ENDC Escola Nacional de Defesa do Consumidor

A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO: PARA ALÉM DA INFORMAÇÃO CREDITÍCIA

CADERNO DE INVESTIGAÇÕES CIENTÍFICAS

Vol. 2

MINISTÉRIO DA JUSTIÇA
SECRETARIA DE DIREITO ECONÔMICO
DEPARTAMENTO DE PROTEÇÃO E DEFESA DO CONSUMIDOR

ENDC Escola Nacional de Defesa do Consumidor

A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO: PARA ALÉM DA INFORMAÇÃO CREDITÍCIA

CADERNO DE INVESTIGAÇÕES CIENTÍFICAS

Vol. 2

Ministério da Justiça
Secretaria de Direito Econômico
Departamento de Defesa e Proteção do Consumidor

B823p

Brasil. Escola Nacional de Defesa do Consumidor
A proteção de dados pessoais nas relações de consumo: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

122 p. : il. fots. p&b.

1. Inviolabilidade pessoal - consumidor. 2. Dados pessoais – Consumidor. 3. Relações de consumo. I. Doneda, Danilo, elab. II. Título.

CDD 342.5

Ficha catalográfica elaborada pela Biblioteca do Ministério da Justiça

Equipe Técnica
Autoria
Danilo Cesar Maganhoto Doneda

Coordenação:
Ricardo Morishita Wada
Juliana Pereira da Silva

Supervisão
Laura Schertel Mendes
Andiara Maria Braga Maranhão
Ana Dalva Saraiva Miranda

SUMÁRIO

APRESENTAÇÃO 7

INTRODUÇÃO 9

CAPÍTULO 1 - Informação pessoal e a sua tutela 15
1.1. Informação e direito
1.2. Bancos de dados
1.3. Informação e dados pessoais
1.4. Classificação da informação pessoal - dados sensíveis
1.5. Técnicas de tutela para os dados pessoais
1.6. Dados pessoais e o direito da informática
1.7. Mudança qualitativa no tratamento de dados pessoais

CAPÍTULO 2 - Proteção de dados pessoais e relações de consumo 37
2.1. Desenvolvimento das leis de proteção de dados
2.2. Princípios de proteção de dados pessoais
2.3. A proteção de dados como um direito fundamental
2.4. Proteção de dados no ordenamento brasileiro

CAPÍTULO 3 - Publicidade comportamental e Perfis de consumidores 57
3.1. Publicidade comportamental e formação de perfis (*profiling*)
3.2. Técnicas utilizadas para o monitoramento e formação de perfis
3.3. Problemas relacionados à publicidade comportamental
3.4. Instrumentos de controle e regulação

CAPÍTULO 4 - Redes sociais 73
4.1. Estrutura e modalidades das redes sociais *online*
4.2. Privacidade, publicidade e riscos das redes sociais

CAPÍTULO 5 - Correio eletrônico não autorizado - spam 87
5.1. Terminologia
5.2. Perfil técnico do spam
5.3. Perfil jurídico do spam
5.4. Perspectivas de combate ao spam

CONCLUSÃO 107

REFERÊNCIAS BIBLIOGRÁFICAS 115

APRESENTAÇÃO

É com muita satisfação que o Departamento de Proteção e Defesa do Consumidor, por meio da Escola Nacional de Defesa do Consumidor, publica o segundo volume do caderno de investigações científicas que trata do tema privacidade e proteção de dados pessoais nas relações de consumo.

O objetivo é discutir e refletir sobre a conexão entre os direitos dos consumidores e a proteção da privacidade, abordando, em capítulos, os seguintes aspectos: I) Informação pessoal e a sua tutela; II) Proteção de dados pessoais e relações de consumo; III) Publicidade comportamental e perfis de consumidores; IV) Redes sociais e V) Correio eletrônico não autorizado (Spam).

O tema é de grande relevância, na medida em que a conexão entre a defesa do consumidor e a proteção de dados é cada dia mais forte em uma economia da informação, em que as empresas buscam ao máximo a personalização da produção, comercialização e da publicidade. No mercado de consumo, os dados pessoais obtidos por meio da utilização de novas tecnologias da informação se transformam em um recurso essencial e valioso, tanto para a redução dos riscos empresariais, como para a fidelização do consumidor.

A adoção dessas tecnologias, que permitem o tratamento massificado de dados pessoais, muitas vezes, não são percebidas como nocivas pelos consumidores, pois podem oferecer também novas possibilidades de empoderamento. Isso se observa em diversas situações em que, por um lado, o aumento da informação pessoal disponível aos fornecedores resulta em aumento de bens e serviços personalizados, mas, por outro, pode ocasionar também a discriminação do consumidor no mercado.

Considerando a complexidade da atual sociedade e os conflitos relacionados à proteção de dados, a presente publicação visa debater o cenário internacional sobre o tema, analisar as normas setoriais existentes sobre a proteção de dados no país, bem como apontar a necessidade de um marco normativo para o Brasil.

Neste sentido, esta obra está em sintonia com o momento em que se inicia o debate público acerca do marco normativo geral pelo Ministério da Justiça sobre proteção de dados pessoais que estabelece princípios e limites para o tratamento de informações pessoais, com a finalidade de proporcionar uma proteção integral ao cidadão.

A riqueza deste conteúdo elaborado pelo ilustre Professor Danilo Doneda, precursor e profundo conhecedor do tema, está na proposta de reflexão acerca dos desafios a serem enfrentados pelo país na sociedade da informação. É fundamental avançar na busca de respostas para novos desafios como aqueles propostos pelas redes sociais, as tecnologias de vigilância, a biometria, o marketing comportamental, entre tantas outras, sempre considerando os valores fundamentais de liberdade e autonomia que inspiram esta disciplina.

Departamento de Proteção e Defesa do Consumidor

Secretaria de Direito Econômico

Ministério da Justiça

INTRODUÇÃO

The new consumer is the product itself.

John Perry Barlow

Os dados pessoais dos consumidores sempre foram atraentes para o mercado. Com dados precisos sobre os consumidores é possível, por exemplo, organizar um planejamento de produtos e vendas mais eficiente, ou mesmo uma publicidade voltada às reais características dos consumidores, entre diversas outras possibilidades. Há pouco tempo atrás, o custo para se obter tais dados pessoais costumava restringir severamente a quantidade destas informações que eram efetivamente coletadas e utilizadas.

A utilização de sistemas informatizados em diversas etapas da cadeia de produção e de consumo, à qual hoje já estamos nos habituando, trouxe consigo uma possibilidade concreta de mudança nesta equação: os sistemas informatizados de hoje têm uma capacidade muito grande de armazenar cada detalhe e sutileza das ações que ajudam a realizar. O consumidor de hoje existe em um ambiente onde muitas de suas ações são, ao menos tecnicamente, passíveis de registro e de posterior utilização.

A abundância da informação passível de ser obtida sobre o consumidor pode caracterizar uma nova vulnerabilidade do consumidor em relação àqueles que detêm a informação pessoal. O acesso do

fornecedor a estas informações é capaz de desequilibrar a relação de consumo em várias de suas fases, ao consolidar uma nova modalidade de assimetria informacional.

Esta nova assimetria informacional não se revela somente no poder a que o fornecedor pode ascender em relação ao consumidor ao tratar suas informações pessoais, porém também em uma nova modalidade de modelo de negócio na qual a própria informação pessoal se objetiva como *commodity*, como um ativo que pode chegar a ser o eixo de um determinado modelo de negócios.

Um exemplo claro de um modelo de negócios que gira em torno da informação pessoal pode ser percebido em numerosos exemplos, muitos deles na atividade de empresas de grande porte, tal como a *Google Inc.* A posição central que o tratamento de informações pessoais possui em seus produtos - grande parte dos quais são oferecidos sem custos ao consumidor -, corrobora a importância fundamental dos dados pessoais no fundamento de seu modelo de negócios. A consciência deste fato e de suas consequências tende a aumentar hoje, já passado um período de "graça" da Internet no qual suas possibilidades e limites reais pareciam pouco claros. Hoje é possível ouvir de um escritor como William Gibson, em recente artigo, que:

> *Nós mesmos geramos produtos para a Google, cada pesquisa que fazemos é uma pequena contribuição. A Google é feita de nós, uma espécie de recife de corais de mentes humanas e seus produtos*[1]

A monetarização dos dados pessoais foi uma tendência amplamente antecipada e que hoje é vital para uma parcela bastante representativa de novos serviços e produtos. Em uma declaração que se tornou bastante popular, a Comissária europeia do consumo, Meglena Kuneva, deixou claro que "os dados pessoais são o novo óleo da Internet e a nova moeda do mundo digital"[2], tornando claro o advento de um novo terreno adentrado pelas relações de consumo, no qual o consumidor passava a ser, em si, a fonte de um ativo que são as suas informações pessoais, suscitando a necessidade de adequação das normas que regulam o consumo para que levem em conta esta nova situação.

---

1 "We generate product for Google, our every search a minuscule contribution. Google is made of us, a sort of coral reef of human minds and their products". William Gibson. "Google's Earth", in: The New York Times. 31 de agosto de 2010.

2 "Personal data is the new oil of the Internet and the new currency of the digital world". Discurso proferido na mesa redonda sobre coleta de dados, direcionamento e perfilação. Bruxelas, 31 de março de 2009.

A abordagem destes dois fatores - a assimetria informacional em si e a monetarização das informações pessoais - não pode prescindir da consideração dos recentes avanços no tema da proteção de dados pessoais. A tendência à regulação da proteção de dados pessoais, que já conta com mais de quatro décadas, foi assimilada e amadurecida dentro do ordenamento jurídico de vários países e objetiva, em síntese, fornecer ao cidadão meios para controlar efetivamente a utilização de seus próprios dados pessoais por terceiros.

A importância capital da proteção de dados na Sociedade da Informação reflete-se, por exemplo, no *status* de direito fundamental que lhe conferiu a Carta de Direitos Fundamentais da União Europeia, referindo-a expressamente em seu Art. 8º:

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

Na ótica da atual legislação de defesa do consumidor, coube à proteção de dados a missão de manter dentro de um determinado equilíbrio a coleta de informações referentes ao inadimplemento do consumidor, para os fins de concessão de crédito. Nesta perspectiva, o art. 43 do Código de Defesa do Consumidor estabeleceu regras que sustentam até hoje a atividade dos bancos de dados de proteção ao crédito.

Nesta sua primeira formulação, a proteção de dados no direito brasileiro procurava estabelecer garantias mínimas para evitar abusos no tratamento de dados creditícios, ao mesmo tempo em que reconhecia

a legitimidade da utilização desta modalidade de informação para o desenvolvimento do crédito para o consumo. Em termos práticos, portanto, apontou para pouco além do que esta perspectiva diretamente vinculada à atividade de concessão de crédito.

Os dados pessoais do consumidor, no entanto, estão presentes em diversas outras fases da relação do consumo, em várias situações que dificilmente podem ser ponderadas utilizando-se estritamente as regras do artigo 43 do Código de Defesa do Consumidor. Do ponto em que nos encontramos, é quase desnecessário ressaltar a importância da informação pessoal em momentos como a pesquisa de hábitos e padrões de consumo, de perfis de compra ou de sua abrangência geográfica, somente para mencionar alguns exemplos.

Os dados de natureza creditícia não são, efetivamente, mais do que uma fração do conjunto de dados pessoais do consumidor que podem ser úteis para o mercado - sendo que, hoje, muitas vezes, são efetivamente tratados sem suscitar a atenção que já é tradicional quando se trata de dados creditícios.

Neste trabalho, procura-se identificar as diversas situações nas quais o tratamento de dados pessoais de consumidores pode resultar em um desequilíbrio na sua relação com os fornecedores, bem como ponderar as soluções possíveis dentro da perspectiva de que o consumidor, como qualquer cidadão, possui direito à sua autodeterminação informativa e que na relação de consumo é imperativa a identificação de instrumentos para fazê-la valer. Ponderar-se-ão, portanto, tanto possíveis soluções hermenêuticas e *de lege ferenda*.

Este enfoque deve, necessariamente, levar em conta as diretrizes específicas de tutela do consumidor e de proteção de dados que estarão diretamente envolvidas. A necessidade de ponderá-las contemporaneamente responde à necessidade de, (i) por um lado, estabelecer mecanismos eficazes para a proteção ao consumidor em um cenário em que seus dados pessoais podem ser utilizados em situações onde aumentem a sua vulnerabilidade e (ii) de outro, estabelecer mecanismos para que este mesmo consumidor mantenha o controle sobre as suas próprias informações, realizando assim os desígnos da autodeterminação informativa.

O aspecto do controle efetivo ao consumidor sobre seus próprios dados, tão caro à proteção de dados, é o ponto que a distingue com maior nitidez da tutela da privacidade propriamente dita - posto que a proteção de dados não se destina meramente à tutela de uma liberdade negativa, de não se expor, porém se realiza ao garantir a cada um a liberdade efetiva de escolher o que será feito com suas próprias informações pessoais. No caso do consumidor, o favorecimento desta liberdade é tão mais importante ao se perceber que

o tratamento de dados pessoais, lícito, leal e transparente, pode ser de interesse do próprio consumidor, à medida em que reflete em uma variedade maior de opções ou no desenvolvimento de produtos e serviços a partir de suas reais necessidades, por exemplo. E é justamente nesse sentido que, aliás, o próprio Código de Defesa do Consumidor, em seu art. 4º, III, prevê 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 (...)".

Os efeitos da inovação e do desenvolvimento tecnológico são claramente perceptíveis na miríade de novas opções e ferramentas colocadas à disposição do consumidor com o desenvolvimento do comércio eletrônico. Além de contar com um rol de ofertas potencialmente maior, o consumidor ganhou ferramentas que tornam a comparação de preços entre vários fornecedores uma realidade bastante palpável. A logística necessária ao comércio eletrônico também se desenvolveu. Em um momento posterior, novas modalidades de serviços que partiam do pressuposto da disponibilidade de informações tornaram-se viáveis, possibilitando que o consumidor pudesse contar com informação e serviços em uma variedade e qualidade que não seriam praticáveis no comércio tradicional[3].

Esta nova realidade apresenta novos riscos, como os que serão verificados ao longo do trabalho. A defesa do consumidor estará justamente incumbida de proporcionar respostas a tais riscos, fornecendo tanto proteção contra utilizações abusivas de suas informações como garantias de que suas escolhas sobre a utilização de seus próprios dados serão livres e transparentes. Estas são as preocupações a serem consideradas nos vários aspectos particulares da utilização de dados pessoais de consumidores que serão examinados neste trabalho, após as considerações conceituais necessárias sobre a natureza destas informações e sobre o desenvolvimento da proteção de dados pessoais.

3 Apenas como exemplos de uma destas possibilidades abertas pelo comércio eletrônico, mencionem-se os sites de leilões online, ou então mecanismos agregadores de pequenos comerciantes, capazes de aumentar o seu mercado potencial bem como a qualidade e quantidade da oferta ao consumidor.

CAPÍTULO 1
INFORMAÇÃO PESSOAL E A SUA TUTELA

Informação é informação, não é matéria nem energia

Norbert Wiener

A informação costuma ser referida como a "matéria-prima" de novos processos econômicos e sociais desencadeados na Sociedade da Informação. A informação pessoal, especificamente, desponta como uma verdadeira *commodity* em torno da qual surgem novos modelos de negócio que, de uma forma ou de outra, procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias da informação. Neste cenário, é mais do que natural que a informação assuma grande relevância, tanto como um bem jurídico ou econômico.

A contemplação destes processos pelo ordenamento jurídico não se faz sem algumas dificuldades quase crônicas. A informação possui algumas características, sejam ontológicas ou então decorrentes da dinâmica de sua utilização, que tornam a sua análise a partir das categorias tradicionais do direito um tanto árdua. É justamente esta peculiaridade que torna útil uma breve incursão ao exame das características e possibilidades da informação antes de adentrar propriamente em sua problemática.

A dificuldade em determinar as características da informação e, consequentemente, de enquadrar seus eventuais efeitos jurídicos, se demonstrou patente à medida em que ela se desprendia dos meios físicos que lhe garantiam uma forma concreta. Tome-se como exemplo um livro: o livro é, hoje, tanto um objeto como uma metáfora de um objeto; tanto um produto com existência concreta em papel como algo metaforizado em um conjunto de informações mantidas e transmitidas em meio eletrônico.

Um dos autores que se defrontou diretamente com este problema, Norbert Wiener, notou esta peculiar característica da informação e, em sua conhecida declaração de que "informação é informação, não

é matéria nem energia"[4] - ressaltando uma eventual estraneidade da informação em relação aos elementos do mundo físico, a matéria e a energia. Afora as possíveis derivações desta afirmação, o que é relevante no momento é que a informação passou a ser percebida como uma nova força motriz, cujas características eram novas.

O homem pode ser considerado, sob certo ângulo, como um processador de informações, tal como de alimentos e energia. O homem recebe informações, delimita seu universo a partir das informações que recebe. Suas ações podem ser determinadas pelas informações que obtém, bem como pelo uso que faz delas. Por outro lado, o homem também é produtor de informações. Informações estas que podem igualmente influenciar outros homens, modelando a impressão e a concepção que outras pessoas tenham sobre cada um de nós.

Em suma, como uma série crescente de ações humanas e, consequentemente, de relações jurídicas, passam pelo filtro da informação, a garantia da fluidez e da ausência de distorções no fluxo de informações para a pessoa e, ao inverso, a partir da pessoa, constitui-se em um dos mais relevantes problemas jurídicos do nosso tempo.

Assim considerado, o núcleo básico do problema jurídico da informação pode ser identificado nos instrumentos destinados a: (i) proporcionar aos interessados a tutela de suas próprias informações; (ii) proporcionar acesso a informações de qualidade e relevância.

O desenvolvimento acelerado das tecnologias da informação suscitou a elaboração de instrumentos que garantam ambas as necessidades. No entanto, como ocorre em situações nas quais o direito é chamado a regular um cenário moldado por uma tecnologia de ponta cujos contornos ainda não se encontram bem definidos, a própria compreensão deste cenário bem como a avaliação dos métodos de maior eficácia costumam ser tormentosos. Assim, torna-se necessário, igualmente, que o ordenamento jurídico facilite e garanta a utilização das novas tecnologias da informação, ao mesmo tempo que estabeleça meios de garantia e proteção contra utilizações indesejáveis destas mesmas tecnologias.

4 "information is information not matter or energy". Norbert Wiener. Cybernetics. Cambridge: MIT Press, 1961.

1.1. Informação e direito

O tema da informação é frequentemente abordado pelo ordenamento em torno de cortes específicos, como, por exemplo, a liberdade de informação, o acesso à informação ou a proteção de informações pessoais. Nestes e em outros casos, o conceito de informação não é tratado de maneira uniforme, o que pode se tornar problemático à medida em que a informação torna-se cada vez mais um elemento central e estes diversos cortes passam também a interagir e a se influenciar mutuamente. Cumpre, portanto, uma breve inclusão sobre a atual posição do conceito de "informação" para o ordenamento.

Em primeiro lugar, observe-se a frequente sobreposição entre os termos "dado" e "informação". O conteúdo de ambos se sobrepõe em várias circunstâncias, o que acarreta uma inadequação na utilização de um termo por outro. Ambos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular.

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

Uma certa polissemia do próprio conceito de informação é claramente visível na obra de Pierre Catala, pioneiro ao abordar de forma sistemática esta temática em seu esboço de uma teoria jurídica da informação, classificando-a em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios; (ii) as opiniões subjetivas das pessoas; (iii) as obras do espírito; e finalmente (iv) as informações que, fora das modalidades anteriores, referem-se a "descrições de fenômenos, coisas, eventos"[5].

Assim, verificamos que o termo "informação" pode se prestar a sintetizar, em determinados contextos, a própria liberdade de informação como fundamento de uma imprensa livre, bem como o próprio direito à informação. O direito à informação se constitui, de fato, na primeira manifestação concreta do

5 Pierre Catala, "Ebauche d'une théorie juridique de l'information", in: Informatica e Diritto, ano IX, jan-apr. 1983, p. 22 (tradução livre).

interesse do ordenamento jurídico pelo tema. Sua posição como direito fundamental hoje é bastante sólida, como o atesta o artigo XIX da Declaração Universal dos Direitos Humanos:

> "*Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e idéias por quaisquer meios e independentemente de fronteiras".*

O direito à informação reflete diretamente uma concepção de liberdade que permite, em suma, proporcionar meios para que o homem interprete de forma autônoma o mundo que lhe cerca, bem como para dele participar de forma ativa.

Um outro perfil particularmente instigante da informação, que apresenta imensa importância para a sua relação com a liberdade contemporânea está ligada ao que interessa diretamente a este trabalho, que é o regime a ser aplicado ao tratamento de informações pessoais.

A informação pessoal é definida comumente como a informação referente a uma pessoa determinada ou determinável[6], apresentando uma ligação concreta com a pessoa. Esta modalidade de informação vem se tornando constantemente mais disponível para uma miríade de utilizações, basicamente por conta da facilidade e do baixo custo de sua coleta e armazenamento com os meios digitais hoje disponíveis.

O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa. Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras. É importante estabelecer este

6 Esta é a base da definição presente tanto no Art. 2 da Convenção n. 108 do Conselho da Europa para a proteção dos indivíduos em relação ao processamento automatizado de dados pessoais como no Art. 1 das Linhas-Guia da OCDE sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais ("personal data" means any information relating to an identified or identifiable individual ('data subject')"). Esta base foi assimilada pela Diretiva Europeia 95/46/CE em seu Art. 2º, que define como "'Dados pessoais "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); (…)". Tal disposição encontra-se incorporada nas várias normativas europeias sobre o tema, por exemplo no Art. 3º da Lei da Proteção de dados (Lei nº 67/98) de Portugal ou no § 3 (1) da Lei Federal de Proteção de Dados da Alemanha.

vínculo concreto e direto, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre uma pessoa, por exemplo, não possuem este vínculo concreto e direto; do mesmo modo que a produção intelectual de uma pessoa, em si considerada, não é *per se* informação pessoal (embora o fato de sua autoria o seja). Pierre Catala identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> "*Ainda que a pessoa em questão não seja a 'autora' da informação, no sentido de tê-la concebido vountariamente, ela é a titular legítima de seus elementos. O seu vínculo com o indivíduo é por demais estreito para que fosse de outra forma. Quando o objeto da informação é um sujeito de direito, a informação é um atributo da personalidade*."[7]

A vinculação da informação pessoal com a personalidade, aqui apontada por Catala, aproxima a tutela das informações pessoais da própria tutela da personalidade e, portanto, dos direitos da personalidade - o que é plenamente justificado pelo reconhecimento de que os dados pessoais são emanações imediatas da própria personalidade, sendo necessário aplicar a estes a tutela devida àqueles que Adriano De Cupis denominou de "direitos essenciais"[8] ou que Paulo Mota Pinto nominou como "um círculo de direitos mínimos"[9] - os direitos da personalidade. As diversas peculiaridades derivadas de fatores como a natureza da informação pessoal ou da sua própria vocação para movimentar mecanismos para sua exploração econômica, porém, tornaram necessário o desenvolvimento de meios de tutela específicos que, se por um lado vão além do instrumental tradicionalmente desenvolvido para a tutela dos direitos da personalidade, destina-se ao fim à tutela da personalidade.

---

7 Pierre Catala, "Ebauche d'une théorie juridique de l'information", in: Informatica e Diritto, ano IX, jan-apr. 1983, p. 20 (tradução livre).

8 "Existem certos direitos sem os quais a personalidade restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto: direitos sem os quais todos os outros direitos subjetivos perderiam todo o interesse para o indivíduo - o que equivale a dizer que, se eles não existissem, a pessoa não existiria como tal. São esses os chamados direitos essenciais, com os quais se identificam precisamente os direitos da personalidade". Adriano De Cupis. Direitos da Personalidade. Lisboa: Livraria Morais. 1961, p. 17; no original: I diritti della personalità, Milano, Giuffrè, 1982, p.13.

9 Carlos Alberto da Mota Pinto, Teoria geral do direito civil. 3a ed. Coimbra: Ed. Coimbra, 1996. p. 87

1.2. Bancos de dados

A sistematização de grandes volumes de informação tornou-se possível com o advento do processamento automatizado de informações, por meio de bancos de dados automatizados. O aumento no volume de tratamento de informações pessoais assim conseguido não foi, porém, meramente quantitativo, pois resultou na viabilização de várias práticas de coleta, tratamento e utilização de informações pessoas que antes, na perspectiva dos arquivos manuais, eram impossíveis ou não se justificariam. Assim, uma série de novas possibilidades para a utilização de dados pessoais surgiu com o advento dos bancos de dados pessoais automatizados.

Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica[10] – e esta lógica costuma ser uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. Que a informação seja capaz de gerar proveito resulta claro ao verificar que é milenar a prática de coleta sistematizada de informações por alguma modalidade de censo populacional, instrumento de imensa serventia para governantes de qualquer época – a ponto dos registros históricos a respeito não serem poucos.

A informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna um elemento fundamental de um crescente número de relações e aumenta sua possibilidade influir em nosso cotidiano, em um crescendo que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais - conforme notou Stefano Rodotà ainda em 1973, "(...) a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada".

