Revista Brasileira de
Risco e Seguro

Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro†

Danilo Doneda
Mestre e Doutor em Direito Civil pela Universidade do Estado do Rio de Janeiro. Foi pesquisador visitante no *Garante per la protezione dei dati personali* da Itália. Atualmente é professor de Direito Civil em diversas universidades e advogado
danilo@doneda.net

Mario Viola
Mestre em Direito Civil e Especialista em Direito do Consumidor pela Universidade do Estado do Rio de Janeiro, Especialista em Direito Privado pela Universidade Federal Fluminense, *Master of Research* e doutorando em Direito pelo Instituto Universitário Europeu, em Florença na Itália. É procurador (licenciado) do Município de Saquarema no Rio de Janeiro e funcionário (licenciado) da CNSeg
m.viola@ig.com.br

Resumo

A utilização de dados pessoais se tornou ferramenta fundamental para o desenvolvimento de diversas atividades, sejam elas de natureza pública ou privada.

Nos setores que trabalham com o risco como fator essencial, como o securitário e o financeiro, a análise desse risco se dá justamente a partir das informações coletadas a respeito dos potenciais clientes. Com base em tal análise, seguradoras e instituições financeiras classificam seus potenciais clientes em categorias previamente estabelecidas, fixando prêmios e taxas de juros de acordo com cada situação ou rejeitando o risco, quando for o caso.

Entretanto, a coleta de informações não pode se dar de forma indiscriminada, devendo observar alguns parâmetros, sendo certo que o principal deles refere-se ao princípio da finalidade.

O presente artigo busca definir os contornos desse "princípio da finalidade" para a análise de risco, seja o risco relacionado à possibilidade de ocorrência do sinistro, no caso da atividade securitária, ou aquele referente à possibilidade de não-pagamento das obrigações contratadas, no caso da financeira, tomando por base não só as normas nacionais que tratam da proteção de dados e da privacidade, mas também a interpretação dada pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça à matéria.

Palavras-Chave

análise de risco; informação; finalidade; proteção de dados.

Sumário

† Artigo recebido em 12/9/2009. Aprovado em 20/9/2009.

Abstract

Risk and personal information: the principle of finality and data protection in the Brazilian Legal System

Danilo Doneda
Masters Degree and PhD in Civil Law from the Universidade do Estado do Rio de Janeiro. He was a visiting researcher at *Garante per la protezione dei dati personali* in Italy. He is currently a professor of Civil Law at several universities as well as being a lawyer.
danilo@doneda.net

Mario Viola
Masters Degree in Civil Law and Specialist in Consumer Law by the Universidade do Estado do Rio de Janeiro, Specialist in Private Law from the Universidade Federal Fluminense, Masters Degree in Research and currently attending Doctorate in law at the European University Institute in Florence, Italy. He is attorney general (in license period) for the city of Saquarema, in the State of Rio de Janeiro and employee (on leave) at CNSeg
m.viola@ig.com.br

Summary

The use of personal data has become a fundamental tool for the development of various activities from the public and private domain.

In industries that work with the risk as a key factor, such as insurance and financial, the analysis of this risk is made possible precisely through the data collected on potential customers. Based on this analysis, insurance companies and financial institutions classify their potential customers into predetermined categories, setting premiums and interest rates according to each situation or, when it is the case, rejecting the risk.

However, the collection of data cannot happen indiscriminately for some parameters must be observed, the main one being the principle of finality.

This article seeks to define the outline of the "principle of finality" for the risk analysis, either the risk related to the possibility of occurrence of a loss in the case of the insurance activity, or concerning the possibility of default over contractual obligations, in the case of financial activity, based not only on national standards that deals with data protection and privacy, but also on the interpretation given by the *Supremo Tribunal Federal* (Supreme Court) and the *Superior Tribunal de Justiça* (Superior Court) on the subject.

Key Words

risk analysis; information; finality; data protection.

Contents

Sinopsis

Riesgo e información personal: el principio de la finalidad y la protección de los datos en el ordenamiento brasileño

Danilo Doneda
Máster y Doctor en Derecho Civil por la Universidad Estatal de Río de Janeiro. Fue investigador visitante en el *Garante per la protezione dei dati personali* de Italia. Actualmente es profesor de derecho civil en diversas universidades y es abogado.
danilo@doneda.net

Mario Viola
Máster en Derecho Civil y Especialista en Derecho del Consumidor por la Universidad Estatal de Río de Janeiro, especialista en Derecho Privado por la Universidad Federal Fluminense, Máster en Investigación (*Master of Research)* y doctorando en Derecho por el Instituto Universitario Europeo, en Florencia, Italia. Es procurador (en licencia) de la ciudad de Saquarema, en el estado de Río de Janeiro y ejecutivo (en licencia) de la CNSeg.
m.viola@ig.com.br

Resumen

El uso de los datos personales se ha convertido en una herramienta fundamental para el desarrollo de diversas actividades, ya sean públicas o privadas.

En los sectores que trabajan con el de riesgo como factor clave, tales como el de seguros y el financiero, el análisis de este riesgo se produce precisamente a partir de los datos recogidos sobre los clientes potenciales. Basándose en este análisis, las compañías de seguros e instituciones financieras clasifican a sus clientes potenciales en categorías predeterminadas, fijando las primas y las tasas de interés de acuerdo a cada situación o rechazando el riesgo, cuando fuera el caso.

Sin embargo, la recopilación de la información no puede darse de forma indiscriminada, sino que deben ser observados algunos parámetros, teniendo en cuenta que el principal se refiere al principio de la finalidad.

Este artículo busca definir los contornos de ese "principio de la finalidad" para el análisis de riesgo, sea el riesgo relacionado con la posibilidad de la ocurrencia del siniestro, en el caso de la actividad de los seguros, o el que se refiere a la posibilidad de incumplimiento de pago de las obligaciones contractuales, en el caso de la actividad financiera, basándose no sólo en las normas nacionales en materia de protección de datos y privacidad, sino también en la interpretación dada por el Supremo Tribunal Federal y por el Superior Tribunal de Justicia sobre el tema.

