PRIVACIDADE E TRANSPARÊNCIA NO ACESSO À INFORMAÇÃO PÚBLICA

Danilo Doneda[1]

RESUMO. O crescimento dos fluxos de informação faz com que esta assuma papel central na definição do modo de exercício das liberdades pessoais. É na liberdade de informação e na proteção de dados pessoais que ocorre a definição do perfil destas liberdades, principalmente através da proteção de dados pessoais e levando em conta as necessidades de transparência e de acesso à informação pública - uma harmonização que deve levar em conta a unidade do tratamento jurídico do tema da informação.
PALAVRAS CLAVE. 1. Privacidade; 2. Informação; 3. Acesso à informação pública; 4. liberdade de informação; 5. Habeas Data; 6. Sociedade da Informação.

ABSTRACT. Ever-increasing flow of data has made information itself become an essential issue when translating some of the fundamental individual freedoms in Information Society. Freedom of information and data protection must be linked to these freedoms and also be treated as two increasingly related fields, as

1 Professor de Direito Civil e Consultor da UNESCO/MCT. ddoneda@gmail.com.

they are related to an unique fundamental question - the uniformity of the issue of information to the Law.
KEYWORDS. 1. Privacy; 2. Information; 3. Access to public information; 4. Freedom of informations; 5. Habeas Data; 6. Information Society.

1. Introdução

Um dos pressupostos da Sociedade da Informação é a convergência e modelagem de uma consistente parcela das relações em torno do fluxo informacional. A ampla disponibilidade de meios para o tratamento da informação faz com que este fluxo informacional crie novas possibilidades de comunicação bem como modifique concretamente formas anteriormente constituídas desta comunicação.

Esta convergência não se dá de forma opaca - pelo contrário, ela deixa marca dos seus efeitos tanto sobre as comunicações em si como nas relações que ajuda a realizar e definir. Dito de outro modo, as possibilidades criadas pelas tecnologias da informação são fatores determinantes da própria natureza das comunicações e dos produtos e serviços que hoje são dela decorrentes.

A informação, seu perfil e suas possibilidades vão, portanto, moldar uma grande parcela das relações que mais diretamente afetam, hoje, a nossa vida cotidiana. demandando atenção especial do ordenamento jurídico para atualizar as garantias tradicionais da liberdade para que estas possam reproduzir neste plano, que poderíamos denominar de "informacional", as mesmas garantias e prerrogativas que seriam naturais em um ambiente não modelado pela informação.

A partir deste panorama geral, há duas garantias específicas referentes à informação que hoje dispõem de uma tradição já consolidada e que enfrentam novos desafios para a sua harmonização na Sociedade da Informação. Estas são as garantias do acesso à informação e a da proteção dos dados pessoais. Como a intensificação nos fluxos de informação provoca novas demandas fortes em relação à transparência e à privacidade, criando um foco de

tensão entre ambos, uma das soluções para estabelecer um balanceamento entre ambas é a abordagem desta problemática a partir das mudanças e nuances da categoria principal da qual ambas derivam - que é o problema da informação. O reconhecimento da unidade do problema da informação é, portanto, essencial para a correta disposição e resolução desta tensão.

2. Informação e liberdade

A noção de liberdade não se configura de forma idêntica em qualquer período ou ambiente. Tome-se, por exemplo, um célebre discurso proferido em 1819 por Benjamin Constant,[2] no qual este comparava a liberdade dos povos da antiguidade clássica com a liberdade dos modernos para concluir, em síntese, pela marcante diferença com que a liberdade era sentida e experimentada em ambos os casos. Para os antigos, a liberdade consistia basicamente na participação em decisões sobre o destino do próprio povo e de seu governo, sem que houvesse uma noção de esfera individual autônoma. Para os modernos, a liberdade acaba tendo conteúdo diverso: sem exercer o poder político de forma direta, porém através da instituição da democracia representativa, moldou-se a noção de liberdade à livre escolha individual e da autonomia pessoal, dentro das quais a tutela da propriedade privada e também de uma esfera privada pessoal era imprescindível.

Partindo da ilustração de Benjamin Constant e avançando de forma livre no tempo, não é possível reconhecer uma ruptura brusca entre a concepção moderna de liberdade e os valores presentes nas sociedades ocidentais contemporâneas. De uma forma geral, como exemplo, tanto o direito de propriedade como a proteção de uma esfera privada e, talvez principalmente, o desenvolvimento dos fluxos

2 Benjamin Constant. "De la liberté des anciens comparée à celle des moderne", in: *Oeuvres politiques de Benjamin Constant*. T. 2. Paris: Charpentier, 1874, pp. 258-287.

comerciais (outra consequência que o autor apontava como oriunda da concepção moderna de liberdade) apresentam-se com vigor em nosso ordenamento jurídico. O que não significa que não possamos notar uma sensível mudança na concepção de liberdade em nosso tempo, que não pode mais ser associada somente à predominância do poder individual, como na concepção liberal de Constant.

À parte uma análise de caráter política mais aprofundada, que não é objeto do presente estudo, ocorre também que as formas de exercício da liberdade sofisticaram-se e se tornaram muito mais complexas. Entre os motivos principais para isto, há que se destacar o desenvolvimento do comércio e a escalada da economia da informação, na qual bens imateriais assumem papel central como fator de desenvolvimento econômico e social.[3]

Não foi somente o aumento no fluxo de informações que influenciou esta mudança na concepção de liberdade. Com o tempo, institutos jurídicos que procuravam tutelar a liberdade típica dos modernos, como por exemplo a propriedade privada, o princípio da isonomia ou a liberdade contratual, foram absorvendo elementos capazes de garantir sua legitimidade em uma sociedade na qual tornou-se fundamental a preocupação com a igualdade material e não somente formal. Assim, valores como a equidade, a solidariedade social e a justiça distributiva passaram a ser estampados em institutos que antes eram apanágio de um liberalismo jurídico bastante forte. Daí se contam as limitações ao direito de propriedade, o dirigismo contratual e outras iniciativas que proporcionaram um novo perfil ao ordenamento jurídico, através, por exemplo, de normas de natureza cogente e protetiva.

A forma pela qual estas modalidades de liberdade são exercidas passou a ser cada vez mais dependente da informação.

---

3 O germe desta idéia, aliás, já se encontra no discurso de Benjamin Constant, para o qual o desenvolvimento do comércio e das liberdades pessoais só podia ocorrer com o aumento das comunicações entre as pessoas.