10 É nesta chave que, por exemplo, a Lei de direitos autorais (Lei 9.610/96) refere-se, em seu Art. 7º, XIII, à possibilidade de englobar as bases de dados no rol de obras protegidas como criação intelectual, reconhecendo a "seleção, organização ou disposição de seu conteúdo" como critérios para fundamentar esta proteção.

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

1.3. Informação e dados pessoais

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

> *"Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade"*[11].

11 Pierre Catala., "Ebauche d'une théorie juridique de l'information", in: Informatica e Diritto, ano IX, jan-apr. 1983, p. 20.

O Conselho Europeu, através da Convenção de Strasbourg, de 1981, ofereceu uma definição que condiz com esta ordem conceitual. Nela, informação pessoal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação"[12]. É explicito, portanto, o mecanismo pelo qual é possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

Em relação à utilização dos termos "dado" e "informação", vale especificar que os termos se sobrepõem em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos servem para representar um fato, um determinado aspecto de uma realidade. No entanto, cada um carrega um peso particular a ser levado em conta.

Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos em um autor que o entende como uma informação em estado potencial, antes de ser transmitida[13]; o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. A doutrina não raro trata estes dois termos – dado e informação - indistintamente, ou então, procede a uma diferenciação algo empírica que merece ao menos ser ressaltada.

Deve-se lembrar ainda que o termo "informação" presta-se igualmente, em certos contextos, a representar diversas ordens de valores. Assim, a "liberdade de informação" como fundamento de uma imprensa livre, bem como seu co-respectivo "direito à informação"[14] podem possuir conteúdo específico e que são mais remotamente relacionados ao tema deste artigo, como no caso do dever de informação pré-contratual do Código de Defesa do Consumidor.

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno desta relação, porém pode

12 Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º.

13 Raymond Wacks. Personal information. Oxford: Clarendon Press, 1989, p. 25.

14 Sobre o tema, v. Luis Gustavo Grandinetti de Carvalho. Direito de Informação e Liberdade de Expressão. Rio de Janeiro: Renovar, 1999.

servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Com o aludido aumento da importância da informação de uma forma geral, foi justamente em torno dela que a temática da privacidade passou a orbitar, em especial ao se tratar de dados pessoais[15]. Esta guinada, que acabou por plasmar o próprio conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas poderiam ser a concepção de uma *informational privacy* nos Estados Unidos, cujo "núcleo duro" é composto pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Federal alemão[16] e a Diretiva 95/46/CE da União Européia (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), com todas as suas conseqüências.

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

1.4. Classificação da informação pessoal - dados sensíveis

A informação pessoal pode agrupar-se em subcategorias, ligadas a determinado aspecto da vida de uma pessoa. Uma tal classificação pode ser o pressuposto para a qualificação das normas a serem aplicadas a determinadas categorias de dados pessoais, assim como acontece para as normas que, por exemplo, aplicam-se diretamente às informações referentes a movimentações bancárias de uma pessoa, que enquadrariam-se no chamado sigilo bancário. Esta setorização pode servir a escopos diferentes, desde uma

15 Sobre o tema, v. Danilo Doneda. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar: 2006.

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

fragmentação da tutela – que se estruturaria em torno de contextos setoriais, e não da pessoa – ou então, dentro de um panorama de tutela integral da pessoa, para mera especificação da abordagem a ser dada.

Neste último sentido, a prática do direito da informação deu origem à criação de uma categoria específica de dados, os dados sensíveis. Estes seriam determinados tipos de informação que, se conhecidas e processadas, prestariam-se a uma potencial utilização discriminatória[17] ou lesiva, particularmente mais intensa e que apresentaria maiores riscos potenciais que a média. Alguns destes dados seriam as informações sobre raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo.

A categoria de dados sensíveis é fruto de uma necessidade pragmática, além de ser importante por exorbitar os cânones "tradicionais" ligados à privacidade, ao revelar a presença de um outro valor digno de tutela neste caso, o princípio da igualdade material, como o seu fundamento[18]. A própria seleção de quais seriam tais dados provém da avaliação de que a circulação de determinadas espécies de informação apresentariam um elevado potencial lesivo aos seus titulares.

A elaboração desta categoria e de disciplinas específicas a ela aplicadas não foi isenta de críticas, como a que afirma que é impossível, em última análise, definir antecipadamente os efeitos do tratamento de uma informação, seja ela da natureza que for[19]. Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo[20].

---

17 Quando determinados "testes de personalidade", realizados como parte da seleção de empregados, passaram a ser contestados, um dos motivos levantados foi o de que eles eventualmente revelariam para o empregador mais do que somente a aptidão para o trabalho e, potencialmente, poderiam revelar informações pessoais que o candidato não estivesse inclinado a revelar e que pudessem facilitar a utilização de critérios discriminatórios para a escolha dos empregados. A investigação realizada fez com que algumas empresas e órgãos governamentais cessassem a aplicação de tais testes, reconhecendo que eles "incluem questões de natureza personalíssima com relação a sexo, moralidade, relações paternas e outros assuntos". Tais questões aproximam-se da noção de dados sensíveis que posteriormente se desenvolveu. Alan Westin. Privacy and freedom, New York: Signet, 1972, pp. 259-260.

18 Stefano Rodotà. Tecnologie e diritti, Bologna: Il Mulino, 1995, p. 85.

19 Vittorio Frosini. Contributi ad un diritto dell'informazione, Napoli: Liguori, 1991, pp. 128-129.

20 "... My name in the London telephone directory or the electoral roll is perfectly harmless, but may name in a list of potential subversives or bad credit risks is capable of doing me harm. There are no harmless data, there are no harmful data. A datum is a datum – it is that which is given. It is what data you string together and what you do with them … which may or may not do harm". Paul Sieghart, "Information privacy and the data protection bill", in: Data protection: Perspectives on information privacy. Colin Bourn; John Benyon (eds.). Leicester: University of Leicester, 1984 apud Colin Bennett. Regulating privacy, Data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, p. 35.

Um outro problema é que a mera proibição da coleta e tratamento – recurso utilizado por algumas das leis sobre a matéria - demonstra-se inviável, pois ocasionalmente o uso de tais dados é legítimo e necessário[21]; além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações deste gênero, como algumas entidades de caráter político, religioso ou filosófico[22]. O tratamento de dados sensíveis é, portanto, possível e mesmo necessário em uma série de circunstâncias, porém deve ser sempre uma exceção justificada pela relevância dos valores em questão e verificado que não há possibilidade de que seja realizada uma utilização discriminatória dos dados.

O regime adotado em relação aos dados sensíveis varia de acordo com as concepções a este respeito em cada ordenamento[23]. Na verdade, deve-se ter em conta que o próprio conceito de dados sensíveis atende à uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal conseqüência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos.

Hoje, no entanto, o próprio conceito de dados sensíveis como fator que fundamenta uma proteção de nível mais elevado tende a ceder à noção de tratamento sensível de dados pessoais. Esta tendência provém do reconhecimento de que não é possível, hoje, predizer os efeitos que um tratamento de dados pessoais possa causar ao seu titular apenas a partir da consideração da natureza dos dados que são tratados. Com as modernas técnicas estatísticas e de análise de dados, até mesmo informações pessoais que, em si, não são sensíveis podem causar tanto (i) um tratamento discriminatório em si, quanto (ii) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não-sensíveis. Em ambos os casos ocorre, efetivamente, justamente aquilo que se procura inibir com a criação de um regime especial para os dados sensíveis, que é a discriminação a partir do tratamento de dados pessoais.

---

21 Tome-se, por exemplo, a pesquisa de caráter científico ou mesmo a atividade médica, para as quais a importância de trabalhar com todos os dados possíveis, inclusive os sensíveis, é capital. Para situações deste tipo são freqüentemente estabelecidos regimes de permissão do tratamento de dados sensíveis, quando a vedação é a regra.

22 Spiros Simitis. “From the market to the polis: The EU Directive on the protection of personal data”, in: 80 Iowa Law Review 445, p. 450.

23 Na França, a Lei 78-17 de 6 de janeiro de 1978 (a lei Informatique et Libertés) proíbe sua utilização, no artigo 31: «Il est interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de l’intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les moeurs des personnes». A própria lei, porém, estabelece regimes de exceção a esta regra. Na Alemanha, ao contrário, a concepção dominante é a de não estabelecer um regime a priori diverso para os dados sensíveis.

1.5. Técnicas de tutela para os dados pessoais

À medida que ganha relevo a utilidade da informação, várias estruturas sociais a recebem como um de seus elementos fundamentais[24]. Neste processo, ela se apresenta ao ordenamento jurídico como um elemento plural, capaz de desencadear processos cujas conseqüências podem ser reconduzidas a um denominador comum somente após um certo esforço.

Dentro do direito privado especificamente, uma opção para tratar desta problemática seria o reconhecimento da qualidade de bem jurídico à informação e, a partir disso, o recurso aos instrumentos do direito de propriedade para a sistematização do tema[25]. O fato da informação não ostentar diretamente um valor não impede a sua verificação e o tratamento específico da informação em diversas circunstâncias, como no sistema da propriedade intelectual, por exemplo.

Uma parcela significativa da doutrina refere-se à identificação de um direito de propriedade sobre os dados pessoais como uma solução para a matéria, assumindo que a criação de um mercado para estes bens proporcionaria uma solução para os problemas através dos mecanismos da teoria econômica para otimização de custos e benefícios[26]. Tal tendência é condizente com o fato que as diversas restrições ao fluxo de informações acabam por criar uma demanda, a ser equacionada ainda dentro do direito privado.

Considerar a informação como um bem jurídico e estender a tutela de caráter patrimonial para os dados pessoais, no entanto, não parece uma solução adequada, em vista da multiplicidade de situações e interesses em torno dos próprios dados pessoais, que não se limitam aos vetores patrimoniais e que seriam irremediavelmente prejudicados se considerados apenas a partir de seu valor econômico.

---

24 A ciência econômica reconhecia na própria natureza da informação a dificuldade clássica em individuá-la para um tratamento objetivo: "... a teoria econômica clássica partia do pressuposto de que a informação constituía por natureza um bem público (public good), livremente disponível e acessível (free flow). Seguia-se que, em virtude do seu caráter difuso, a informação não podia ter um valor econômico". John Oliver. Law and economics. An introduction. George Allen & Urwin, 1979, p. 72.

25 Maria Eduarda Gonçalves. Direito da informação. Coimbra: Almedina, 1995, p. 10.

26 v. James Rule; Lawrence Hunter. "Towards a property right in personal data", in: Visions of privacy: Policy choices for the digital age. Colin Bennett. Toronto: University of Toronto Press, 1999, pp. 165-181. Lawrence Lessig, em análise sobre o tema da privacy e da proteção de dados pessoais, propõe um mecanismo de proteção em moldes proprietários, em consonância com tradicional tendência dentro da cultura jurídica norte-americana e, em especial, com a influência de Richard Posner. Esta conclusão (e outras) de Lessig foi analisada em detalhe nas críticas de Marc Rotenberg. "What Larry doesn't get", in: Stanford Technology Law Review, 1/2001, <stlr.stanford.edu>; e de David Post. "What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace", in: 52 Stanford Law Review 1439 (2000).

Esta ampla gama de interesses que se relacionam com a informação revela-se nas ocasiões como no caso típico do direito de autor. Neste caso, a informação que preenche determinados requisitos – por exemplo, originalidade, exterioridade, caráter artístico, literário ou científico, autoria etc. – passa a ser uma obra de titularidade (na maioria das vezes) do seu autor[27]. Estabelece-se assim um direito real (além dos direitos pessoais incluídos no caso) que possibilita a exploração comercial da obra pelo seu autor, uma das finalidades do sistema de direito autoral.

O problema, porém, se encontra além do fato de considerar ou não a informação como um bem jurídico, mas em possibilitar que ela seja abordada pelo ordenamento jurídico de forma hábil a possibilitar a atuação de todos os interesses em questão e dos valores a serem ponderados[28], sob pena de distorções por conta da utilização de institutos jurídicos cujas características remontam a outra realidade.

Em uma perspectiva diversa podemos observar um processo de objetivação relacionado aos dados pessoais que, sem corresponder a uma patrimonialização, os considera como elementos objetivos da abordagem que a matéria vem recebendo[29]. Conforme veremos, esta disciplina desenvolve-se no sentido de estabelecer referências objetivas na informação em si e não somente no sujeito ao qual ela é relacionada. Assim, limites e barreiras que atuam diretamente sobre a informação são estabelecidos pela lei, que passa a sujeitar diretamente a informação. Esta objetivação da informação pessoal, porém, tem caráter instrumental e atende mais a critérios de funcionalidade das medidas legislativas do que ao processo de sua assimilação a um sistema de tutela baseado em direitos reais (mesmo que com adaptações)[30]. Surge a necessidade de uma tutela dinâmica, que acompanhe os dados em sua circulação, sem concentrar-se no sujeito (como ocorre geralmente quando se trata do direito à privacidade). A informação pessoal pode ser desvinculada da pessoa, em um certo sentido: ela pode circular, submeter-se a um tratamento, ser comunicada etc. Porém, até o ponto em que continue sendo uma informação "pessoal", isto é, que identifique a pessoa a qual se refere, ela mantém um vínculo específico com ela, e sua valoração específica deve partir deste dado básico. Por força da vinculação intrínseca entre a informação pessoal e a pessoa à qual ela se refere, que é efeito dos dados serem sua representação direta, tal informação deve ser entendida como uma extensão da sua personalidade.

---

27 V. Lei de Direitos Autorais, Lei 9.610/98.

28 Davide Messinetti exclui, a priori, este raciocínio ao estabelecer um perfil do tratamento jurídico da informação: "Sotto il profilo giuridico, ragionare in termini de "appropriazione" non aiuta a centrare il tipo di problema proposto". David Messinetti. "Circolazione dei dati personali e dispositivi de regolazione dei poteri individuali", in: Rivista Critica del Diritto Privato, 1998, p. 346.

29 Tal objetivação teve como conseqüência até mesmo o nome algo falacioso pelo qual a matéria é geralmente conhecida: na "proteção de dados pessoais" - cujo objetivo final não é a tutela dos dados pessoais em si, porém das pessoas às quais estes dados se referem

30 Neste sentido, v. Ettore Giannantonio. "Dati personali" (verb.) in: Enciclopedia del diritto. Aggiornamento vol. VI, Milano: Giuffrè, 2002, pp. 351-358.

1.6. Dados pessoais e o direito da informática

O desenvolvimento acelerado da informática a partir da década de 1950 suscitou a atenção do jurista, o que deu vazão a estudos pioneiros sobre a área. Um dos precursores foi Lee Loevinger, que denominou de *Jurimetrics* (Jurimetria) uma disciplina que estudaria a utilização de métodos informáticos aos processos de decisão típicos do direito[31]. Termos como *computer law* começaram a ser utilizados, e uma primeira cátedra universitária relativa à nova área, denominada *information technology law*, surgiu no ano de 1960 na Universidade de Londres[32].

Em síntese, emular uma disciplina que compreenda uma metodologia da problemática jurídica da informação relacionada às tecnologias da informação é algo que pretendem, em graus diversos, as chamadas *computer law*, *cyberlaw*, o "direito da informática", e mesmo um "direito da informação"[33] ou *information law*, entre outras, que almejam incluir as regras, conceitos e princípios relativos aos procedimentos tecnológicos do processamento eletrônico de informações[34]. Todavia, tal profusão de rótulos que pretendem abarcar a disciplina jurídica da informação nas diversas partes de seu espectro há de ser vista mais como reflexo do processo de formação de espaços de discussão e experimento, do que uma verdadeira solução de continuidade com uma determinada tradição jurídica[35].

Não se trata propriamente, neste caso, de meramente definir critérios formais para associar determinada matéria a um ramo do direito; o que é mais importante é que se abram espaços para a reflexão jurídica em torno desta problemática, reconhecendo e adaptando-se às suas peculiaridades, com o cuidado de não fugir do domínio do direito. Neste ponto, cumpre estar atento para tentativas de subtrair algum aspecto da realidade

---

31 Lee Loevinger propunha, mais precisamente, a utilização de métodos das ciências consideradas exatas e, em especial, da informática, no campo do direito. Em seu primeiro artigo sobre o assunto ("Jurimetrics", in: Minnesota Law Review, 33/1949, p. 455-ss.), propunha, por exemplo, a criação de um enorme banco de dados que os agentes encarregados da proteção antitrust deveriam estudar para determinar se uma determinada empresa se encontrava em uma posição dominante. Ainda hoje a escola de Loevinger e da Jurimetria marca sua influência na obra de autores como o italiano Mario Lozano, além de contar com o periódico Jurimetrics para sua divulgação.

32 Vittorio Frosini. "Towards information law", in: Informatica e diritto. vol. V, n. 2, 1995, p. 10.

33 Como em Maria Eduarda Gonçalves. Direito da informação, cit.

34 Vittorio Frosini. "Towards information law", cit., p.12.

35 Críticas contra a nominação e a própria existência destas novas "disciplinas" jurídicas não faltam, geralmente focadas sobre dois argumentos: o de que a tecnologia não apresenta, per se, elementos os quais o direito já existente, com sua flexibilidade, não possa resolver; e também que o direito que se agrupa em torno da tecnologia não possui a coerência sistemática suficiente para formar uma disciplina jurídica. v. Joseph Sommer. "Against ciberlaw", in: Berkeley Technology Law Journal, 15:3, 2000, <www.law.berkeley.edu/journals/btlj/articles/vol15/sommer/sommer.html>.

tecnológica da regulação jurídica, tentativas que podem remeter a uma eventual opção de caráter ideológico e se fundamentariam tecnicamente em uma interpretação distorcida do particularismo da matéria.

O advento da informática e as mudanças políticas e sociais que lhe são correlatas constituem um ponto de inflexão em torno do qual sua problemática jurídica muda de dimensão, não somente em termos quantitativos como também qualitativos. O mero fato da informação ser processada por computadores representa, por si, uma mudança nas conseqüências de seu tratamento. Alguns destes efeitos são mensurados quantitativamente, isto é, são decorrência do maior volume de informação que pode ser processado. Porém, não é somente a quantidade de informação processada que diferencia o tratamento informatizado de dados, mas também novos métodos, algoritmos e técnicas podem ser utilizados para este fim, operando igualmente uma mudança *qualitativa* no escopo do tratamento de dados pessoais.

O diferencial que a informatização proporcionou ao tratamento de dados pessoais apresenta, portanto, um perfil quantitativo e outro qualitativo; um baseado na "força bruta", no poder de processar mais dados em menos tempo, e o outro em aplicar técnicas sofisticadas a este processamento de forma a obter resultados mais valiosos. Combinados, representam a base técnica que potencialmente pode ser aplicada a toda coleta de dados pessoais e que deve ser levada em consideração em qualquer enfoque funcional da disciplina de dados pessoais. O quadro pode ser representado também em outros termos, como o econômico, ainda que correndo-se o risco de uma análise mecanicista de uma situação complexa: Roberto Pardolesi, por exemplo, afirma que, graças ao desenvolvimento dos meios de armazenamento e processamento de dados, cresceria exponencialmente o custo para se manter uma informação em segredo; a privacidade ficaria mais custosa, à medida que se torna mais econômica e acessível a utilização dos dados pessoais[36].

1.7. Mudança qualitativa no tratamento de dados pessoais

A mudança *qualitativa* no tratamento dos dados pessoais, à qual aludimos, baseia-se na utilização de novos métodos, algoritmos e técnicas. De algumas destas técnicas nos ocuparemos e traçaremos breve descrição.

36 Roberto Pardolesi. "Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità", in: Diritto alla riservatezza e circolazione dei dati personali. Milano: Giuffrè, 2003, p. 11.

Dentre elas está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. Esta técnica, conhecida como *profiling*, que iramos explorar mais adiante neste trabalho, pode ser aplicada a indivíduos bem como estendida a grupos. Nela, os dados pessoais são tratados, com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de formular uma "meta-informação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros vários da vida desta pessoa. O resultado possibilita obter um quadro das tendências de futuras decisões e comportamentos de uma pessoa ou grupo. A técnica pode ter várias aplicações desde, por exemplo, o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais se atribuísse maior possibilidade de realizar atos contra o interesse nacional; bem como uma finalidade privada, como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores (possibilitando, portanto, a publicidade comportamental), dentre inumeráveis outras.

Um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, pois seria o seu único aspecto visível a diversos sujeitos que com ela interagem. Este perfil estaria, em diversas circunstâncias, fadado a se confundir com a própria pessoa[37].

A partir do momento em que um perfil eletrônico é a única parte da personalidade de uma pessoa visível a alguém, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que entes com os quais ela se relaciona levam em consideração o pressuposto de que ela adotará um comportamento pré-definido de acordo com seu determinado perfil aliado a técnicas preditivas de seu comportamento, o que tem como conseqüência uma efetiva diminuição de sua liberdade de escolha[38].

O fato deste "perfil" ser algo que se contraponha à própria realidade da pessoa foi notado por vários autores, que verificaram a criação de um nosso correlato digital, um *corpo eletrônico*, composto de nossos dados. Tal idéia mostra-se recorrente, embora externada por meio de uma terminologia variada – como *digital persona*[39], *avatar* ou pessoa virtual. Pierre Lévy procura ilustrá-la:

---

37 Danièle Bourcier. "De l'intelligence artificielle à la personne virtuelle: émergence d'une entité juridique ?», in : Droit et Société, n. 49, 2001, p. 850.

38 Para além do senso comum de que "não se oferece comida de cães para os proprietários de gatos", a utilização de técnicas de *direct marketing* e, de forma geral, o aumento das informações em mãos de fornecedores sobre os consumidores apresenta uma série de implicações que podem efetivamente cercear a liberdade de escolha do consumidor. v. Simson Garfinkel. Database nation. Sebastopol: O'Reillly, 2000, passim, esp. pp. 155-175.

39 "The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual". Roger Clarke. "The digital persona and its application to data surveillance", in: The Information Society, 10, 2 (junho 1994) apud Richard Turkington; Anita Allen. Privacy law. Cases and materials. St. Paul: West Group, 1999, p. 313.

> *"O meu corpo pessoal é a manifestação temporária de um enorme 'hipercorpo' híbrido, social e tecnobiológico. O corpo contemporâneo se assemelha a uma chama. Ele costuma ser minúsculo, isolado, separado, quase imóvel. Depois, ele chega a fugir de si mesmo, intensificado pelos esportes ou pelas drogas, passa através de um satélite, ergue ao céu um braço virtual bem alto..."*[40].

Alan Westin cunhou o termo *data shadow*[41] – sombra de informações – como uma metáfora para identificar fatos e opiniões de uma pessoa armazenados em bancos de dados, que a acompanham por onde quer que ela vá. Talvez no caso do *data shadow* a metáfora da sombra tenha sido condescendente, pois há ocasiões em que o mero fato de que informações sobre uma determinada pessoa são colhidas ou levadas em consideração pode passar inteiramente despercebido por ele próprio, por mais atento que ele esteja - a *data shadow* pode ser, portanto, mais discreta do que a verdadeira sombra.

O processo de coleta de informações pessoais, se não é algo novo em si, desenvolveu-se bastante com a sofisticação das estruturas administrativas estatais e privadas. Com o advento do computador e da possibilidade de digitalizar informações, ela se torna mais útil e também praticamente onipresente. Juntamente com a circulação destas informações, estes seriam os requisitos para a construção da *datasphere* – um conjunto de informações que compreenderia dados sobre nós e nossas ações:

> *"Uma vez que os eventos do nosso cotidiano são sistematicamente armazenados em um formato legível por uma máquina, esta informação ganha uma vida toda própria. Ela ganha novas utilidades. Ela se torna indispensável em operações comerciais. E ela usualmente é transmitida de um computador a outro, de um negócio a outro, entre os setores público e privado"*[42].

---

40 Pierre Lévy. Qu'est-ce que le virtuel? Paris: La Découverte, 1998, p. 30.

41 Alan Westin. Privacy and freedom. New York: Atheneum, 1967, pp. 163-168.

42 Simson Garfinkel. Database nation, cit., p. 75.

Uma outra técnica bastante utilizada é a do *data mining*. Ela consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos[43]. Assim, a partir de uma grande quantidade de informação em estado bruto e não classificada podem ser identificadas informações de potencial interesse[44].

A possibilidade de se obter informações úteis a partir do *data mining* cresce à medida em que aumenta a quantidade de informação em "estado bruto" disponível. Esta é a conseqüência do aumento da capacidade de armazenamento de informações em diversos tipos de memória, desde os remotos cartões perfurados, passando pelos DVD-ROM e chegando ao panorama atual da *cloud computing*. Uma maior quantidade de informação pode ser armazenada a um custo cada vez menor, em uma linha evolutiva que vem de décadas e que não será interrompida em um futuro tão próximo. A informação que provavelmente não seria sequer registrada sem o auxílio do computador, ou que seria apagada de sua memória caso os custos de armazenamento fossem maiores, tem maior chance de permanecer armazenada com os atuais custos de armazenamento. Desloca-se, assim, do paradigma do esquecimento para um outro paradigma, o da Memória, de acordo com a imagem evocada por Viktor Mayer-Schönberger[45].

