaboração mais ampla dos direitos da personalidade. (...)
> Além disso, frontalmente ameaçado é o direito à imagem, tão caro nos modelos jurídicos da atualidade. A idoneidade financeira sempre foi – e cada vez mais é – um componente essencial da honorabilidade do ser humano. (...)
> Indiretamente, sofre o direito (=liberdade) de que todos são titulares de livremente contratar no mercado. Ora, uma vez 'negativado', com seu crédito aniquilado, são remotas, para não dizer inexistentes, as possibilidades de o consumidor exercer tal prerrogativa constitucional, pois vivemos num modelo de sociedade – a de consumo – impregnado pela regra de que os bancos de dados têm sempre a última palavra no momento da contratação. (...)
> Por essas e outras razões, vem o legislador e estabelece limites formais e materiais para a coleta, manutenção e divulgação de dados sobre o consumidor. Assinala-se, finalmente, que o registro irregular não viola somente dispositivos do CDC, mas amiúde ofende direitos de índole constitucional.

Não obstante o importante papel exercido pelo Código de Defesa do Consumidor de limitação dos bancos de dados de consumo, sabe-se que a complexa temática da proteção de dados pessoais não se esgota nos princípios assegurados pelo Código. Isso ocorre, porque, em uma sociedade da informação, em que os dados pessoais dos consumidores, trabalhadores e cidadãos passam a ser considerados insumos da produção, somente uma ampla e variada

estrutura jurídica e administrativa é capaz de oferecer os mecanismos necessários para fazer valer os direitos fundamentais do cidadão à privacidade, liberdade e igualdade.

Vejamos, a seguir, de que modo o regime legal de proteção à privacidade pode contribuir para se lograr a proteção da personalidade.

3.3. Regime legal de proteção de dados pessoais

Nos países com capitalismo avançado, o regime legal de proteção de dados pessoais pode ser compreendido como a legislação ordinária, geralmente fundamentada na Constituição, cuja finalidade é a de regular o tratamento de dados pessoais na sociedade. É, portanto, o exercício do poder do Estado para intervir no processamento de dados, buscando preservar a coletividade e os direitos fundamentais dos cidadãos.[266] Essa regulação deve ser considerada não apenas como o controle do Estado sobre a economia ou sobre a sociedade, mas também o controle sobre os seus próprios órgãos que realizam tratamento de dados pessoais.

Muito embora existam diversas formas de se regulamentar a privacidade, como por meio de previsões constitucionais, *privacy torts*, mecanismos contratuais determinados legalmente, nos últimos 30 anos, as leis gerais de proteção de dados pessoais se firmaram como umas das formas mais eficazes de se proteger a privacidade nos países desenvolvidos.[267]

A abrangência dessas normas e o seu âmbito de aplicação variam de país para país, conforme o seu próprio processo político. É possível, no entanto, observar semelhanças e tendências. Como visto, embora o início das legislações de proteção de dados pessoais tenha ocorrido em razão do temor do poder de processamento de dados pelo Estado, logo se viu que o perigo também residia no setor privado. Desse modo, a Diretiva Européia de 1995 orientou

[266] BENNET, Colin e RAAB, Charles. *The governance of privacy.* Op. Cit., p. 125.
[267] Idem, Ibidem, p. 126.

os países a promulgarem leis abrangentes que compreendessem tanto o setor público, quanto o setor privado. Esse movimento acabou por influenciar também países como Canadá e Austrália, que buscaram, cada um dentro de sua estrutura federativa, abarcar também a regulamentação do setor privado.[268] Fora dessa tendência estão apenas os Estados Unidos, que possuem uma regulação abrangente somente para o setor público, não regulamentando o tratamento de dados realizado pelo setor privado. É o que afirma Colin Bennett:

> Os Estados Unidos são agora o único país industrial avançado que ainda não aprovou, nem está em processo de aprovar, uma lei de proteção de dados que abranja também as atividades do setor privado. Embora o *Privacy Act* de 1974 seja um exemplo desse tipo de legislação, ele é aplicado apenas ao governo federal e sua implementação tem sido muito limitada. No âmbito do poder executivo federal, o Departamento de Administração e Orçamento é tido como o supervisor da aplicação da referida lei pelas agências e órgãos do governo. No entanto, não é uma autoridade "empenhada", em contraste com as agências de proteção à privacidade de outros países, e o seu impacto tem sido tanto esporádico, como brando. Nos Estados Unidos, a adoção de legislação geral para o setor privado tem sido fortemente resistida, e embora existam diversas normas setoriais, a privacidade é protegida de uma forma bastante incompleta.[269]

Como visto, percebe-se que o sistema americano de proteção de dados pessoais deixa a desejar, se comparado ao modelo abrangente europeu e que vem sendo, aos poucos, adotado por outros países. Com relação à coexistência de normas setoriais com uma norma geral de proteção à privacidade, essa possibilidade é reconhecida pela Diretiva Européia de 1995, desde que a normas setoriais tenham como finalidade regular setores específicos de forma a complementar a regulação realizada pela lei geral.

A importância do modelo de lei geral reside no fato de que ela constrói uma arquitetura regulatória, capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro setor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação. As leis gerais de proteção de dados pessoais constituíram o meio pelo qual a maioria dos países internalizou em seus ordenamentos jurídicos os princípios consagrados em

[268] Idem, Ibidem, p. 130.
[269] Idem, Ibidem, p. 131 (tradução livre).

instrumentos internacionais (*Fair Information Principles*). Assim, o regime legal de proteção de dados foi o instrumento adequado encontrado para atribuir direitos subjetivos aos titulares dos dados pessoais, bem como para impor limitações e obrigações aos responsáveis pelo tratamento de dados.