Palabras-Clave

análisis de risco; información; finalidad; protección de datos.

Sumario

1. Introdução

O tratamento automatizado de informações pessoais suscitou o desenvolvimento de institutos jurídicos que procurassem oferecer meios efetivos de tutela da privacidade e garantir o direito à autodeterminação de cada pessoa em relação às próprias informações pessoais. Dentre esses institutos, o princípio da finalidade destaca-se por estar presente em diversas legislações que tratam do assunto e por sua capacidade de colher aspectos dos diversos interesses conflitantes na disciplina da proteção de dados. Uma melhor compreensão do perfil e das possibilidades desse princípio possibilita uma maior adequação da proteção de dados às situações reais que esta pretende regular.

O princípio da finalidade é um dos princípios que se desenvolveram com o surgimento de normativas destinadas à tutela dos dados pessoais. Em uma síntese inicial, podemos associar esse princípio à necessidade de uma informação pessoal, após ser coletada, somente poder ser utilizada para a finalidade que justificou a sua coleta, garantindo a toda pessoa que seus dados serão utilizados somente para os fins que ela autorizou no momento da coleta dos dados.

O efetivo posicionamento desse princípio dentro de um sistema de proteção de dados, no entanto, deve ser analisado após definirmos em que consiste a proteção de dados e qual sua real função no ordenamento jurídico. O processamento automatizado de informações tornou-se um elemento essencial em diversas atividades nas últimas décadas. Tanto a iniciativa privada como o Estado defrontam-se com a necessidade de intensificar o processamento de informações para atender, respectivamente, a mercados cada vez maiores ou para aumentar a eficiência da administração pública.

A automatização do processamento de informações passou a ser indispensável frente às crescentes demandas de uma sociedade massificada, ao ponto que, hoje, em várias circunstâncias, seria impensável abrir mão desse novo recurso.[1] A tecnologia aplicada ao tratamento de informações, por outro lado, faz crescer o risco de invasão da privacidade e do controle sobre os indivíduos, através do uso abusivo de suas informações pessoais, o que incentivou o surgimento de institutos jurídicos capazes de contrabalançar essa tendência e proporcionar ao cidadão o controle sobre seus próprios dados pessoais.

Institutos dessa natureza desenvolveram-se com vigor nas últimas décadas. Sem entrar nos detalhes de um complexo desenvolvimento legislativo, pode-se afirmar que suas feições têm raízes nos princípios de proteção de dados pessoais que começaram a ser esboçados no

[1] Para ilustrar a imprescindibilidade dos meios automatizados de processamento de dados, vale a menção a uma experiência também ligada ao setor automotivo: em 1970, o *New York Department of Motor Vehicles* administrava informações referentes a 8,3 milhões de condutores e 7,2 milhões de veículos (incluindo dados sobre o licenciamento, seguros e multas), em uma estrutura de arquivação manual que se demonstrava inviável para fazer frente ao acréscimo anual de 5% a 6% na frota nova-iorquina. Antes da informatização do serviço, o licenciamento de um automóvel novo chegava a demorar meses. Westin; Baker, 1972, p. 66-70.

início da década de 1970. Esses princípios, aos quais se costuma fazer referência como sendo *Fair Information Principles*,[2] arraigaram-se em diversas legislações sobre proteção de dados e formam a espinha dorsal dos primeiros documentos internacionais de maior alçada sobre o tema, a Convenção 108 do Conselho da Europa[3] e as Linhas-guia da OCDE,[4] ambos do início da década de 1980.

Estes princípios, em extrema síntese, são (RODOTÀ, 1999. p. 62; SAMPAIO, 1997, p. 509): (i) o princípio da publicidade (ou transparência), pelo qual a existência de um banco de dados pessoais deve ser de conhecimento público; (ii) o princípio da exatidão, pelo qual os dados pessoais devem corresponder à realidade e ser atualizados; (iii) o princípio da finalidade, pelo qual os dados pessoais devem ser utilizados para fins compatíveis com o motivo que fundamentou a sua coleta; (iv) o princípio do livre acesso, pelo qual o titular do dado pessoal tem o direito de conhecê-lo e, se for o caso, retificá-lo; e (v) o princípio da segurança física e lógica, pelo qual os dados pessoais devem ser protegidos do acesso não autorizado, tanto fisicamente (pelo acesso físico ao sistema informático) como logicamente (pelo acesso telemático ao sistema). Esses princípios, ao lado de outros, podem ser identificados, em graduações diversas, nas várias legislações que hoje se ocupam do tema.

O recente desenvolvimento legislativo sobre o tema é pautado pela necessidade de equilibrar interesses que gravitam entre dois polos: de um lado, a proteção do indivíduo e da sua privacidade na Sociedade da Informação e, de outro, a necessidade de estabelecer um patamar de licitude para que os vários serviços que fazem uso de dados pessoais possam operar com maior eficácia, respeitados os direitos individuais.

---

[2] Nos Estados Unidos, a *Secretary for health, education and welfare* realizou um estudo bastante influente na área, que concluiu pela relação direta entre a privacidade e os tratamentos de dados pessoais, além da necessidade de estabelecer a regra do controle individual sobre as próprias informações. Esse controle seria efetivado através de garantias como as de que:
"– 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 elas são utilizadas.
– 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 desses dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso desses dados." Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.

[3] Convenção 108 do Conselho da Europa – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.

[4] *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. Acesso em 20.12.2008.

Essa necessidade de equilíbrio entre a tutela do indivíduo e o livre uso de dados pessoais é uma das tônicas da disciplina. Ela está presente, por exemplo, no caráter essencialmente remedial da tutela dos dados pessoais no ordenamento jurídico norte-americano, que reconhece um espaço livre para a utilização desses dados (DONEDA, 2006, p. 261-306); ou em outro marco regulatório, a legislação comunitária europeia sobre o tema, na qual essa dicotomia encontra-se presente de forma cristalina.