A liberdade de informação já era reconhecida como um direito fundamental em países ocidentais desde finais do século XVIII,[4] concebida como "a liberdade que protege um todo constituído pelo direito à ser informado, a formar a sua opinião com base nesta informação e a exprimir a sua opinião a outrem".[5] Desde suas primeiras formulações, a liberdade de informação se posicionou como uma especialização da liberdade de expressão, esta compreendendo a prerrogativa genérica de exprimir as próprias opiniões, idéias, informações e, assim, assumindo função essencial tanto como um direito fundamental quanto como ingrediente necessário ao correto equilíbrio político nas democracias representativas.

3. O problema jurídico da informação

A informação costuma ser referida como a "matéria-prima" das novas engrenagens econômicas e sociais desencadeadas na Sociedade da Informação. À parte a valoração que ela pode receber como bem jurídico e econômico, é necessária uma breve inclusão sobre suas próprias características e possibilidades.

A dificuldade em determinar as características da informação e, consequentemente, de enquadrar seus eventuais efeitos jurídicos, se demonstrou patente a partir do momento em que ela passou a exercer sua influência para além dos meios físicos que lhe garantiam uma forma concreta. Um dos autores que se defrontou diretamente com o problema, Norbert Wiener, marcou este desafio com um conhecido aforisma segundo o qual *information is information not matter or energy*[6] - ressaltando uma eventual estraneidade da informação em relação aos elementos do mundo físico, a matéria e a

4 Tal concepção properou a partir de John Stuart Mill, cf. *Ensaio sobre a liberdade*. São Paulo: Escala, 2007.

5 Maria Eduarda Gonçalves. *Direito da informação.* Coimbra: Almedina, 1994, p. 24.

6 Norbert Wiener. *Cybernetics.* Cambridge: The MIT Press, 1965 p. 132.

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 qual 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 delas faz. 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, temos que a garantia de que o seu fluxo para o homem e a partir do homem não seja viciado ou distorcido 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.

Verificamos a tendência do ordenamento delinear o tema da informação em torno de cortes como o da liberdade de informação,

do acesso à informação ou da proteção de informações. Cabe agora o questionamento sobre qual é, afinal, este objeto denominado informação.

O termo "informação" presta-se igualmente a sintetizar, em determinados contextos, a própria liberdade de informação como fundamento de uma imprensa livre, bem como o próprio direito à informação.[7] O direito à informação, conforme já aludido, constitui-se na primeira manifestação concreta do interesse do ordenamento jurídico pelo tema. Sua posição como direito fundamental hoje é bastante sólida, podendo ser mencionado neste sentido 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 ao homem luzes para interpretar de forma autônoma o mundo que lhe cerca, bem como para dele participar de forma ativa.

Porém, um perfil particularmente instigante da informação e que apresenta imensa importância para a sua relação com a liberdade contemporânea está ligada ao regime a ser aplicado ao tratamento de informações pessoais.

A informação pessoal apresenta uma ligação concreta com a pessoa, sendo uma informação referente a uma pessoa determinada ou determinável. Este gênero de informações torna-se constantemente mais disponível para uma miríade de utilizações, basicamente por conta da facilidade e baixo custo de sua coleta e armazenamento com os meios digitais hoje disponíveis. Podemos afirmar que, hoje, a informação deixa traços cada vez mais perceptíveis e difíceis de

---

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

cancelar, e que o seu armazenamento fácil e barato tornou-se em um incentivo econômico para que se mantenham informações antes mesmo de refletir sobre seu eventual uso.

A informação pessoal 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). Pierre Catala 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.*[8]

O Conselho Europeu, através da Convenção de Estrasburgo, de 1981, ofereceu uma definição que condiz com esta ordem conceitual. Para a Convenção, informação pessoal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação".[9] É explicito, portanto, o mecanismo pelo qual é

---

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

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

possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

4. Informações pessoais

A informação pessoal transformou-se na última e, hoje, provavelmente, na maior fronteira da tutela da privacidade.[10]

Esta guinada, que acabou por plasmar o próprio conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas poderiam ser a concepção de uma *informational privacy* nos Estados Unidos, cujo "núcleo duro" é composto pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Federal alemão[11] e a Diretiva 95/46/CE da União Européia (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), com todas suas as suas conseqüências.

Trata-se, portanto, de uma tendência à concentração das questões referentes à privacidade nas hipóteses que implicam no tratamento de dados pessoais, sugerindo fortemente que, por uma questão de eficácia jurídica, o ordenamento se preocupe imediatamente com a regulação do tratamento destes dados, visando a proteção mediata e completa do titular dos dados, que é a pessoa. Ressalte-se, no

---

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

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

entanto, que a proteção dos dados pessoais, durante seu desenvolvimento como matéria jurídica, manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo-lhe características próprias.

O seu desenvolvimento acarretou que, forçosamente, questões relacionadas à privacidade cada vez refletissem o fato de havia passado a ser a informação pessoal, com todas as suas características, que vinculava a sua tutela e redefinia seu campo de atuação e os remédios jurídicos cabíveis. Assim, a privacidade passou a se condicionar ainda mais à tecnologia, cujo desenvolvimento marcava indelevelmente as novas possibilidades de tratamento da informação.

A menção à tecnologia e à privacidade como bases para a definição da personalidade moderna não era de forma alguma uma novidade - aliás, o clássico artigo *The right to privacy,* de Warren e Brandeis, que ajudou a definir as feições atuais do direito à privacidade acaba por a vincular diretamente aos avanços tecnológicos já no ano de 1890.[12]

5. Privacidade e a proteção de dados pessoais

Esta forte ligação da privacidade com as informações pessoais influenciou, conforme ressaltado, as modalidades de tutela da privacidade, no que foi uma mudança quantitativa. Ao invés de um direito puramente individual, a privacidade assumiu também caráter coletivo - visto que o uso abusivo de dados pessoais pode se referir a grandes grupos de pessoas e não somente a indivíduos determinados. Ela também assumiu um forte caráter internacional, dada a facilidade dos dados pessoais superarem limites espaciais, incentivando a harmonização legislativa entre diversos países e

12 "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'." Samuel Warren, Louis Brandeis. "The right to privacy", 4 *Harvard Law Review* 193 (1890), pp. 19.

blocos comerciais. E, de uma forma geral, a privacidade tornou-se um componente ainda mais importante para a composição dos valores da liberdade e igualdade que o cidadão de um determinado país pode usufruir.

A informação - e esta é mais uma dificuldade derivada da sua natureza - depende do contexto. Em determinadas circunstâncias ou lugares, uma informação pessoal pode ser revelada sem consequências negativas. Em outros, não. Assim, desenvolveu-se a idéia de que seria necessário um critério para legitimar a utilização de informações pessoais por terceiros, critério este que recaiu sobre o consentimento do titular. Até hoje o consentimento é peça fundamental para que uma determinada informação pessoal tenha seu tratamento autorizado.