Ademais, o regime legal de proteção de dados, na maioria dos países, estabeleceu uma autoridade administrativa competente para fazer cumprir a legislação. A experiência das últimas décadas dos órgãos administrativos de proteção de dados pessoais demonstrou que a existência desses órgãos é essencial para a implementação da legislação e da cultura da privacidade no país:

> A existência de autoridades supervisoras robustas tem sido considerada como condição sine qua non para a adequada proteção à privacidade, visto que as leis não são vistas como auto-implementáveis e que a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine.[270]

Variadas são as funções exercidas pelos órgãos administrativos criados para implementar a política de proteção de dados pessoais nos diversos países. É possível, no entanto, apontar as principais funções por eles exercidas, quais sejam, de ouvidores (*ombudsman*), auditores, consultores, educadores, orientadores de política pública, negociadores, bem como de responsáveis pela implementação e cumprimento da legislação.

3.3.1. Âmbito de aplicação

O âmbito de aplicação do regime legal de proteção de dados, embora convergente nos diversos países europeus, pode variar, em função dos seguintes requisitos: i) se o tratamento de dados pessoais visa a finalidades gerais ou à defesa e à segurança do Estado; ii) se os dados são armazenados para uso estritamente pessoal, para uso da própria empresa ou para fins de comercialização; iii) se a operação visa ao tratamento de dados de pessoa física ou jurídica;

[270] Idem, Ibidem, p. 134 (tradução livre).

iv) se o tratamento dos dados é feito de forma automatizada ou não e; v) se os dados são tratados/armazenados por organismos privados ou públicos.

Ressalta-se que o âmbito de aplicação das leis de proteção de dados pessoais não é estabelecido de modo uniforme nas diversas legislações sobre o tema. Portanto, buscar-se-á demonstrar alguns critérios importantes para a sua delimitação, a partir de exemplos de legislações e da solução adotada pela Diretiva Européia 95/46/CE.

O regime de proteção de dados pessoais proposto pela referida Diretiva exclui de seu âmbito o tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado, o bem-estar econômico do Estado e as atividades do Estado no domínio do direito penal[271]. Além disso, está excluído também desse regime o tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, como, por exemplo, correspondência ou listas de endereços[272]. No entanto, se o tratamento for realizado para fins comerciais da própria empresa, ele não está excluído do regime de proteção de dados pessoais.

Com relação ao âmbito de aplicação subjetivo, pode-se dizer que a maioria das legislações de proteção de dados pessoais optou por circunscrever a sua aplicação às pessoas físicas, excluindo de seu âmbito o tratamento de dados de pessoas jurídicas[273]. É o caso da Diretiva Européia 95/46/CE, que determina que os dados das pessoas jurídicas não são objeto da sua regulamentação[274]. Conforme afirma Colin Bennet, "a política de privacidade informacional desenvolveu-se, doméstica e internacionalmente, com a pressuposição de que

[271] Diretiva Européia 95/46/CE, art. 3, 2.

[272] Diretiva Européia 95/46/CE, art. 3, 2.

[273] BENNET, Colin e RAAB, Charles. *The Governance of Privacy*. Op. Cit., p. 11.

[274] "Considerando" 24 da Diretiva Européia 95/46/CE: "as legislações relativas à proteção das pessoas jurídicas a respeito do tratamento dos dados que lhe digam respeito não são objeto da presente Diretiva".

os interesses de grupos, corporações e outras organizações, bem como a informação sobre elas, deveriam ser tratados a partir de outros instrumentos legais"[275].

Interessante é a discussão acerca da aplicação do regime das leis de proteção de dados pessoais ao tratamento manual de dados, uma vez que o debate público centra-se, geralmente, na violação da privacidade principalmente nos meios informáticos. A definição desse âmbito de aplicação varia nas diferentes legislações, inclusive nos países da União Européia.

É de se notar que a primeira lei de proteção de dados pessoais do mundo, a Lei do Estado alemão de Hesse, de 1970, limitava-se a regulamentar o tratamento automatizado dos dados pessoais[276].

A Diretiva Européia 95/46/CE é bastante clara ao tratar ambos de forma indistinta, nos termos de seu art. 3º, 1: "A presente directiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados." É importante perceber, no entanto, que os bancos de dados não automatizados somente se submetem ao regime de proteção de dados pessoais quando minimamente organizados e estruturados[277].

Entende-se importante que a proteção de dados pessoais possa abranger ambos os tipos de bancos de dados, na medida em que a potencialidade dos danos à personalidade reside não exatamente na informatização, mas no tratamento dos dados em si e na obtenção de informações que representem de forma objetiva o individuo perante a sociedade, gerando

---

[275] BENNETT, Colin e RAAB, Charles. *The Governance of Privacy*. Op. Cit., p. 11.

[276] BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 77.

[277] É o que afirma o "Considerando" 27 da Diretiva 95/46/CE: Considerando que a protecção das pessoas se deve aplicar tanto ao tratamento automatizado de dados como ao tratamento manual; que o âmbito desta protecção não deve, na prática, depender das técnicas utilizadas, sob pena de se correr o sério risco de a protecção poder ser contornada; que, em todo o caso, no que respeita ao tratamento manual, a presente directiva apenas abrange os ficheiros e não as pastas não estruturadas; que, em particular, o conteúdo de um ficheiro deve ser estruturado de acordo com critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais; que, em conformidade com a definição da alínea c) do artigo 2º, os diferentes critérios que permitem determinar os elementos de um conjunto estruturado de dados pessoais e os diferentes critérios que regem o acesso a esse conjunto de dados podem ser definidos por cada Estado-membro; que as pastas ou conjuntos de pastas, bem como as suas capas, que não estejam estruturadas de acordo com critérios específicos, de modo algum se incluem no âmbito de aplicação da presente directiva;" (grifo nosso)

conseqüências para a sua vida. Afinal, também os bancos de dados manuais podem apresentar erros quantos aos dados pessoais, bem como podem propiciar a transferências desses dados a terceiros.