Esta dinâmica apresenta implicações no que interessa às informações pessoais. Aumenta a quantidade de informação disponível sobre uma pessoa em várias bases de dados, informações estas que podem influenciar a sua vida futura – uma simples busca na Internet pelo nosso nome ou pelo de pessoas conhecidas pode, em vários casos, elucidar o significado prático do registro aleatório de informações a nosso respeito. Ganha peso a imagem do computador como o cão de guarda da sociedade da informação, que não esquece jamais. Vance Packard, ciente desta situação, alertou para seus efeitos, ainda em 1966:

> *"Hoje, com episódios de nosso passado sendo cada vez mais armazenados em aquivos de computadores, a possibilidade de 'começar de novo' está se tornando sempre mais difícil. A noção cristã de redenção é incompreensível para o computador"*[46].

43 Daniele Bourcier. "De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ?», cit., p. 851.

44 Alguns grandes sistemas já se utilizam desta técnica, como o controverso sistema ECHELON, que filtra informações interceptadas a partir de redes de telecomunicações para análise de pressupostos objetivos de segurança (v. Estudo realizado para o Parlamento Europeu: Duncan Campbell. "The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition", in: <www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf>.

45 Viktor Mayer-Schönberger: Delete. The Virtue of Forgetting in the Digital Age. Pinceton: Princeton University Press, 2009.

46 Vance Packard, em depoimento ao Subcommittee of the committee on government operations. House of Representatives, in: The computer and invasion of privacy. U.S. Government Printing Office: Washington, 1966, p. 12.

Ao apontar para um futuro no qual nosso passado estaria "estampado" em nós, Packard foi um dos primeiros (senão o primeiro) a chamar a atenção para mudanças bastante concretas e pouco visíveis que estariam embutidas nestas novas tecnologias e que eram conseqüência de sua capacidade de memorização – já que as outras discussões relacionadas à erosão da privacidade costumavam relacioná-la basicamente com a tecnologia de vigilância e outras formas mais "literais", digamos, de controle. Mostrava-se embutida na utopia informática o mito da memória total, uma utopia negativa – como assunto que foi explorado por Borges em seu conto *Funes el memorioso*: o personagem Funes, após sofrer um acidente, passou a gozar de uma memória total, isto é, tornou-se incapaz de se esquecer do que quer que seja. Ele sabia de todos os detalhes de tudo que acontecia em sua vida – porém, com isso, perdeu a capacidade de agir e, em especial, de generalizar[47].

A grande dificuldade na abordagem das técnicas descritas – e de tantas outras – é que elas também encerram um dualismo que dificulta uma análise simplificada. É patente o risco de cair em um reducionismo insensível a outras aplicações da tecnologia e da "pessoa virtual", que eventualmente possam ser úteis para o desenvolvimento da personalidade ou para outros fins que não afrontem necessariamente interesses protegidos. As mesmas técnicas, utilizadas em outros contextos, podem se demonstrar úteis à expressão da própria personalidade.

Um destes casos seria a utilização do anonimato em ambientes virtuais. A possibilidade de comunicação anônima pode ser um instrumento útil para que uma pessoa se relacione dentro de um determinado meio, sem sofrer as conseqüências das pressões sociais e o risco de preconceitos (nem as benesses da exposição da própria personalidade, diga-se também). Nestas ocasiões, a utilização de um *avatar* – que funcionaria nestes casos como o pseudônimo de outrora - pode lhe proporcionar uma boa desenvoltura. Vale notar que, neste caso, pretende-se tutelar o livre desenvolvimento da personalidade através da liberdade de associação, expressão e relacionamento – que eventualmente estaria diminuída com a identificação da pessoa. Desta forma, a tecnologia torna possível o acesso a certos níveis de anonimato e pseudonímia que possibilitam a fruição de liberdades fundamentais[48].

---

47 Jorge Luis Borges. "Funes el memorioso", in: Artifícios. Madrid: Alianza, 1995, pp. 7-18.

48 A rede Internet é o espaço por excelência para o desenvolvimento destes avatares que proporcionam uma mobilidade livre de pré-condicionamentos. Esta é mesmo uma das qualidades de sua arquitetura que mais se destacaram durante sua popularização – por muito tempo circulou a máxima de que "na Internet ninguém pode saber se você não é um cão", sublinhando a tênue linha que liga a identidade virtual à certeza de uma determinada identidade real. O desenvolvimento da tecnologia da Internet, porém, mudou um pouco este quadro e talvez o mude ainda mais no futuro, com uma provável diminuição da esfera de anonimato possível na rede. v. Lawrence Lessig. The future of ideas. Vintage: New York, 2002, passim.

Esse dualismo se reflete na abordagem dada pelo ordenamento a questões do gênero. E revelam uma certa hesitação ou, como identificou Herbert Burkert, um verdadeiro desafio: hoje, o mesmo legislador que permite (e eventualmente promove) a pseudonímia e a criptografia na Internet, também busca formas de identificar quem é a pessoa atrás de cada e-mail[49], bem como procura estabelecer regras para a retenção de dados de tráfego em redes de computadores[50], em um árduo debate entre segurança e liberdades individuais cujas proporções devem ser examinadas em outra sede.

Enfim, as técnicas mencionadas – o *profiling* e o *data mining* – são, na verdade, apenas duas representações básicas das múltiplas possibilidades de obtenção de utilidades a partir de dados pessoais. Neste momento, mais do que uma análise pormenorizada destas e outras técnicas, vale ressaltar um elemento essencial a muitas modalidades de coleta e tratamento de dados pessoais: a de que elas podem provocar um distanciamento entre a informação conscientemente fornecida pela pessoa e a utilidade na qual ela é transformada.

Podemos identificar a existência de uma "informação de base", proveniente diretamente de uma pessoa, e uma "informação-resultado"[51], consistente na aplicação de um método de tratamento à informação de base, de forma a gerar alguma utilidade àquele que realiza o tratamento. Este "método" pode ser uma operação de análise estatística da informação, como pode também abranger os sofisticados meios de obtenção de informações a partir de dados brutos como o *data mining*. Porém o essencial é a mencionada diferença entre uma informação e outra – o que também é chamado de secundarização da informação. É justamente isto que terá como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade.

49 Herbert Burkert. "Privacy – data protection. A German/European perspective", in: Governance of Global Networks in the Light of Differing Local Values. Christoph Engel; Kenneth Keller (eds.). Baden-Baden: Nomos, 2000, pp. 43-69, p. 62.

50 É do que trata, dentre diversas outras normas, a Diretiva 2006/24/CE, sobre "retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending".

51 A terminologia ("informations de base" e "information-résultat") é tomada de empréstimo a Pierre Catala. Pierre Catala. cit., p. 23.

CAPÍTULO 2
PROTEÇÃO DE DADOS PESSOAIS E RELAÇÕES DE CONSUMO

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade no que hoje costumamos denominar de Sociedade da Informação[52].

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

A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo. Também destas suas características específicas deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental - uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação.

---

52 Sobre a expressão "sociedade da informação", v. David Lyon. "The roots of the information society idea", in: The media studies reader. Tim O'Sullivan; Yvonne Jewkes. (editores). London: Arnold, 1998, pp. 384-402; v. tb. Manuel Castells. A sociedade em rede (A era da informação, economia, sociedade e cultura). V. 1. São Paulo: Paz e Terra, 1999.

Considerados em si, em uma abordagem meramente técnica, os dados pessoais são meras partículas de informação que podem ser tratadas como qualquer outra. Tecnicamente, são cada vez maiores as possibilidades da informação ser colhida, apropriada, transmitida, processada ou comercializada. Do ponto de vista técnico, portanto, a informação é cada vez mais facilmente manipulável como um objeto capaz de gerar utilidades.

A proteção de dados pessoais surgiu justamente como forma de regular a utilização da informação pessoal durante o seu tratamento, isto é, nas várias operações às quais ela pode ser submetida após ter sido colhida por uma forma qualquer. Perdido o vínculo que poderíamos descrever como "físico" com seu titular, portanto, a informação pessoal manter-se-ia vinculada a ele através de um vínculo jurídico, determinados pelas normas de proteção de dados pessoais e justificadas pela identidade desta informação com a pessoa.

Técnicas de proteção da pessoa por meio da tutela de bens que dela podem se destacar não são propriamente novidade - pense-se, por exemplo, no caso de um direito da personalidade como o direito à imagem. No caso da proteção de dados pessoais, porém, a experiência demonstrou a necessidade de técnicas de tutela muito mais específicas do que as presentes no arcabouço clássico de tutela dos direitos da personalidade, seja pela complexidade técnica que envolve a matéria como pelo fato de que o processamento de dados pessoais é quase sempre opaco aos olhos do seu titular, dificultando a sua reação.

Sobre este pano de fundo desenvolveram-se, nas últimas quatro décadas, diversas normativas destinadas a regular a utilização de dados pessoais, que ficaram conhecidas como normas sobre proteção de dados pessoais, conforme examinaremos a seguir.

2.1. Desenvolvimento das leis de proteção de dados

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos, que veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados[53]. Este desenvolvimento foi intenso nas cerca de quatro décadas

53 V. José Luis Piñar Mañas, "el derecho fundamental a la protección de datos personales (LOPD)", in: Protección de datos de carácter personal en Iberoamérica. José Luis Piñar Mañas (dir.). Valencia: Tirant Lo Blanch, 2005, pp. 19-36.

que a disciplina ostenta. A mudança do enfoque dado à proteção de dados neste período pode ser entrevisto na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger[54], que vislumbra diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura a técnicas mais específicas, aplicáveis às tecnologias adotadas para o tratamento de dados.

A primeira destas gerações de leis[55] pretendia regular um cenário no qual centros de processamento de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo destas leis girava em torno da concessão de autorizações para a criação destes bancos de dados e do seu controle *a posteriori* por órgãos públicos[56]. Estas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) destas normas.

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado desta tecnologia, sem que se soubesse ao certo suas conseqüências, fez com que se optasse por princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados[57]. Este enfoque era natural, visto a motivação destas leis ter sido a "ameaça" representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática destas leis era algo tecnocrática e condicionada pela informática – nelas, tratavam-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo[58].

Estas leis de proteção de dados de primeira geração não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações. A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da "diáspora" dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a lei francesa de proteção de dados pessoais de 1978, intitulada *Informatique*

---

54 Viktor Mayer-Scönberger. "General development of data protection in Europe", in: Technology and privacy: The new landscape. Phillip Agre, Marc Rotenberg (orgs.). Cambridge: MIT Press, 1997, pp. 219-242.

55 Exemplo destas leis de primeira geração são a Lei do Land alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados, sueca, que foi o Estatuto para bancos de dados de 1973 – Data Legen 289, ou Datalag, além do Privacy Act norte-americano de 1974.

56 José Adércio Leite Sampaio. Direito à intimidade e à vida privada. Belo Horizonte: Del Rey, 1997., p. 490.

57 cf. Spiros Simitis. "Il contesto giuridico e politico della tutela della privacy", in: Rivista Critica del Diritto Privato, 1997, p. 565.

58 Viktor Mayer-Scönberger. "General development of data protection in Europe", cit., pp. 223-224.

et Libertées[59]. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão[60].

Não tardou para que se observasse novamente um mudança de paradigma na matéria: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito freqüentemente na sua exclusão de algum aspecto da vida social. Uma terceira geração de leis, surgida na década de 80, procurou sofisticar a tutela dos dados pessoais, que continuou centrada no cidadão, porém passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa.

A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas neste sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava inclui-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nesta relação que não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa. Outra técnica é, paradoxalmente, a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre por conta do pressuposto de que determinadas modalidades de tratamento de dados

59 Lei 78-17 de 6 de Janeiro de 1978.

60 Como representante desta geração de leis, podemos mencionar também a lei austríaca (Datenschutzgesetz (DSG), Lei de 18 de outubro de 1978, nº 565/1978); além de que as constituições portuguesa e espanhola apontam neste sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde.

pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual – como é o caso para certas modalidades de utilização de dados sensíveis.

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

2.2. Princípios de proteção de dados pessoais

Mesmo com a mudança de perfil das leis de proteção de dados com a sua maturação, é possível reagrupar seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em vários ordenamentos – no que podemos verificar uma interessante convergência das soluções legislativas sobre a matéria em diversos países bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e, de certa forma, a sua vinculação com a proteção da pessoa e com os direitos fundamentais.

O núcleo básico dos princípios de proteção de dados que até hoje são utilizados tem as suas origens em uma série de discussões que, na segunda metade da década de 1960, acompanhou a tentativa do estabelecimento do *National Data Center* - que consistiria basicamente em um gigantesco e jamais realizado banco de dados sobre os cidadãos norte-americanos para uso da administração federal[61].

61 O National Data Center foi projetado para reunir as informações sobre os cidadãos norte-americanos disponíveis em diversos órgãos da administração federal em um único banco de dados – a partir de um projeto original, que pretendia unificar os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Simson Garfinkel. Database nation. Sebastopol: O'Reillly, 2000, p. 13. Após acirradas discussões sobre a ameaça potencial que representaria às liberdade individuais, o governo norte-americano desistiu do projeto. v. Arthur Miller. Assault on privacy. Ann Arbor: University of Michigan, 1971.

Após o fracasso da tentativa de instituição deste banco de dados centralizado, vários dos temas que foram levantados em meio à discussão sobre sua possibilidade continuaram a ser desenvolvidos. No início da década de 1970, a *Secretary for Health, Education and Welfare (HEW)* reuniu uma comissão de especialistas que divulgou, em 1973, estudo que conclui pela relação direta entre a privacidade e os tratamentos de dados pessoais, e pela necessidade de estabelecer a regra do controle sobre as próprias informações:

> *"A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei"*[62].

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

> *"- Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.*

62 E.U.A., Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973, disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>.

- Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.

- Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.

- Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.

- Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados"[63].

Tais regras apresentaram um conjunto de medidas que passou a ser encontrado em várias das normativas sobre proteção de dados pessoais, às quais se passou a referir como *Fair Information Principles*.

Os *Fair Information Principles constituiram-se em uma espécie de "núcleo comum"* a diversas normativas sobre proteção de dados, seja na Europa como nas Américas. Sua influência foi marcante, por exemplo, nos documentos normativos mais influentes sobre a matéria da década de 1980, como a Convenção n.108 do Conselho da Europa (Convenção de Strasbourg)[64] e as *Guidelines* da OCDE[65], amas do início da década de oitenta. A influência dos *Fair Information Principles* é marcante até os dias de hoje, a ponto de que o trabalho de sua atualização é constante, sendo que a enunciação mais recente destes princípios foi

63 idem.

64 Convenção nº 108 do Conselho Europeu – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.

65 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, disponível em: <www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. Este influente documento lista como princípios de proteção de dados: "(1) collection limitation principle; (2) data limitation principle; (3) purpose specification principle; (4) use limitation principle; (5) security safeguard principle; (6) openness principle; (7) individual participation principle". Ulrich Wuermeling. "Harmonization of European Union Privacy Law", in: 14 John Marshall Journal of Computer & Information Law 411 (1996), p. 416.

realizada pelo *Department of Homeland Security* norte-americano no ano de 2008[66]. É possível elaborar uma síntese destes princípios[67]:

1 - *Princípio da transparência*, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento.

2 - *Princípio da qualidade*, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.

3 - *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

4 - *Princípio do livre acesso*, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.

5 - *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

66 <http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf>.

67 cf. Stefano Rodotà. Repertorio difine secolo. Bari: Laterza, 1999. p. 62. José Adércio L. Sampaio. Direito à intimidade e à vida privada. Belo Horizonte: Del Rey, 1999, pp. 509 - ss.

Há diversas modificações e adaptações destes princípios, quase sempre a partir deste mesmo núcleo comum. Assim, por exemplo, leis como a alemã tratam de um princípio da *necessidade*[68], que vincularia o tratamento de dados pessoais quando estes forem estritamente necessários para se atingir um determinado objetivo legítimo, princípio este aparentado com o princípio da proporcionalidade e mesmo com a noção de *data minimization*, presente na última revisão dos *Fair Information Principles*.

2.3. A proteção de dados como um direito fundamental

Em alguns países, a tutela autônoma dos dados pessoais foi um primeiro passo rumo a sua consideração como um direito fundamental. Este fenômeno observa-se, basicamente, em países cujo ordenamento reflete o sistema jurídico europeu-continental. Ainda, países que sofreram uma mudança de regime político que lhes proporcionou a reelaboração de suas cartas fundamentais foram os primeiros nos quais foi possível observar uma tendência à consideração da problemática relacionada à informática e à informação pessoal em nível constitucional. Neste sentido, nas constituições da Espanha[69] e de Portugal[70]

---

68 O princípio da necessidade, ou da redução de dados, está presente na seção 3a da Lei Federal de Proteção de Dados da Alemanha (Bundesdatenschutzgesetz) de 2002, na seguinte redação: "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."(tradução oficial). Também está presente no Art. 3 do Código para a Proteção de Dados Pessoais da Itália, literalmente referido como princípio da necessidade do tratamento de dados e com o seguinte teor: "1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

69 A Constituição espanhola de 1978 contém os seguintes dispositivos:

Art. 18. – (...) 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos

(...) Art. 105. – (...) b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas"

70 A constituição portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:

"Artigo 35.º (Utilização da informática)

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

se encontram dispositivos destinados a enfrentar os problemas da utilização da informática e, no caso da Constituição portuguesa, uma referência explícita à proteção de dados pessoais

É possível considerar a Convenção n. 108 do Conselho da Europa como o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais. Em seu preâmbulo, a convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao artigo 8º da Convenção Européia para os Direitos do Homem[71]. Posteriormente, também transparece com clareza a presença dos direitos fundamentais na Diretiva 95/46/CE sobre proteção de dados pessoais na União Européia[72]. Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais".

O documento europeu que levou mais adiante esta sistemática foi, certamente, a Carta dos Direitos Fundamentais da União Européia, proclamada em 7 de dezembro de 2000. Seu artigo 8º, que trata da "proteção de dados pessoais", inspira-se no artigo 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

71 Art. 8º, Convenção Européia

1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

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

do tratado instituidor da União Européia[73], e consolida a técnica que já era legitimada pelo legislador e pela doutrina de vários países europeus de considerar a tutela dos dados pessoais como um direito autônomo em relação à tutela da privacidade. Não obstante, nota-se um duplo matiz: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio através do estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais[74].

2.4. Proteção de dados no ordenamento brasileiro

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

É possível identificar, no nosso tecido normativo, que as expressões mais fortes relacionadas à proteção de dados encontram-se nas garantias constituionais - em particular as garantias relacionadas à intimidade, à vida privada e à ação de Habeas Data - e na proteção às informações do consumidor nos termos do Código de Defesa do Consumidor.

---

73 "Artigo 286.

1. A partir de 1 de Janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.

2. Antes da data prevista no n.o 1, o Conselho, deliberando nos termos do artigo 251, criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adaptará as demais disposições que se afigurem adequadas".

74 Este caráter levou alguns autores a desencorajarem a leitura da diretiva em chave de direitos fundamentais do homem em relação à informação pessoal, apesar de reconhecerem que, "dal punto di vista più genuinamente privatistico, non v'è dubbio che la direttiva ... sia destinata a diventare un punto di riferimento fondamentale nella ricostruzione sistematica dei diritti della personalità, almeno nella misura in cui il concetto di personalità si trovi a far i conti con la realtà informatica e telematica". v. Francesco Macario. "La protezione dei dati personali nel diritto privato europeo", in: Vicenzo Cuffaro. Vicenzo Ricciuto. La disciplina del trattamento dei dati personali. Torino: Giappechelli, 1997, pp. 8-9.

A Constituição brasileira contempla o problema da informação inicialmente através das garantias à liberdade de expressão[75] e do direito à informação[76], que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infra-constitucional, destaca-se o Código de Defesa do Consumidor, cujo artigo 43, estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibiltando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro[77].

O Habeas Data, instituto que no direito brasileiro tem a forma de uma ação constitucional, foi introduzido pela Constituição de 1988[78]. Com um *nomen iuris* original, introduziu em nosso ordenamento o direito de acesso, carregando com si algo da carga semântica do Habeas Corpus. A sua influência em outras legislações latino-americanas chegou a provocar a discussão sobre a existência de um modelo de proteção de dados que circule dentro do subcontinente[79].

O Habeas Data brasileiro surgiu basicamente como um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e, portanto, não apresentava influência direta da experiência européia ou norte-americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época.

---

75 Constituição brasileira, art. 5º, IX; art. 220.

76 Constituição brasileira, art. 5º, XIV; art. 220; incluindo o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos (art. 5º, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5º, XXXIV).

77 Cf. Ana Paula Gambogi Carvalho. "O consumidor e o direito à autodeterminação informacional", in: Revista de Direito do Consumidor, n. 46, abril-junho 2003, pp. 77-119.

78 Constituição Federal, art. 5º, LXXII:

"Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo"

79 Sobre o tema, v. Oscar Puccinelli. El habeas data en Indoiberoamérica. Bogotá: Temis, 1999.

Posteriormente o habeas data foi regulamentado pela Lei 9.507, de 1997. A ação de habeas data visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente. Por meio dela, o cidadão pode acessar e retificar seus dados pessoais em bancos de dados "de entidades governamentais ou de caráter público" (posteriormente ampliou-se o sentido deste "caráter público", incluindo-se os bancos de dados referentes a consumidores, mesmo que administrados por privados). A ação não é acompanhada, porém, de instrumentos que possam torná-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais: além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, algo que se percebe em vários dos seus pontos estruturais, como a necessidade de sua interposição através de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados, ela é, substancialmente, um instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação. Não surpreende, portanto, que há certo tempo a doutrina brasileira tenha assumido posição majoritariamente crítica em relação à ação, tratando-a ora como "um remédio de valia, no fundo, essencialmente simbólica", para Luís Roberto Barroso[80], ou de "uma ação voltada para o passado", para Dalmo de Abreu Dallari[81].

O Código de Defesa do Consumidor (Lei 8.078/90), especificamente em seu artigo 43, estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros" e é a peça normativa mais moderna e eficaz presente em nosso ordenamento no que diz respeito à proteção de dados. O Código, tendo marcado fortemente o ordenamento civil brasileiro, induziu o próprio civilista a promover uma modernização em sua disciplina que irradiou-se para além das relações de consumo[82]. Estruturando-se em um sistema moderno, efetivamente preocupado com a proteção do consumidor, o CDC inevitavelmente deparou com o problema representado pela utilização abusiva da informação sobre consumidores em bancos de dados. Não por acaso, a proteção ao consumidor continua até hoje a suprir muitas das lacunas deixadas pela ausência de um marco normativo específico relacionado aos dados pessoais.

---

80 Luís Roberto Barroso. "A viagem redonda: habeas data, direitos constitucionais e provas ilícitas", in: Habeas data. Teresa Arruda Alvim Wambier (coord.). São Paulo, RT, 1998, p. 212.

81 Dalmo de Abreu Dallari. "O habeas data no sistema jurídico brasileiro", in: Revista de la Faculdad de derecho de la Pontifícia Universidad Católica del Peru, n. 51, 1997, p. 100.

82 v. Gustavo Tepedino. "As relações de consumo e a nova teoria contratual", in: Temas de direito civil. Rio de Janeiro: Renovar, 1999, pp. 199-216.

As disposições do CDC revelam, como foco de preocupação do legislador, o estabelecimento de equilíbrio na relação de consumo através da interposição de limites ao uso da informação sobre o consumidor pelo fornecedor (que estaria justificado, de um certo ponto de vista, na efetivação da transação com maior segurança). Assim, por exemplo, o registro de dados negativos sobre um consumidor não poderá ser mantido por um período maior de 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e, implicitamente, o cancelamento justificado[83]. Podemos reconhecer neste diploma legislativo a presença de alguns dos princípios de proteção de dados pessoais que examinamos anteriormente, ainda que de uma forma resumida e inserida em um contexto – o das relações de consumo - que impede que esta disciplina assuma os contornos de um sistema geral de proteção de dados pessoais, muito embora possa fornecer parâmetros interpretativos úteis que, pela sua generalidade, podem ter sua eficácia irradiada para outras situações.

Neste sentido, cabe verificar que na doutrina podemos encontrar propostas para uma interpretação de caráter expansivo da normativa do Código de Defesa do Consumidor, de forma a identificar a presença dos princípios de proteção de dados pessoais que se comunicam a outras situações. Assim, por exemplo, entende-se a existência do princípio da finalidade, através da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo que os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que motivaram a sua coleta[84] – o que pode servir como fundamentação para o reconhecimento de um princípio de vedação da coleta de dados sensíveis e da comercialização de bancos de dados de consumidores[85].

---

83 Ana Paula Gambogi Carvalho sustenta o sentido de que até mesmo o pedido do consumidor para incluir dados a seu respeito no cadastro seria pertinente através da ação de habeas data. Ana Paula Gambogi Carvalho. "O consumidor e o direito à autodeterminação informacional", in: Revista de Direito do Consumidor, n. 46, abril-junho 2003, pp. 77-119.