Na União Europeia, a tutela dos dados pessoais tem seu marco fundamental na própria Carta dos Direitos Fundamentais da União Europeia, que faz referência ao direito fundamental de proteção de dados pessoais: "Art. 8º 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito."[5]

Ao mesmo tempo, as Diretivas europeias[6] que tratam do tema o fazem estabelecendo demarcações precisas entre o interesse do indivíduo na proteção de seus dados e a existência de um patamar legítimo e concreto de utilização desses dados por terceiros para fins lícitos. Não é meramente simbólico o fato de a Diretiva 46/95/CE intitular-se como uma "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", visto que a livre circulação dos dados pessoais foi um dos imperativos para a consolidação do mercado comum europeu, um dos objetivos maiores do direito comunitário.[7] Esse equilíbrio se manifesta, por exemplo, no *considerando nº 3* da referida Diretiva, ao reconhecer que "(…) a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exige não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas."

---

[5] O artigo ainda prevê, na sua sequência:
"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 em lei. Todas as pessoas têm o direito de aceder aos dados coligados que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento dessas regras fica sujeito a fiscalização por parte de uma autoridade independente."

[6] Que são: a Diretiva 46/95/CE, "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados"; e a Diretiva 2002/58/CE, "relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)" e relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE .

[7] Note-se que o livre fluxo de dados e mesmo a consideração das informações pessoais como bens a serem regulados pela economia de mercado eram tradicionalmente defendidos pela Comissão Europeia, que somente passou a harmonizar essa perspectiva após reconhecer que as legislações e orientações jurisprudenciais de vários países europeus apontavam para a necessidade de uma tutela forte para os dados pessoais. Spiros Simitis. "From the Market To the Polis: The EU Directive on the Protection of Personal Data". In: 80 *Iowa L. Review* 445 (1995), pp. 446-447.

A utilidade dos dados pessoais é patente em diversas atividades, tanto no setor privado quanto no público, que se valem de informações pessoais para operar com maior eficiência. Tome-se, por exemplo, atividades que trabalham com o risco como fator essencial, como por exemplo a securitária ou a financeira. Ambas se utilizam da análise do risco, seja o risco relacionado à possibilidade de ocorrência do sinistro, no caso da atividade securitária, seja aquele referente à possibilidade de não-pagamento das obrigações contratadas, no caso da financeira. A partir dessa análise, seguradoras e instituições financeiras classificam seus potenciais clientes em categorias previamente estabelecidas, fixando prêmios e taxas de juros de acordo com cada situação ou rejeitando o risco, quando for o caso (CUNHA, 2009, p. 22).

Para realizar essa análise, as respectivas atividades se valem de informações acerca do potencial cliente, relativas a seus hábitos, finanças e saúde, entre outras, procurando, tanto quanto possível, reduzir as possibilidades de celebrar um contrato com elevado risco, seja de ocorrência do sinistro ou de inadimplência, através de mecanismos que enquadrem o referido contrato em uma determinada probabilidade estatística (MEYER, 2004, p. 29).[8]

As informações sobre potenciais clientes estão presentes em bases de dados já existentes (eg. cadastros de proteção ao crédito) ou são obtidas através de informações prestadas pelo cliente (eg. preenchimento de questionário de avaliação de risco, proposta de financiamento de veículo). Na análise de uma proposta, seguradoras e instituições financeiras têm por norma consultar as bases de dados às quais têm acesso, tanto próprias como de terceiros, para confirmar a veracidade dos dados informados e obter outras informações que julguem importantes para a correta análise do risco.

Essa utilização de dados pessoais pode tornar a atividade empresarial mais segura e previsível, tornando-a, ao mesmo tempo, mais atrativa para os próprios consumidores, pela possibilidade de manter o custo do produto em um patamar menor após a diminuição do risco potencial de inadimplemento (ou de ocorrência do sinistro) – daí a relevância social da utilização de informações pessoais. Por outro lado, o risco da utilização abusiva destas informações, com prejuízo para seu titular, sugere a adoção de medidas restritivas em relação aos tratamentos possíveis de dados pessoais. Verificada a necessidade de regular este sensível equilíbrio, cuidar-se-á a seguir das normas que proporcionam a tutela dos dados pessoais no ordenamento brasileiro.

[8] *"Risk classification assures that premiums are financially prudent or adequate to enable the insurer to meet its contractual obligations to its policy holders. It allows the insurer to determine premiums that are appropriate to levels of risk. The more underwriting information available to the insurer, the more precise it can be in determining appropriate premiums. This protects both insurer and policy holders from the insurer becoming insolvent due to inadequate premiums."*

2. A proteção de dados no ordenamento jurídico brasileiro

O Brasil, ao contrário do que ocorre em outros países (mesmo países vizinhos, como Argentina e Uruguai),[9] não possui uma norma geral que trate da proteção de dados pessoais,[10] apresentando apenas provisões constitucionais de caráter geral e algumas normas setoriais sobre a proteção de dados.

A Constituição da República reconhece, em seu Art. 5º, inciso X, a vida privada, a intimidade, a honra e a imagem como direitos fundamentais. O mesmo Artigo, em seus incisos XI, XII e XIV, garante proteção a outros aspectos da privacidade.[11] Além disso, o inciso LXXII do mesmo Art. 5º prevê um novo remédio constitucional no que toca à proteção de dados pessoais, que é a ação de *habeas data* (BESSA, 2003. p. 107).

No mesmo sentido, o Código Civil incluiu, em seu Artigo 21, o direito à privacidade no rol de direitos da personalidade.

Entretanto, a única norma que trata especificamente da proteção de dados, exceção feita à norma que regulamenta a ação de *habeas data*,[12] é o Código de Proteção e Defesa do Consumidor que, em seus Artigos 43 e 44, regula a manutenção de bancos de dados e cadastros de consumidores, estabelecendo uma série de garantias para estes últimos.[13] Nele é perceptível, ainda que timidamente, a influência das normas mais modernas relacionadas à proteção de dados pessoais, com referência a alguns dos princípios de proteção de dados anteriormente citados (CARVALHO, 2003, pp. 77-119).

---

[9] Na Argentina existe a Lei 25.326, e no Uruguai foi recentemente promulgada a Lei 18.331, uma norma de proteção de dados similar à argentina.