O critério do consentimento, porém, não basta, e isto se verificou logo no início das primeiras tentativas de legislar a respeito. O consentimento supõe o conhecimento do titular das informações sobre o tratamento destas, bem como sobre as suas consequências - algo que poucas pessoas têm. Para sanar este *defcit*, foram desenvolvidas as noções como a do direito de acesso às próprias informações pessoais e a transparência em relação à existência dos bancos de dados de informações pessoais e dos seus critérios básicos de funcionamento.

A íntima ligação que a proteção de dados começava a apresentar com a liberdade e a complexidade das situações que poderiam daí advir originaram um outro foco de preocupações, que era o tratamento de dados sensíveis.

A categoria dos dados sensíveis - que são, em suma, dados que revelam informações sobre uma pessoa que podem potencialmente dar origem à discriminação caso sejam conhecidos por terceiros - além de levar aos seus limites o nível de proteção concedido aos dados pessoais, constitui um ponto de análise valioso por possibilitar identificar a sensibilidade de um ordenamento aos problemas mais graves que envolvem a informação pessoal e as garantias fundamentais da pessoa, como a sua própria liberdade.

Isso se dá pelo fato que a tutela dos dados sensíveis não corresponde, como em outros casos, a uma espécie de extensão das prerrogativas típicas da privacidade aplicadas ao cenário do tratamento automatizado de dados pessoais. No caso dos dados sensíveis, mais do que a privacidade, estão em jogo outros aspectos da personalidade merecedores de tutela como a igualdade (consubstanciada na garantia de não-discriminação por meio dos dados sensíveis) e a própria liberdade (presente na garantia de uma ampla liberdade de ação independente de constrições aplicadas por terceiros a partir de considerações com base em informações sensíveis). A bem da verdade, a noção de que o controle sobre os próprios dados pessoais seja uma garantia da própria dignidade - sendo, decididamente, mais do que uma expansão ou atualização das antigas concepções sobre a privacidade - conta com um forte argumento a seu favor na observação da categoria dos dados sensíveis e das suas características estruturais.

A categoria dos dados sensíveis emergiu da prática de alguns ordenamentos e também de considerações de alguns dos pioneiros que trataram da matéria, ao verificaram a existência de certos dados cuja natureza intrínseca os tornassem mais inclinados a revelarem aspectos da personalidade capazes de submeter seu titular a um julgamento inoportuno por terceiros, diminuindo-lhe o campo de escolhas de vida e submetendo-a a modalidades de discriminação, preconceito e controle.[13] Para a identificação de quais seriam os

13 Mencione-se apenas como um exemplo de uma informação que tipicamente pode dar azo a posturas discriminatórias e restritivas da liberdade - por exemplo, os dados genéticos de uma pessoa, capazes de proporcionar um conhecimento probabilístico acurado sobre a eventualidade do desenvolvimento de determinadas patologias durante seu período de vida. Uma informação deste gênero pode ser de extremo interesse para seus potenciais empregadores, por exemplo, ou para seguradoras ou administradoras de planos de saúde que, de posse destas informações, poderiam adaptar o relacionamento que teriam com cada empregado ou cliente. Do ponto de vista destes sujeitos, a reação torna-se mais segura por diminuir o seu risco intrínseco; do ponto de vista da pessoa em si, cria-se o grande dilema de criar uma categoria de sujeitos que não possam conseguir emprego ou o possam somente sob más condições em vista de uma determinada configuração

dados que se prestassem a proporcionar tais efeitos, a Diretiva 95/46/CE, por exemplo, qualificou como sensíveis os "dados pessoais reveladores de origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, associação a sindicatos e o processamento de dados envolvendo a saúde ou a vida sexual".[14]

É verdade que, como é eventualmente lembrado, qualquer dado pessoal e não somente o dado sensível é passível de, em determinadas circunstâncias, dar origem à discriminação ou ao controle, diminuindo as liberdades de escolha de uma pessoa. Os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados não sensíveis - tanto é que os dados não sensíveis também merecem proteção, apenas em uma escala inferior. O motivo dos dados sensíveis merecerem uma proteção mais intensa é justamente uma consideração probabilística de que tais dados são mais afeitos a apresentarem problemas mais graves quando de sua má utilização - daí exatamente o fato de denominá-los como "sensíveis" em relação aos demais, enfatizando sua peculiaridade neste sentido.

Reconhecida a existência e as características destes dados sensíveis, restou às normativas que tratam do tema estabelecer as modalidades de proteção especialmente assinaladas a estes dados. Na União Européia, por exemplo, a Diretiva 95/46/CE estabeleceu um princípio de padrão e exceção pelo qual o processamento de dados

---

genética que os revela como menos aptos; ou então restringiria e até impediria o acesso desta mesma pessoa a um seguro pessoal ou a um plano de saúde que, por suas características genéticas, aumentaria o valor de seu seguro ou plano de saúde. A questão é relevante a ponto de que uma das poucas iniciativas relacionadas à proteção de dados pessoais que contam com boas chances de tornar-se lei federal nos Estados Unidos ser exatamente o chamado GINA - *Genetic Information Nondiscrimination Act* - aprovado pelo Senado no dia 24 de abril de 2008.

14 Art. 8.1 da Diretiva 95/46/CE. Na argentina, a Lei 25.326 sobre Proteção de dados pessoais inclui entre suas definições no ser. art. 2. os dados sensíveis como "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

sensíveis como padrão é proibido, porém permitiu um número limitado de hipóteses de exceção – em particular nos casos em que o processamento ocorreria no melhor interesse do titular dos dados.

Uma tutela diferenciada para os dados sensíveis pode ser verificada, por exemplo, na sistemática de sua atuação no direito italiano: neste ordenamento, para que os entes públicos possam realizar o tratamento de dados sensíveis, é necessária uma norma que o permita; já para que entes privados o façam é imprescindível, além do consentimento informado do titular do dado, uma autorização específica da Autoridade italiana de proteção de dados pessoais.[15] Tal autorização será dada após considerar, entre outros fatores, a proporcionalidade entre o objetivo a ser alcançado com o respectivo tratamento e o dano, real ou potencial, ao titular dos dados sensíveis. Em um quadro normativo deste gênero, como assinala Stefano Rodotà, revela-se fortemente a opção por uma tutela positiva da dignidade humana, baseada no artigo 1º da Carta de Direitos Fundamentais da União Européia, que exige que a dignidade humana deve ser "respeitada e protegida".[16]

Desta modalidade de tutela, podem ser extraídas algumas conclusões.