Com relação aos bancos de dados públicos e privados, existem duas questões importantes: i) sobre a necessidade e a conveniência de regulamentar o tratamento de dados por organismos privados; e ii) sobre a aplicação do mesmo regime de proteção a ambos. Não existe, com relação a esse tema, consenso na União Européia, nem na legislação dos EUA. A divergência é significativa, na medida em que enquanto alguns países tutelam sem significativas distinções o tratamento dos dados pessoais nos setores público e privado, outros determinam regimes jurídicos bastantes distintos para cada um, como é o caso dos EUA.

A Diretiva Européia 95/46/CE determina que tanto o tratamento de dados realizado pelo poder público, quanto o realizado pelo setor privado, estão submetidos ao mesmo regime de proteção, estabelecendo uma exceção de aplicação apenas em relação ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado, o bem-estar econômico do Estado e as atividades do Estado no domínio do direito penal, que não estão abrangidos pela Diretiva[278]. Assim, salvo essa questão específica, não determina tutela diferente em razão da titularidade do banco de dados.

No entanto, na própria União Européia o tema não é unânime. A Espanha, por exemplo, estabeleceu regimes distintos em função da titularidade pública ou privada do banco de dados, embora ambos estejam regulamentados pela mesma lei (LORTAD). Na referida lei, os bancos de dados públicos são submetidos a uma disciplina mais rígida, pois necessitam para a sua criação de uma norma geral, submetida a controle jurisdicional, enquanto os bancos de dados privados podem ser criados livremente e estão submetidos unicamente à Agência de Proteção de Dados. Tal opção legislativa foi criticada por Pérez-Luño, por entender que os

[278] Ao definir o responsável pelo tratamento de dados pessoais, a Diretiva inclui, nesse conceito, o poder público: Art. 2, d: «Responsável pelo tratamento», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais"

danos causados pelo setor privado à privacidade são tão expressivos como os gerados pelo Estado[279].

Na Alemanha, predominou a concepção de que os setores público e privado deveriam ser regulamentados de modo semelhante, por se reconhecer que o risco à violação da privacidade existe em ambos os casos. Como afirma Benedikt Buchner, no início das discussões para a aprovação da Lei sobre Proteção de Dados Pessoais alemã de 1977 (Bundesdatenschutzgesetz - BDSG), predominava a concepção de que o principal risco à privacidade informacional dos cidadãos advinha do Estado[280]. No entanto, afirma ele, que já havia alguns doutrinadores que constataram a expressiva utilização pelas empresas privadas dos dados pessoais, percebendo que tal ameaça também poderia partir do setor privado. Assim, a Lei de 1977 compreendeu também a regulação do setor privado, tendo recebido elogios da doutrina, que caracterizou tal circunstância como a concretização dos direitos fundamentais dos cidadãos[281].

No entanto, a referida lei foi substituída pela Lei Federal de Proteção de Dados Pessoais de 1990, que, diferentemente da anterior, regulou de forma diferente o tratamento de dados pessoais pelo Estado ou pela iniciativa privada[282]. Tal fato foi bastante criticado pelos juristas alemães. Posteriormente, com a tentativa de conformação dessa legislação às diretivas da União Européia, reduziu-se, gradualmente, a diferenciação entre a regulamentação do tratamento de dados pessoais efetuado pelo Estado ou pelas empresas privadas. Desde então, afirma Buchner, a doutrina e a legislação alemãs têm buscado tratar ambos os setores de forma semelhante, sob o fundamento principal de que o direito à autodeterminação

[279] PÉREZ LUÑO, *Manual de Informática e Derecho*. Op. Cit., p. 57.

[280] BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Tübingen: Mohr Siebeck, 2006, p. 28.

[281] Idem, Ibidem, p. 30.

[282] A principal diferença de regulamentação dos setores público e privado na Lei de 1990 era a seguinte: enquanto o principio da finalidade vigorava para o tratamento de dados pessoais pelo Estado em todas as fases do tratamento, para o setor privado, tal princípio somente era exigido de forma geral. (BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Op. Cit., p. 34.)

informativa do cidadão é único[283]. Nesse mesmo sentido, foi promulgada a lei alemã mais recente de proteção de dados pessoais de novembro 2006.

Importa ressaltar que, nos EUA, o panorama a respeito do referido assunto é bastante diferente. Nesse país, em que não há uma lei abrangente sobre a proteção de dados pessoais, mas diversas normas setoriais, a estrutura legal para a proteção desse direito compreende duas leis básicas: o "Fair Credit Reporting Act", de 1970, e o "Privacy Act", de 1974[284]. Enquanto o primeiro aplica-se às empresas que emitem relatórios sobre os consumidores, em caso de análise de risco de crédito, assinatura de seguro e de contratação de empregados, o segundo aplica-se somente às agencias governamentais federais ou às empresas privadas que administram um sistema de registro para o governo.