[10] Nesse sentido são as palavras de Maria Celina Bodin de Moraes, na introdução à versão em Português da obra de Stefano Rodotà (*A vida na sociedade da vigilância – Privacidade Hoje*. Rio de Janeiro: Renovar, 2008, p. 12): *"A escolha brasileira, porém, ainda não está feita. Espera-se que o idêntico respeito à dignidade humana, consagrado no Art. 1º, III, de nossa Constituição, bem como a tradição civilista que nosso sistema encerra, aliados à chamada globalização através dos direitos, permita a aproximação ao modelo europeu, através de uma legislação por princípios."*

[11] *"XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;*
XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;"

[12] A ação de *habeas data* foi regulada pela Lei 9.507, de 12 de novembro de 1997.

[13] A Lei Complementar 105, de 10 de Janeiro de 2001, que dispõe sobre o sigilo das operações de instituições financeiras, traz, em seu artigo 1º, §3º, algumas regras que também têm repercussão na proteção de dados pessoais.

A primeira das garantias a esse respeito é o direito do consumidor de ser comunicado[14] de que a informação sobre ele está sendo processada (Artigo 43, §2º). Essa comunicação deve ser feita antes que o dado seja efetivamente utilizado,[15/16] com o intuito de possibilitar ao consumidor o exercício dos demais direitos conferidos pelo CDC, sendo reconhecida em jurisprudência a possibilidade de indenização por dano material e moral no caso da ausência ou intempestividade dessa comunicação.[17] Basta, porém, que o gestor da base de dados comprove que enviou a notificação ao consumidor sobre a inclusão de seu dado no cadastro ou base de dados, não sendo necessária a prova de que o consumidor recebeu tal comunicado.[18]

Os outros direitos do consumidor estabelecidos pelo CDC no que toca à proteção de seus dados pessoais são os direitos de acesso (BENJAMIN *et al.*, 2007, p. 413) e de retificação (BENJAMIN *et al.*, 2007, p 416), que possibilitam a ele consultar toda e qualquer informação pessoal a seu respeito armazenada "em cadastros, fichas, registros e dados pessoais e de consumo arquivados" e, no caso de encontrar alguma incorreção, solicitar a retificação do dado (Artigo 43, caput e §3º). Na hipótese de lhe ser negado o exercício de tais direitos, o consumidor poderá se valer dos procedimentos judiciais ordinários (Artigo 43, § 4º) ou da já citada ação de *habeas data*.[19]

---

[14] Apesar de o Código estabelecer responsabilidade solidária entre o administrador do cadastro ou base de dados e o fornecedor de bens ou serviços que solicitou a inclusão do dado no que toca à notificação do consumidor, o Superior Tribunal de Justiça pacificou entendimento, através da Súmula 359, de que *"cabe ao órgão mantenedor do Cadastro de Proteção ao Crédito a notificação do devedor antes de proceder à inscrição".*

[15] Não há no Código de Defesa do Consumidor qualquer menção a respeito do momento em que a comunicação deve ser feita, entretanto, doutrina e jurisprudência entendem que a notificação deve ser realizada em momento anterior à efetiva inserção da informação em base de dados para utilização, a fim de que o consumidor tenha tempo suficiente de exercer seus direitos no que toca ao armazenamento de seus dados pessoais.

[16] No Rio de Janeiro, a Lei Estadual 3.244/99 estabelece o período de dez dias anteriores à efetiva inserção da informação em base de dados para utilização como um período razoável. Disponível em http://www.alerj.rj.gov.br/processo2.htm. Acesso em 20.12.2008.

[17] 1. É ilegal a inscrição de nome de devedor nos serviços de proteção ao crédito sem a notificação prévia exigida pelo Art. 43, § 2º, do Código de Defesa do Consumidor. 2. Incabível, entretanto, o pagamento de indenização a título de dano moral quando o devedor, ciente da dívida, tem o seu nome inscrito em órgãos de proteção ao crédito. 3. Recurso especial provido parcialmente. (REsp 1010881/RS, Rel. Ministro João Otávio de Noronha, 4ª T., j. 26/08/2008, DJe 08/09/2008). Disponível em: http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=ausencia+e+notificacao+e+cadastro+e+dano+e+moral&&b=ACOR&p=true&t=&l=10&i=1#. Acesso em 20.12.2008.

[18] Processual Civil – Agravo Regimental em Agravo de Instrumento – Recurso Especial obstado em 2º grau – Código de Defesa do Consumidor, Art. 43, § 2º – Caracterização de notificação por escrito do consumidor, no endereço fornecido pelo credor – inexistência de obrigação legal do órgão de proteção ao crédito em notificar por meio de aviso de recebimento – precedentes – recurso improvido. (AgRg no Ag 963.026/RJ, Rel. Min. Massami Uyeda, 3ª T., j. 15/05/2008, DJe 06/06/2008). Disponível em: http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=notificacao+e+consumidor+e+protecao+e+credito&&b=ACOR&p=true&t=&l=10&i=3#. Acesso em 20.12.2008.

[19] A ação de *habeas data* foi regulada pela Lei 9.507, de 12 Novembro de 1997. Disponível em http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm. Acesso em 20.12.2008.

Além disso, o Artigo 43, em seus §§ 1º e 5º, estabelece que qualquer informação negativa a respeito do consumidor que restrinja o acesso ao crédito por parte deste não seja armazenada por mais de cinco anos.[20] Aqui, mais uma vez, poderá o consumidor fazer uso das vias judiciais para fazer valer seu direito e pleitear indenização, tanto por danos materiais quanto morais, caso o gestor do cadastro ou base de dados descumpra tal dever.

3. As modalidades de tratamento de dados pessoais

Há uma série de procedimentos referentes à utilização de dados pessoais, como, por exemplo, a coleta, a organização, a consulta, a interconexão, o bloqueio, a transmissão, a difusão e a destruição, dentre outros.[21] Todos esses constituem modalidades de tratamento dos dados pessoais.[22]

Em linhas gerais, qualquer operação que tenha como objeto dados pessoais qualifica-se como tratamento e, como tal, deve ser avaliada em conformidade com as regras e princípios de proteção a esses dados. Há, no entanto, particularidades em relação a cada tratamento, geralmente relacionadas à forma com que cada um deles efetivamente opera.