84 Em relação à legitimidade para o acesso aos arquivos de consumo, afirma Antonio Herman Benjamim: "A acessibilidade depende, pois do prenchimento de duas condições cumulativas: a) solicitação individual decorrente de b) uma necessidade de consumo. Fora disso, qualquer utilização implicará mau uso, sujeitando os infratores (o que dá e o que recebe) às sanções penais, civis e administrativas aplicáveis às hipótese de invasão da privacidade". Antonio Herman de Benjamim et ali. Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto. 9ª ed. Rio de Janeiro: Forense Universitária, 2007, p. 448.

85 Remete-se, para esta leitura, ao trabalho de Ana Paula Gambogi Carvalho, "O consumidor e o direito à autodeterminação informacional ...", cit. Ao ilustrar a presença do princípio da finalidade, a autora refere-se à decisão da 6ª turma do STJ da qual transcrevemos o seguinte trecho: "Quando uma pessoa celebra contrato especificamente com uma empresa e fornece dados cadastrais, a idade, o salário, endereço, é evidente que o faz a fim de atender às exigências do contratante. Contrata-se voluntariamente. Ninguém é compelido, é obrigado a ter aparelho telefônico tradicional ou celular. Entretanto, aquelas informações são reservadas, e aquilo que parece ou aparentemente é algo meramente formal pode ter conseqüências seríssimas (...) Daí, é o próprio sistema da telefonia tradicional, quando a pessoa celebra contrato, estabelece, como regra, que o seu nome, seu endereço e o número constarão no catálogo; entretanto, se disser que não o deseja, a companhia não pode, de modo algum, fornecer tais dados (sic)." STJ, 6a Turma, Recurso ordinário em Habeas Corpus nº 8.493/SP, rel. Min. Luiz Vicente Cernicchiaro, j. 20.5.1999. DJ 02/08/1999, p. 224.

No entanto, mesmo com o grande avanço representado pelas disposições do Código de Defesa do Consumidor e também pela sua interpretação extensiva, trata-se de uma tutela de certa forma limitada; o que se verifica não somente em relação à sua incidência – em situações caracterizadas como relações de consumo – porém pelo caráter de suas disposições. Verifique-se, quanto a isso, que a origem material das disposições do seu artigo 43 foi inspirada, de acordo com o próprio responsável pela elaboração do anteprojeto desta seção do CDC, na normativa norte-americana de proteção ao crédito estabelecida pelo National Consumer Act e pelo Fair Credit Reporting Act – FCRA, de 1970.[86]

Afora estes marcos que podem ser utilizados para compor um cenário fragmentado do tratamento normativo à questão da proteção de dados pessoais no Brasil, a única menção expressa ao caráter de direito fundamental da proteção de dados pessoais em um documento oficial assinado pelo governo brasileiro encontra-se na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo governo brasileiro em 15 de novembro de 2003. No item 45 da referida Declaração, lê-se que:

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

Parece existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória dos problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; sobre a característica sigilosa ou não de uma determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições

86 v. Antonio Herman Vasconcelos e Benjamen. Código brasileiro de defesa do consumidor. Comentado pelos autores do anteprojeto. cit., p. 327. O FCRA foi posteriormente incorporado ao capítulo VI do Consumer Credit Protection Act.

para o uso de informações específicas, sem levar na devida conta os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais.

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

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

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

Neste sentido, recentemente, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais, endossando tese de Tércio Sampaio Ferraz Júnior segundo a qual o ordenamento brasileiro tutelaria o sigilo das comunicações – e não dos dados em si[87].

87 "Em primeiro lugar, a expressão "dados" manifesta uma certa impropriedade "Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática.

Os dados aqui são os dados informáticos (v. incs. XIV e LXXII)". A interpretação faz sentido. O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Note-se, para a caracterização dos blocos, que a conjunção 'e' uma correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo. Mas, se alguém entra nesta transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados.

Nesta decisão fica saliente a dificuldade em tratar do tema da informação pessoal de uma forma diversa daquela binária – sigilo/abertura, público/privado – de forma que reflita a complexidade da matéria da informação.

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

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

O favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, isto é, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados, é necessário para superar a situação de anacronismo em que se encontra a tutela atual dos dados pessoais em nosso ordenamento, situação esta que deixa descobertas as liberdades fundamentais. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa nas vicissitudes da Sociedade da Informação.

A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativo a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-lo!". Tércio Sampaio Ferraz Jr. "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado", in: Revista da Faculdade de Direito da Universidade de São Paulo, vol. 88, 1993, pp. 447.

CAPÍTULO 3
PUBLICIDADE COMPORTAMENTAL E PERFIS DE CONSUMIDORES

As políticas de proteção ao consumidor devem ir além da tutela das informações pessoais e devem considerar o fato de que o consumidor possui um perfil e que ele pode ser abordado diretamente a partir deste perfil, mesmo que ninguém saiba o seu nome real.

Meglena Kuneva

Um dos maiores contrastes entre o contrato, em sua formulação clássica, e o contrato de consumo está ligado à informação na fase pré-contratual e aos efeitos jurídicos da oferta e publicidade.

À publicidade, originalmente encapsulada em uma fase contratual referida como fase das tratativas ou de negociações preliminares, não eram associados efeitos jurídicos vinculantes. Esta ausência de compromisso entre as partes era, aliás, uma tônica em toda a fase pré-contratual, que a concebia como uma forma de garantir a liberdade das partes para uma livre prospecção das condições do contrato, do seu objeto e para o seu eventual arrependimento, antes que houvesse uma proposta ou a sua respectiva aceitação. Neste ambiente a princípio descompromissado, somente após a proposta ser formalmente caracterizada, a ela lhe seriam associados efeitos vinculantes.

Nesta concepção do momento pré-contratual como um balcão aberto para a livre negociação, o espaço destinado à publicidade era o de uma mera *invitatio ad offerendum*, um convite para a negociação ou contratação posterior, igualmente isento de vinculatividade e pelo qual o ofertante somente responderia caso configurado o *dolus malus*.

As mudanças no perfil do contrato tradicional até o contrato de consumo são objeto de extensa e autorizada bibliografia[88] . Dentre os diversas mudanças estruturais no perfil do instituto, uma das mais relevantes é a identificação e amadurecimento de uma dimensão informacional no contrato de consumo, a ser abordada com critérios específicos que não coadunam com a regra da não-vinculatividade da fase pré-contratual.

Nos contratos de consumo, há uma assimetria informacional entre o consumidor e fornecedor, que as atuais práticas publicitárias apenas intensificaram. A distinção entre a publicidade e os outros canais de comunicação que proporcionam a troca de informações entre fornecedor e consumidor tornou-se, recentemente, vaga e imprecisa - mais ainda com o fortalecimento do comércio eletrônico -, dificultando qualquer tentativa de estabelecer os efeitos práticos desta distinção[89]. A constatação de que, nos contratos eletrônicos, o consumidor costuma contar com pouco mais do que a informação obtida pelo meio eletrônico para realizar suas opções fez ainda com que as responsabilidades na fase pré-contratual fossem ampliadas definitivamente, com a equiparação da publicidade à oferta pelo Código de Defesa do Consumidor. Desta forma, o contrato de consumo passou a se diferenciar do contrato tradicional também pelo seu enfoque próprio à questão da publicidade, que pode, resumidamente, caracterizar-se por: (i) basear-se em uma acepção ampla do conceito de publicidade; (ii) ressaltar a responsabilidade decorrente da mera atividade publicitária; (iii) incluir também vedações específicas à publicidade enganosa ou abusiva.

No entanto, mesmo esta maior abrangência do conceito de publicidade não afasta o fato de que o modelo paradigmático de publicidade do Código de Defesa do Consumidor apresenta forte marca do seu tempo e concentra-se no fenômeno da veiculação da mensagem publicitária pelos meios de comunicação de massa, em um típico modelo de difusão do "centro para a periferia".

Uma forma quase instintiva para obter maior eficiência para esta mensagem publicitária é a sua veiculação em veículos de mídia dirigidos precisamente ao perfil do consumidor que teria maior interesse pelo produto ou serviço anunciado - esta é a chamada publicidade contextual, que busca a inserção da mensagem publicitária em um contexto no qual ela se harmonize com os interesses presumidos do consumidor.

Em paralelo a esta prática, o chamado *marketing direto* procura compilar, em bases de dados de consumidores, aqueles com maior potencial de compra para serem abordados diretamente. Tais bases de dados com informações pessoais sobre consumidores passaram a representar uma ferramenta valiosa

88 Por todos, v. Claudia Lima Marques. Contratos no Código de Defesa do Consumidor. 5ª ed., São Paulo: RT, 2005.

89 A este respeito, considere-se, por exemplo, as estratégias de utilização de redes sociais por fornecedores, que em diversos casos, além de apresentarem informações estritamente publicitárias, também podem oferecer informações de suporte, de formação sobre temas referentes à sua atividade, além de desenvolver estratégias típicas de redes sociais como a formação de comunidades de consumidores.

e justificaram inclusive o nascimento dos primeiros programas de fidelização que, na década de 1980, começaram a ser oferecidos por fornecedores a seus consumidores mais frequentes e fiéis justamente para obter seu perfil mais acurado, em troca de eventuais vantagens e recompensas.

As possibilidades de obter informações sobre os consumidores aumentaram drasticamente nos últimos anos, basicamente pela intensificação da utilização da Internet e com o desenvolvimento em paralelo de tecnologias que, direta ou indiretamente, permitem o monitoramento dos consumidores.

Uma das consequências mais claramente visíveis da informatização de muitos aspectos de nossa vida cotidiana é justamente a possibilidade de registro de muitos dos diversos atos que realizamos através de meios informatizados. Em um novo paradigma com o qual ainda não nos acostumamos completamente, muitos dos nossos atos que antes seriam efêmeros e gerariam consequências apenas imediatas ou previsíveis dentro de determinados padrões já pré-concebidos, passam a ser não apenas atos mas também informações que podem ser utilizadas por nós mesmos e, frequentemente, por terceiros - abrindo a possibilidade, neste caso, de serem utilizadas em um contexto diferente daquele no qual praticamos nossos atos e com finalidades também diversas, eventualmente fugindo ao nosso poder de previsão e controle.

Os atos de consumo - incluindo muitos atos realizados em momentos anteriores ao consumo em si - proporcionam, neste panorama, a compilação de abundante informação sobre o consumidor, o que veio a modificar o perfil do fluxo informacional entre fornecedor e consumidor: agora, é possível ao fornecedor saber detalhes não somente sobre grupos de consumidores, porém sobre o consumidor individualmente considerado, o que abre a possibilidade de sua abordagem de forma pretensamente individualizada. O consumidor, enfim, aos olhos da atividade de marketing, não é mais somente o destinatário de informações porém tornou-se fonte de informações que vão determinar a forma como ele poderá ser abordado e tratado.

Neste ponto é necessário refletir sobre as consequências deste novo paradigma informacional nas relações de consumo. Se por um lado, aumentaram os meios para que o consumidor muna-se de informações sobre produtos, serviços e fornecedores, o que lhe proporciona uma vantagem potencial em relação a um paradigma anterior no qual a informação era restrita ao contato direto e fontes de comunicação limitadas, aumentou também o fluxo de informações em sentido inverso. Neste particular, note-se que as mudanças no fluxo de informações a partir do consumidor para o fornecedor não foram apenas de ordem quantitativa, porém mudaram seu próprio perfil, com a possibilidade de individualização do consumidor. Desta forma, o fato do consumidor ter se tornado fonte de informações não reflete propriamente em seu empodeiramento - a possibilidade é toda que, ao contrário, esta grande mudança qualitativa na natureza do fluxo de informações

sobre o consumidor para o fornecedor seja um fator de agravamento da própria assimetria informacional entre ambos.

Cumpre verificar agora a natureza destas informações que são provenientes dos consumidores. Muitos dos dados obtidos do consumidor não são na maioria das vezes, manifestações de sua expressão livremente articulada, porém informações agregadas a partir de seu comportamento cotidiano - seja pela mera navegação na internet, em situações de consumo e tantas outras. Estas informações comportamentais não são ponderadas e refletidas pelo consumidor - como o é a mensagem publicitária pelo fornecedor - e, mais ainda, sua disponibilização é hoje apenas precariamente controlada pelo próprio consumidor.

A publicidade comportamental (*behavioral advertising*) representa a fronteira na qual se desenvolvem as novas tecnologias de abordagem do consumidor a partir da utilização intensiva de informações pessoais a seu respeito. Seus efeitos devem ser cuidadosamente assimilados pela prática consumerista pois, além do risco concreto de ampliar a assimetria informacional na relação de consumo, soma-se uma boa parcela de outros riscos inerentes à utilização de dados pessoais, refletindo na potencial discriminação entre consumidores, na relativização da idéia de escolha livre e outros.

A publicidade comportamental utiliza-se, naturalmente, de informações sobre o comportamento de uma pessoa para que lhe seja especificado o tipo de abordagem que seria o mais adequado. Hoje, com a grande penetração da rede Internet, uma das fontes de dados mais visadas para a obtenção de dados que permitam estabelecer o "perfil" de um consumidor a partir do seu comportamento é justamente o conjunto de hábitos de sua navegação na Internet, conforme observa a própria *Federal Trade Comission* norte-americana, em documento no qual caracteriza especificamente a publicidade comportamental *online*:

> "*A publicidade comportamental é o monitoramento das atividades de um consumidor quando conectado à Internet - incluindo as pesquisas que ele fez, as páginas que ele visitou e o conteúdo consultado - com a finalidade de fornecer-lhe publicidade dirigida aos interesses individuais deste consumidor*"[90].

90 Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles. FTC Staff Report. http://www.ftc.gov/os/2007/12/P859900stmt.pdf

A presença de sofisticados mecanismos para obter tais dados de navegação é cada vez mais ostensiva e generalizada[91] e é em grande parte responsável por um dos fluxos comerciais mais recentes relacionados à Internet.

É fundamental notar, no entanto, que a compilação de perfis de comportamento tem a publicidade comportamental como apenas uma de suas potenciais finalidades. Hoje, a forte dinâmica deste mercado o coloca em posição de destaque, porém qualquer atividade que possa ter a ganhar com um conhecimento mais apurado de uma pessoa ou uma possibilidade de antever suas opções futuras tem muito a ganhar com a existência destes perfis. Desta forma, somente para fornecermos alguns exemplos, tanto campanhas eleitorais como o recrutamento de recursos humanos, a compilação de históricos clínicos ou a precificação de seguros, além de tantos outros, podem apresentar um interesse potencial nestes perfis, levando a situações de relativização da liberdade de escolha e mesmo de discriminação que, embora possam ultrapassar o alcance da relação de consumo, decorrem desta estrutura montada no âmago da publicidade para o consumidor. Não seria a primeira vez que o direito do consumidor encontra-se na vanguarda da regulação de uma atividade cujos efeitos potenciais podem, a curto e médio prazo, ultrapassar largamente a alçada da proteção do consumidor, e este fato apenas ressalta a vocação deste ramo do direito para ser também um laboratório de soluções e técnicas jurídicas que possam se demonstrar viáveis e, ao fim, transferidas e traduzidas para outras situações.

3.1. Publicidade comportamental e formação de perfis (profiling)

A coleta e agregação de informações sobre consumidores e o seu enquadramento em um certo perfil são condições preliminares para a publicidade comportamental. A partir deste perfil, o consumidor é exposto a uma mensagem publicitária sob medida, cujas chances de se enquadrar dentro de seus interesses é presumivelmente maior, de acordo com os critérios do mecanismo utilizado. As diversas técnicas destinadas

91 A consciência sobre a amplitude dos métodos de monitoramento on-line dos internautas foi pública e intensamente debatido em uma série de reportagens investigativas que o jornal Wall Street Journal passou a publicar em agosto de 2010. O jornal realizou testes que revelaram que o conjunto dos 50 sites mais populares nos Estados Unidos instalam nos computadores de seus visitantes cerca de 2,224 arquivos ("cookies") especificamente destinados a monitorar os hábitos de navegação daqueles que acessam os respectivos sites. Disponível em: <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>.

a estabelecer este perfil - *profiling* -, fazem com que o consumidor seja caracterizado a partir de seus hábitos e atos. Levando em conta os comportamentos observados em históricos de compras anteriores, produtos visualizados e outros dados pessoais disponíveis, estabelece-se uma presunção de quais seriam os seus interesses.

O potencial das técnicas de *profiling* cresceu nos últimos anos, especificamente pela mudança de um simples paradigma: conforme já ressaltamos, cada vez mais os nossos atos passaram a deixar rastros e de serem capazes de se transformar em informação. Este é o paradigma da memória, identificado por Mayer-Scöemberger[92]. Este novo paradigma da memória se antepõe ao paradigma anterior, que era do esquecimento. No paradigma do esquecimento, os atos cotidianos eram evanescentes e seus traços quase sempre restavam apenas em nossa memória e na daqueles com que compartilhávamos momentos - quando restavam e quando não eram ofuscados ou obscurecidos. A vida cotidiana estava, portanto, sujeita às leis do esquecimento e dúvida e aos tantos outros mecanismos e condicionamentos culturais que moldam a nossa psique.

As comunicações intermediadas pelas mais modernas tecnologias da informação são as que vão modificar e reformular o paradigma da memória. Ao se reduzir as atividades humanas ao denominador comum da comunicação - a mera informação - estas tornam-se também facilmente registráveis, com o aumento na capacidade de armazenamento e o decréscimo do seu custo.

Além disso, mesmo atividades realizadas fora do ambiente eletrônico estão sujeitas ao chamado paradigma da memória. Neste particular, atente-se que os estudos sobre a vigilância apontam para o fenômeno dos dispositivos de vigilância que, instalados nos mais diversos locais públicos, permitem a sobrevivência em formato digital de ações que, a princípio, poderiam ser realizadas sem a intermediação de meios digitais.

O estabelecimento de um perfil para um determinado consumidor não é, taxativamente, um mal em si - muito embora apresente grande potencial para tornar-se um mal caso o consumidor não tenha consciência efetiva do que ocorre. No *profiling,* estão em jogo não somente aspectos da privacidade do consumidor, porém da sua própria autonomia decisional e liberdade de escolha, valendo aqui um relance ao que Yves Poullet caracteriza como sendo as duas faces da privacidade moderna: de um lado, a proteção da intimidade e, de outro, a garantia da auto-determinação e da própria liberdade[93].

92 Viktor Mayer-Scöemberger. Delete. The Virtue of Forgetting in the Digital Age. Princeton: Princeton University Press, 2009.

93 Yves Poullet. "Data Protection Legislation: What's at Stake for our Society and our Democracy?", in: Computer Law & Security Review, Vol. 25, Is. 3, 2009, pp. 211-226.

Ao se cogitar destes efeitos do *profiling* nesta fase pré-contratual, caberia um breve parêntesis sobre uma lição que a teoria do direito pode nos fornecer a partir dos fundamentos da caracterização do sujeito de direito como uma entidade puramente abstrata. O sujeito de direito, alvo de críticas constantes da doutrina por ser um instrumento que aliena a pessoa da realidade através de uma abstração conceitual, é, por outro lado, também uma garantia de igualdade de ordem formal da qual não se pode abrir mão em inúmeras situações. Sendo o sujeito de direito puramente abstrato, as diferenças pessoais não são levadas em conta para a atribuição abstrata de direitos e deveres entre iguais. Tendo sido contestada esta figura justamente por sua excessiva neutralidade e tendo sido sujeitada à uma utilização instrumental, é forçoso constatar que o seu enfraquecimento pode estar na raiz de um problema que enfrentamos hoje, que é a hipertrofia da individualização do sujeito da relação jurídica - o que contribuiria justamente para o enfraquecimento da pessoa que se encontre em uma situação de vulnerabilidade - como é o resultado da assimetria informacional potencializada pelas técnicas de publicidade comportamental. Ironicamente, portanto, as tentativas de regulação da publicidade comportamental muitas vezes podem ser interpretadas como uma tentativa contemporânea de recriar, com meios tanto jurídicos como técnicos, traços do sujeito abstrato de direito em relações cuja superexposição aos remédios da individualização e personificação gerou uma série de efeitos colaterais.

3.2. Técnicas utilizadas para o monitoramento e formação de perfis

Há diversas técnicas para a obtenção de dados sobre os consumidores com fins de realização de publicidade comportamental.

Na Internet, é cada vez mais frequente a utilização de técnicas de monitoramento da navegação de um determinado usuário. Estas técnicas podem se basear na navegação em determinados sites, afiliados a um dos diversos serviços de monitoramento da navegação na Internet (*tracking*). Estes serviços podem monitorar a navegação dentro de um determinado site ou grupo de sites pertencentes a uma mesma organização (por exemplo, um mecanismo que monitore a navegação em todos os sites pertencentes à empresa Google Inc.), bem como podem ser multi-site, ou seja, serviços que monitorem a navegação em diversos sites, pertencentes a organizações diversas que seriam filiadas a este serviço de monitoramento.

Outro modelo para obtenção de dados comportamentais é a implementação de um serviço de interceptação do fluxo de dados entre o usuário da Internet e o site que este visita. Esta interceptação baseia-se no próprio provedor de acesso à Internet e, em seus modelos mais comuns, opera através da análise do fluxo bruto de informações entre o usuário e o provedor de conteúdo através de técnicas que procuram determinar informações consideradas relevantes dentro dos pacotes de informação que são os *containers* do fluxo de dados na internet - técnica denominada de DPI (*Deep Packet Inspection*).

Ambos os modelos lançam desafios, em relação a razoável expectativa do usuário da Internet de que as suas comunicações e a sua navegação interessam e são visíveis apenas a ele e aqueles com os quais se comunica. Por este motivo, a necessidade de que o usuário da Internet tenha consciência do fato de sua navegação poder ser monitorada e escrutinada é indispensável.

Além de saber sobre o monitoramento, como garantias mínimas da posição do consumidor, é necessário que o usuário da Internet tenha concordado com esta prática e que este consentimento seja efetivamente livre e informado. Como condições para o consentimento livre e informado, é necessário que o monitoramento se processe de forma clara e transparente e que sejam fornecidas aos usuário informações sobre quais dados serão colhidos, a forma como eles serão utilizados e por quem serão utilizados, entre outras informações essenciais. Além disso, é fundamental que o usuário tenha condições de desistir a qualquer momento de ser objeto deste monitoramento[94].

O modelo que baseia o monitoramento da navegação da Internet no provedor de acesso apresenta certas peculiaridades que colocam o consumidor em situação ainda menos favorecida e que, hoje, provocam reações por vezes desfavoráveis de reguladores quanto à sua viabilidade e licitude. Ocorre, nestes casos, que o monitoramento se processa em uma camada mais profunda do processo de navegação que é o próprio fornecimento de serviço de acesso à internet, fazendo com que toda a sua navegação esteja potencialmente sujeita à interceptação e escrutíneo - e não apenas a navegação em sites determinados ou em serviços do protocolo HTTP. Além disto, neste modelo, qualquer tipo de controle direto pelo usuário ou tentativa de determinar o mecanismo utilizado para o monitoramento é virtualmente impossível pelo fato do mecanismo estar instalado diretamente no provedor de acesso e, portanto, fora de sua zona de controle.

94 Um estudo compreensivo sobre os direitos do usuário da Internet em relação às práticas propostas no âmbito de auto-regulação pode ser consultada em: Online behavioral advertiging: Industry's current self-regulatory framework is necessary, but still insufficient on its own to protect consumers. Center for Democracy & Technology, Washington, 2009.

Além do monitoramento direto, outra forma de obter informações sobre usuários da Internet para possibilitar a publicidade comportamental á a chamada mineração de dados. A mineração de dados (*data mining*) consiste, basicamente, no recurso a técnicas estatísticas para a identificação de infomação relevante para uma determinada atividade a partir de grandes volumes de informação em estado bruto.

A esta informação em estado bruto, cuja possibilidade de acesso é cada vez mais comum, costuma-se denominar *Big Data.* O conceito de *Big Data* não se refere a uma técnica de processamento de informações em si, porém às gigantescas massas de dados que as modernas técnicas de comunicação tornaram possível armazenar e processar, mas cuja análise é severamente dificultada justamente pelo seu tamanho.

Uma questão subjacente a esta técnica é o fato de que ela potencializa a dissociação entre os fatos representados pela informação armazenada e o contexto no qual estes se encontram e dentro do qual assumem seu significado próprio.

A dependência entre informação e contexto não é novidade, mas o tratamento de grandes volumes de dados pessoais faz disso um problema maior justamente pela dificuldade em se estabelecer o contexto de grandes volumes de informação, o que demanda soluções que não são somente de ordem técnica. Conforme recentemente afirmou Danah Boyd:

> *"A mera visualização de pedaços de informações não significa que sempre se saiba a lógica cultural por detrás deles"*

E ainda:

> *"Cada vez mais, vejo que cientistas da computação confundem rastros comportamentais com lógica cultural"*[95]

95 Danah Boyd, "Big Data: Opportunities for Computational and Social Sciences", in: <http://www.zephoria.org/thoughts/archives/2010/04/17/big-data-opportunities-for-computational-and-social-sciences.html>.