Nesse sentido, resta claro que a estrutura normativa americana para a proteção da privacidade é bipartida, regulando de forma diversa o setor público e o setor privado[285]. Além dessa característica dualista, pode-se dizer que a legislação tem um viés liberal acentuado, regulamentando com mais severidade e amplitude o tratamento de dados pessoais realizado pelo setor público[286]. Como afirma Colin Bennett, nos EUA, predomina a concepção de que o setor privado se auto-regulamenta, na medida em que o tema da privacidade se tornou um diferencial competitivo e um requisito para se obter a confiança do consumidor[287]. Assim, prevalecem, nesse país, códigos voluntários de boas práticas no setor privado, em detrimento de uma regulamentação estatal[288].

---

[283] BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*. Op. Cit., p. 34.

[284] SOLOVE, Daniel. A Model Regime of Privacy Protection. In: *University f Illinois Law Review*, Vol. 2006, p. 3.

[285] Idem, Ibidem, p. 8.

[286] BUCHNER, Benedikt. Informationelle Selbstbestimmung im Privatrecht. Op. Cit., p. 5. Para críticas à estrutura legal americana referente à proteção da privacidade informacional, ver também: SOLOVE, Daniel. A Model Regime of Privacy Protection. In: *University f Illinois Law Review*, Vol. 2006.

[287] BENNETT, Colin e GRANT, Rebecca (Ed). *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, 1999, p. 11 (Introdução).

[288] Idem, Ibidem, p. 11.

Nesse sentido, percebe-se que as legislações de diversos países tratam de forma distinta o âmbito de aplicação da proteção de dados pessoais em relação à titularidade do banco de dados. Enquanto alguns optam por um sistema unificado, ao regular o tratamento dos dados pessoais pelos setores público e privado de forma semelhante, outros preferem fazê-lo de forma diferente em cada um dos setores.

Entende-se que a melhor solução é o modelo adotado pela Alemanha de uma regulamentação única, respeitando-se, naturalmente, as especificidades de cada setor, na medida em que se está a falar de um único direito à privacidade e à proteção de dados pessoais, cujo titular é o cidadão. Ademais, compreende-se não haver hoje mais qualquer motivo para se pensar que o tratamento de dados pessoais pelo setor privado é menos danoso à população, principalmente a partir da constatação geral de que existe atualmente uma verdadeira indústria de dados pessoais ("Database Industry"[289]), conforme será desenvolvido no capítulo 3 desta dissertação.

3.3.2. O regime de proteção de dados no Brasil

Após essa breve análise a respeito do modelo de legislação geral de proteção de dados pessoais, cumpre examinar como ocorre no Brasil a proteção da privacidade, em face da ausência de uma lei geral que regulamente a matéria.

O tratamento de dados pessoais no âmbito de uma relação de consumo está sujeito como visto à Constituição federal e à legislação de proteção ao consumidor. Além disso, nos países em que existem leis ordinárias de proteção de dados pessoais, estas geralmente incidem sobre o tratamento de dados pessoais realizado na relação de consumo. Isso ocorre na maioria dos países da União Européia, no Canadá e na Austrália (em alguns estados), mas não é o caso do Brasil, que carece de legislação ordinária com essa finalidade. Não existe nenhuma

[289] SOLOVE, Daniel. A Model Regime of Privacy Protection. Op. Cit., p. 362.

legislação no país que tenha como principal objetivo estabelecer a regulação estatal do tratamento de dados pessoais na sociedade.

Existem alguns projetos de lei tramitando no Congresso Nacional. Um deles é de iniciativa do governo, mas dificilmente poder-se-ia afirmar que o seu objetivo é a regulação estatal da matéria. Trata-se do Projeto de Lei 5.870, encaminhado ao Congresso pelos Ministros da Fazenda e da Justiça, mais conhecido como projeto do cadastro positivo. O referido projeto de lei recebeu tal denominação por autorizar o processamento de dados dos consumidores relativos à sua adimplência, muito embora a sua finalidade geral seja a de regulamentar os bancos de dados de proteção ao crédito.

Entende-se que o referido PL não atende às necessidades da sociedade brasileira no século XXI, em que o fluxo de dados pessoais tornou-se um dos fatores de produção para as empresas, podendo acarretar graves danos à coletividade de consumidores e aos indivíduos. Isso porque, a pretexto de regular informações positivas no crédito, o referido PL autoriza o livre tratamento e circulação de dados pessoais na sociedade de consumo, sem impor limites significativos ao processamento de dados pessoais e sem prever mecanismos adequados de controle do consumidor sobre esse processamento. Assim, se por um lado, o PL autoriza livremente o tratamento de dados, por outro, ele não assegura mecanismos fortes de proteção à personalidade do consumidor. Além desses graves problemas, o projeto não institui qualquer órgão administrativo de proteção dos dados pessoais e, portanto, está na contramão da experiência internacional bem sucedida na matéria.

Nos moldes em que foi proposto, o PL não tem a pretensão de se constituir em uma lei geral de proteção de dados pessoais, nem para o setor público, nem para o setor privado. Nesse sentido, a sua finalidade parece ter sido a de unicamente legalizar e legitimar a conduta atual das empresas de processar ilimitadamente dados pessoais dos consumidores e de transferi-los sem qualquer conhecimento do titular dos dados.

O PL 5.870, nos moldes em que foi formulado, pode gerar efeitos contrários aos que foram pretendidos quando da sua elaboração: ao invés de ampliar o crédito e reduzir as taxas de juros do mercado, pode acarretar uma grande insegurança jurídica, tendo em vista os enormes riscos aos quais os cidadãos ficarão expostos em razão da livre circulação e do livre tratamento de dados pessoais, sem a contrapartida da adequada proteção da privacidade. Ademais, ele pode suscitar também questionamentos a respeito de sua constitucionalidade, se for compreendido como atentório aos direitos fundamentais consagrados na Constituição federal, como o direito à privacidade, à liberdade e à igualdade.