Pelo ordenamento brasileiro, a compilação de um banco de dados com informações pessoais não é sujeita, *a priori*, a uma eventual autorização ou mesmo notificação, muito embora possa se sustentar a necessidade da publicidade sobre a sua existência.

A alimentação do banco de dados pessoais pode se dar, basicamente, de duas formas: pela coleta dos dados diretamente dos seus titulares ou pela transferência de dados pessoais armazenados em um outro banco de dados. Em ambas as situações, tanto o consentimento como o princípio da finalidade assumem importância capital.

O consentimento do titular pode tornar lícito tanto o fornecimento voluntário dos próprios dados como o seu posterior repasse a terceiros, visto que é o elemento principal a ser levado em conta ao serem cogitadas ambas as possibilidades (DONEDA, 2006, p. 370). A finalidade, por sua vez, caracteriza-se como uma espécie de afetação dos dados pessoais,

---

[20] No mesmo sentido é a Súmula 323 do Superior Tribunal de Justiça: *"A inscrição de inadimplente pode ser mantida nos serviços de proteção ao crédito por, no máximo, cinco anos."*

[21] Apesar da definição do que se entende por "tratamento de dados pessoais" ser, por natureza, ampla e não exaustiva, a ponto de por vezes ser definida como "qualquer coisa que se possa realizar com a informação pessoal" (v. Pablo Palazzi. *La protección de los datos personales en la Argentina.* Buenos Aires: Errepar, 2004, p. 18.), é muito comum a enumeração das modalidades de tratamento, ainda que de forma ampla. A Diretiva 46/95/CE, por exemplo, define em seu Art. 2.b.: "«Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição."

[22] A terminologia "tratamento de dados pessoais" costuma ser preferida em relação a sinônimos como "processamento de dados pessoais" nas legislações de países de língua latina, conforme atesta a sua adoção pela lei italiana, portuguesa e espanhola.

já que a relação de compatibilidade com o objetivo para o qual os dados foram fornecidos acompanha-os e deve ser levada em conta em qualquer tratamento posterior ao qual sejam submetidos.

Há outras modalidades de tratamento de dados pessoais muito frequentes, como, por exemplo, o cruzamento e a interconexão de bases de dados diversas. Tais modalidades, no entanto, não serão consideradas no presente estudo.

Uma outra modalidade de tratamento bastante frequente é a transmissão de dados pessoais. Pela transmissão, os dados pessoais são enviados da pessoa ou entidade que realiza o tratamento para terceiros. Essa fase costuma definir a própria incidência da legislação de proteção de dados pessoais,[23] pois os bancos de dados criados e mantidos para fins estritamente particulares – isto é, que não se destinam a ser transmitidos para terceiros – não se sujeitam a essa regulação. Também é importante distinguir a transmissão, que se refere ao envio dos dados a destinatário específico, da difusão, que consiste na sua divulgação para um universo aberto e não definido de destinatários.

4. A utilização de dados pessoais para a proteção do crédito e análise de risco e o princípio da finalidade

Com o avanço da tecnologia da informação nas ultimas décadas, a economia mundial passou de uma economia baseada na indústria para uma economia baseada na informação. A informação, a partir de determinado ponto de vista, tornou-se a principal matéria-prima da economia global (KUNER, 2003).[24]

No Brasil, esse fenômeno é perceptível, por exemplo, no caso dos bancos de dados de proteção ao crédito, cuja importância se verifica pelo fato de, direta ou indiretamente, serem fundamentais para a tomada da decisão sobre a concessão ou não de crédito. Tal atividade, que no Brasil opera de forma sistemática, ao menos desde meados da década de 1950[25] e que não depende de autorização prévia, não é em si ilícita, como nota Castro (2005):

> A par das vantagens enunciadas na sua utilização pelas instituições que concedem crédito, deve sublinhar-se que estes tratamentos de dados não são ilícitos, sendo, até, legítimos, visto que o custo do crédito é também função do risco do credor. A legitimidade destes tratamentos dependerá do respeito pelos princípios fundamentais de proteção de dados, bem como pelos direitos dos seus titulares (CASTRO, 2005, p. 198).

[23] Tome-se por exemplo a Lei de *habeas data* que, em seu Art. 1º, estabelece que "considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros (…)" – note-se que a respectiva tutela apenas se aplica aos bancos de dados considerados de caráter público.

[24] *Information has become the new raw material of the world economy. Just as, in past centuries, iron, wood, and coal were the foundation upon which the economy was based, so nowadays it is data and information.*

[25] Em 1955, foi criado em Porto Alegre, por comerciantes da cidade, o Serviço de Proteção ao Crédito – SPC, tendo sido a primeira instituição do gênero no Brasil. Bessa, 2003, p. 25-27.

Nesse mesmo sentido são as palavras de Casado (2000), em relação a um dos cadastros mais representativos do gênero, o cadastro da Serasa:[26]

> Este cadastro ocupa nos dias de hoje uma assustadora importância no mercado de consumo de crédito bancário. Diz-se assustadora pois quem determina a concessão de crédito ao consumo, de forma indireta, é este cadastro. Com a inscrição na Serasa, mesmo que justificada, as chances de conseguir qualquer crédito são praticamente inexistentes, mesmo que se comprove ser detentor de um notável patrimônio e se apresentem garantias sérias ao pagamento da operação pleiteada (CASADO, 2000, p. 179-180).