Primeira, que o paradigma da inviolabilidade da vida privada, enunciação clássica cujas variantes ressoam na legislação brasileira e de outros países, revela-se pouco realista ao se aplicar de forma absoluta aos fenômenos típicos de proteção de dados: conforme já examinado, existe efetivamente a possibilidade de penetrar em

---

15 "Os dados sensíveis somente podem ser tratados com o consentimento por escrito do seu titular e a prévia autorização do Garante, observando-se os pressupostos e os limites estabelecidos pelo presente Código, bem como pela lei e pelos regulamentos". trad. livre do art. 26,1 do *Codice in materia di protezione dei dati personali* (Decreto legislativo n. 196, de 30 de junho de 2003).

16 Assim estabelece a Carta de Direitos Fundamentais da União Européia (2000/C 364/01):
"Artigo 1º - Dignidade do ser humano
A dignidade do ser humano é inviolável. Deve ser respeitada e protegida."

determinados espaços privados, desde que observados certos requisitos como, por exemplo, o consentimento do interessado e uma fundamentação razoável e proporcional aos fins almejados.[17] A inviolabilidade, matizada com caráter absoluto e típica de um determinado período de maturação da categoria dos direitos da personalidade, não pode ser aplicada ao tratamento de dados pessoais como característica genérica, a não ser após uma relativização que, de fato, acaba por esvaziar seu próprio conteúdo e razão de ser. Também não é adequada pelo motivo das ferramentas típicas para o controle do fluxo de informações pessoais (e inclusive dos dados sensíveis) terem caráter mediador e dinâmico, servindo para a autodeterminação da esfera privada levando em conta as particularidades de cada situação, e não como meros escudos, como no paradigma anterior.[18]

Uma outra conclusão diz respeito aos valores tutelados através da proteção objetiva dos dados sensíveis, que já não são somente aqueles que podem ser reconduzidos à proteção da privacidade em um sentido "clássico". Note-se que a tutela extremamente forte prevista pelo legislador italiano situa-se acima de uma regra genérica segundo a qual a qualificação necessária para a colocação de uma informação pessoal em circulação é a obtenção do consentimento do titular desta informação. Aqui, o mero consentimento não basta e o fato de se requerer uma autorização de órgão público reflete

17 Tome-se, por exemplo, o caso de uma Igreja e a sua possibilidade de administrar um banco de dados no qual constem os nomes de seus paroquianos. A informação referente à fé religiosa é uma informação sensível, não obstante neste caso o seu tratamento é legítimo por ser a única forma de atingir o objetivo desejado e por ser proporcional ao fim almejado, por não implicar em qualquer discriminação às pessoas nele presentes. Caso semelhante se dá com os dados tratados no âmbito sanitário, como históricos clínicos ou prontuários: tais dados, se por um lado devem ser tratados com extrema parcimônia e dentro de limitações específicas por terceiros em geral, hão de ser tratados pelos profissionais da área médica sempre que estes deles os necessitem para atividades ligadas à terapia e diagnóstico do titular dos dados sensíveis.

18 Neste paradigma, a proibição absoluta do tratamento de dados sensíveis não é uma alternativa realista.

diretamente o fato que a norma procura garantir não somente a intimidade ou a autonomia do cidadão, porém a sua igualdade - componente essencial da dignidade humana que é posta em risco quando do tratamento de dados sensíveis.

O fator realmente relevante que faz com que a a lei estabeleça uma tutela mais forte para os dados sensíveis é o risco da classificação, de estigmatização do indivíduo por conta da divulgação de suas convicções pessoais mais íntimas. Tal proteção se afigura, ainda, como um dos "paradoxos da privacidade", conforme observa Stefano Rodotà, justamente porque o efeito da proteção específica destinada aos dados sensíveis não é somente ou especificamente o fortalecimento da esfera privada, senão a "garantia plena de sua esfera pública através do exercício incondicional dos direitos civis e políticos" - justamente através da atribuição de conotações fortemente privadas a tais informações com o objetivo de garantir a esfera pública.[19] Em outras palavras, a privacidade é fortalecida com o objetivo de assegurar uma ampla liberdade de ação na esfera pública - em um paradoxo emblemático do novo papel assumido pela privacidade na Sociedade da Informação.

O Habeas Data, além de simbolizar correntes doutrinárias que verificaram a necessidade de regular o fluxo de informações pessoais como medida necessária para a garantia da liberdade, é também o *nomen iuris* do instrumento moldado pelo legislador brasileiro para garantir o acesso e retificação de dados pessoais em poder de terceiros. O Habeas Data, no ordenamento jurídico brasileiro, é uma ação constitucional coma função de garantir ao cidadão o acesso a seus dados pessoais em poder de terceiros. Como instituto, foi previsto com primazia pela Constituição de 1988 e apresenta a peculiaridade de ter influído em outras legislações latino-americanas.

Esta sua inserção em outros ordenamentos latino-americanos não chega a surpreender. Afinal, fatores de ordem geopolítica parecem

19 Stefano Rodotà. *La vita e le regole*. Milano: Feltrinelli, 2007, pp.107-108.

ter contribuído decisivamente para isso. Um instituto do gênero tenha uma especial razão de ser em sociedades recém-saídas de regimes militares, como ocorria em diversos países latino-americanos na década de 1980, em cujas sociedades persistia o trauma pelo uso autoritário da informação.[20] Após o fim destes regimes, um instrumento para a requisição das informações pessoais em mãos do poder público era desejado e necessário, seja para a tutela dos direitos fundamentais envolvidos como também pelo seu importante papel na formação de uma cultura democrática. É este o breve arcabouço histórico da situação em que foi concebido o Habeas Data, para proporcionar ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados.[21]

A maior inspiração do nosso legislador não era uma eventual influência do pensamento jurídico europeu ou norte-americano, cuja experiência com a temática relativa à utilização da tecnologia para o processamento de dados pessoais já era desenvolvida. Podemos especular sobre um particularismo, entre cujas causas está o fato de que as conseqüências derivadas de tais tecnologias apresentam-se, de forma geral, defasadas e atenuadas na América Latina do que em países desenvolvidos. Também conta, decisivamente, a falta de um modelo bem estruturado e claro para servir como exemplo - na época, as experiências européias ainda desenvolviam-se isoladamente, cada qual com suas idiossincrasias.

---

20 A tal situação faz referência Luís Roberto Barroso: "Uma das distorções mais agudas do ciclo militar-autoritário no Brasil (...) foi o uso e, sobretudo, o abuso na utilização de informações que diferentes organismos armazenavam sobre pessoas. (...) Envolvendo-se na política ordinária, os órgãos de segurança mergulharam em terreno pantanoso de perseguições a adversários, operando freqüentemente nas fronteiras da marginalidade. A chamada *comunidade de informações* passou a constituir um poder paralelo e agressivo, que, por vezes, sobrepunha-se ao poder político institucional, valendo-se de meios ilícitos para fins condenáveis". 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. 211.