Entende-se que o melhor modelo a ser adotado no Brasil é o modelo de uma legislação geral de proteção de dados pessoais, que abarque tanto o setor público, quanto o privado, e que se constitua em um verdadeiro sistema de regulação do processamento de dados na sociedade. Para tanto, seria necessário, como já visto, o estabelecimento de um órgão administrativo, responsável pela supervisão, auditoria, implementação da legislação e atendimento dos cidadãos que sofreram danos em decorrência do tratamento ilícito de dados pessoais.

4.

CONCLUSÃO

A utilização massiva de dados pessoais por organismos estatais e privados, a partir de avançadas tecnologias da informação, apresenta novos desafios ao direito à privacidade. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais[290].

Nesse contexto, destaca-se a técnica de construção de perfis pessoais, a partir dos quais podem ser tomadas decisões a respeito dos cidadãos, afetando diretamente as suas vidas e influenciando o seu acesso a oportunidades sociais. Crescem, portanto, os riscos à personalidade do cidadão, na medida em que esses perfis, verdadeiros clones virtuais, representam informações fragmentadas e descontextualizadas, que podem ser utilizadas de modo a prejudicar a liberdade e as chances de vida do indivíduo. Esses riscos, ampliados pela utilização da tecnologia da informação, tornam imperativa a regulamentação jurídica da matéria. [291]

A questão da violação da privacidade na sociedade da informação não deve se resumir à compreensão determinista de que a tecnologia é a responsável pelo problema. Ao revés, o

[290] ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data em Chile e información comparativa. In: *Anuário de Derecho Constitucional Latioamericano 2005*, Tomo II, Konrad Adenauer Stiftung, p. 449.

[291] PÉREZ LUÑO, Antonio-Enrique. *Manual de Informática e Derecho.* Barcelona: Editorial Ariel, 1996, p. 43.

debate sobre a proteção de dados pessoais deve ter como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade.

Em razão de modificações sociais e da evolução tecnológica, a discussão sobre os danos causados pelo processamento de dados pessoais não se restringe mais à ameaça do poder do Estado, mas abrange hoje também o setor privado, que utiliza massivamente dados pessoais para atingir os seus objetivos econômicos.

A análise do tratamento de dados pessoais no âmbito da relação de consumo deve considerar de forma prioritária a vulnerabilidade do consumidor nesse processo. Afinal, os dados pessoais representam virtualmente a pessoa perante a sociedade, podendo ampliar ou reduzir o acesso às oportunidades no mercado. Dessa forma, tem-se como necessária a ação do Estado para a proteção dos dados pessoais do consumidor, pois o mercado, ao invés de contribuir para a superação da sua vulnerabilidade, na realidade, acaba por reforçá-la.

Nos países da União Européia, a tutela jurídica dos dados pessoais dá-se a partir de um aparato constitucional e legal, no qual se destaca uma lei geral de proteção de dados pessoais. A finalidade da lei geral, geralmente fundamentada na Constituição, é a de regular todo o tratamento de dados pessoais realizado na sociedade, tanto pelo setor público, quanto pelo setor privado. É, portanto, o exercício do poder do Estado para intervir no processamento de dados, buscando preservar a coletividade e os direitos fundamentais dos cidadãos.[292]

As leis gerais de proteção de dados pessoais se firmaram como umas das formas mais eficazes de se proteger a privacidade nos países desenvolvidos, pois nelas foram estabelecidos os princípios gerais para o tratamento de dados, os direitos subjetivos dos titulares dos dados pessoais, as limitações e as obrigações dos responsáveis pelo tratamento de dados, bem como a criação de autoridades administrativas competentes para a implementação da legislação.

No Brasil, o tratamento de dados pessoais no âmbito de uma relação de consumo está sujeito à Constituição Federal e ao Código de Defesa do Consumidor. Ocorre, no entanto, que

[292] BENNET, Colin e RAAB, Charles. *The governance of privacy.* Op. Cit., p. 125.

não existe nenhuma legislação no país que tenha como principal objetivo estabelecer a regulação estatal do processamento de dados, o que impossibilita o estabelecimento de princípios harmônicos sobre o tema, dificulta o controle dos riscos do tratamento de dados, impede a adequada reparação aos cidadãos dos danos causados pelo tratamento ilegal de dados e impossibilita a autodeterminação do indivíduo sobre os seus dados pessoais.

É possível inferir que a economia da informação pessoal influenciará as experiências do consumidor no século XXI de forma ainda mais marcante que no século XX. Nesse complexo contexto de processamento e fluxo de dados pessoais, é provável que as organizações de consumidores e ativistas não se restrinjam ao conceito de privacidade para proteger os consumidores, buscando outros parâmetros que protejam a coletividade de consumidores contra a discriminação no mercado de consumo, a vedação do acesso a bens e serviços e a aleatória transferência de riscos.

Assim, é provável que os conflitos jurídicos e políticos a respeito da coleta, do uso e da revelação da informação pessoal tornem mais amplos, complexos e diversos que os atuais questionamentos restritos ao tema da privacidade. Ademais, pode-se inferir que o assunto se desdobre para abranger também a questão acerca da distribuição dos riscos oriundos da economia da informação pessoal na sociedade.

Sob essa ótica e para possibilitar a resposta adequada aos desafios sociais advindos da revolução tecnológica, é fundamental que o direito brasileiro seja reconstruído a ponto de compreender e solucionar os novos problemas enfrentados pelo cidadão na era da informação[293].

A aplicação efetiva do direito individual fundamental à proteção de dados pessoais depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na realização de uma democracia da

[293] PÉREZ LUÑO, Antonio-Enrique. *Manual de Informática e Derecho*, Op. Cit., p. 10.

informação que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados.