O próprio Supremo Tribunal Federal, ao julgar em sede de medida cautelar a Ação Direta de Inconstitucionalidade 1.790-5 DF, reconheceu a importância dos bancos de dados e arquivos de consumo, ressaltando que a convivência entre a proteção da privacidade e os arquivos de consumo é um imperativo da economia fundada na sociedade de massas:

> 3. A convivência entre a proteção da privacidade e os chamados arquivos de consumo, mantidos pelo próprio fornecedor de crédito ou integrados em bancos de dados, tornou-se um imperativo da economia da sociedade de massas: de viabilizá-la cuidou o CDC, segundo o molde das legislações mais avançadas: ao sistema instituído pelo Código de Defesa do Consumidor para prevenir ou reprimir abusos dos arquivos de consumo, hão de submeter-se as informações sobre os protestos lavrados, uma vez obtidas na forma prevista no edito impugnado e integradas aos bancos de dados das entidades credenciadas à certidão diária de que se cuida: é o bastante a tornar duvidosa a densidade jurídica do apelo da arguição à garantia da privacidade, que há de harmonizar-se à existência de bancos de dados pessoais, cuja realidade a própria Constituição reconhece (Art. 5°, LXXII, in fine) e entre os quais os arquivos de consumo são um dado inextirpável da economia fundada nas relações massificadas de crédito.[27]

No mesmo sentido, o Superior Tribunal de Justiça, em decisão recente em recurso repetitivo, conforme noticiado no informativo de jurisprudência 380 do STJ, destacou que:

> (...) O serviço de proteção ao crédito existe para procurar manter a higidez no sistema, de modo que elevar riscos, consequentemente, eleva preços não só das mercadorias como do próprio dinheiro, por meio dos juros.[28]

---

[26] A própria Serasa reconhece o papel fundamental que exerce nas decisões sobre concessão de crédito e de negócios de uma maneira geral, como se infere de texto contido em seu site na internet: *"Como maior banco de dados da América Latina sobre consumidores, empresas e grupos econômicos, a Serasa participa da maioria das decisões de crédito e de negócios tomadas no Brasil, respondendo on-line/real-time a 3,5 milhões de consultas por dia, demandadas por mais de 300 mil clientes diretos e indiretos."* Disponível em: http://www.serasa.com.br/empresa/serasa/index.htm. Acesso em 20.12.08.

[27] Ação Direta de Inconstitucionalidade 1.790-5 DF, Rel. Ministro Sepúlveda Pertence, Tribunal Pleno, D.J. 08.09.2000. Disponível em http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=1790&processo=1790. Acesso em 20.12.2008.

[28] REsp 1.062.336-RS e REsp 1.061.134-RS, Rel. Min. Nancy Andrighi, 1ª Seção, julgados em 10/12/2008. http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=835#. Acesso em 20.12.2008.

Além disso, a Lei Complementar 105/2001, que disciplina o sigilo bancário, reconheceu a importância dos repositórios de informações, ao elencar, no §3º de seu Art. 1º, dentre as hipóteses que não configuram violação de sigilo bancário:[29]

> I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
> II – o fornecimento de informações constantes de cadastros de emitentes de cheques sem provisão de fundos e de devedores inadimplentes a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil.

Vê-se, portanto, que os repositórios de informações sobre consumidores possuem um papel relevante para a sociedade de consumo como um todo, sendo necessária a convivência entre o direito à privacidade (ou, mais especificamente, à proteção de dados pessoais) e à livre iniciativa (como reflexo da autonomia da vontade) (CUNHA, 2009, p. 35), já que o acesso a essas informações é fundamental para a tomada de decisões, no que se refere à realização de negócios de massa, como os de seguros e crédito.

A bem da verdade, o Código de Defesa do Consumidor trabalha com uma perspectiva abrangente de informações pessoais em bancos de dados, tanto que sua aplicabilidade não se restringe à atividade de crédito – muito embora este seja o seu campo de aplicação dominante. Essa constatação não passou desapercebida a Bessa, que em sua obra sobre bancos de dados de proteção ao crédito reconheceu que:

> Os bancos de dados podem possuir propósitos absolutamente diversos, que vão desde a obtenção de informações para fins históricos, estatísticos, passando pelos arquivos de proteção ao crédito, até aqueles que coletam informações úteis às companhias seguradoras (BESSA, 2003, p. 177).

[29] Há quem questione a constitucionalidade dos dispositivos em comento. Leonardo Roscoe Bessa. *O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito*. São Paulo: Revista dos Tribunais, 2003, p. 269-270.*"Todavia, a troca de informações 'para fins cadastrais', prevista no inciso I, é situação bastante abrangente que enseja questionamentos de índole constitucional, especialmente em face do princípio da inviolabilidade da privacidade (Art. 5º, II, da CF). Afinal, que espécies de informações serão consideradas para fins cadastrais? Qual a finalidade da troca de informações? Tudo indica que se pretende, com o dispositivo, conferir possibilidade de acesso às informações positivas do consumidor. A constitucionalidade da nova disposição deverá ser aferida em face do princípio da proporcionalidade que, em ultima instância, visa a preservar o núcleo essencial do direito (v. Itens 2.3 e 2.4)."*

Esse entendimento se coaduna com o disposto no *caput* do Art. 43 do Código de Defesa do Consumidor, quando trata do acesso do consumidor "às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes." (BENJAMIN *et al., 2007,* p. 414).[30]

Entretanto, o fornecimento de tais informações aos diversos atores envolvidos nas relações de consumo de massa, como, por exemplo, as seguradoras e bancos, não pode se dar de forma indiscriminada, devendo observar alguns parâmetros, sendo certo que o principal deles refere-se ao princípio da finalidade.

De acordo com o princípio da finalidade, o motivo da coleta ou fornecimento de um dado deve ser compatível com o objetivo final do tratamento ao qual esse dado será submetido. Desta forma, seja quando o dado for coletado diretamente do consumidor, seja quando houver a consulta a um repositório de dados, a sua utilização sempre estará vinculada ao motivo que fundamentou essa coleta. Cria-se, assim, uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, de modo que esta deva ser levada em consideração em qualquer tratamento ulterior.

O princípio da finalidade pode ser tomado como corolário de um pressuposto segundo o qual a informação pessoal, como expressão direta da personalidade de seu titular, nunca perde seu vínculo com este. Antes de ser meramente abstrata e sujeita à livre disposição, essa informação, à medida que identifica alguma característica de uma pessoa, permanece sempre vinculada a ela, e sua utilização pode refletir diretamente em seu titular.