21 Bancos de dados de caráter público, conforme será discutido a seguir.

De todo modo, podemos identificar algumas importantes influências externas, sendo a maior delas provavelmente a das Constituições de dois países europeus também recém-saídos de períodos ditatoriais, Espanha[22] e Portugal.[23] Nelas, apresentam-se dispositivos destinados a afrontar os problemas da utilização da informática e, no caso da Constituição portuguesa, uma referência bastante explícita à proteção de dados pessoais.

Como antecedentes legislativos mais imediatos, note-se que, mesmo antes de 1988, as legislações estaduais do Rio de Janeiro e de São Paulo possuíam leis que dispunham sobre o direito de acesso e retificação de dados pessoais, além de apresentar elementos que até hoje não foram expressos em normativa federal, como o princípio da finalidade ou o consentimento informado.[24]

O instituto do Habeas Data foi introduzido pela Constituição brasileira de 1988, em seu artigo 5º, LXXII.[25] Seu caráter e seu

---

22 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"

23 A Constituição portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35º, no qual estabelece alguns parâmetros básicos para a proteção de dados pessoais.

24 Trata-se, no Rio de Janeiro, da Lei Estadual nº 824, de 28 de dezembro de 1984, originária de projeto do deputado Eduardo Chuahy, que "Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no Estado do Rio de Janeiro e dá outras providências"; e em São Paulo, da Lei Estadual nº. 5702, de 5 de junho de 1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa". Note-se que a lei paulista refere-se textualmente aos dados em arquivos da administração pública, "inclusive em fichários policiais", o que parece indicar qual seria a provável motivação da norma.

25 Cujo teor é: "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".

próprio *nomen iuris* são devidos à influência de José Afonso da Silva[26] e já estavam presentes no Projeto de Constituição elaborado pela Comissão Provisória de Estudos Constitucionais (conhecida como Comissão Afonso Arinos). A expressão *Habeas Data* foi pinçada por José Afonso da Silva, responsável por esta parte do projeto, da obra do espanhol Firmín Morales Prat.[27] No entanto, não é Morales Prat a quem se deve a expressão. Em 1981, Vittorio Frosini a utilizava com desenvoltura, após identificar uma "liberdade informática", ou seja, uma extensão da liberdade pessoal como exigência imposta pelo desenvolvimento tecnológico, alude à importância do Habeas Corpus para a liberdade pessoal e acrescenta que: "poder-se-ia dizer, com uma paráfrase de caráter metafórico, que na legislação dos Estados modernos é necessário hoje um *Habeas Data*, um reconhecimento do direito do cidadão de dispor dos próprios dados pessoais, assim como ele tem o direito de dispor livremente do próprio corpo".[28] E é tranqüilamente possível retroceder ainda mais: note-se que Stefano Rodotà, em 1973, fez menção ao direito de acesso como um *habeas scriptum* – que seria um sinônimo para o

---

26 Clèmerson Merlin Clève. "*Habeas data:* algumas notas de leitura", in: *Habeas data.* Teresa Arruda Alvim Wambier (coord.). São Paulo: RT, 1998, p. 75.

27 O *habeas mentem* seria, para Morales Prat, um aspecto da "*privacy* pessoal" que atualizaria garantias tradicionais, como a liberdade de domicílio, a presunção da inocência, o direito de defesa, além de outros, que não estariam abarcados pelo "caduco" Habeas Corpus face às situações criadas pelo desenvolvimento tecnológico. Já o *Habeas Data* seria parte de uma estratégia integrada para a "construção de um estatuto jurídico da intimidade" que, considerando uma manifestação da *privacy* como um "direito de controle da circulação de informações pessoais" projetada sobre os bancos de dados, se traduziria em um direito de acesso a estes dados, acompanhado de faculdades em controlar seu conteúdo. Nas palavras do autor, se trata de "que o sujeito possa *modular* sua 'identidade informática' para que lhe seja fiel". Firmín Morales Prat. *La tutela penal de la intimidad; "Privacy", e informática*. Barcelona: Destino, 1984, pp. 30-43. A expressão *habeas mentem* tinha sido antes utilizada por Stefano Rodotà, em: "Progresso técnico e problemi istituzionali nella gestione delle informazioni", in: *Privacy e banche dati.* Nicola Matteucci (cur.). Bologna: Il Mulino, 1981, p. 131.

28 v. Vittorio Frosini. "La protezione della riservatezza nella società informatica", in*: Informatica e Diritto.* fascículo 1°, janeiro-abril, 1981, pp. 9-10.

Habeas Data.[29] Aquelas que parecem as menções absolutamente mais remotas do termo "Habeas Data" remetem, finalmente, ao ano de 1970: mencione-se o artigo de Steven Weber publicado na *University of San Francisco Law Review* intitulado *Habeas Data: The right of privacy versus computer surveillance*,[30] bem como a declaração prestada pelo professor Alan Westin à revista *National Geographic*, na qual afirma, após mencionar a função que exerceu o Habeas Corpus na época em que foi criado, que:

> *Talvez precisemos hoje de uma espécie de ação de 'Habeas Data' – que obrigue tanto o governo como corporações privadas a revelar as informações que eles coletaram e que estão utilizando para realizar julgamentos sobre um indivíduo, e a justificar o porquê de faze-lo.*[31]

O Habeas Data, como já intuía Westin, apresenta paralelos com o Habeas Corpus. Tal paralelismo justifica-se pela intenção de se aproveitar da carga semântica que a expressão acumulou, e serve para sua introdução como instrumento de garantia individual. A origem do Habeas Corpus é inglesa, mais especificamente a *common law* do alto medievo. Sua evolução posterior foi marcada pela edição de vários *Habeas Corpus Act*[32]- a começar pelo primeiro e mais freqüentemente mencionado, de 1679. Blackstone referiu-se ao

---

29 Rodotà considerava este *habeas scriptum* uma garantia circunscrita a aspectos puramente defensivos da disciplina dos dados pessoais, inábil a formar a sua base. Stefano Rodotà. *Elaboratori elettronici e controllo sociale*. Bologna: Il Mulino, 1973, p. 121.

30 5 *U.S.F. Law Review* 358, pp. 358-377 (1970).