Tais advertências remetem diretamente à nossa questão específica, nos casos em que informações pessoais agregadas através de técnicas de DPI ou de *Data Mining* são utilizadas para que sejam traçados perfis comportamentais com o fim de oferecimento de publicidade comportamental. A partir do corolário fundamental de que não é possível denominar um perfil desta natureza como um perfil das *preferências* de uma pessoa, mas somente tentar inferir algo a partir de um determinado padrão de comportamento pretérito, entra também o fato de que este comportamento é condicionado por uma série de variáveis contextuais - culturais, econômicas, sociais - todas capazes de distorcer a interpretação da interpretação pessoal agregada, ainda que esta seja volumosa e, em si, fiel à realidade.

3.3. Problemas relacionados à publicidade comportamental

A utilização de dados comportamentais como forma de influenciar a interação futura de uma pessoa - por exemplo, cuidando para que lhe seja veiculada apenas a publicidade que mais se ajuste ao seu pretenso perfil comportamental - pode limitar o rol de escolhas futuras daquela pessoa a partir de um perfil que foi inferido de seu comportamento passado. Este fenômeno já chegou a ser denominado de *boxing*[96], segundo a metáfora de que as possibilidades oferecidas a uma pessoa são fechadas - encaixotadas - em torno de presunções realizadas por ferramentas de análise comportamental, guiando desta forma as suas escolhas futuras. A publicidade assim encaminhada teria o efeito colateral de uniformizar padrões de comportamento em torno de padrões definidos pelos algorítimos e categorias utilizadas por tais ferramentas, diminuindo de fato a diversidade e o rol de escolhas apresentados a uma pessoa. Algo semelhante ocorre, por exemplo, com o oferecimento de notícias personalizadas através de mecanismos e jornais *online* que determinam os tópicos sobre os quais um leitor deseja se informar - eliminando, desta forma, a possibilidade de que este leitor tenha acesso à informação periférica, alheia aos seus pretensos interesses mas que eventualmente poderiam de fato lhe interessar.

Alguns dos problemas relacionados à formulação de perfis para marketing comportamental são também resultantes do desvio da finalidade da coleta dos dados e não seriam, propriamente, relacionados diretamente à publicidade em si. São casos em que, a partir de dados coletados para a elaboração destes

96 Abrams, Martin. "Boxing and concepts of harm", in: Privacy and Data Security Law Journal, set. 2009, pp. 673-676.

mencionados perfis, alimentam-se outras atividades, sem o conhecimento ou autorização do consumidor, conforme já mencionado anteriormente.

Uma outra atividade questionável possibilitada pelo recurso aos dados comportamentais consiste na variação do preço a ser cobrado (*adaptative pricing*) por um produto ou serviço a partir do perfil do consumidor, identificando pessoas que estariam dispostas a pagar mais por possuírem perfil que demonstraria esta inclinação. Desta forma, torna-se possível discriminar consumidores a partir de critérios individuais, o que viola o princípio da igualdade dos consumidores perante o mercado e configura-se diretamente em uma prática discriminatória. É evidente, por outro lado, que a prática do *adaptative pricing* pode parecer uma pálida ameaça ao se prospectar com outras possíveis utilidades potenciais destes dados comportamentais em atividades ilícitas, como a aplicação de golpes através da Internet especialmente modelados segundo o perfil e as vulnerabilidades específicas de um usuário, apenas para fornecer um exemplo.

Outra possibilidade concreta de desvio da finalidade dos dados recolhidos para a elaboração de perfis de consumidores é a própria discriminação de determinados consumidores em sentido estrito. Nesta hipótese, determinados perfis poderiam ter negado o acesso a determinados bens ou serviços (por exemplo, uma negativa quanto à compra de um determinado bem por se verificar no perfil a consulta anterior a sites que tratam de proteção ao crédito, sugerindo ao fornecedor - sem dados concretos - que tratar-se-ia de um potencial inadimplente).

3.4. Instrumentos de controle e regulação

A prática do marketing comportamental online é relativamente recente, apesar de já poder ser tratada como um traço estrutural de muitos modelos de negócios baseados na Internet. A necessidade de garantir os direitos do consumidor neste ambiente contra práticas abusivas, bem como de lhe proporcionar a efetiva proteção sobre suas próprias informações pessoais vem sendo, portanto, tema de iniciativas regulatórias em aspectos como, entre outros, a garantia do consentimento livre do consumidor para a atuação destes serviços, a salvaguarda de sua privacidade, a transparência desta atividade e a possibilidade de recusar-se a continuar recebendo publicidade comportamental, entre outros.

Em relação ao consentimento, um aspecto a ser levado em conta é que a necessidade de informar ao consumidor sobre a publicidade comportamental não se exaure no momento da obtenção do consentimento para a sua realização. A ser tomado desta forma, o consentimento do consumidor mais se assemelharia - e correria o risco de ser tratado - como um objetivo a ser atingido pelo fornecedor em um determinado momento do que uma escolha livre, consciente em relação às opções disponíveis, cujos efeitos prolongam-se no tempo.

Para isso, devem ser proporcionadas ao consumidor as condições para perceber e identificar claramente quando uma mensagem publicitária comportamental lhe é dirigida, de forma a distingui-la das demais em situações onde tal dúvida possa ocorrer. Somente desta forma o consumidor poderá dispor de elementos para julgar efetivamente a conveniência do recebimento desta modalidade de publicidade e também para buscar solucionar eventuais abusos.

A dificuldade em conceber uma prática eficaz para o fornecimento de consentimento para o recebimento de publicidade dirigida na Internet, com todas as implicações que verificamos existir em relação ao monitoramento da navegação, suscita o recurso a formulações mais criativas deste consentimento. O consentimento que se deve pretender para tal tipo de publicidade deve ser aquele informado e livre de constrições; deve informar ao consumidor ao menos sobre a forma e modalidade da coleta de dados, quem os recolhe e quem os utilizará e quais dados estarão sendo coletados.

O consentimento requerido para esta modalidade de publicidade acaba por se relacionar diretamente com a informação necessária para proporcionar uma decisão livre do usuário a seu respeito. Assim, há de se aventar que não basta a remissão a textos contidos em determinadas seções de um site de comércio eletrônico[97], porém deve haver um meio de informação presente em toda e qualquer ocasião na qual a informação comportamental for colhida, bem como a publicidade apresentada a um consumidor com base em seu perfil deve ser identificável como tal.

O caráter continuativo do oferecimento de publicidade comportamental também apresenta implicações quanto ao consentimento. Não só a possibilidade de revogação do consentimento deve estar sempre presente, como esta possibilidade deve ser disponibilizada de forma ostensiva e mesmo facilitada. É esta a noção que por vezes é denominada de *ongoing consent* ou que foi vislumbrada em recente documento

97 Como é o caso das populares "políticas de privacidade".

do grupo de trabalho sobre proteção de dados da União Européia, que chegou a sugerir um mecanismo no qual houvesse a expiração deste consentimento após um determinado período de tempo[98].

Embora estas novas modalidades de consentimento estejam ainda em graus variados de adoção - variando desde estudos ou propostas oficiais até implementações práticas - a sua discussão dá mostras de que os modelos tradicionais de consentimento que costumam acompanhar diversas normativas de proteção de dados pessoais dificilmente geram bons resultados quando utilizados na dinâmica da publicidade dirigida. E também de que, neste caso, assume grande relevância a tentativa de revigorar o controle do consumidor sobre os seus próprios dados, proporcionando eficácia real à sua vontade para que determine de fato o tratamento a ser realizado de seus dados e não se resuma ao mecanismo - muitas vezes meramente formal e desprovido de efeitos práticos - de um consentimento prestado sem reflexão e quase que imediatamente esquecido.

Existem ainda as ferramentas administradas por grupos ou coalizões do próprio setor privado, que procuram facilitar que os consumidores que assim desejarem optem por não terem a sua navegação monitorada.Uma destas iniciativas é a da NAI (*Network Advertising Initiative*), que reúne empresas que trabalham com publicidade dirigida e análise de tráfego de rede e a proposta do seu *NAI Opt-out Tool* é, basicamente, uniformizar e facilitar o recurso ao *opt-out* dos diversos mecanismos de monitoramento da navegação administrados por empresas membros da NAI[99].

O *NAI Opt-out Tool* caracteriza-se como um mecanismo de auto-regulação oferecido a qualquer interessado no próprio site da NAI, que oferece a opção de recusar o monitoramento da navegação na Internet realizado pelos mecanismos das empresas membros de forma facilitada, sem ser necessária a recusa individual para cada uma delas. Há um formulário bastante claro em uma única página, pelo qual pode-se optar individualmente pelos mecanismos dos quais solicitar o *opt-out* ou então solicitá-lo, de uma vez só, para todas as empresas membros.

Ao mesmo tempo em que esta iniciativa destaca-se pela transparência e pela facilidade de uso da ferramenta de *opt-out*, o seu contraste com a situação em que se encontra o consumidor que eventualmente pretenda solicitar o não monitoramento de forma individual dá mostras de como seria árdua esta tarefa, dado o grande número de ferramentas de monitoramento atualmente em uso.

98 Opinião 2/10 do Grupo de Trabalho do Art. 29 da União Européia.

99 De acordo com dados fornecidos pela NAI, cerca de 60 empresas membros participam do NAI Opt-out Tool (dados de setembro de 2010), incluíndo Google, Microsoft e Yahoo!. <http://www.networkadvertising.org/participating/>.

A ferramenta, no entanto, apesar de facilitar a autodeterminação no tocante ao monitoramento da navegação, está longe de ser um remédio completo. As empresas que não são membros da NAI não têm seus mecanismos de monitoramento afetados pelo *NAI Opt-out Tool*, e, mesmo as que são, por vezes requerem passos adicionais além do formulário para concretizar a desativação.

Uma outra proposta que, muito embora ainda não seja mais do que uma especulação, tem um potencial concreto para tornar-se uma ferramenta importante para fornecer aos consumidores uma importante retomada de controle sobre seus dados através de uma técnica ligada ao consentimento é a *Do Not Track List*, uma lista de pessoas que não desejam submeter-se ao monitoramento de sua navegação na Internet mantida por uma organização governamental que, reporta-se, está em estudos pela FTC (*Federal Trade Commission*). Esta lista inspira-se francamente em uma outra lista mantida pela FTC, a *Do Not Call List*, que se destina ao bloqueio de marketing telefônico e que teve sua viabilidade e eficácia comprovadas por anos de utilização. Resta, no entanto, além de verificar se tal lista efetivamente virá a ser implementada, quais serão as suas características e os seus resultados.

Em uma breve síntese podemos, portanto, identificar como algumas modalidades alternativas de consentimento: (i) o consentimento reiterado proposto pelo Grupo de Trabalho "Artigo 29", na União Europeia; (ii) o mecanismo de *opt-out* genérico implementado pela NAI (*Network Advertising Initiative*); e (iii) a eventual *Do Not Track List*, em estudos pela FTC (*Federal Trade Commission*). Note-se que, nesta área, mesmo uma indústria com razoável experiência com a auto-regulação como a da publicidade não vem demonstrando ser capaz de elaborar regras e produtos condizentes com uma legítima expectativa de privacidade dos consumidores, o que reforça a posição segundo a qual a intervenção legislativa se faz necessária nesta área, com uma legislação sobre proteção de dados que proporcione ao consumidor garantias de privacidade e segurança em sua navegação na Internet.

CAPÍTULO 4
REDES SOCIAIS

Não cometa o erro de achar que você é o cliente do Facebook, você não é - você é o produto. Os seus clientes são os seus anunciantes.

Bruce Schneier

Entre as aplicações mais óbvias para as tecnologias da informação estão as que proporcionam comunicação e interação entre pessoas. Afora as tantas possibilidades de acesso, armazenamento e compartilhamento de informação, a possibilidade de contatos diretos entre pessoas, mediados pelas tecnologias da informação, é um elemento que tradicionalmente torna o meio tecnológico mais palatável e que pode funcionar como um verdadeiro indutor para a adoção massificada de uma determinada tecnologia ou sistema.

No caso da Internet, por exemplo, sua rápida popularização teve como pano de fundo a transformação do correio eletrônico - o *e-mail* - como um novo instrumento natural e universal de comunicação, cuja rapidez, preço e robustez na maioria das vezes não permitia comparação com as modalidades tradicionais de comunicação.

Além da consolidação do correio eletrônico como plataforma universal, não tardou o surgimento de ferramentas que procurassem implementar na gramática das tecnologias da informação alguma modalidade

de rede social. Em uma rede social, pessoas (que, na teoria das redes, denominam-se "nós") ligam-se umas às outras através de critérios determinados (como amizade, interesses comuns e outros).

Mesmo antes da popularização da Internet, fenômenos semelhantes eram claramente visíveis nas comunidades de usuários agregadas em torno das BBS[100] (*Bulletin Board System*) surgidas na década de 1970 e que, até serem suplantadas pela própria Internet, comprovaram a viabilidade de uma interação efetiva e de que era viável a formação e administração de uma rede social apenas através de ferramentas das tecnologias da informação.

O ambiente da Internet foi bastante propício a diversas formulações de interações sociais que, em um sentido lato, assemelham-se às redes sociais. Alguns jogos foram a primeira grande expressão deste fenômeno, em particular os MUDs (*Multi-User Dungeon*) desenvolvidos a partir de 1980. Os MUDs são ambientes virtuais nos quais diversas pessoas se conectam ao mesmo tempo e se relacionam entre si, assumindo uma personalidade diversa da sua (um *avatar*). Tendo sido criados com uma interface textual, são uma espécie de antecessores das experiências que vieram a seguir, com a incorporação de elementos gráficos e a utilização plena dos recursos que se tornaram disponíveis com o desenvolvimento da Internet, que são os ambientes de realidade virtual. Tais ambientes, dos quais são exemplo os "mundos virtuais" como *Second Life*[101], apresentam um caráter acentuadamente lúdico, justamente por não fomentarem a interação direta entre seus participantes, porém através do personagem - o *avatar* - que estes utilizam para se apresentar perante os demais participantes e com eles interagir.

A interação direta e uma efetiva transposição da ideia de rede social para a Internet foi efetivamente realizada pelos *sites* de redes sociais *online*, que começaram a surgir na Internet a partir de 1997. Estes *sites* procuram captar usuários que, após inscreverem-se e elaborarem um perfil de si próprios, passariam a se relacionar com os demais usuários. Agora, o mencionado perfil era formado por informações pessoais verdadeiras do próprio usuário. O fato de que o modelo das redes sociais *online* pressupõe o tratamento de dados pessoais dos seus usuários, aliado à grande penetração e volume de usuários que tais redes apresentam, faz com que o tema seja, hoje, de extrema relevância para a proteção de dados pessoais na Internet.

---

100 *Bulletin Board System* é o nome de sistemas informatizados que permitem a troca de mensagens, informações e programas entre diversos usuários que acessavam um computador central por meio de uma conexão telefônica. Os *BBS* foram populares antes da popularização da Internet

101 *Second Life* é um jogo que proporciona aos seus participantes a interação em um ambiente gráfico virtual, no qual estes criam suas próprias identidades.

Aquela que ficou conhecida como a primeira rede social *online* foi a *Six Degrees*. O próprio nome desta rede social é uma referência direta à teoria dos seis graus de separação, que é frequentemente mencionada ao se tratar do tema. Por esta teoria, haveria um máximo de seis graus de relações pessoais que ligariam (ou separariam!) toda pessoa viva de qualquer outra pessoa. A teoria, cuja formulação remonta a Gugliermo Marconi e até hoje é objeto de estudos[102], serve como uma fundamentação para o crescimento exponencial no volume de usuários de redes sociais *online* nos últimos anos, algo que resulta concreto ao se constatar que as redes mais utilizadas, como *Facebook*, *Twitter*, *MySpace* e outras contêm hoje seus usuários na casa das centenas de milhões.

4.1. Estrutura e modalidades das redes sociais online

As redes sociais online podem ser sinteticamente definidas como, "serviços prestados por meio da Internet que permitem a seus usuários gerar um perfil público, alimentado por dados e informações pessoais, dispondo de ferramentas que permitam a interação com outros usuários, afins ou não ao perfil publicado"[103]. Danah Boyd e Nicole Ellison, por sua vez, denominam de redes sociais *online* os "serviços baseados na Web que permitem a indivíduos: (1) construir um perfil público ou semi-público dentro de um determinado sistema, (2) articular uma lista de outros usuários deste sistema com os quais se quer estabelecer um relacionamento, e (3) visualizar e navegar pela sua lista de conexões e pela aquela de outros através do sistema"[104].

Há diversas modalidades destas redes. As maiores e mais conhecidas são sistemas inteiramente dedicados à atividade de *social networking*. São casos que poderíamos classificar como redes sociais

---

102 "E-mail study corroborates six degrees of separation", in: Scientific American. 8 de agostto de 2003. <http://www.scientificamerican.com/article.cfm?id=e-mail-study-corroborates>.

103 Agencia Española de Protección de Datos / Instituto Nacional de Tecnologías de la Comunicación. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales. Madrid, 2009, p. 6.

104 Danah Boyd, Nicole Ellison. "Social Network Sites: Definition, History, and Scholarship". 2007. <http://www.guilford.edu/about_guilford/services_and_administration/library/libguide_images/boyd.pdf>.

próprias ou generalistas, cujo maior atrativo apresentado aos seus usuários é justamente a formulação de seu próprio perfil pessoal e a interação com os demais usuários desta rede social. É o caso das redes sociais como o *Facebook*, *Orkut*, *MySpace*, *Hi5*, *Zing*, *Maktoob* e diversas outras.

Há também redes sociais que poderíamos denominar como impróprias, que seriam aquelas que funcionam como um apêndice de outro serviço ou ferramenta, gravitando e existindo em função deste. Estas redes impróprias podem oferecer um conjunto parcial das ferramentas típicas de interação encontradas nas redes sociais próprias, e podem ser mencionados como exemplos as redes sociais presentes em sites de comércio eletrônico (tais como o da *Amazon.com*, *eBay* ou o *Mercado Livre*) ou em sites que tem como objetivo primordial o intercâmbio de conteúdo e não propriamente a interação social mas que também cultivam suas próprias comunidades de usuários (tais como o *Slideshare* ou o próprio *YouTube*).

As redes sociais que possuem maior volume de usuários e que são, efetivamente, as maiores responsáveis pela inovação e modelagem do perfil destas ferramentas, são as redes sociais próprias ou generalistas, aquelas dedicadas inteiramente à interação entre seus usuários como atividade principal.

Dentre as redes sociais impróprias, pode-se ainda destacar que há ao menos duas categorias de grande importância. Uma delas é a das redes sociais estruturadas em torno do intercâmbio de conteúdo. Este conteúdo é geralmente alguma espécie de mídia eletrônica - como nos exemplos já mencionados, documentos e apresentações, no caso do *Slideshare* ou vídeos, no caso do *YouTube*, entre outros. A utilização de ferramentas típicas de redes sociais pode aumentar a eficácia deste intercâmbio de conteúdo, através da formação de comunidades de interesses específicos e do intercâmbio de opiniões e críticas, apenas para dar um exemplo.

Outra categoria que estaria dentro do âmago das redes sociais imprópria é a das redes sociais profissionais, dedicadas especificamente a um determinado setor do mercado ou a atividades profissionais em geral. Neste último caso, destaca-se hoje a rede *Linkedin*.

Em todas as modalidades de redes sociais *online* apresentadas, há uma constante em sua forma de atuação e, consequentemente, no seu modelo de negócios. Todas procuram alcançar uma base razoável de usuários para, com base nesta rede de pessoas e interesses interconectados, partir para a exploração comercial propriamente dita, visto que os eventuais lucros derivados das redes sociais *online* não provém diretamente dos seus usuários, cuja participação não é onerosa.

É a partir da caracterização do modelo de negócios das redes sociais *online* e na verificação de quem são efetivamente, seus clientes e usuários, que é possível determinar uma justificativa conjuntural para os riscos para a privacidade presentes nesta atividade. A necessidade de partir desta consideração como um *prius* para um estudo deste gênero foi ressaltada por Ilse Aigner, Ministra do consumo da República Federal da Alemanha, ao ressaltar que:

> *Todos que visitam um site de uma rede social devem ter consciência de que se trata de um modelo de negócio. O serviço oferecido não é gratuito. Nós, usuários, pagamos por este serviço com as nossas informações privadas*[105].

Nesta declaração encerra-se uma distinção fundamental entre usuários, e cliente das redes sociais *online* a se ter em conta: seus clientes, aqueles que efetivamente contratam a rede social em troca de um serviço mediante retribuição, não são seus usuários porém terceiros que, de alguma forma, apresentam interesse na base de dados e na rede de usuários. Estes clientes poderiam ser, no exemplo mais óbvio, anunciantes que buscariam visibilidade focada dentro de grupos ou comunidades especificamente ligadas ao seu ramo de atuação. Poderiam ser também desenvolvedores de software que incluíssem na rede social uma versão de seus sistemas para promovê-lo e angariar mais usuários, além de diversas outras possibilidades.

A dinâmica de funcionamento de uma rede social *online* prevê que seus usuários se apresentem perante os demais por meio de suas informações pessoais - sejam estas dados identificativos, gostos, opiniões, mensagens, fotografias, vídeos - enfim, basicamente todos os aspectos de uma vida passíveis de encontrarem expressão em formato digital.

O usuário da rede social, mesmo não sendo o cliente deste modelo de negócios, é um consumidor e possui todos os direitos deste ao se utilizar de um serviço de interatividade que a própria rede social fornece gratuitamente, visando o seu próprio lucro a partir de proventos oriundos de outra parte - basicamente a partir dos dados pessoais fornecidos pelos seus usuários e que a tornem atrativa para seus clientes.

---

105 The Independent, 15 de julho de 2010. <http://www.independent.co.uk/news/media/german-minister-calls-for-internet-honour-code-2027047.html>.

Além disso, outro aspecto fundamental a levar em conta é que a rede social *online* é, basicamente, um intermediário. É um mediador entre emitente e destinatário de uma determinada mensagem. Sua existência se justifica, por um lado, pelas vantagens que podem trazer aos seus usuários em termos de proporcionar-lhes uma interação social com características e dinâmica próprias e, por outro, pelas vantagens que o acúmulo de informações pessoais sobre os usuários pode trazer ao proprietário desta rede.

Como o modelo de negócios de uma rede social condiciona o valor de uma rede à quantidade de informações pessoais que ela administra e a forma com este volume de informações possa ser utilizado de forma rentável, é natural que elas incentivem seus usuários a alimentá-las com seus próprios dados. A indução ao fornecimento dos próprios dados pessoais é constante no relacionamento da rede social *online* com seus usuários, e a forma com que este convite ao compartilhamento é realizado pode ser relevante para que se verifique se há, efetivamente, vontade livre e informada quanto aos efeitos deste compartilhamento no momento em que os dados pessoais são fornecidos[106].

O compartilhamento de informações pessoais é da própria natureza da atividade social e também é parte estrutural das redes sociais *online*. Nas interações sociais tradicionais, dispomos de mecanismos culturais, desenvolvidos com o tempo e profundamente arraigados em nossa cultura que nos proporcionam uma ideia razoável das expectativas que podemos nutrir sobre o que será feito com a informação que revelamos a alguém ou difundimos de forma mais ampla. A partir desta expectativa, estamos em condições de exercer um determinado controle sobre as nossas informações, dosando a sua revelação para determinadas pessoas e situações. Assim, informações mais reservadas podem ser reveladas com maior facilidade a pessoas mais próximas, que são consideradas como meritórias de maior confiança; já as informações cujo trânsito mais amplo possa ser tolerado são informações que mais facilmente revelaríamos a pessoas com as quais tenhamos um relacionamento somente esporádico, e assim por diante.

Por complexo que este mecanismo de interação social e compartilhamento de informações possa parecer, ele é familiar à nossa cultura e parte integrante de nossos hábitos cotidianos. Ele proporciona uma razoável expectativa de controle sobre nossas próprias informações, dispondo de um mecanismo sancionatório próprio no qual a quebra de confiança na revelação de informações pessoais pode ser punido com uma sanção social proporcional.

---

106 A este respeito e apenas como exemplo, verifique-se os termos algo inocentes com os quais os usuários de algumas das mais populares redes sociais online são convidados a compartilhar suas próprias informações: "No que você está pensando agora?" ou, na versão em inglês, "What's in your mind" (Facebook); e ainda o "What's happening?", no Twitter (cuja interface não está disponível em português).

O mesmo não ocorre com as interações mediadas pelas redes sociais *online*, nas quais o nível de compartilhamento das informações pessoais depende diretamente do intermediário nas comunicações - a rede social em si. A mera existência deste intermediário como entidade autônoma na comunicação pode ser opaca a grande parte dos usuários das redes sociais, cuja motivação para a interação não costuma provir da rede em si, porém das pessoas - seus conhecidos e relacionamentos, que também são usuários da rede. Mas o ponto é que, em última análise, este intermediário - e não as partes da comunicação em si - tem o poder de determinar o tratamento a ser dado às informações pessoais que as partes compartilham.