É justamente neste espaço entre a maleabilidade da informação pessoal em si e a necessidade de estabelecer um mecanismo de controle efetivo da pessoa sobre ela que se inserem as regras específicas sobre proteção de dados. No caso específico, através do princípio da finalidade, é possível estabelecer um mecanismo que evite a chamada utilização secundária da informação pessoal à revelia do seu titular. Esse princípio é tanto mais importante ao se levar em conta que, quebrando-se o vínculo entre o consentimento do uso dos dados pessoais para um fim específico, estar-se-ia abrindo a possibilidade para qualquer uso secundário da informação pessoal e, por consequência, tornando inócuos outros meios de proteção e controle dessa informação por parte do seu titular.

---

[30] *"(...) Ao consumidor é assegurado acesso às informações arquivadas, quaisquer que sejam elas ("dados pessoais e de consumo) e qualquer que seja o local onde se encontrem armazenadas ("cadastros, fichas, registros e dados"). É indiferente sejam os dados arquivados pelo próprio fornecedor (nos termos do conceito do Art. 3º) ou, diferentemente, por entidade prestadora de serviço a terceiros, como Serviços de Proteção ao Crédito – SPCs, SERASA e congêneres. Em outras palavras, a raison d'être da lei brasileira é, pois, conferir ao consumidor acesso amplo e irrestrito às informações a seu respeito, colhidas de outra fonte que não ele próprio, estejam elas onde estiverem: em organismos privados ou públicos, em cadastros internos das empresas ou em banco de dados prestador de serviços a terceiros.(...) Ressalte-se que o caput do Art. 43 não limita o direito de acesso aos SPCs. Ao revés, é até prolixo ao mencionar 'cadastros', 'fichas', 'registros', 'dados pessoais' e 'dados de consumo'."* No mesmo sentido, vide Mario Viola de Azevedo Cunha. *Privacidade e Seguro: a coleta e utilização de dados nos ramos de pessoas e de saúde*. Rio de Janeiro: Funenseg, 2009, p. 22.

Esse princípio, apesar de ser enunciado com destaque em diversas leis sobre dados pessoais, não é literalmente referido pela legislação brasileira. Sua relevância, no entanto, pode ser atestada tanto através de uma leitura sistemática das disposições legais referentes à proteção de dados como pelas menções que lhe reserva a jurisprudência. Assim, o Superior Tribunal de Justiça, em emblemático caso relatado pelo Ministro Ruy Rosado de Aguiar, reconheceu a existência do princípio da finalidade como limitador da atividade dos bancos de dados de consumo:

> 2. O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento.
>
> É evidente o benefício que dele decorre em favor da agilidade e da segurança das operações comerciais, assim como não se pode negar ao vendedor o direito de informar-se sobre o crédito do seu cliente na praça, e de repartir com os demais os dados que sobre ele dispõe.
>
> Essa atividade, porém, em razão da sua própria importância social e dos graves efeitos dela decorrentes – pois até para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização de sua finalidade, não se transforme em causa e ocasião de dano social maior do que o bem visado.[31]

Os autores do anteprojeto do Código de Proteção e Defesa do Consumidor, ao tratarem do acesso de fornecedores a dados de consumidores armazenados em arquivos ou bases de dados de consumo, estabelecem como critério de legitimação a presença de uma "necessidade de consumo", que nada mais é do que a realização do princípio da finalidade, além, é óbvio, do requisito de que haja uma solicitação individual. Ou seja, a solicitação do dado deve estar vinculada a um negocio jurídico específico que se pretenda realizar entre o solicitante do dado (fornecedor de serviços, no caso sob análise) e o titular do dado (consumidor) (BENJAMIN *et al.*, 2001. p. 389/390).[32]

[31] REsp 22.337/RS, Rel. Min. Ruy Rosado de Aguiar, 4ª Turma. D.J. em 20.03.1995. Disponível em http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?processo=22337&&b=ACOR&p=true&t=&l=10&i=2. Acesso em 20.12.2008.

[32] *"A acessibilidade depende, pois, do preenchimento de duas condições cumulativas: solicitação individual decorrente de 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 hipóteses de invasão de privacidade. (...) Em acréscimo, a solicitação individualizada precisa estar conectada a uma negociação de consumo. Esse requisito busca proteger o consumidor contra a utilização das informações sobre ele arquivadas para outros fins que não aqueles inerentes ao regular e normal funcionamento do mercado de consumo, a única justificativa para a existência de tais entidades."*

O vínculo entre a informação e a sua finalidade não é, no entanto, absoluto. Como ressaltamos, a relação entre a utilização dos dados e a finalidade para a qual foram coletados não deve ser interpretada de forma restritiva, mas sim como uma relação de compatibilidade entre os fins e a modalidade da coleta.[33] Há de existir, em suma, uma relação de proporcionalidade entre a finalidade do tratamento e os interesses em questão e o motivo da coleta.

Vários critérios têm sido utilizados para mensurar essa proporcionalidade, como, por exemplo, o fato de o titular dos dados poder antecipar que seus dados seriam utilizados para aquela finalidade (ainda que não literalmente mencionada) (CASTRO, 2005, p. 231), quando os dados a serem tratados forem indispensáveis para a realização da atividade pretendida, ou quando a finalidade apresentar um interesse público relevante.[34]

A compatibilidade entre o motivo da coleta e a utilização do dado em si há de ser verificada pela aplicação do princípio da proporcionalidade, possibilitando o recurso a critérios específicos para avaliar se a utilização do dado não é abusiva e exacerba os limites que razoavelmente poderiam ser cogitados pelo seu titular no momento do fornecimento, bem como se há, em cada caso, interesses relevantes que possam sugerir ser necessária uma maior elasticidade e tolerância com utilizações mais amplas de dados pessoais. Essa ponderação não pode ser feita em abstrato: "Somente analisando o caso concreto, com uma criteriosa ponderação dos valores em jogo, é possível alcançar a resposta" (BESSA, 2003, p. 187).