31 Peter White, "Behold the computer revolution", in: *National Geographic*. vol. 138, novembro de 1970, p. 631.

32 O instituto evoluiu de uma possibilidade de petição direta ao soberano, que era mais uma possibilidade deste controlar a administração da justiça, para tornar-se uma garantia do cidadão perante os tribunais do Reino Unido. Para registro, a expressão utilizada, *habeas corpus ad subiiciendum*, é a abreviação de uma antiga fórmula processual do *common law*: "Praecipimus tibi quod 'corpus' x, in custodia vestra detentum, ut dictur, una cum causa captionis et detentionis suae, quocumque nomine idem x, censeatur in eadem, 'habeas' coram nobis apud Westminster, 'ad subiiciendum'et recipiendum ea quae cúria nostra de eo ordinari continget hac parte". Paolo Biscaretti de Ruffia. "Habeas corpus" (verb.) in: *Enciclopedia del diritto.* v. XIX, Milano: Giuffrè, 1970, pp. 941-945.

Habeas Corpus como *the great and efficacious writ*[33]- e esta sua importância o acompanhou quando transportado para os Estados Unidos, assim como para outros países, mesmo os de tradição de *civil law*.

O Habeas Data, tal qual o Habeas Corpus, é um instituto de caráter remedial, como o *writ of mandmus* (EUA) ou o *amparo* (Espanha e diversos países da América Latina). No direito brasileiro, é uma das ações constitucionais que fazem parte de um conjunto de instrumentos para a garantia de direitos individuais e coletivos. Esta sua posição no ordenamento deve ser entendida no âmbito de uma reação, que se deu no momento em que a sociedade e o próprio ordenamento se recompunham de um período no qual diversas liberdades individuais foram suprimidas. Neste contexto, o Habeas Data foi uma das medidas destinadas a sanar um "déficit" de liberdades individuais, bem como de consolidar as bases democráticas do novo sistema e dificultar uma volta a um regime ditatorial.[34]

Afora a forte conotação política que acompanhou o instituto no Brasil, hoje merece ênfase o enfoque do Habeas Data à luz das suas concepções originárias, como as de Westin e Frosini, que enfatizavam seu caráter de garantidor de uma nova liberdade, no sentido informacional. O Habeas Corpus é uma garantia para a liberdade no sentido físico - no que protege à locomoção do próprio corpo. Não abrange, porém, as emanações informacionais deste corpo, que se concretizam justamente no fluxo de dados pessoais cujas consequências, independentemente de considerações quanto ao espaço e à liberdade dita "física", são capazes hoje de influenciar decididamente na esfera de liberdade do cidadão.

Assim, ganha vigor a imagem que contrapõe simbolicamente a liberdade do corpo físico, tutelada pelo Habeas Corpus, àquela do

---

33 William Blackstone. *Commentaries on the law of England*, v. III, Oxford: Clarendon Press, 1765-1769, p. 121.

34 J. M. Othon Sidou. *As garantias ativas dos direitos coletivos*. 3ª. ed., Rio de Janeiro: Forense, 1989, p. 452.

novo corpo eletrônico, formado pelo conjunto disseminado de informações sobre uma pessoa em mãos de terceiros e cuja tutela é tarefa do Habeas Data - não no sentido estrito da ação constitucional do direito brasileiro, mas de uma enunciação da liberdade informática. A autonomia em relação aos próprios dados pessoais torna-se um elemento fundador de uma nova enunciação da liberdade contemporânea - como exprimiu Stefano Rodotà, ao notar que "A civilização moderna nasceu com o *Habeas Corpus*; a cidadania eletrônica exige um *Habeas Data.*"[35]

6. Perfil normativo da proteção de dados pessoais

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

A primeira destas quatro gerações de leis era composta por normas que refletiam o estado da tecnologia e a visão do jurista à época,

35 Stefano Rodotà. *A vida na Sociedade da Vigilância. A privacidade hoje.* Danilo Doneda e Luciana Cabral Doneda (trad.). Rio de Janeiro: Renovar, 2008, p. 162.

pretendendo regular um cenário no qual centros elaboradores 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. 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. Esta primeira geração de leis vai aproximadamente até a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de seu uso indiscriminado sem conhecer 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, além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados. 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.

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, rígido e detalhado. 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 *Loi Informatique et Libertées*, além da já mencionada *Bundesdatenschutzgesetz*. A

característica básica que diferencia tais leis das anteriores é que sua estrutura não gira mais em torno do fenômeno computacional em si, mas da consideração da privacidade e da proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da lei francesa).

Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses. Além disso, o controle, nos moldes das leis anteriores, tornou-se inviável, dada a fragmentação dos centros de tratamento dos dados pessoais. Assim, foi criado um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela.

Estas leis apresentavam igualmente seus problemas, o que motivou uma subseqüente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado 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 relevante 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.

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

Entre as técnicas utilizadas, 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 que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual pela dificuldade de se tenha uma real noção dos efeitos decorrentes do tratamento de dados – 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 do 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 Diretiva 95/46/CE e a Diretiva 2000/58/CE.

As aludidas gerações de leis sobre proteção de dados pessoais fazem referência, não por acaso, a uma linguagem própria da informática e exprime a lógica da busca por modelos jurídicos mais ricos e completos.[36] Não obstante uma mudança de perfil da proteção de dados com os anos, é possível reagrupar materialmente os seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em diversos ordenamentos – no que podemos verificar uma forte manifestação da 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 sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais.

Destes princípios, alguns se encontram já presentes nas leis de primeira e segunda geração, tendo sido desenvolvidos pelas leis posteriores. Uma busca mais larga poderá, porém, traçar suas origens em uma serie 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.[37]

---

36 Stefano Rodotà. *Repertorio di fine secolo.* Bari: Laterza, 1999, p. 103.

37 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 discussõos sobre a ameaça potencial que representaria às liberdade individuais, o governo norte-americano desistiu do projeto. 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, pois se o *National Data Center* em si não vingou, a realidade era que muitos outros bancos de dados pessoais de menor âmbito iam se estruturando. Uma das áreas na qual esta discussão ecoou com maior força foi a da saúde, pela justificada preocupação com o tratamento de dados médicos por sistemas informatizados. No início da década de 1970, a *Secretary for health, education and welfare*, nos Estados Unidos, reuniu um comissão de especialistas que divulgou, em 1973, estudo que conclui pela relação direta entre a privacidade e os tratamentos de dados pessoais, além de da necessidade de estabelecer a regra do controle sobre as próprias informações:

> *A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais for a 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.*[38]

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

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

---

38 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 corrigir ou retificar um registro de informações a seu respeito.*
> *- Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve toar as devidas precauções para evitar o mau uso destes dados".*[39]

Tais regras, de caráter marcantemente procedimental, 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*. Este "núcleo comum" encontrou expressão como um conjunto de princípios a serem aplicados na proteção de dados pessoais principalmente com a Convenção de Estrasburgo e nas *Guidelines* da OCDE,[40] no início da década de oitenta. É possível elaborar uma síntese destes princípios:[41]

1 - Princípio da transparência (ou da publicidade), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para funcionar, da notificação à uma autoridade sobre sua existência; ou do envio de relatórios periódicos. Igualmente, as modalidades de utilização das informações pessoais devem ser divulgadas.