O caráter fechado e centralizado das redes sociais é, de certa forma, paradoxal em relação à prática de induzir a abertura entre seus usuários e acelerar as dinâmicas de relacionamento social, tão características destas redes. Além de serem fechadas, elas tendem a promover uma fidelização de seus próprios usuários que é dificilmente perceptível em um primeiro momento - novamente, auxiliadas pelo fato de que são intermediários razoavelmente opacos nas relações entre seus usuários. Assim, a rede social pode se tornar, principalmente após ter angariado um bom número de usuários, um intermediário quase que necessário para uma série de interações sociais.

Um outro aspecto a se considerar é a tendência inercial à concentração de usuários em redes sociais que já possuam um grande número de inscritos, com a finalidade de otimizar o seu círculo de relações entre as pessoas que já estão inscritas e em detrimento de redes menores, nas quais a probabilidade de encontrar pessoas com as quais queira se relacionar pode ser proporcionalmente menor. Esta seria uma vantagem competitiva concreta, capaz de criar uma barreira à criação de novas redes sociais, bem como um empecilho para que um usuário opte por inscrever-se em uma rede social concorrente pois, mesmo com a gratuidade da inscrição e utilização, há o custo objetivo de "começar de novo", abrindo mão das informações com que anteriormente tinha alimentado a rede da qual pretende sair e na iminência de ter que reestruturar a partir do zero a sua rede de contatos pessoais.

Este modelo fechado e centralizado das redes sociais não é, porém, a única arquitetura possível. Recentemente, o idealizador de uma nova rede social que se pretende construída sobre plataformas abertas e decentralizadas enfatizou este ponto, ao declarar que:

"*Em nossas vidas reais, nós conversamos uns com os outros. Não há necessidade de confiar nossas comunicações a um intermediário*"[107].

As expectativas sobre como serão tratadas as informações pessoais dependem diretamente deste intermediário, do gestor da rede social. Suas ações podem determinar, por exemplo, o compartilhamento destas informações com terceiros; a exposição destas informações em perfis públicos ou semi-restritos; a sua utilização para a categorização do usuário dentro de um determinado perfil de comportamento e tantas outras modalidades de tratamento possíveis - que não raro extrapolam as possibilidades de tratamento de informações pessoais compartilhadas nas interações sociais tradicionais.

Frente a estas possibilidades, de pouca valia são os condicionamentos culturais tradicionais que possibilitam o controle da difusão de informações pessoais. As redes sociais deixam clara, portanto, uma nova vulnerabilidade dos seus usuários que consiste, entre outros fatores, na escarsa possibilidade destes conhecerem os efeitos do compartilhamento de suas informações; de terem que confiar não somente nos destinatários das informações para confirmar suas expectativas de privacidade porém também em um intermediário que tem um interesse particular e objetivo em tratar suas informações pessoais para seu próprio proveito. Construir, dentro desta nova equação que compreende os interesses em torno do tratamento de informações pessoais, mecanismos que garantam um efetivo controle e garantam as expectativas de utilização destas informações é um desafio aberto.

4.2. Privacidade, publicidade e riscos das redes sociais

O incentivo ao compartilhamento de informações pessoais é também por vezes apregoado como uma nova tendência dominante ou, em uma variação, como um novo padrão de interação social, próprio das novas gerações. O fundador da rede social Facebook, Mark Zuckerberg, declarou certa vez que a abertura e o compartilhamento de informações pessoais corresponderia à uma evolução de uma "norma social", no sentido de que denotaria um mudança nos costumes socialmente percebidos como normais[108]

107 http://www.nytimes.com/2010/05/12/nyregion/12about.html

108 "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people (…). That social norm is just something that has evolved over time" "Privacy no longer a social norm, says Facebook founder", in: The Guardian. 11 de janeiro de 2010. <http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>.

em relação ao fluxo de informações pessoais. Nesta declaração se pode perceber, ao mesmo tempo, uma tensão entre uma noção implícita de norma jurídica, utilizada para tutelar a privacidade e os dados pessoais em ocasiões nas quais estes encontrem-se em risco por conta das redes sociais, e a dita "norma social", que representaria, neste ponto de vista, uma evolução dos costumes, com vistas a uma nova percepção de normalidade representada pela abertura e compartilhamento de informações pessoais.

Esta opinião, no entanto, não pode ser considerada sem que se leve em conta o interesse das próprias redes sociais em que esta abertura seja aceita e vista com naturalidade. Mas também entre sujeitos cujos interesses não estão diretamente identificados com os das redes em si, podemos verificar que há defensores de um modelo de abertura como novo paradigma das relações sociais.

A idéia da publicidade e abertura da vida privada não são tão recentes. Desde antes da eclosão do fenômeno das redes sociais, ouvem-se leituras sobre a iminência da substituição do paradigma da privacidade pelo da transparência nas relações sociais[109]. Em um panorama que ainda não tinha a ver com o tratamento automatizado de informações pessoais, Karl Popper chegou a definir os defensores da privacidade como inimigos da "sociedade aberta"; ao passo que outros, como Martin Heidegger, pareceram mais preocupadas com os reflexos culturais deste "apego à privacidade", alertando para o perigo da perda da memória - a *Mnemosine*[110] - como conseqüência das tendências consolidadas no direito ao esquecimento, algo que poderíamos evocar na obrigação, freqüentemente presente nas leis de proteção de dados pessoais, de se processar um mínimo de informações necessárias e de, em várias circunstâncias, apagá-las após certo período.

No entanto, interpretar este incremento na exposição e fluxo de informações pessoais através de redes sociais como o epítome das tendências em uma sociedade é render-se a uma forma de determinismo tecnológico fortemente influenciada por uma visão unilateral dos interesses em jogo no novo modelo de negócios proposto. À intensa exposição a que se submetem vários usuários de redes sociais, correspondem, por sua vez, mecanismos que permitam o controle efetivo das informações a seu respeito, garantidos ainda seus direitos de cancelar sua participação na rede, levando consigo os vestígios desta participação.

---

109 David Brin. The transparent society. Massachusetts: Addison-Wesley, 1998.

110 Na mitologia grega, a deusa da Memória e mãe (com Zeus) das nove musas. Mário da Gama Kury. Dicionário de Mitologia Grega e Romana. Jorge Zahar: Rio de Janeiro, 1990, pp. 405. Heidegger manifestou tal preocupação em seu ensaio O que é pensar, evocando o poema Mnemosine, de Holderin.

Este efetivo controle do usuário sobre as próprias informações deve se verificar em todos os momentos de sua interação com a rede social. Em sua inscrição, como já comentado, deve-se atentar para que esteja informado sobre as modalidades de tratamento a que suas informações pessoais estarão submetidas, através de uma política de privacidade clara e precisa e do recurso a outros meios que garantam que sua inscrição não se efetive sem o real conhecimento das suas consequências.

Na sua inscrição, há também de se atentar para o fato de que as redes sociais estão disponíveis também a menores que utilizam a Internet. A coleta e tratamento de dados relativos a menores costuma ser regulada com certo rigor em diversos países[111], é outro tema bastante sensível.

Na utilização da rede social, há ainda a possibilidade de que terceiros que não sejam inscritos na rede tenham seus dados difundidos. Isto ocorre quando tais dados são introduzidos na rede social por usuários regularmente inscritos, que podem descrever a participação deste terceiro em algum evento, publicar fotografias nas quais este terceiro é retratado ou, de alguma outra forma, tratar os dados pessoais de terceiros sem que tenham autorização para tal. Nestes casos, apesar da divulgação não autorizada ter partido de um ato do usuário registrado da rede social, é relevante o fato de que a divulgação da informação de terceiro se dá através da estrutura da rede social elaborada exatamente para o fim de fomentar o intercâmbio de informações e obter proveito desta atividade, abrindo a possibilidade para que possa ser responsabilizada pelo eventual dano causado a este terceiro.

Um outro potencial risco à privacidade potencializado com as redes sociais é a tendência à incorporação de serviços de geo-localização. Isto se realiza com o compartilhamento de coordenadas geográfica precisas sobre a localização de um usuário, a partir da integração de aparelhos de GPS (*Global Positioning System*) em diversos aparelhos eletrônicos de consumo, como telefones celulares. O fornecimento de coordenadas de localização abre tanto a possibilidade para que a localização atual de uma determinada pessoa seja determinada, o que pode ocasionar riscos à sua segurança pessoal e patrimonial, como pode permitir o mapeamento das áreas de circulação e interesse habituais de uma pessoa por serviços especializados, gerando dados que podem ser agregados a serviços de publicidade comportamental.

Por fim, outro delicado problema nas redes sociais refere-se à saída de um usuário de uma determinada rede. É necessário, como garantia do controle de cada usuário sobre os próprios dados pessoais

111 Note-se que, no ordenamento jurídico norte-americano, o Children's Online Privacy Protection Act - COOPA, de 1998, estabelece normas de proteção dos dados de menores relativamente rigorosas para uma tradição jurídica que ainda não estabeleceu normas de caráter genérico para a proteção de dados de adultos.

e da sua exposição em uma rede social, que exista a possibilidade do completo cancelamento de todas as informações pessoais pertinentes a este usuário dos arquivos da rede. Este cancelamento, mais do que uma elaboração pontual de um "direito ao esquecimento", refere-se diretamente a um ato de liberdade e do exercício dos poderes atinentes ao consentimento sobre a exposição dos próprios dados. Ao obter os dados pessoais de seus usuário mediante o consentimento, não ocorre propriamente a transferência dos direitos de disposição sobre tais dados do usuário para a rede social, pois estes, por serem dados pessoais, continuam sendo uma expressão direta da pessoa do usuário e continuam a manter com ele uma relação direta e inafastável. Assim, cabe à rede social reconhecer este caráter dos dados pessoais e fornecer aos seus usuários instrumentos que efetivamente realizem o cancelamento completo dos dados pessoais que lhes foram fornecidos por seus usuários.

O cancelamento dos dados pessoais em uma rede é a face mais extrema de uma garantia genérica do controle dos usuários de uma rede sobre seus próprios dados. A necessidade de definir instrumentos para este controle genérico verifica-se, por exemplo, no imperativo de fazer com que o próprio *design* da interface das redes sociais não acabe por ofuscar ou dificultar o exercício desta opção. Outro exemplo implica em dar passo além do mero cancelamento, ao proporcionar mecanismos que permitam a um usuário obter cópias de todas as informações pessoais que ele próprio forneceu a uma rede social (das quais, muito provavelmente, não possui cópias sistematizadas). Estes mecanismos, que atualmente encontram-se em diversos graus de implementação em algumas redes sociais, permitem tanto uma gestão mais direta e simplificada dos próprios dados pessoais como também permite que o cancelamento das informações e a saída da rede não seja inibida pelo receio da perda definitiva destas pelo seu próprio titular.

Além da mera cópia, hoje também discute-se o conceito de portabilidade dos dados pessoais. Por portabilidade de dados pessoais, entende-se a possibilidade de copiar e transferir os próprios dados pessoais inseridos em um determinado serviço (no nosso caso, em uma rede social), de forma a permitir a sua re-utilização em outro serviço similar ou para outro uso possível[112]. A portabilidade, além de ser um importante princípio de gerenciamento de dados a ser levado em conta ao se analisar eventuais práticas concorrenciais abusivas, é capaz de fornecer ao usuário de uma rede social um nível relativamente alto e sofisticado, para os padrões atuais, de controle sobre seus próprios dados, diminuindo concretamente uma vantagem desproporcional que a rede pode ter em relação ao usuário que mais dela se utiliza.

112 Um exemplo atual de implementação deste conceito em serviços disponíveis para consumidores é o da Google que, com seu projeto denominado Data Liberation Front (http://www.dataliberation.org/) procura inserir em diversos serviços e produtos da empresa ferramentas que permitem tornar efetiva tal portabilidade.

CAPÍTULO 5
CORREIO ELETRÔNICO NÃO AUTORIZADO - "SPAM"

O problema do *spam*[113] é relevante para o consumidor ao ameaçar inibir a utilização de uma ferramenta - o *e-mail* - cujas qualidades sempre pareceram obscurecer seus eventuais pontos fracos. O *e-mail*, como forma de comunicação veloz, econômica e acessível, foi a primeira grande aplicação que ajudou a transformar a Internet em um meio de comunicação de grande alcance. O crescimento da prática do *spam*, no entanto, contribui para torná-lo uma ferramenta cada vez menos confiável e útil, capaz de substituir em diversas circunstâncias outros meios, eventualmente mais custosos.

Estimou-se o volume total de *spam* como cerca de 89% do universo total de *e-mail*s enviados através da Internet no arco dos últimos 12 meses[114]. O problema do *spam* compreende tanto um aspecto individual como um coletivo, ao turbar a utilização pessoal da própria caixa postal eletrônica e também ao diminuir a eficácia global de uma poderosa ferramenta de comunicação.

A dificuldade em conceber meios técnicos para diminuir o volume de *spam* é muitas vezes potencializada pela ausência de um patamar jurídico que permita identificá-lo com clareza e perseguir seus responsáveis. Na falta destas especificações, corre-se o risco de atacar um problema disposto em termos excessivamente generalizados, impossível de ser completamente abrangido exatamente pela excessiva generalidade de sua definição. Daí a necessidade de explicitar o que se entende como *spam* como primeiro passo.

113 Adaptação e atualização de trabalho publicado originalmente na coletânea Direito e Internet 2. Newton De Lucca, Adalberto Simão Filho (orgs.). São Paulo: Quartier Latin, 2008.

114 Estimativa presente no MessageLabs Intelligence Report (2010) <http://www.messagelabs.com/resources/press/49913>.

5.1. Terminologia

O termo "*spam*" é um neologismo surgido na esteira da popularização da Internet. Originalmente, refere-se a uma determinada marca de alimento enlatado[115]. Não é possível precisar quando foi empregado pela primeira vez no contexto que agora examinamos: talvez em meados da década de 1980, quando um usuário de um sistema informatizado causou problemas técnicos com a repetição automática da palavra "*spam*" em um ambiente multi-usuário[116]; ou então, na mesma época, alguns grupos de discussão da USENET[117] começavam a enfrentar mensagens enviadas em massa. O que parece certo é que o termo foi inspirado em um célebre quadro do grupo humorístico Monty Python[118].

Uma definição "utópica" do *spam* poderia aponta-lo como todo *e-mail* que não seja útil ao destinatário, ou que este tenha preferido não haver recebido. Uma definição "prática" seria aquela que identificasse objetivamente no *spam* elementos que o qualificassem como inútil e indesejado e pudesse orientar os mecanismos de repressão à sua prática. Entre estes dois pólos, porém, há uma série de incertezas e inconsistências.

115 O termo SPAM™ (em letras maiúsculas) refere-se a um produto, uma espécie de carne enlatada (provavelmente uma espécie de contração a partir das palavras SPiced hAM), produzida pela Hormel Foods Corporations, que detém os direitos sobre a marca. <http://www.spam.com/ci/ci_in.htm>.

116 Este usuário participava em um MUD (Multi-User Dungeon - uma espécie de jogo no qual vários participantes interagem on-line), e criou um pequeno programa que fazia com que a palavra "Spam" aparecesse incessantemente na tela dos demais participantes, impedindo sua participação. J. D. Falk. The Net abuse FAQ revision 3.2, §2.4. <http://www.cybernothing.org/faqs/net-abuse-faq.html#2.4>, cf. David Sorkin. "Technical and legal approaches to unsolicited eletronic mail". 35 U.S.F. Law Review 325 (2001).

117 A USENET reúne grupos de discussões sobre variados temas, nos quais os inscritos podem postar e-mails que ficam a disposição de todos os interessados. Um forte traço da origem da utilização do termo "spam" na USENET é oferecido por algumas das definições do termo spam presentes no Jargon file: "2. to cause a newsgroup to be flooded with irrelevant or inappropriate messages; (...); 4. To bombard a newsgroup with multiple copies of a message. ". O Jargon File é um popular glossário de termos técnicos referentes à Internet e sua cultura. V. < http://www.catb.org/jargon/html/S/spam.html>.

118 Neste sketch, que se passa em um restaurante, uma garçonete tentava dar informações sobre o menu - no qual todas as opções incluíam spam, o que irrita um cliente. Ao mesmo tempo, um grupo de vikings que se encontra no restaurante canta, ao fundo: "Spam, spam, spam, spam! Lovely spam! Wonderful spam!" – com vigor cada vez maior, até o ponto de tornar impossível o trabalho da garçonete. Deste quadro o termo "spam" foi tomado de empréstimo para representar algo que seja absolutamente irrelevante para uma determinada discussão e que tire a atenção do seu foco principal.

Já de início, as tentativas de definição parecem muito mais motivadas pela conveniência do que propriamente refletir uma determinada acepção em si. É comumente aceita[119] sua sinonímia com "correio eletrônico comercial não solicitado"[120], a qual abrange o núcleo central das mensagens percebidas como *spam*, porém carrega um certa inconsistência que se evidencia pelo fato de que há diversas mensagens geralmente percebidas como *spam* que não possuem caráter comercial, bem como, sob determinados enfoques, é possível identificar mensagens "não solicitadas", com caráter comercial, que podem não merecer esta qualificação.

Note-se ainda que o âmbito de aplicação do termo não é somente o *e-mail* da Internet, pois sua utilização vem se propagando para outros protocolos de comunicação eletrônicos (SMS, *chat on-line* e outros)[121] e sistemas informáticos nos quais não há propriamente a troca de mensagens[122]. Em um limite extremo, são englobadas até mesmo algumas modalidades de comunicação que independem de redes de computadores[123], não obstante que a tendência à utilização do termo *spam* esteja associado com maior propriedade com as variadas formas de abusividade identificadas no âmago das comunicações eletrônicas de uma forma geral.

Na busca de um denominador comum, nem mesmo a generalização dos *e-mails* comerciais não solicitados como *spam* não é capaz, por si só, de proporcionar um patamar jurídico ou mesmo técnico[124] dentro do qual tratar a questão de maneira completamente segura - visto que o *spam*, nesta ótica, não se diferenciaria qualitativamente de diversas práticas de marketing direto.

---

119 dicionários

120 ou UCE (Unsolicited Commercial E-mail).

121 Na União Européia, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (Diretiva relativa à privacidade e às comunicações eletrônicas) endereça o problema sem referir-se diretamente ao termo "spam", preferindo uma referência genérica como "comunicações eletrônicas não solicitadas". Assim, são abrangidas outras formas de comunicação eletrônica.

122 Cite-se como exemplo o "vandalismo" do qual são vítimas certos sites que permitem a elaboração coletiva de seu conteúdo, como os sitemas Wiki (v. <http://en.wikipedia.org/wiki/Wikipedia:Vandalism>); ou então a utilização indiscriminada de meta-tags para fazer com que um site apareça com maior destaque nos mecanismos de busca na Internet, ambas práticas que são também eventualmente rotuladas como "spam".

123 Algumas chamadas telefônicas realizadas automaticamente, em regra para fins de marketing direto, são eventualmente denominadas phone spam.

124 Como é confirmado pela arquitetura dos principais filtros desenvolvidos para bloquear o spam. Estes filtros não tem como seu pressuposto de funcionamento qualquer definição estática sobre o spam (seu caráter comercial, por exemplo), porém se baseiam em regras (linguísticas, heurísticas e outras) que estabelecem uma alta probabilidade de uma mensagem ser do gênero que uma pessoa preferiria "não ter recebido").

Para enquadrarmos a questão, é necessário identificar alguns elementos básicos que o *spam* pode apresentar de forma mais ou menos acentuada:

- o caráter comercial;

- o envio em massa;

- a uniformidade de seu conteúdo;

- o fato de não ter sido solicitado pelo destinatário.

Sobre o caráter comercial do *spam*, já foi aludida a freqüência com que esta sua característica é mencionada como essencial. Salta aos olhos, no entanto, o fato de que não é impossível nem mesmo raro que *e-mails* sem caráter comercial direto ou até indireto acabem por ser considerados como *spam* – e, mais importante, que o tratamento que eles mereçam seja idêntico àquele dos *e-mails* comerciais tidos como *spam*. Nesta grande categoria do *spam* não-comercial estariam incluídas, por exemplo, as mensagens com conteúdo fictício elaboradas com a intenção de fraudar de alguma maneira o destinatário. Tal fraude poder-se-ia processar seja através da instalação de vírus, *trojans*, *spyware* ou congêneres no computador do destinatário, seja pela tentativa de obter dados pessoais de forma ilícita ou então por inúmeros outros meios – todos dificilmente reconduzíveis a qualquer aspecto licitamente "comercial". Assim, malgrado a finalidade comercial direta ou indiretamente verificável em um *spam* "clássico", é de se ter em conta que esta não é uma característica a ser tomada como absoluta.

O envio em massa e a uniformidade do conteúdo do *spam* são características da sua própria modalidade de propagação. Como a taxa de resposta é baixíssima, o *spam* somente se justifica quando realizado em um determinado volume que garanta um mínimo de respostas positivas para o intento do seu remetente. Portanto, é uma prática quase sempre massificada, que tem como conseqüência a impossibilidade de personalização de seu conteúdo – que é uniforme e padrão ou, em casos específicos, pode compreender modificações mínimas realizadas justamente para que o destinatário, por conta destas, não perceba tratar-se propriamente de um *spam*. Estas, porém, são regras apenas qualitativas, por não concentrarem-se no conteúdo da comunicação. Como conseqüência, apesar de praticamente todo *e-mail* considerado abusivo e classificado como *spam* apresentar estas duas características, ainda resta o fato de que, em poucos e raros casos, uma única mensagem, ainda que dirigida a um só destinatário, possa ser considerada como *spam*.

A idéia de que um *e-mail* não foi "solicitado" pelo seu destinatário deve ser examinada com a devida cautela. Em uma interpretação excessivamente literal, a grande maioria dos *e-mail*s (e das comunicações em geral) não são estritamente "solicitados" pelo destinatário, porém lhe são dirigidos no âmbito de contatos anteriores ou de interesses específicos. Talvez a expressão "não solicitada" fosse melhor traduzida por algo que representasse o fato de que o destinatário, tendo sabido do teor da mensagem, tivesse preferido não tê-la recebido – que, por sua vez, peca pelo extremo subjetivismo. Fato é que a expressão "não solicitado" é de uso generalizado, e cabe a integração de sua interpretação, que deve ser realizada sob a ótica da boa-fé no sentido de que o *e-mail* deva apresentar algum interesse objetivo potencial para seu destinatário. É relevante ainda que, nas perspectivas de abordagem da matéria a partir de regras de proteção de dados pessoais e também de regras de *opt-in*, o conteúdo da referida solicitação integrar-se-á essencialmente pela verificação do consentimento prévio do destinatário ao recebimento do *e-mail*.

Uma definição que procura equilibrar os elementos apresentados é fornecida pelo *Jargon File*:

> *"Enviar e-mails em massa, não solicitados, idênticos ou quase idênticos, geralmente contendo publicidade. Utilizado em particular quando os endereços foram extraídos do tráfego de rede ou de bancos de dados sem o consentimento dos destinatários. (...)"*[125].

Conclui-se, enfim, que o atual estado da matéria não recomenda que o tema do *spam* seja encerrado em uma definição abstrata fechada, pois apresentaria o risco de excluir da sua esfera de abrangência *e-mails* que sejam percebidos como *spam* e que mereçam ser tratados como tal. Feita esta consideração, a classificação de uma mensagem como *spam* deve (i) levar em conta a presença (ainda que não de todas) das 4 características acima delineadas e (ii) ponderar se o envio da mensagem pode responder a algum interesse do remetente ou mesmo que não possa lhe acarretar um dano, concreto ou potencial.

---

125 O mencionado Jargon File trata o termo "spam" como verbo transitivo, verbo intransitivo e substantivo. Entre as 6 definições que ele fornece para o termo, destacamos a de número 5: "5. To mass-mail unrequested identical or nearly-identical email messages, particularly those containing advertising. Especially used when the mail addresses have been culled from network traffic or databases without the consent of the recipients. Synonyms include UCE, UBE. As a noun, 'spam' refers to the messages so sent.". The Jargon File, in: <http://www.catb.org/~esr/jargon/html/S/spam.html>.

5.2. Perfil técnico do spam

O motivo imediato da larga disseminação do *spam* é que a tecnologia atual disponibiliza os meios necessários para a sua prática[126]. As características intrínsecas do sistema de correio eletrônico presente na Internet[127] permitem o envio em massa de *e-mail*s, com uma possibilidade bastante razoável de ocultar o remetente, com relativa facilidade - o que leva alguns críticos a caracterizá-lo como uma verdadeira patologia deste sistema, como um verdadeiro "*bug*"[128]. Diante do perfil dos usuários da rede hoje, o *spam* é certamente uma característica inseparável da tecnologia[129].

A bem da verdade, pode-se reconduzir o surgimento do *spam* e a dificuldade em enfrentá-lo à própria concepção estrutural - ou, pode-se dizer, à arquitetura[130] - da Internet. Os mentores do sistema de *e-mail* não tinham consciência de que estavam projetando um sistema que posteriormente prestar-se-ia à uma utilização em massa, no momento em que idealizaram um sistema simples e extremamente eficaz de troca de mensagens que incorporava o princípio de design *end-to-end* típico da Internet:

> *"... [n]ós queríamos um sistema de e-mail extremamente barato com o qual qualquer um pudesse mandar mensagens a qualquer outra pessoa, que protegesse a comunicação anônima, valorizasse valores como a liberdade de expressão e a possibilidade de enviar mensagens não solicitadas"*[131].