Assim, entendemos ser necessário criar no país uma cultura jurídica apta a compreender a proteção dos dados pessoais como um direito fundamental autônomo, que tem origem no direito à privacidade, mas dele se separa, em razão das transformações sociais e tecnológicas. Cumpre também estabelecer no país uma arquitetura regulatória, capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro setor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação. Isso exige instrumentos legais próprios, órgãos reguladores específicos, uma rede de especialistas e juristas, um robusto grupo de ativistas dispostos a demonstrar todo tipo de abuso e violações, uma crescente comunidade acadêmica especializada no tema, bem como uma rede internacional, pela qual se realiza o intercâmbio de experiências e idéias.

5.

BIBLIOGRAFIA

AGRE, Philip. Introduction. In: AGRE, Philip e ROTENBERG, Marc (Ed). *Technology and Privacy: The New Landscape*. Cambridge: MIT Press. 1997.

ALCALÁ, Humberto Nogueira. "Autodeterminación informativa y hábeas data em Chile e información comparativa." In: *Anuário de Derecho Constitucional Latioamericano 2005*, Tomo II, Konrad Adenauer Stiftung.

ALPERT, Sheri. "Protecting medical privacy: challenges in the age of genetic information". In: *Journal of Social Issues.* Vol. 59. No. 2, 2003.

ARGENTINA: "Protección de Datos Personales". In: Investigaciones 1 (1998), p. 121, Secretaria de Investigaión de Derecho Comparado, Corte Suprema de Justicia de La Nación, República Argentina.

ARIÈS, Philippe e CHARTIER, Roger (org.). *História da vida privada 3: da Renascença ao Século das Luzes*. Tradução: Hildegard Feist. São Paulo: Companhia das Letras, 1991.

BAUDRILLARD, Jean. *A sociedade de consumo*. Tradução: Artur Morao. Lisboa: Edições 70, 2007.

BAUMANN, Zygmunt. *A liberdade*. Lisboa: Editorial Estampa, 1989.

_____. *Modernidade Líquida*. Tradução: Plínio Dentzein. Rio de Janeiro: Jorge Zahar Ed., 2001.

_____. *The individualized society*. Cambridge: Polity Press, 2001.

BELLEIL, Arnaud. *@-privacidade. O mercado dos dados pessoais: protecção da vida privada na idade da internet.* Tradução: Paula Rocha Vidalinc. Lisboa: Instituto Piaget, 2001.

BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Cornell University Press, 1992.

_____ e RAAB, Charles. *The Governance of Privacy: policy instruments in global perspective*. Cambridge: The MIT Press, 2006.

_____ e GRANT, Rebecca (Ed). *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, 1999.

BESSA, Leonardo Roscoe. *O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito*. São Paulo: Revista dos Tribunais. 2003.

BIRD, Drayton. *Bom senso em marketing direto*. Tradução: Michelangelo Di Vito. São Paulo: Makron Books, 2000.

BOWKER, Geoffrey C. e STAR, Susan Leigh. *Sorting things out: classification and its consequences*. Cambridge: MIT Press, 2000.

BRIN, David. *The transparent society: Will technology force us to choose between privacy and freedom?* New York: Basic books, 1998.

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

CAENEGEN, R. C. van. *Uma introdução histórica ao direito privado*. Tradução: Carlos Eduardo Machado. São Paulo: Martins Fontes, 1995.

CANARIS, Claus-Wilhelm. *Direitos fundamentais e direitos privados*. Tradução: Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Edicoes Almedina, 2006.

CANOTILHO, Gomes e MACHADO, Jónatas, *Reality Shows e Liberdade de Programação.* Coimbra: Coimbra Editora, 2003.

CARVALHO, Ana Paula Gambogi. "O Consumidor e o Direito à Autodeterminação informacional: considerações sobre os bancos de dados eletrônicos." In: *Revista de Direito do Consumidor*. No. 46, Ano 12, abril-junho de 2003.

CARVALHO NETO, Menelick. "A Hermenêutica Constitucional sob o paradigma do Estado Democrático de Direito." In: *Notícia do Direito Brasileiro*. Nova Série, no. 6, 1998, pp. 233-250.

CASTELLS, Manuel. *A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede.* Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999.

_____ *A Galáxia da Internet. Reflexões sobre a internet, os negócios e a sociedade.* Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

CASTRO, Catarina Sarmento e. *Direito da Informática, Privacidade e Dados Pessoais.* Coimbra: Almedina, 2005.

COSTA JÚNIOR, Paulo José da. *O direito de estar só: tutela penal da intimidade*. 2 Ed. São Paulo: Revista dos Tribunais, 1995.

DE CUPIS, Adriano. *Os direitos da personalidade*. 1 Ed. Campinas: Romana Jurídica, 2004.

DE LA CUEVA, Pablo Lucas Murillo. "La construcción del derecho a la autodeterminación informativa." In: *Revista de Estudios Políticos* ,104 (Nueva Época), Abril/Junio 1999, Madri.

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

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação. Possibilidades e limites*. São Paulo: Revista dos Tribunais, 1980.

DRUMMOND, Victor. *Internet, privacidade e dados pessoais*. Rio de Janeiro: Lumen Juris, 2003.

DWORKIN, Ronald. *O império do direito*. Tradução: Jefferson Luiz Camargo. São Paulo: Martins Fontes, 1999.