---

39 idem.

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

41 cf. Stefano Rodotà. *Repertorio di fine secolo,* cit. p. 62; José Adércio L. Sampaio. *Direito à intimidade e à vida privada*. Belo Horizonte: Del Rey, 1999, pp. 509 - ss; Manoel J. Pereira dos Santos. "Princípios para a formação de um regime de proteção de dados pessoais", in: *Direito & Internet. Vol. II*. Newton De Lucca, Adalberto Simão Filho (coord.). Quartier Latin, São Paulo, 2008, pp. 355-376.

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

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 tem acesso ao banco de dados onde suas informações estão armazenadas, podendo obter cópias destes registros, com a conseqüente possibilidade de controle destes dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.

5 - Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. Entre os riscos mencionados estão os riscos de acesso físico direto ao sistema tanto como o de acesso remoto (ou lógico).

6 - Princípio da proporcionalidade, pelo qual dados pessoais somente podem ser tratados se forem relevantes e pertinentes em relação à finalidade para o qual foram coletados, evitando sua utilização excessiva. Em algumas legislações, este princípio é reforçado pelo princípio da necessidade, pelo qual somente podem ser utilizados dados pessoais caso a finalidade almejada não possa ser atingida de outro modo.

Estes princípios, ainda que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais,

formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência à autonomia da proteção de dados pessoais e a sua consideração como um direito fundamental em diversos ordenamentos. É possível considerar a Convenção de Estrasburgo 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. Posteriormente, também transparece com clareza a presença dos direitos fundamentais na Diretiva 95/46/CE sobre proteção de dados pessoais na União Européia. Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais".

O documento europeu que levou mais adiante 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 Estrasburgo, na Diretiva 95/46/CE e no artigo 286º do tratado instituidor da União Européia. 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.

7. Conclusão

A necessidade de tratar da informação como um bem jurídico fez com que o ordenamento jurídico se visse às voltas com a necessidade de adaptar e também de criar institutos para este aumento da importância da informação - as mais recentes evoluções em matéria de direito autoral podem ser um exemplo das adaptações em curso, bem como o surgimento de uma disciplina de proteção de dados pessoais é um exemplo da formulação *ex novo* de uma disciplina.

Ocorre que a informação e, em especial, a informação pessoal, possui características específicas que, ao mesmo tempo que que a fazem um objeto peculiar, acabam por criar similitudes entre as diversas ocasiões em que a informação é tratada pelo ordenamento jurídico. Deste modo, identificamos um forte argumento para um tratamento unitário do tema da informação nas diversas ocasiões em que o ordenamento trata de questões que dizem respeito diretamente a ela.

O tratamento unitário da informação é decorrência direta da sua recente importância e também de suas características naturais de transmissibilidade e imaterialidade, que facilita seu tráfego e, consequentemente, a sua utilização em diversas situações distintas.

Além de seu tratamento unitário, é necessário que o tratamento reservado à informação leve em conta sempre as implicações da utilização desta para as próprias liberdades pessoais, que, na Sociedade da Informação, estruturam-se cada vez mais em torno dos vetores do livre acesso à informação e também da liberdade do indivíduo quanto às decisões sobre a veiculação e utilização de suas informações pessoais. A regulação jurídica da informação defronta-se, portanto, com a delicada tarefa de regular tanto as amplas possibilidades de acesso à informação como os casos em que este acesso deve ser restrito, no caso em que se tratem de informações pessoais.

Por complexo que seja, este desafio somente pode ser levado a cabo com sucesso ao partir-se da análise do problema atual da informação de forma integrada, considerando-a em relação às suas

características e aos efeitos de sua utilização para depois, com a consciência de que o acesso e a proteção da informação são faces da mesma moeda, elaborar normativas compatíveis e complementares em tema de acesso à informação e a proteção de dados pessoais.

Tal técnica não é propriamente uma novidade recente. Pode não ter sido mero acaso o fato do primeiro país a possuir uma lei nacional de proteção de dados pessoais, a Suécia,[42] ter sido também o primeiro país a ter elaborado normas sobre o acesso à documentos e à informação pública.[43] Nos Estados Unidos, a edição de uma lei de proteção de dados para o setor público Federal, o *Fair Credit Reporting Act (*FCRA, de 1974), seguiu o *Freedom of Information Act* (FOIA, de 1966). A tendência a se tratar das duas esferas concomitantemente ou, ao menos, harmonicamente, é a tônica em diversos países.

No caso brasileiro, dada a ausência de normativa específica a respeito de proteção de dados pessoais bem como de uma norma que regule de forma ampla o acesso à informação pública, há de se notar que o projeto de lei 219/2003, que trata justamente do acesso à informação pública (que, no momento da finalização deste ensaio, encontrava-se aprovado pela Câmara dos deputados e aguardando os trâmites legislativos posteriores) contém previsão específica em relação à proteção de dados pessoais em seu art. 31.[44] O referido artigo, que

---

42 *Datalag*, de 1973.

43 O ordenamento jurídico sueco conta com uma lei de liberdade de imprensa (denominada *Tryckfrihetsförordningen*) desde o longínquo ano de 1766. Tal lei, além de impedir a prática da censura prévia, garante a toda pessoa o direito de obter de qualquer órgão público informações constantes de documentos oficiais, instituindo o princípio da publicidade (*Offentlighetsprincipen*) para a informação pública.

44 O referido artigo prevê em sua redação atual (junho de 2010):
"Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§1o As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de cem anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

estabelece um regime de proteção específico para as informações pessoais (ao lado daquelas sigilosas), que somente poderiam ser objeto de tratamento mediante o consentimento de seu titular ou em situações específicas, faz prova da aludida necessidade de afrontar de forma unitária os problemas referentes ao acesso à informação bem como o da proteção de informações pessoais.

A ausência de regulamentação específica sobre proteção de dados pessoais no Brasil faz com que, neste e em outros diplomas normativos, seja necessário estabelecer referências e instrumentos de proteção particulares aos dados pessoais, sem a possibilidade de recorrer a um estatuto geral sobre o tema e sempre correndo-se o risco de estabelecer um patamar de proteção fraco ou em contradição com outras disposições similares.