O recurso à ponderação na aplicação do princípio da finalidade não se configura como necessariamente danoso ao titular dos dados, por eventualmente ampliar as hipóteses de utilização dos mesmos: observe-se que a disciplina de proteção de dados pessoais estrutura-se entre a necessidade de tutela de um direito fundamental, por um lado, e o estabelecimento de parâmetros de licitude para o tratamento de dados pessoais por diversos sujeitos que tenham interesse legítimo. Neste sentido, uma ponderação que não deixe de lado os interesses do titular pode contribuir para ampliar a utilização dos dados pessoais em situações que não ofereçam riscos suplementares.

---

[33] Neste sentido, p. ex., o considerando (28) da Diretiva 95/46/CE da União Europeia:
"(28) Considerando que qualquer tratamento de dados pessoais deve ser efectuado de forma lícita e leal para com a pessoa em causa; que deve, em especial, incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com o tratamento; que essas finalidades devem ser explícitas e legítimas e ser determinadas aquando da recolha dos dados; que as finalidades dos tratamentos posteriores à recolha não podem ser incompatíveis com as finalidades especificadas inicialmente"; ou o artigo 4,1 da Lei Orgânica 15/1999, da Espanha: "2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos…"

[34] As duas últimas hipóteses foram mencionadas no Parecer 22/2001 da Comissão Nacional de Proteção de Dados de Portugal, que julgou lícita uma transmissão de dados pessoais que exacerbava a finalidade especificada em sua coleta, com base nesses argumentos. Disponível em http://www.cnpd.pt/bin/decisoes/2001/htm/par/par022-01.htm. Acesso em 27.12.2008.

5. Conclusão

Partindo-se da constatação de que a proteção de dados pessoais é um direito fundamental reconhecido por diversos ordenamentos jurídicos, sua aplicação em casos concretos depende da ponderação entre o controle sobre os próprios dados pessoais e a utilização que deles se pretende fazer – além das suas respectivas implicações em relação à razoável expectativa de privacidade do indivíduo. Malgrado a inexistência de uma norma geral sobre proteção de dados pessoais no ordenamento brasileiro, tal ponderação tem como fundamentos legislativos principais as provisões constitucionais concernentes à privacidade e proteção de dados pessoais, bem como o Código de Defesa do Consumidor.

O elemento crucial para realizar essa ponderação é a observância ao princípio da finalidade, como critério hábil para estabelecer limites para a utilização de dados pessoais, tanto no momento da coleta quanto do fornecimento desses dados a terceiros, levando em conta a proteção devida ao titular dos dados.

Conforme se infere da própria natureza da disciplina de proteção de dados pessoais, é relevante que se atinja um equilíbrio entre as liberdades e direitos individuais tutelados através da proteção de dados pessoais e da garantia da circulação da informação necessária às relações comerciais (GONÇALVES, 1994, p. 96).

Tal equilíbrio será obtido através da aplicação do princípio da proporcionalidade, pelo qual avaliam-se os interesses em questão, procurando tutelar o conteúdo essencial do direito à privacidade,[35] ao mesmo tempo em que se leva em conta a necessidade da utilização dos dados pessoais no caso concreto.[36]

[35] *"… Mostra-se evidente no mundo contemporâneo a permanente colisão entre a privacidade e todos os demais direitos tutelados na sociedade globalizada. Cabe ao intérprete, pois, mais do que simplesmente alardear a inviolabilidade teórica dos direitos fundamentais, delimitá-los em sua concreta atuação."* Gustavo Tepedino, Heloísa Helena Barboza e Maria Celina Bodin de Moraes (orgs.). Código Civil interpretado conforme a Constituição, v. I, 2ª ed., Rio de Janeiro: Renovar, 2007, p. 61.

[36] Neste sentido pronunciou-se mais de uma vez o Superior Tribunal de Justiça: *"Doutrina e jurisprudência estão acordes quanto à inexistência de direito absoluto à privacidade, porque pode ser afastada a proteção deste direito quando razões plausíveis superarem o direito individual"* (STJ, 2a. T., ROMS 9887, Rel. Min. Eliana Calmon, j. 14.08.2001, DJ 01.10.2001); *"O direito à privacidade é constitucionalmente garantido. Todavia, não é absoluto, devendo ceder em face do interesse público"* (STJ, 1a. T., ROMS 15771, Rel. Min. José Delgado, j. 27.05.2003, DJ 30.06.2003).

6. Referências bibliográficas

BENJAMIN, Antonio Herman de Vasconcellos et al. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto**. 7. ed. Rio de Janeiro: Forense Universitária: 2001. p. 389/390.

BENJAMIN, Antônio Herman de Vasconcellos et al. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.** 9. ed. São Paulo: Forense, 2007. p. 413, 414 e 416.

BESSA, Leonardo Roscoe. **O Consumidor e os Limites dos Bancos de Dados de Crédito**. São Paulo: Revista dos Tribunais, 2003. v. 25. p. 107. (Biblioteca de Direito do Consumidor)

BESSA, Leonardo Roscoe. **O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito**. São Paulo: Revista dos Tribunais, 2003, p. 177 e 187.

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

CASADO, Márcio Mello. **Proteção do Consumidor de Crédito Bancário e Financeiro**. São Paulo: Revista dos Tribunais, 2000, v. 15, p. 179-180. (Biblioteca de Direito do Consumidor)

CUNHA, Mario Viola de Azevedo. **Privacidade e Seguro**: a coleta e utilização de dados nos ramos de pessoas e de saúde. Rio de Janeiro: Funenseg, 2009, p. 22 e 35.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 261-306 e 370.

GONÇALVES, Maria Eduarda. **Direitos de informação**. Almedina: Coimbra, 1994, p. 96.

KUNER, C. **European Data Protection Law and Online Business**. New York: Oxford University Press, 2003.

MEYER, Roberta B. “The Insurer Perspective”. In: ROTHSTEIN, Mark A. **Genetics and Life Insurance:** Medical Underwriting and Social Policy. Massachusetts: The MIT Press, 2004, p. 29.

RODOTÀ, Stefano. **Repertorio di fine secolo**. Bari: Laterza, 1999. p. 62.

SAMPAIO, José Adércio L. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1997, p. 509.

SARMENTO E CASTRO, Catarina. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005, p. 198 e 231.