_____. *Uma Questão de Princípio*. São Paulo: Martins Fontes, 2000.

_____. *Levando os direitos a sério*. Tradução: Nelson Boeira. Sao Paulo: Martins Fontes, 2002.

_____. *Domínio da vida: aborto, eutanásia e liberdades individuais*. Tradução: Jefferson Luiz Camargo. Sao Paulo: Martins Fontes, 2003.

_____.*A virtude soberana: a teoria e a prática da igualdade*. Tradução: Jussara Simões. São Paulo: Martins Fontes, 2005, p. IX.

_____.*Is Democracy possible here? Principles for a new political debate.* Princeton: Princeton University Press, 2006.

_____.*O direito da liberdade: a leitura moral da Constituição norte-americana*. Tradução: Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2006.

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

ERNST, Morris L. e SCHWARTZ, Alan U. *Privacy: The right to be let alone*. New York: The Macmillan Company, 1962.

FEATHERSTONE, Mike. *Cultura de consumo e pós-modernismo*. Tradução: Julio Assis Simoes. São Paulo: Studio Nobel, 1995.

FOUCAULT, Michel. *Microfísica do poder*. Tradução: Roberto Machado. 22 Ed. Rio de Janeiro: Edicoes Graal, 2006.

FRANKENBERG, Günther. *A Gramática da Constituição e do Direito*. Trad. Elisete Antoniuk, Belo Horizonte: Del Rey, 2007.

GANDY, Oscar. *The Panoptic Sort. A Political Economy of Personal Information.* Boulder: Westview Press, 1993.

_____ e SCHILLER, Herbert. "Data mining and surveillance in the post-9.11 environment". *For presentation to the Political Economy Section, IAMCR*. Barcelona, July, 2002.

GARCÍA, Clemente García. *El derecho a la intimidad y dignidad em la doctrina del Tribunal Constitucional*. Murcia: Universidad de Murcia, Servicio de Publicaciones, 2003.

GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. O'Reilly Media: California, 2000.

GRINOVER, Ada Pelegrini (et al). *Código Brasileiro de defesa do consumidor comentado pelos autores do anteprojeto. 8 ed. Rio de Janeiro: Forense Universitária, 2005.*

HÄBERLE, Peter, “A Dignidade Humana como Fundamento da Comunidade Estatal”, In: SARLET, Ingo Wolfgang, *Dimensões da Dignidade. Ensaios de Filosofia do Direito e Direito Constitucional.* Porto Alegre: Livraria do Advogado Editora, 2005.

_____ “Incursus. Perspectiva de una doctrina constitucional del mercado: siete tesis de trabajo”. In: HÄBERLE, Peter. *Nueve ensayos constitucionales y una lección jubilar.* Trad.: Luciano Parejo Alfonso e outros. Lima: Palestra Editores, 2004.

HABERMAS, Jürgen. *Identidades nacionales e postnacionales.* Trad.: Manuel Jiménez Redondo. Editorial Tecnos: Madri, 1994.

_____. *Direito e Democracia: entre facticidade e validade*, volume I e II. Trad: Flávio Beno Siebeneichler. Rio de Janeiro: Tempo brasileiro, 1997.

_____. *Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa.* Trad.: Flávio Kothe. Rio de Janeiro: Tempo Brasileiro, 2003.

_____. *O Futuro da Natureza Humana.* Trad. Karina Jannini. São Paulo: Martins Fontes, 2004.

HESSE, Konrad. *Derecho constitucional y derecho privado*. Tradução: Ignacio Gutiérrez Gutiérrez. Madrid: Editorial Civitas, 1995.

HIGUERAS, Manuel Heredero. *La Directiva Comunitaria de Protección de los datos de carater personal.* Pamplona: Aranzadi Editorial, 1997.

KANT, Immanuel. *Crítica da Razão Prática.* Trad. Valerio Rohden. Edição Bilíngüe. São Paulo: Martins Fontes, 2003.

KOSELLECK, Reinhart. *Crítica e Crise: uma contribuição à patogênese do mundo burguês.* Trad.: Luciana Castelo Branco. Rio de Janeiro: EDUERJ: Contraponto, 1999.

LACE, Susane. The *Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005.

LEITAO, Débora Krischke; LIMA, Diana Nogueira de Oliveira; e MACHADO, Rosana Pinheiro. *Antropologia e consumo: diálogos entre Brasil e Argentina*. Porto Alegre: AGE, 2006.

LESSIG, Lawrence. The Architecture of Privacy, Draft 2, p. 17, Artigo apresentado na Conferência Taiwan Net '98, Taipei, Março de1998. Acessível em http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf , acessado em 16/01/2008, 20:40

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

LOCKE, John. *Dois Tratados sobre o governo.* Trad: Julio Fischer. São Paulo: Martins Fontes, 1998.

LOJKINE, Jean. *A revolução informacional*. Tradução: José Paulo Netto. 3 Ed. São Paulo: Cortez, 2002.

LYON, David. "Surveillance as social sorting. Computer codes and mobile bodies." In: *Surveillance as Social Sorting. Privacy, risk and digital discrimination.* LYON, David (Ed). Londres: Routledge, 2003.

_____. *Surveillance as Social Sorting. Privacy, risk and digital discrimination.* LYON, David (Ed). Londres: Routledge, 2003.

_____. *The Electronic Eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 1994.

MACEDO Jr, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor*. 2ª. Ed. São Paulo: Editora Revista dos Tribunais, 2006.

MARKESINIS, Basil S (ed.). *Protecting Privacy*. New York: Oxford University Press, 1999.

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico).* São Paulo: Revista dos Tribunais, 2004.

_____. (et al). Manual de Direito do Consumidor. São Paulo: Ed. Revista dos Tribunais, 2007.

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

MAYER-SCHÖNBERGER, “Generational Development of Data Protection in Europe”. In: *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, 2001.