No caso do Projeto de Lei 219/2003, o tratamento de informações pessoais é um motivo de restrição à faculdade de acesso ao documento público. Esta regra reconhece uma primazia da tutela da informação pessoal em relação ao mandamento da transparência,

---

II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. trata este artigo será responsabilizado por seu uso indevido.
§2o Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
§3o O consentimento referido no inciso II do §1o não será exigido quando as informações forem necessárias:
I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III – ao cumprimento de ordem judicial;
IV – à defesa de direitos humanos; ou
IV – à proteção do interesse público e geral preponderante.
§4o A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como ações voltadas para a recuperação de fatos históricos de maior relevância.
§5o Regulamento disporá sobre os procedimentos para tratamento de informação pessoal."

que somente não será observada quando a divulgação da informação for legitimada pelo consentimento expresso do titular dos dados ou em uma das hipóteses em *numerus clausus* nas quais este consentimento é dispensável.

Ao incorporar a regra do consentimento expresso,o Projeto de Lei deu um largo passo ao encontro de uma efetiva tutela da informação pessoal e da efetiva liberdade e privacidade dos cidadãos.

O Projeto, talvez conscientemente, não adentrou em maiores detalhes as diversas circunstâncias em que o mero consentimento do titular dos dados pode não ser suficiente para tutelar direitos pessoais e de terceiros (caso de dados sensíveis), nem em outras situações de consentimento tácito ou não-específico em que a divulgação de dados pessoais é realizada de forma sistemática (pense-se em várias formas de divulgação de informações jurisdicionais ou na divulgação de salários e gastos com funcionários públicos, por exemplo).

É provavelmente pela complexidade do tema, que escapa à alçada de um diploma normativo cujo tema específico é o acesso à informação, que o parágrafo 5º do referido artigo acaba por aludir a que "Regulamento disporá sobre os procedimentos para tratamento de informação pessoal". E aí está presente um defeito relativamente grave do Projeto de Lei: reconhecer o tratamento das informações pessoais e a proteção de dados como um apêndice que possa ser tratado pela via regulamentar. Salta aos olhos, assim, a abordagem desproporcional ao problema da informação, visto que a emergência de uma normativa de acesso à informação não foi acompanhada de idêntico esforço no sentido de estabelecer regras para a proteção de dados pessoais.

Um tratamento unitário do informação pelo ordenamento jurídico brasileiro, portanto, faz-se necessário como pressuposto para a garantia das liberdades individuais na Sociedade da Informação, bem como para que os fluxos de informação tornem-se mais seguros e viáveis com a sua legitimação. Das duas modalidades principais de regulação, quais sejam, o acesso à informação e a proteção de dados pessoais, a primeira delas apresenta grau maior de maturidade em

nosso ordenamento, enquanto com relação à última são pertinentes maiores preocupações dado a ausência de previsões normativas específicas sobre diversos de seus aspectos fundamentais. Em relação a este ponto, note-se que o crescente anacronismo do ordenamento jurídico brasileiro corre o risco de aumentar ainda mais caso não se atente para o desenvolvimento de uma série de padrões internacionais em tema de proteção de dados, como por exemplo o modelo europeu da Diretiva 95/46/CE de fato acaba por ser, como o *Privacy framework* da APEC (no espaço Ásia-Pacífico) procura se tornar ou como algumas iniciativas como a redação de uma resolução para a identificação de padrões globais para a proteção da privacidade e de dados pessoais foi recentemente aprovada na Conferência Internacional de Comissários de Privacidade em Estrasburgo.[45]

Referências

BARROSO, Luís Roberto. "A viagem redonda: Habeas Data, direitos constitucionais e provas ilícitas", in: Habeas Data. Teresa Arruda Alvim Wambier (coord.). São Paulo: RT, 1998.

BLACKSTONE, William. Commentaries on the law of England, v. III, Oxford: Clarendon Press, 1765-1769.

BISCARETTI DE RUFFIA, Paolo. "Habeas corpus" (verb.) in: Enciclopedia del diritto. v. XIX, Milano: Giuffrè, 1970, pp. 941-945.

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

CONSTANT, Benjamin. "De la liberté des anciens comparée à celle des moderne", in: Oeuvres politiques de Benjamin Constant. T. 2. Paris: Charpentier, 1874.

CLÈVE, Clèmerson Merlin. "Habeas data: algumas notas de leitura", in: Habeas data. Teresa Arruda Alvim Wambier (coord.). São Paulo: RT, 1998.

45 <http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf>.

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

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>.

FROSINI, Vittorio. "La protezione della riservatezza nella società informatica", in: Informatica e Diritto. fascículo 1°, janeiro-abril, 1981.

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

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

GONÇALVES, Maria Eduarda. Direito da informação. Coimbra: Almedina, 1994.

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

MORALES PRAT, Firmín. La tutela penal de la intimidad; "Privacy", e informática. Barcelona: Destino, 1984.

OTHON SIDOU, J. M. As garantias ativas dos direitos coletivos. 3ª. ed., Rio de Janeiro: Forense, 1989.

PEREIRA DOS SANTOS, Manoel J. "Princípios para a formação de um regime de proteção de dados pessoais", in: Direito & Internet. Vol. II. Newton De Lucca, Adalberto Simão Filho (coord.). Quartier Latin, São Paulo, 2008.

RODOTÀ, Stefano. "Progresso técnico e problemi istituzionali nella gestione delle informazioni", in: Privacy e banche dati. Nicola Matteucci (cur.). Bologna: Il Mulino, 1981.

— A vida na Sociedade da Vigilância. A privacidade hoje. Danilo Doneda e Luciana Cabral Doneda (trad.). Rio de Janeiro: Renovar, 2008.

— Elaboratori elettronici e controllo sociale. Bologna: Il Mulino, 1973.

— La vita e le regole. Milano: Feltrinelli, 2007.

— Repertorio di fine secolo. Bari: Laterza, 1999.

SAMPAIO, José Adércio. Direito à intimidade e à vida privada. Belo Horizonte: Del Rey, 1999, pp. 509.

STUART MILL, John. Ensaio sobre a liberdade. São Paulo: Escala, 2007.

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

WARREN, Samuel, Louis BRANDEIS. "The right to privacy", 4 Harvard Law Review 193 (1890).

WEBER, Steven. "Habeas Data: The right of privacy versus computer surveillance", in: 5 U.S.F. Law Review 358, pp. 358-377 (1970).

WHITE, Peter, "Behold the computer revolution", in: National Geographic. vol. 138, novembro de 1970.

WIENER, Norbert. Cybernetics. Cambridge: The MIT Press, 1965 p. 132.

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