126 O problema potencial do abuso das possibilidades que vinham se delineando com o uso do email não passou desapercebido já de início pelo seu principal mentor, Jonathan Postel, que em 1975 publicou o RFC 0706, On the junk mail problem, no qual se lê: "In the ARPA Network Host/IMP interface protocol there is no mechanism for the Host to selectively refuse messages. This means that a Host which desires to receive some particular messages must read all messages addressed to it. It would be useful for a Host to be able to decline messages from sources it believes are misbehaving or are simply annoying". The Internet Society: Internet Engineering Task Force (1975), < http://www.ietf.org/rfc/rfc0706.txt>.

127 "The physical cost, at least in the USA, of a single e-mail is insignificant. We've worked hard to make it that way". Brad Templetons, "Top Mistakes of some anti-spam advocates", in: < http://www.templetons.com/brad/spam/>

128 Claudio Allocchio. "Lo spam: 'bug' oppure... 'feature'?", in: La rete contro lo spam, che cos'è, come combatterlo. Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, pp. 8-15.

129 Cosimo Comella, "Spam, sicurezza e privacy tra soluzioni tecnologiche e intervento normativo", in: La rete contro lo spam, che cos'è, come combatterlo, cit. , p. 31.

130 Cf. Lawrence Lessig. Code and other laws of cyberspace. Basic Books: New York, 1999.

131 Brad Templeton. "Reflections on the 25th anniversary of spam". <http://www.templetons.com/brad/spam/spam25.html> .

O envio de *e-mail* através da rede Internet baseia-se em uma tecnologia bastante eficiente (e duradoura), baseada no protocolo SMTP (*Simple Mail Transfer Protocol*), desenvolvido em 1982 por Jonathan Postel[132]. Este protocolo permite o envio de mensagens eletrônicas com eficiência e rapidez, a um baixíssimo custo (uma vez disponível a infra-estrutura necessária). Por outro lado, o protocolo não dispõe de mecanismos que permitam a identificação e autenticação segura[133] do usuário ou o controle do volume de tráfego que este origina.

Que este fosse um risco real já o demonstra o que veio a ser considerado o primeiro *spam* jamais enviado - de autoria de um funcionário da DEC, em 1978[134]. Práticas do gênero, contudo, são provavelmente quase tão antigas quanto a própria idéia do correio eletrônico[135].

O caso que alertou efetivamente os usuários da rede para os riscos representados pelo *spam* ocorreu em 1994, quando dois advogados norte-americanos especializados em imigração, ofereceram seus serviços através de uma mesma mensagem[136] postada em dezenas de milhares de grupos de discussão da USENET. Esta mensagem, que oferecia serviços para auxiliar a obtenção de um *Green Card*, atingiu um grande número de usuários e proporcionou aos seus autores a duvidosa honra de serem conhecidos como os primeiros grandes *spammers*[137]. Este foi um evento que de certa forma marcou a história da própria Internet, dado que até a época a utilização da rede era quase que completamente "não-comercial". Esta mensagem deixou claro que chegara o momento que a extrema liberdade de utilização da rede, característica da sua arquitetura, já poderia se prestar a certos abusos.

---

132 Jonathan Postel, RFC 821: Simple Mail Transfer Protocol. The Internet Society: Internet Engineering Task Force (agosto 1982), <http://www.ietf.org/rfc/rfc0821.txt>.

133 O conteúdo do campo "from:", relativo ao remetente, pode ser forjado (através do spoofing) sem maiores dificuldades. É possível para um perito, mesmo assim, retraçar a origem de um e-mail, ao menos na grande maioria dos casos.

134 Este e-mail foi enviado para os usuários da ARPANET (a rede de computadores na qual o e-mail ganhou grande popularidade e que é uma das redes ancestrais da Internet), convidando-os para comparecerem à uma apresentação de um novo computador. Uma cópia deste e-mail está disponível em < http://www.doneda.net/spam/1st.htm>.

135 O administrador de sistema de correio eletrônico (ainda não em rede, porém em um só computador com diversos usuários) conta ter se deparado, em 1971, com uma mensagem de cunho pacifista para os usuários de um determinado sistema do MIT (Massassuchets Insititute of Technology). Para este administrador, o usuário que a postou teria abusado de seu privilégio para fazer uma espécie de mass mailing inapropriado. Segundo ele, cogitou-se do problema ao se desenhar o próprio sistema de correio eletrônico, porém, na época (como hoje), as medidas contra spam não parecem largamente eficazes.. Wired. n. 4, 1998.

136 Os advogados eram Lawrence Canter e Martha Siegel; a mensagem foi enviada para cerca de 6000 grupos de discussão da USENET no intervalo de tempo de aproximadamente 90 minutos.

137 O termo spammer se refere à pessoa que envia habitualmente as mensagens consideradas como spam.

Em relação a este primeiro e paradigmático caso, em um primeiro momento, houve uma espécie de "retaliação" por parte dos que haviam recebido esta e outras mensagens do gênero, seja reclamando diretamente aos provedores de acesso a partir dos quais a mensagem se originava (que freqüentemente encerravam as contas dos remetentes destas mensagens), seja através de meios mais venais como a utilização de *mail bombs*[138]. A partir daí o *spam* começou a se sofisticar, fazendo recurso a diversos métodos para transpor as dificuldades que lhe vinham sendo dispostas, como, por exemplo, a mudança dos cabeçalhos para retirar qualquer menção a endereços verdadeiros dos remetentes, uma prática que passou a ser largamente utilizada pelos *spammers* (e que ganhou a denominação de *spoofing*)[139]. Desde então, uma alternância sucessiva entre medidas para repressão do *spam* (por parte da indústria e dos usuários) e técnicas para superá-las (por parte dos *spammers*) tem sido uma constante.

O *spam*, considerado em si, é uma forma bastante econômica de alcançar um grande número de destinatários para uma determinada mensagem. Algumas tentativas de quantificação de seus custos chegam a valores em torno de um centésimo de centavo de dólar por mensagem enviada, o que torna sua prática atrativa mesmo com uma taxa de resposta por parte de seus destinatários bastante baixa.

Como qualquer *e-mail*, o *spam* é constituído objetivamente pelo conteúdo da mensagem em si (o "corpo" da mensagem) e pelo seu cabeçalho (que contém, entre outros, os campos referentes ao remetente, destinatário, assunto e data)[140]. Para que seja remetida, é necessário, no mínimo, fornecer o endereço do destinatário e enviá-la para um servidor de *e-mail* ligado à Internet. O conteúdo da mensagem (que tecnicamente poderia até ser nulo) no caso do *spam* costuma ser a mensagem não-solicitada em si.

A prática do *spam* pressupõe que se disponha ao menos de: (i) uma lista de endereços de destinatários extensa e relacionada ao mercado potencial que se pretenda atingir tanto quanto possível; (ii) meios técnicos específicos para o envio massificado de *e-mail*s.

Hoje, a maior parte do *spam* é enviado por meio de *open relays*, que consistem em servidores SMTP abertos para envio de *e-mail* que permitem sua utilização anônima, isto é, que podem ser utilizados por qualquer

138 Mail bombs são programas capazes de enviar milhares de e-mails para um determinado endereço, dificultando ou impossibilitando o destinatário de utilizar a própria conta de e-mail.

139 Além do puro spoofing, uma outra técnica bastante utilizada por spammers é o registro em serviços de e-mail gratuitos para a obtenção de um endereço eletrônico válido somente para o envio do spam e, posteriormente, abandonado. Do ponto de vista do destinatário do spam, porém, o efeito é o mesmo, pois lhe é negada a identificação de um endereço verdadeiro para a resposta.

140 Conforme especificado no RFC 2822 (v. <http://tools.ietf.org/html/rfc2822>).

um e não somente pelos inscritos no servidor do qual faz parte. A utilização destes *open relays*[141] dificulta a real identificação da origem do *spam* e, mais ainda, reduz em muito a possibilidade de responsabilizar o provedor de acesso do qual foi originário o *spam.*

5.3. Perfil jurídico do spam

A antijuridicidade do *spam* pode ser constatada basicamente pela utilização ilícita e abusiva dos dados pessoais do seu destinatário. Esta abusividade há de ser avaliada tomando-se em conta o conjunto de fatores que envolve a forma pela qual o endereço de e-mail foi coletado e está sendo utilizado, a natureza do e-mail em si e a ponderação de outros valores, como a garantia da liberdade de expressão.

Um endereço de correio eletrônico é expressão de um dado de caráter pessoal referente a um indivíduo - e por este motivo deve ser resguardado através dos instrumentos de proteção de dados pessoais disponíveis[142]. Não é por outro motivo que a repressão ao *spam* nos países que dispõem de sistemas de proteção aos dados pessoais é realizada propriamente por estes sistemas, apesar do fato dos efeitos do *spam* se fazerem notar em muitas outras ocasiões não vinculadas diretamente aos dados pessoais (como na proteção ao consumidor, por exemplo).

A partir desta ótica, há uma consideração fundamental: de que os *e-mails* não são informações públicas e que, portanto, somente pode ser objeto de tratamento no caso do respectivo[143] consentimento.

Certamente a rede Internet aumentou as possibilidades de troca de informações, em especial ao permitir que cada indivíduo possa disponibilizar informações sobre si em larga escala. A idéia de "publicação" varou novas fronteiras e assume novas conotações em um contexto *on-line*. Exatamente por este motivo, o perfil que assume esta disponibilização deve ser encarado de forma específica. Não é possível concordar, por exemplo, com a afirmação segundo a qual a publicação (ou divulgação, ou difusão) de um endereço de *e-mail*

---

141 *Open relays* são computadordes ligados à Internet que funcionam como servidores de e-mails configurados para permitir que qualquer remetente, e não apenas somente aqueles autorizados, envie e-mails por meio deles.

142 Giovanni Buttarelli, "La attività del Garante in materia di prevenzione dello spam", in: in: La rete contro lo spam, che cos'è, come combatterlo. Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, p. 25.

143 cf. Diretiva 97/66/CE do parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações.

através da Internet tenha como efeito necessário uma imediata transformação deste em um dado público e, portanto, passível de utilização generalizada por terceiros – no que estaria incluído o envio de *spam*.

A bem da verdade, a disponibilização de um *e-mail* na Internet equivale a colocá-lo em uma fonte pública – no sentido de ser pública e livremente acessível, de acordo com as características da rede. Porém é válida a sua utilização sem qualquer critério? Não, pelo fato que a referida disponibilização certamente ocorreu para atender a determinados interesses e expectativas de quem a fez, inserindo no contexto desta publicação uma finalidade objetiva que geralmente pode-se induzir do contexto em que se insere. Assim, por exemplo, o *e-mail* de um advogado disponibilizado em seu *site* pessoal ou do seu escritório tem como finalidade maior o contato profissional. Outras utilizações não profissionais podem ser aceitáveis, porém outras, em particular as que se enquadram na prática do *spam*, podem configurar uma utilização abusiva e indevida deste endereço, exatamente pelo amplo desvio de finalidade.

A União Européia trata do tema em algumas importantes diretivas[144], das quais a principal é a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas). Nesta diretiva, utiliza-se basicamente um sistema de *opt-in*[145] como controle de legitimidade do e-mail comercial[146]. Na adoção pela diretiva do regime de *opt-in* foram levados em conta, entre outros motivos, a identificação e adequação desta técnica ao regime de proteção e dados pessoais vigente[147], além da avaliação de que um sistema de *opt-in* poderia ser implementado com maior facilidade, a partir de um quadro normativo mais simples do que os de *opt-out*[148].

144 A Diretiva é um instrumento normativo típico da União Européia. A função básica da Diretiva é de uniformização legislativa. A aprovação de uma diretiva implica que cada país-membro adapte, em um certo período de tempo, seu próprio ordenamento jurídico aos moldes estabelecidos pela diretiva, em um processo que leva o nome de transposição. v. Klaus-Dieter Borchardt. O ABC do direito comunitário. Bruxelles: Comissão Européia, 2000.

145 Ainda no texto do considerado (40), ressaltamos: "(...) No que diz respeito a essas formas de comunicações não solicitadas para fins de comercialização directa, justifica-se que se obtenha, antes de essas comunicações serem enviadas aos destinatários, o seu consentimento prévio e explícito. (...)".

146 Conforme instituído pelo seu art. 13(1): "A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrônico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio".

147 Regime este instituído pela Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

148 Nos sistemas baseados no *opt-out*, o envio de e-mails é permitido mesmo sem a autorização prévia do destinatário, sendo que cabe a este manifestar-se expressamente para que não receba mais as mensagens. Nos sistemas baseados no opt-in, é necessário o consentimento prévio do destinatário para legitimar o envio do e-mail.

O sistema de *opt-in* da diretiva é "temperado" por exceções, a ponto de ser referido por parte da doutrina como um sistema de "*opt-in* modificado" ou simplesmente "*soft opt-in*"[149]. A primeira exceção, prevista no art.13(2), permite que, no caso em que o endereço de *e-mail* foi obtido no contexto da venda de produto ou serviço[150], o fornecedor utilize este endereço para o envio de mensagens proporcionais referentes a produtos ou serviços "análogos". A segunda exceção é de ordem subjetiva e se encontra no art. 13(5), que prevê que a regra do *opt-in* não valerá para os e-mails enviados a pessoas jurídicas.

Nos Estados Unidos, uma forte tradição de marketing direto e a ampla disseminação do uso da Internet fez do *spam* um tema já tratado há anos, tanto em tentativas de auto-regulação como pelos próprios tribunais norte-americanos. Também merecem ser citadas as diversas leis estaduais em matéria do *spam*, que hoje já se contabilizam na maioria dos estados.

Em 2003 foi aprovada a primeira normativa federal de largo alcance sobre a matéria, o *CAN-SPAM Act*[151], normativa que prescreve um sistema de *opt-out* como padrão para o envio de mensagens comerciais não solicitadas, bem como fortalece o papel da *Federal Trade Commission* – FTC – como o ente com a função de combater o *spam* em um nível nacional.

Percebe-se, a uma primeira análise, a diferença entre um enfoque mais restritivo para o tratamento do *spam*, que é o da União Européia, e um outro, mais tolerante, que é o norte-americano. Ainda que funcionem como indutores de soluções, é necessário ressaltar que nenhum destes alcançou um grau absoluto de eficácia devido a diversos motivos, dos quais talvez o maior seja o alto grau de internacionalização da rede.

149 John Magee, "The law…", cit., p. 371.

150 Como "contexto da venda" hão de ser compreendidas somente as hipóteses nas quais houve efetivamente a venda de um produto ou serviço, sem compreender eventuais relacionamentos de caráter pré-contratual que não se desenvolveram ao ponto da efetiva venda. John Magee, "The law ...", cit., p. 372.

151 O acrônimo se refere a Controlling the Assault of Non-Sollicited Pornography and Marketing Act, codificado como 15 U.S.C. §770, que se auto-define como "An Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet". Esta norma foi aprovada pelo senado em 25/11/2003, pelo Congresso em 8/12/2003, assinada pelo presidente em 16/12/2003 e entrou m vigor em 1º de janeiro de 2004.

5.4. Perspectivas de combate ao spam

As primeiras soluções aventadas para o problema do *spam* se baseavam na aplicação de normas informais de conduta e políticas de utilização de sistemas informatizados para tentar coibir a utilização destes para o envio de *spam*. Estas iniciativas se materializavam em medidas como os referimentos à *netiquette*[152], a códigos de conduta elaborados por associações de usuários e entidades, técnicas ou não, além de outras que contavam com a participação direta de usuários da rede.

O recurso à legislação passou a ser considerado com maior seriedade a partir do momento no qual a regulação interna da rede não mais parecia fazer frente ao problema do *spam*. E, de início, constatou-se que as maiores dificuldades a serem enfrentadas neste âmbito não eram propriamente a qualificação e caracterização da atividade como ilícita, porém a busca de formas eficazes de reprimi-la[153].

As técnicas mais utilizadas como patamar legislativo para a regulação do *spam* consistem basicamente na adoção de um modelo de *opt-in* ou de *opt-out*. No modelo de *opt-in*, estipula-se que somente poderão ser enviadas mensagens de cunho comercial e promocional com o prévio consentimento do destinatário; ao invés, em um modelo de *opt-out*, não é necessário o consentimento prévio e uma mensagem deste mesmo teor poderia ser enviada, porém deve existir a possibilidade do destinatário optar por não receber mais mensagens promocionais ou comerciais se assim posteriormente o desejar – efetuando, portanto, um controle *a posteriori*.

É necessário lembrar que estas técnicas podem eventualmente ser aplicadas de maneira fracionada e mesmo combinadas. Como exemplo, note-se que o modelo de *opt-in* adotado na União européia não é absoluto, existindo exceções à regra que fazem com que o modelo seja, na prática, denominado de *soft opt-in*.

Em um sistema de *opt-out*, a comunicação comercial e promocional ocupa um maior espaço. No entanto, tais sistemas apresentam como conseqüência a necessidade da criação de listas de *opt-out*, sejam públicas ou privadas, na qual constem os *e-mails* daqueles que não desejam receber mensagens. Tais listas são, é forçoso notar, um risco em si próprias: como consistem em uma relação de *e-mail*s, muito provavelmente válidos e operantes, não é simples evitar que *spammers* inescrupulosos delas se

152 A netiquette é uma denominação para uma espécie de código de comportamento informal para a utilização não abusiva da Internet.

153 "... tracking down spammers in cyberspace is more difficult than finding legal theories under which to charge them". Diane Plunkett Latham, "Electronic commerce in the 21st century: Article, spam, remedies", in: 27 Wm. Mitchell Law Review 1649, (2001), p. 1651.

aproveitem para compor a sua própria lista de endereços[154]. Assim, uma *Do-Not-Email-List* (que seria o equivalente da *Do-Not-Call-List*[155], mantida pela FTC para regular as chamadas telefônicas automatizadas) que teoricamente pode ser um instrumento para reforçar um sistema de opt-out, represente um perigo provavelmente maior do que o benefício que ela possa criar.

Finalmente, as tentativas de implementar medidas técnicas para tentar impedir o *spam* datam igualmente dos primeiros momentos em que este foi percebido como um entrave às comunicações em rede.

Os filtros anti-spam são provavelmente a resposta tecnológica mais difundida. Estes filtros procuram automatizar o que é procedimento cotidiano para muitos usuários ao abrir sua caixa postal: a seleção visual dos *e-mail*s indesejados e sua eliminação. Ao realizar uma varredura nos *e-mail* em uma caixa postal, o filtro separa as mensagens que considera serem *spam* das demais. Estes *e-mail*s separados podem ser apagados ou, o que é mais recomendável, vistoriados ulteriormente pelo usuário.

O filtro pode estar localizado no servidor[156] ou no cliente de *e-mail*[157]. O processo[158] utilizado pelo filtro para classificar as mensagens como *spam* é determinante para sua eficiência. Malgrado sua comprovada utilidade para diminuir de forma notável o volume de *spam*, os filtros apresentam um sério problema em relação a sua confiabilidade em casos específicos. O fato de não conseguirem distinguir o *spam* das mensagens legítimas com eficácia absoluta os inviabilizam como uma solução completa para o problema.

Uma ilustração precisa deste problema é a possibilidade de que ocorram falsos positivos. O falso positivo se dá quando uma mensagem legítima é erroneamente considerada como *spam* pelo critério do filtro. Para que não ocorra a perda de mensagens legítimas devido aos falsos positivos, é necessário que a mensagem identificada pelo filtro como *spam* seja armazenada à parte, em uma espécie de "quarentena" ou

---

154 "... It might actually do more harm than good, because it would make an enormous list of valid e-mail addresses available to the entire world". Michael Fischer. "The right to spam? Regulating electronic junk mail", in: 23 Columbia Law Journal & Arts 363 (2000), pp. 411-412.

155 v. < https://www.donotcall.gov>.

156 Diversos servidores de e-mail dispoem de seus próprios filtros anti-spam, sejam sistemas de e-mail corporativo (que costumam ser bastante restritivos) como várias soluções comerciais e mesmo gratuitas que incluem interfaces de webmail, como o Gmail beta ou o Yahoo! Mail).

157 Praticamente todos os principais clientes de e-mail mais utilizados (Mozilla Mail, Outlook Express, Eudora, Pegasus e outros) possuem algum tipo de filtro anti-spam implementado.

158 Tais processos são baseados em métodos estatísticos para classificar documentos em categorias. Um dos processos mais utilizados na identificação do spam é o filtro Bayesian. v. Paul Graham, "A plan for spam", in: < http://www.paulgraham.com/spam.html>.

de "*e-mail* de segunda classe", que há de ser revisada visualmente pelo usuário mais cauteloso. Portanto, a rigor, a utilização de filtros não elimina a necessidade de conferência visual das mensagens recebidas e, ao aumentar a possibilidade que ela jamais seja lida pelo seu destinatário, diminui a eficiência do sistema de correio eletrônico como um todo e contribui para a erosão da confiança do usuário neste meio.

Além disso, ressalte-se que há uma espécie de corrida entre *spammers* e desenvolvedores de filtros que se assemelha àquela entre desenvolvedores de vírus de computadores e seus antagonistas, os fabricantes de software anti-vírus. À medida que os filtros evoluem, *spammers* buscam meios para ultrapassar as novas barreiras criadas - com o incentivo da boa margem de lucro garantida caso tenham sucesso. Para fechar o circuito, cabe aos desenvolvedores de filtros bloquear a nova técnica desenvolvida pelo *spammer*, em uma escalada cujos custos são forçosamente bancados pelos provedores de acesso, comerciantes e usuários da rede em geral[159].

Outro meio técnico é a autenticação do *e-mail*. Como autenticação de *e-mail* compreende-se um procedimento pelo qual um terceiro, para todos ou apenas alguns propósitos, verifica a identidade do remetente do *e-mail* perante o seu destinatário, assegurando sua proveniência e efetuando um controle *a priori* sobre o que será lido ou o que terá maior importância dentro do volume total de *e-mails* recebidos por este usuário. Este mencionado terceiro pode ser uma autoridade certificadora, nos moldes das que hoje existem para a gestão da assinatura digital na ICP-BR[160] e em outros países.

Com um mecanismo de autenticação generalizado na Internet, o resultado seria o caminho livre para as mensagens devidamente certificadas, cujos remetentes seriam facilmente identificados e, caso haja abusos, processados com o auxílio de uma devida legislação anti-*spam*. Mensagens não certificadas poderiam ser meramente excluídas do tráfego da rede ou relegadas a um grau inferior de importância.

Alguns pontos discutíveis de uma solução do gênero fazem referência ao fato que ela enfraquece a noção da liberdade e do princípio da eficácia em atingir o destinatário final – ambas responsáveis diretas pela rápida popularização do *e-mail*. Um sistema de autenticação, além de relegar à marginalidade o *e-mail* anônimo, à medida que estabelece distinções entre mensagens com diversas hierarquias, insere um custo que pode determinar diferentes níveis de acesso à rede - pois a gestão da certificação por terceiros, entidades que geralmente são também responsáveis pela identificação de seus clientes, impõe um custo extra para

159 Adam Mossoff. "Spam - Oy, what a niusance!", in: 19 Berkeley Technology Law Review 625 (2004), p. 633.

160 Infra-estrutura de chaves públicas brasileira <http://www.icpbrasil.gov.br/>.

o envio de *e-mail*. Em um arremedo de comparação, seria algo como se a todo remetente de uma carta convencional em uma agência dos Correios fosse solicitada a exibição da cédula de Identidade.

Outra solução de natureza técnica é a compilação de listas de servidores e o bloqueio seletivo do envio dos *e-mail*s que deles se originem. Estes servidores são os mais freqüentemente utilizados para o envio de *spam*, seja por possuírem *open relays*, por serem "tolerantes" em relação ao envio de *spam* ou por outros motivos[161]. Hoje, uma boa parcela dos serviços de *e-mail* se utilizam de ao menos uma destas listas, conhecidas como *blacklists*, disponíveis.

Um problema comum às *blacklists* é a restrição universal aplicada aos *e-mails* originários de um dado domínio (ou em casos extremos de um determinado país!), que impede igualmente aos legítimos usuários inscritos neste determinado domínio de se comunicar através de servidores que utilizam uma determinada *blacklist*. Assim, como ocorre com os filtros, deve-se ter em conta que a eficiência das *blacklists* é apenas parcial e que, em meio a sua utilização, mensagens legítimas podem se perder e também um considerável volume de *spam* pode ultrapassar esta barreira. A utilização cumulativa de sistemas de filtros e *blacklists* pode aumentar a eficiência, porém certamente irão manter ou mesmo potencializar estes mencionados problemas de fundo.

A compilação de uma *blacklist* pode ainda gerar problemas para seus autores como o pedido de ressarcimento pela inscrição de um determinado domínio, inserindo um custo que certamente pode inibir a disseminação e desenvolvimento desta técnica. Por fim, note-se que as *blacklists* são também eventualmente associadas à atentados contra a liberdade de expressão, por serem um dos meios técnicos utilizados por alguns sistemas de efetiva censura, como por exemplo aqueles estruturados pelos governos de Cuba e da República Popular da China[162].