MCCRACKEN, Grant. *Cultura e consumo. Novas abordagens ao caráter simbólico dos bens e das atividades de consumo*. Tradução: Fernanda Eugenio. Rio de Janeiro: MAUAD, 2003.

MENDES, Gilmar Ferreira (et al). *Curso de Direito Constitucional*. São Paulo: Ed. Saraiva, 2008.

MILL, John Stuart. *A liberdade; Utilitarismo*. Trad. Eunice Ostrensky. São Paulo: Martins Fontes, 2000.

MILLER, Arthur R. *The assault on privacy: computers, data banks, and dossiers*. Michigan: The University of Michigan Press, 1971.

MURILLO DE LA CUEVA, Pablo Lucas, *El derecho a la autodeterminación informativa*. Madri: Tecnos, 1990.

NEUMANN, Ulfried. “Die Tyrannei der Würde: Argumentationstheoretische Erwägungen zum Menschenwürdeprinzip.” In: Archiv. für Rechts- und Sozialphilosophie, 1998, vol. 84, nº2.

OLIVEIRA, Marcelo Andrade Cattoni de. *Devido Processo Legislativo. Uma justificação democrática do controle jurisdicional de constitucionalidade das leis*. Belo Horizonte: Mandamentos, 1999.

ORTIZ, Ana Isabel Herrán. *La Violación de la Intimidad en la Protección de Dados Personales*. Madri: Dykinson, 1999.

PENNOCK, J. Roland. e CHAPMAN, John W (ed.). *Nomos XIII: Privacy*. New York: Atherton Press, 1971.

PÉREZ LUÑO, Antonio-Enrique. *Cibernética, informática y derecho. Un análisis metodológico*. Bolonia: Real Colegio de Espana, 1976.

_____. *Manual de Informática e Derecho.* Barcelona: Editorial Ariel, 1996.

PERLINGIERI, Pietro. *Perfis do direito civil: introdução ao direito civil constitucional*. Tradução: Maria Cristina de Cicco. 3. Ed. Rio de Janeiro: Renovar, 2002.

PERROT, Michelle (org.). História da vida privada 4: da Revolução Francesa à Primeira Guerra. Tradução: Denise Bottman e Bernardo Joffily. São Paulo: Companhia das Letras, 1991.

PINTO, Cristiano. "Arqueologia de uma distinção: o publico e o privado na experiência histórica do direito. In: OLIVEIRA PEREIRA, Claudia Fernanda (org.). *O novo direito administrativo brasileiro: Estado, agências e Terceiro Setor*. Belo Horizonte: Forum, 2003.

POSNER, Richard A. "An Economic Theory of Privacy". In: *Regulation (May/June)*. 1978.

_____ "The Right of Privacy". In: *Georgia Law review*, 12. 1978

REGAN, Priscilla M. (2002) "Privacy as a Common Good in the Digital World", In: *Information, Communication & Society*, 5:3.

ROSEN, Jeffrey. *The unwanted gaze: the destruction of privacy in America*. New York: Vintage Books, 2001.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: *uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1998.

SAMARAJIVA. Rohan. "Interactivity as though privacy mattered." In: *Technology and Privacy: The New Landscape*. Massachusetts: The MIT Press, 2001.

SARLET, Ingo Wolfgang (org.) *A constituição concretizada: construindo pontes com o público e o privado*. Porto Alegre: Livraria do Advogado, 2000.

SARMENTO, Daniel. Direitos Fundamentais e Relações Privadas. Rio de Janeiro: Lumen Juris, 2004.

SARMENTO, Daniel e GALDINO, Flávio. *Direitos Fundamentais: estudos em homenagem ao professor Ricardo Lobo Torres.* Rio de Janeiro: Renovar, 2006.

SCHWARTZ, Paul. "Privacy and Democracy in Cyberspace". In: *Vanderbilt Law* Review 52: 1609 – 1702.

SCHWENKE, Mathias. *Individualisierung und Datenschutz*. Wiesbaden: Deutscher Universitäts-Verlag, 2006.

SMITH, Robert Ellis. *Privacy. How to protect. What´s left of it.* Garden City: Anchor Press/Doubleday, 1979.

SOLOVE, Daniel J.. *The digital person: technology and privacy in the information age*. New York: New York University Press, 2004.

_____. "A Model Regime of Privacy Protection." In: *University of Illinois Law Review*, Vol. 2006.

TEPEDINO, Gustavo. *Temas de direito civil*. 2 Ed. Rio de Janeiro: Renovar, 2001.

_____. *Obrigações: Estudos na perspective civil-constitucional*. Rio de Janeiro: Renovar, 2005.

_____, BARBOZA, Heloisa Helena e MORAES, Maria Celina Bodin de. *Código Civil interpretado conforme a Constituição da República. Rio de janeiro: Renovar, 2004.*

TUROW, Joseph. *Niche envy: marketing discrimination in the digital age*. Cambridge e Londres: The MIT Press, 2002.

VIEIRA, Tatiana Malta. *O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante da tecnologia da informação*. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

WACKS, Raymond. *Personal Information: Privacy and the Law*. Oxford: Clarendon Press, 1989.

WARREN e BRANDEIS, "The Right to Privacy". In *Harvard Law Review*, Vol IV, Dezembro 15, 1890, No. 5.

WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1970.

_____ (Ed.) Information Technology in a democracy. Cambridge: Harvard University Press, 1971.

_____ Databanks in a Free Society: Computers, Record-keeping and Privacy. A Project of the Computer Science & Engineering Board National Academy of Sciences. Nova York: Quadrangle/ The New York Times Book Company, 1972.