Uma outra solução que pode ser mencionada são as *whitelist*, listas de servidores que desempenham o papel oposto ao das *blacklists*, isto é, contêm os servidores dos quais aceitam o envio de *e-mail*. A lógica do funcionamento da *whitelist* é inversa: a princípio, todos os *e-mail*s devem ser bloqueados exceto aqueles que têm origem nos servidores constantes na *whitelist*. Como se depreende da sua arquitetura, é um sistema muito mais restritivo e pouco compatível com uma arquitetura de rede aberta, cuja utilização encontra maior justificação somente em sistemas corporativos que podem (ou devem) prescindir de *e-mail*s vindos

161 Geralmente os mantenedores das blacklists são bastante explícitos em relação à sua política de inclusão de servidores. v. <http:///www.mail-abuse.org/rbl/usage.html>.

162 Conhecida jocosamente como the great firewall of China.

de fora de um determinado circuito. Por outro lado, sua utilização como um dos indícios para determinar o *score* de um determinado *e-mail* para efeitos de filtragem vem crescendo.

Além das medidas mencionadas, é necessário abrir um parêntesis para mencionar a importância que assumem as várias formas de ativismo anti-*spam*.

Um fenômeno que acompanhou o *spam* foi o surgimento de uma espécie de associacionismo ligado à luta anti-*spam*. Vários grupos de ativismo anti-*spam* foram criados em diversos países, como o CAUCE[163] nos Estados Unidos (e, na Europa, o Euro-CAUCE[164]), CAUBE[165] na Austrália, Junkbusters[166], Anti-spam-br[167] no Brasil. Algumas outras organizações, em sua proposta contra o *spam*, mantêm ferramentas para combatê-lo, como a *Spamhaus* ou a MAPS, entre outras, que mantém atualizadas *blacklists*, além de informações sobre provedores de acesso que toleram a propagação de *spam* através de seus servidores, de países nos quais a prática é mais crítica ou nos quais a legislação local é demasiadamente flexível[168], de indivíduos ou organizações que enviam *spam* em larga escala.

Considerada a situação peculiar do e-mail como ferramenta aberta de comunicação e permeável a uma prática perniciosa como o *spam,* verificamos que abordar este problema por meio do seu aspecto comercial e do sistema de *opt-in* é um passo na direção certa, porém, caso venha desacompanhado de outras medidas como a cooperação internacional, a perseguição de grupos organizados e a própria educação dos usuários da rede, pode ser apenas uma solução provisória que pouco ou nada muda o quadro geral da matéria.

A ampla tendência à adoção de legislação anti-*spam* nos últimos anos, a conscientização dos usuários da Internet e também o desenvolvimento dos diversos meios técnicos para identificar e bloquear o *spam* se, por um lado, não resolveram o problema e nem sequer diminuíram de forma significativa o volume de *spam*, por outro lado tornaram a tarefa de um spammer um tanto mais complexa e sofisticada. Naturalmente, a efusão de barreiras contra o *spam* exige maior qualificação do *spammer* para ultrapassá-las,

---

163 Coalition Against Unsolicites Commercial E-mail, <http://www.cauce.org>.

164 <www.euro.cauce.org>.

165 Coalition Against Bulk E-mail, <http://www.caube.org.au>

166 <http://www.junkbusters.com>.

167 <http:// http://www.antispam.br>

168 Note-se a respeito a incômoda observação da Spamhaus sobre a demasiada flexibilidade da legislação brasileira na área como um dos motivos para a proliferação da prática do spam no Brasil. <www.spamhaus.org>.

o que reflete na tendência de "concentração" na área, com o surgimento dos chamados "*spam kings*", que concentram o envio de *spam*.

Portanto, e conforme intuído por muitos dos que se ocupam do tema, o combate ao *spam* tem várias frentes, das quais a legislativa é somente uma delas. As diversas medidas – informais, técnicas e legislativas – apresentam cada qual sua importância particular dentro do que podemos apontar como as duas grandes linhas básicas de atuação necessárias. A primeira destas linhas é a repressão do *spam* no direito interno, por meio de consolidação de normas, de códigos de conduta e da ação de grupos de pressão para que a atividade seja regulada e delimitado um patamar de ilicitude – em especial através da consideração do problema à luz dos princípios de proteção de dados pessoais. A segunda linha parte da consideração do âmbito internacional do problema e baseia-se na cooperação internacional e intercâmbio de informações para que sejam identificados os sujeitos responsáveis pelo envio massificado de *spam*, com o fim de isolá-los e, com os meios disponíveis em cada caso, inviabilizar a sua atividade.

CONCLUSÃO

O ciberespaço, há não muito tempo atrás, era um espaço determinado, que nós visitávamos periodicamente, mergulhando nele a partir do nosso mundo físico. Hoje, o ciberespaço saltou para fora. Colonizou o físico.

William Gibson[169]

O consumo está destinado a mudar seu perfil com as novas tecnologias, mesmo em áreas e detalhes que vão muito além do que hoje entendemos como comércio eletrônico e seus problemas típicos. Estamos em uma fase na qual a experiência e técnicas de venda *online* comunicam-se para as práticas tradicionais, remodelando mercados e modificando a experiência possível do consumidor.

O comércio eletrônico, portanto, não é mais meramente uma alternativa para os canais tradicionais de consumo e para as formas usuais de relacionamento entre fornecedor e consumidor. As técnicas desenvolvidas no comércio eletrônico tendem a colonizar o comércio "tradicional", "físico", estabelecendo novos limites e fazendo com que sua própria gramática acabe por ser dominante em uma série crescente de situações.

Estas novas técnicas da economia da informação, antes de se projetarem para o consumo cotidiano, foram idealizadas e se desenvolveram em um ambiente que era, de certa forma, próprio, protegido contra influências externas e baseado no fluxo livre de informações como patamar técnico das aplicações e plataformas que se desenvolviam.

169 http://www.nytimes.com/2010/09/01/opinion/01gibson.html

Em um período no qual estas novas técnicas ainda estavam relegadas a situações específicas ou de nicho, é provável que esta cultura de grande liberalidade no tratamento de informações não proporcionasse maiores problemas. A utilização em grande escala destas técnicas, no entanto, aliada à enorme penetração da rede Internet e de diversas modalidades de comércio eletrônico, mudaram substancialmente esta equação e tornaram a informação um importante - senão o fundamental - elemento de uma nova economia.

A administração da liberdade dos fluxos de informação, que por vezes foi tomada por um ideal dos primórdios da Sociedade da Informação, demonstrou-se potencialmente delicada neste novo panorama. Novas e poderosas estruturas de poder passaram a se formar em torno do domínio e controle sobre a informação - e, em particular, sobre a informação pessoal, cujo tratamento interessa diretamente à pessoa, sua privacidade e liberdade.

A necessidade de uma regulação para os tratamentos de informação pessoal dos consumidores na Sociedade da Informação tem, portanto, este pano de fundo e representa justamente um momento de inflexão, no qual as idéias de liberdade absoluta e gratuidade no manuseio da informação pessoal cedem ante a evidências de que o domínio sobre a informação pode ser instrumentalizado para finalidades diversas. Por exemplo, reconheceu-se que há um valor agregado pelos consumidores a diversos produtos oferecidos "livre e gratuitamente", que é a sua informação pessoal.

A proteção de dados chega hoje a se projetar como um direito autônomo e que necessita de uma tutela ampla e genérica. A sua tutela possui fundamento constitucional e assume a feição de um direito fundamental, posto que se destina à proteção da pessoa perante interesses provindos de uma multiplicidade de fontes, sejam aquelas situadas na esfera privada como na pública.

Tanto o setor privado como o público possuem seus próprios motivos que justificam seu interesse em obter dados pessoais em grande volume, muitos dos quais já foram vislumbrados neste trabalho. Em ambos os setores, também podem ser identificados interesses na formação de uma esfera privada de cada indivíduo, na qual seus dados pessoais podem estar protegidos - o que torna qualquer formulação de políticas públicas a respeito uma tarefa bastante intrincada.

Para o setor privado, por exemplo, a promoção da privacidade e autodeterminação do consumidor é um importante instrumento para a consolidação da confiança e, efetivamente, diversas iniciativas inovadoras para proporcionar o aumento de controle do consumidor sobre suas próprias informações podem atingir alto grau de eficácia em setores cuja regulação é, no mínimo, incipiente. A proteção de dados para o setor

privado, porém, não é um objetivo senão um meio, e não se pode perder de vista que qualquer iniciativa de tutela da privacidade e dos dados pessoais de consumidores pelo setor privado está sempre limitada e condicionada pelo modelo de negócios de uma empresa que, em última análise, irá impor sua própria dinâmica.

Neste cenário, como imperativo para garantir a liberdade e privacidade dos consumidores tanto no ambiente digital como fora dele, conclui-se pela necessidade de um marco normativo que trata especificamente da proteção de dados pessoais.

Este marco normativo não deve encerrar-se nas questões atinentes ao consumo. Apesar de boa parte das questões referentes à utilização de dados pessoais ter relação direta ou indireta com uma relação de consumo, os direitos que um marco normativo do gênero visa a garantir extrapolam o universo da relação de consumo e relacionam-se à manutenção da liberdade e livre desenvolvimento da personalidade, garantidas as expectativas de privacidade. São garantias e valores a serem preservados de forma análoga, exista ou não a possibilidade de caracterizar-se uma relação de consumo.

Vista a necessidade de generalizar as garantias relacionadas à proteção de dados, é forçoso reconhecer também que uma ênfase exagerada no recurso a ferramentas e técnicas consumeristas para efetivar as garantias referentes à proteção de dados pessoais deve ser encarada com cautela. Elementos patrimonialistas que estão presentes nestas ferramentas podem induzir a uma comodificação e mercantilização dos dados pessoais, o que pode ser vislumbrado, por exemplo, nas várias modalidades e propostas de transações envolvendo dados pessoais em troca de vantagens para os consumidores. O reconhecimento da necessidade de preservação de um vínculo e do controle das informações pessoais por seus titulares deve ensejar o reconhecimento amplo, dentro do próprio direito do consumidor, do caráter personalíssimo destas informações e de que, em muitas hipóteses, é inadequado o seu tratamento por meio de instrumentos puramente negociais.

Observada ainda a amplitude das garantias relacionadas à proteção de dados pessoais, verifica-se que estas possuem um rico campo de aplicação dentro das relações de consumo. Rico e, também, mais amplo do que o ângulo pelo qual elas são tradicionalmente enfocadas, que é o da proteção dos dados de consumidores em bancos de dados de proteção ao crédito. Assim, verificamos que diversas questões relacionadas à privacidade e proteção de dados de consumidores não se enquadram nos moldes da tutela reservada pelo Código de Defesa do Consumidor aos dados pessoais constantes em bancos de dados de

proteção ao crédito, porém abrangem novas fronteiras como a da publicidade comportamental, da utilização de redes sociais e das novas modalidades de informes creditícios que tendem a se expandir.

Na publicidade comportamental, verificou-se a necessidade de, entre outros pontos, proporcionar maior transparência sobre as modalidades de coleta e utilização de dados pessoais para fins de envio de publicidade dirigida baseada em comportamento, que quase sempre se processa sem que o consumidor o saiba ou tenha uma noção clara das suas consequências, aumentando a informação do consumidor e considerando que o consentimento para que ele seja exposto a esta prática deve ser cuidadosamente determinado, livre, informado, continuado e elaborado a partir de padrões e práticas que garantam-lhe, efetivamente, liberdade e privacidade. Ainda, certas práticas particularmente intrusivas devem ser limitadas e consideradas abusivas. Verificado tanto o enorme potencial para a utilização abusiva de informações colhidas para análise comportamental como a prática em si desta modalidade publicitária, ambas não contempladas pelo estágio atual de reflexão da legislação e jurisprudência pátrias, configura-se como extremamente temeroso introduzir tais práticas sem uma necessária reflexão prévia. Esta reflexão deve contemplar a análise de modelos de tutela já implementados em países que trabalham com esta questão há mais tempo e a introdução de garantias de proteção da privacidade e dos dados pessoais e dos dados de navegação dos consumidores - ainda que aparentemente anônimos ou anonimizados.

No caso das redes sociais, verifica-se que o consumidor, ao utilizar-se de um serviço que, para ele, é gratuito, proporciona à rede social a consolidação de volumes imensos de dados pessoais sobre si que, segundo o modelo de negócios típico destas redes, serão explorados economicamente. Destacou-se uma crônica falta de transparência no fornecimento de informações claras sobre a utilização e consequências do tratamento dos dados pessoais de seus usuários, bem como a debilidade de muitos sistemas de controle de exposição dos dados pessoais, configurando-se uma situação de clara desvantagem para o consumidor que enseja tanto a aplicação das normas de proteção ao consumidor quanto de normas específicas destinadas à regulação da proteção de dados nas redes sociais.

Ainda, constatou-se que a elaboração dos mecanismos de proteção ao crédito no Brasil em torno da negativação de determinados consumidores não é a única alternativa em vista, dada a possibilidade da utilização de diversos outros dados indicativos para alimentar sistemas de análise creditícia. A utilização destes outros sistemas, ainda que escapem à sistemática atual do Código de Defesa do Consumidor, que autoriza específica e unicamente o tratamento da informação sobre o inadimplemento de dívidas pelo consumidor, constitui-se em uma tendência francamente observável em outros países. Sistemas alternativos

de *credit scoring*, no entanto, caso tornem-se viáveis perante um patamar jurídico vindouro, deverão contar, para que sejam legítimos, com instrumentos que proporcionem ao consumidor meios para evitar situações de abuso e discriminação, garantindo-lhe que os seus dados sejam tratados com transparência e lealdade e proporcionando-lhe efetivo controle sobre a sua utilização.

Afora as situações específicas que já se podem delinear em nosso cotidiano, retome-se o que afirmamos em torno da convergência dos chamados mundo físico e mundo digital, cujos limites serão sempre menos visíveis e cuja delimitação, provavelmente, tende a ser desnecessária em tantas hipóteses. De forma análoga, os próprios limites entre as hipóteses que mencionamos neste trabalho tendem a se tornarem tênues: por exemplo, as modernas técnicas de tratamento da informação pessoal sugerem a real possibilidade, por exemplo, de que em um futuro próximo, a própria navegação pela Internet e pelas redes sociais possa proporcionar substratos para a formação de um perfil comportamental de um indivíduo que poderá influir em sua análise de risco para fornecimento de crédito. Neste panorama, que aliás é bastante concreto, os temas do monitoramento da navegação pela Internet e a análise creditícia tornam-se, basicamente, um só.

Estes não são meros indícios, porém constatações a partir de uma realidade que, embora em rápida evolução, dá mostras concretas de seu potencial. Urge, neste momento, a consolidação de um marco normativo de proteção de dados pessoais hábil a propiciar respostas a situação, sejam de consumo ou não, que garantam ao cidadão a liberdade e controle sobre suas próprias informações pessoais.

Este marco normativo, para cumprir esta missão, deve estruturar-se em torno dos princípios de proteção de dados pessoais baseados nos *Fair Information Principles*, bem como deve se concretizar na forma de uma lei federal que procure dar força ao reconhecimento da proteção de dados pessoais como um direito fundamental. Ele deve também proporcionar um regime de proteção diferenciado, mais forte, para os dados sensíveis, bem como para os tratamento sensíveis de dados pessoais, reconhecendo que qualquer eventual exceção que permita o tratamento de dados sensíveis deve estar fundamentada em motivos relevantes, ressalvadas todas as garantias fundamentais em questão e caracterizada cabalmente a ausência de discriminação no tratamento específico destes dados.

É indispensável, por fim, para lograr os objetivos de uma normativa do gênero, a instituição de uma estrutura administrativa dedicada que zele pela aplicação da lei, na forma de uma autoridade independente de proteção de dados, vista a complexidade da matéria e a necessidade do fornecer respostas rápidas e eficazes aos problemas enfrentados pelos consumidores e cidadãos. A instituição de uma autoridade independente de proteção de dados é uma técnica utilizada em outras normativas que tratam da matéria, em

países que a reconheceram como indispensável. A autoridade proporciona, como principais vantagens, além da desobstrução do poder judiciário de um grande volume demandas específicas relacionadas à proteção de dados, um meio eficaz para realizar as fiscalizações necessárias, o fomento da auto-regulação e de códigos de boas condutas de acordo com os parâmetros legais, a orientação e educação do consumidor e cidadão e também do setor público e privado sobre os direitos protegidos pela lei e as suas formas específicas de defesa e atuação, entre diversas outras funções. E, ainda, a existência da autoridade se afigura como indispensável para a efetiva harmonização da normativa brasileira sobre proteção de dados com as de diversos outros países que também a utilizam, o que é uma condição para proporcionar uma proteção real ao cidadão e ao consumidor no plano internacional como igualmente para favorecer o livre fluxo de dados e as transações comerciais que envolvem tais dados, sempre no respeito às normas de proteção de dados e às garantias fundamentais de liberdade e privacidade.

BIBLIOGRAFIA

Adam Mossoff. "Spam - Oy, what a niusance!", in: 19 *Berkeley Technology Law* Review 625 (2004).

Adriano De Cupis. *I diritti della personalità*, Milano, Giuffrè, 1982.

Alan Westin. *Privacy and freedom*. New York: Atheneum, 1967.

Ana Paula Gambogi Carvalho. "O consumidor e o direito à autodeterminação informacional", in: *Revista de Direito do Consumidor*, n. 46, abril-junho 2003, pp. 77-119.

Antônio Herman de Vasconcelos e Benjamim *et ali*. "Código Brasileiro de Defesa do Consumidor. Comentado pelos autores do anteprojeto" 9ª ed., Rio de Janeiro: Forense Universitária, 2007.

Carlos Alberto da Mota Pinto, *Teoria geral do direito civil*. 3a ed. Coimbra: Ed. Coimbra, 1996.

Claudia Lima Marques. *Contratos no Código de Defesa do Consumidor.* 5ª ed., São Paulo: RT, 2005.

Claudio Allocchio. "Lo *spam*: 'bug' oppure... 'feature'?", in: *La rete contro lo spam, che cos'è, come combatterlo*. Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, pp. 8-15.

Colin Bennett. *Regulating privacy, Data protection and public policy in Europe and the United States.* Ithaca: Cornell University Press, 1992.

Cosimo Comella, "*Spam*, sicurezza e privacy tra soluzioni tecnologiche e intervento normativo", in: *La rete contro lo spam, che cos'è, come combatterlo*, Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, pp. 42-60.

Dalmo de Abreu Dallari. "O habeas data no sistema jurídico brasileiro", in: *Revista de la Faculdad de derecho de la Pontificia Universidad Católica del Peru*, n. 51, 1997, pp. 95-113.

Danah Boyd, "Big Data: Opportunities for Computational and Social Sciences", in: <http://www.zephoria.org/thoughts/archives/2010/04/17/big-data-opportunities-for-computational-and-social-sciences.html>.

Danah Boyd, Nicole Ellison. "Social Network Sites: Definition, History, and Scholarship". 2007. <http://www.guilford.edu/about_guilford/services_and_administration/library/libguide_images/boyd.pdf>.

Danièle Bourcier. "De l'intelligence artificielle à la *personne virtuelle*: émergence d'une entité juridique ?", in : *Droit et Société,* n. 49, 2001, p. 847-871.

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

David Brin. *The transparent society*. Massachusetts: Addison-Wesley, 1998.

David Lyon. "The roots of the information society idea"*,* in: *The media studies reader*. Tim O'Sullivan; Yvonne Jewkes. (editores). London: Arnold, 1998, pp. 384-402

David Post. "What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace", in: 52 *Stanford Law Review* 1439.

David Sorkin. "Technical and legal approaches to unsolicited eletronic mail". 35 *U.S.F. Law Review* 325 (2001).

Davide Messinetti. "Circolazione dei dati personali e dispositivi de regolazione dei poteri individuali", in: *Rivista Critica del Diritto Privato*, 1998, pp. 339-407.

Diane Plunkett Latham, "Electronic commerce in the 21st century: Article, spam, remedies", in: 27 *Wm. Mitchell Law Review* 1649, (2001).

E.U.A., *Records, computers and the rights of citizens.* Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973, disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>.

Ettore Giannantonio. "Dati personali" (verb.) in: *Enciclopedia del diritto.* Aggiornamento vol. VI, Milano: Giuffrè, 2002, pp. 351-358.

Giovanni Buttarelli, "La attività del Garante in materia di prevenzione dello *spam*", in: in: *La rete contro lo spam, che cos'è, come combatterlo*. Laura Abba e Giorgio Giunchi (coord.). Società Internet: Lucca, 2004, p. 21-32.

Gustavo Tepedino. "As relações de consumo e a nova teoria contratual", in: *Temas de direito civil*. Rio de Janeiro: Renovar, 1999, pp. 199-216.

Herbert Burkert. "Privacy – data protection. A German/European perspective", in: *Governance of Global Networks in the Light of Differing Local Values*. Christoph Engel; Kenneth Keller (eds.). Baden-Baden: Nomos, 2000, pp. 43-69.

James Rule; Lawrence Hunter. "Towards a property right in personal data", in: *Visions of privacy: Policy choices for the digital age*. Colin Bennett. Toronto: University of Toronto Press, 1999.

John Oliver. *Law and economics. An introduction*. George Allen & Urwin, 1979.

Jorge Luis Borges. "Funes el memorioso", in: *Artifícios*. Madrid: Alianza, 1995.

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

José Luis Piñar Mañas, "el derecho fundamental a la protección de datos personales (LOPD)", in: *Protección de datos de carácter personal en Iberoamérica.* José Luis Piñar Mañas (dir.). Valencia: Tirant Lo Blanch, 2005, pp. 19-36.

Joseph Sommer. "Against ciberlaw", in: *Berkeley Technology Law Journal*, 15:3, 2000, <www.law.berkeley.edu/journals/btlj/articles/vol15/sommer/sommer.html>.

Lawrence Lessig. *Code and other laws of cyberspace*. Basic Books: New York, 1999.

_____. *The future of ideas*. Vintage: New York, 2002.

Lee Loevinger. "Jurimetrics", in: *Minnesota Law Review,* 33/1949, p. 455-ss.

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

Luís Roberto Barroso. "A viagem redonda: *habeas data,* direitos constitucionais e provas ilícitas", in: *Habeas data.* Teresa Arruda Alvim Wambier (coord.). São Paulo, RT, 1998, pp. 202-221.

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

Marc Rotemberg. "What Larry doesn't get", in: *Stanford Technology Law Review,* 1/2001, <stlr.stanford.edu>

Maria Eduarda Gonçalves. *Direito da informação.* Coimbra: Almedina, 1995.

Martin Abrams. "Boxing and concepts of harm", in: *Privacy and Data Security Law Journal*, set. 2009, pp. 673-676.

Michael Fischer. "The right to *spam*? Regulating electronic junk mail", in: 23 *Columbia Law Journal & Arts* 363 (2000).

Norbert Wiener. *Cybernetics*. Cambridge: MIT Press, 1961.

Oscar Puccinelli. *El habeas data en Indoiberoamérica.* Bogotá: Temis, 1999.

Pierre Catala, "Ebauche d'une théorie juridique de l'information", in: *Informatica e Diritto*, ano IX, jan-apr. 1983, pp 15-31.

Pierre Lévy. *Qu'est-ce que le virtuel?* Paris: La Découverte, 1998.

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

Richard Turkington; Anita Allen. *Privacy law. Cases and materials.* St. Paul: West Group, 1999.

Roberto Pardolesi. "Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità", in: *Diritto alla riservatezza e circolazione dei dati personali*. Milano: Giuffrè, 2003, p. 1- 57.

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

Spiros Simitis. "From the market to the polis: The EU Directive on the protection of personal data", in: 80 *Iowa Law Review* 445.

Spiros Simitis. "Il contesto giuridico e politico della tutela della privacy", in: *Rivista Critica del Diritto Privato*, 1997, pp. 563-581.

Stefano Rodotà. *Repertorio di fine secolo.* Bari: Laterza, 1999.

_____. *Tecnologie e diritti,* Bologna: Il Mulino, 1995.

Tércio Sampaio Ferraz Jr. "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado", in: *Revista da Faculdade de Direito da Universidade de São Paulo*, vol. 88, 1993.

Ulrich Wuermeling. "Harmonization of European Union Privacy Law", in: 14 *John Marshall Journal of Computer & Information Law* 411 (1996).

Viktor Mayer-Schönberger: *Delete. The Virtue of Forgetting in the Digital Age*. Pinceton: Princeton University Press, 2009.

_____. "General development of data protection in Europe", in: *Technology and privacy: The new landscape*. Phillip Agre, Marc Rotenberg (orgs.). Cambridge: MIT Press, 1997, pp. 219-242.

Vittorio Frosini. "Towards information law", in: *Informatica e diritto*. vol. V, n. 2, 1995, p. 7-16.

_____. *Contributi ad un diritto dell'informazione*, Napoli: Liguori, 1991.

Yves Poullet. "Data Protection Legislation: What's at Stake for our Society and our Democracy?", in: *Computer Law & Security Review*, Vol. 25, Is. 3, 2009, pp. 211-226.

Departamento de Proteção
e Defesa do Consumidor

Secretaria de
Direito Econômico

Ministério
da Justiça

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA