

INFORMAÇÕES SOBRE O ARTIGO

Área do Artigo: Direito Civil (Responsabilidade Civil)

Título: *Aplicação restrita das excludentes de responsabilidade civil à atividade de coleta, gestão e armazenamento de dados de outrem*

Autor: Leonardo Netto Parentoni

E-mail: parentoni@gmail.com

Instituição à qual se vincula o autor: USP (Atualmente cursando o Doutorado em Direito Comercial)

Resumo

Este artigo aborda a aplicação restritiva das excludentes de responsabilidade civil à atividade de coleta, gestão e armazenamento de dados de outrem, enfocando seus aspectos peculiares e os conceitos técnicos envolvidos na discussão.

Palavras-chave: responsabilidade civil, dados pessoais.

Abstract

This paper discusses personal liability applied to the activity of collect, administrate and safeguard personal data, putting into spot some peculiar aspects of the subject and the technical concepts related to it.

Keywords: personal liability, personal data.

1. Introdução.

A cada segundo, acontecem cerca de um milhão de *clicks* nas páginas da *internet*¹. Esse montante ilustra a imensidão de dados continuamente transmitidos através da rede.

Dentre os vários significados constantes do dicionário, o que mais se relaciona à palavra dado, no sentido em que aqui empregada, é “informação relativa a um indivíduo, capaz de identificá-lo”². Porém, o dicionário transmite a falsa impressão de que os termos *dado* e *informação* são sinônimos quando, na verdade, constituem conceitos tecnicamente distintos:

“Embora sejam ocasionalmente tratados como equivalentes, os ‘dados’ constituem a matéria-prima e ‘informação’, os dados processados, ou seja, o conjunto

¹ Estatística constante de: ROSA, Mário. *A Reputação na Velocidade do Pensamento: Imagem e Ética na Era Digital*. São Paulo: Geração Editorial, 2006. p. 34.

² Dicionário Eletrônico Houaiss. Verbetes “dado”.

de dados relevantes a que se atribui um significado determinado.”³

No Direito positivo brasileiro, o Decreto nº 97.057/1988, que regulamentou a Lei Geral de Telecomunicações (Lei nº 4.117/1962), traz a definição técnica de dados⁴.

Há que se destacar, também, a existência de várias *espécies de dados*, na medida em que o tratamento jurídico de cada uma delas é distinto⁵.

2. Legislação Comparada.

No Direito estrangeiro, as primeiras preocupações com a regulamentação dos dados pessoais remontam à década de 70⁶. Todavia, foi somente na década seguinte que surgiu uma iniciativa transnacional sobre o tema, oriunda da Organização para a Cooperação e Desenvolvimento Econômico – OECD. Trata-se das Diretivas sobre a Proteção da Privacidade e o Fluxo Transfronteiriço de Dados Pessoais, de 23 de setembro de 1980⁷.

No âmbito da Comunidade Européia, o tema é atualmente regulado pela Diretiva nº 95/46 do Parlamento Europeu, de 24 de outubro de 1995⁸, enquanto nos Estados Unidos da América há apenas uma orientação do Departamento de Comércio, datada de 21 de julho de 2000, denominada *Safe Harbour Privacy Principles*⁹, cujo intuito é compatibilizar a atuação das empresas norte-americanas com o regime de tratamento de dados adotado pela Comunidade Européia.

³ SANTOS, Manoel J. Pereira dos. Princípios para Formação de um Regime de Dados Pessoais. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2. p. 357.

⁴ Mais precisamente, a referida lei foi originariamente regulamentada pelo Decreto nº 52.026, de 20 de maio de 1963, tendo sido este alterado pelo Decreto nº 97.057, de 10 de novembro de 1988. “Art. 6º Para os efeitos deste Regulamento Geral, dos Regulamentos Específicos e das Normas complementares, os termos adiante enumerados têm os significados que se seguem:

(...)

23º) Dado - informação sistematizada, codificada eletronicamente, especialmente destinada a processamento por computador e demais máquinas de tratamento racional e automático da informação.”

⁵ Sobre o tema, aprecie-se: VASCONCELOS, Pedro Pais de. *Direito da Sociedade da Informação: Protecção de dados pessoais e direito à privacidade*. Coimbra: Coimbra Editora, 1999. v. I. p. 245.

Vide também: SANTOS, Manoel J. Pereira dos. Princípios para Formação de um Regime de Dados Pessoais. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2. p. 357-358.

⁶ Conforme: DONEDA, Danilo. *Da Privacidade à Protecção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006. p. 206.

Podem ser citados, por exemplo, a lei sueca conhecida como Datalagen, de 11 de maio de 1973, o Privacy Act norte-americano, de 1974, as leis dinamarquesas nº 243 e 244, ambas de 08 de julho de 1978, além da Constituição portuguesa de 1976, que tratava do tema em seu artigo 35.

⁷ Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, from Organization for Economic Cooperation and Development – OECD. Disponível em <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>. Consultado em 15/02/2009.

⁸ Diretiva nº 95/46 da Comunidade Européia. Disponível em <http://www.cert.fnmt.es/legsoporte/Directiva%2095_46_CE%20Datos%20CaracterPersonal.pdf>. Consultado em 15/02/2009.

⁹ Safe Harbour Privacy Principles. Disponível em <<http://www.export.gov/safeHarbor/SHPRINCIPLESFINAL.htm>>. Consultado em 15/02/2009.

Em ambas se verificam, basicamente, sete princípios¹⁰: 1) O *site* que pretende coletar dados deve informar isso ao interessado; 2) A partir da informação mencionada acima, o interessado tem o direito de decidir se permite ou não a coleta; 3) É necessária a autorização expressa do interessado para que o *site* possa repassar os dados coletados a terceiros; 4) Deve haver uma clara política de segurança para que se evite a perda de dados; 5) Deve-se assegurar a integridade dos dados coletados, evitando sua adulteração; 6) É garantido o pleno acesso do interessado a seus dados, inclusive com a possibilidade de retificação; e 7) Deve haver instrumentos que garantam a efetiva fiscalização e o cumprimento dos seis princípios mencionados acima.

Talvez fosse interessante, *de lege ferenda*, acrescentar outro princípio a essa lista. Trata-se da necessidade de garantir ao usuário pleno acesso a todas as funcionalidades de um *site*, mesmo se ele optar por não fornecer dados pessoais, desabilitando tal opção no seu navegador de *internet*¹¹. Na prática, o que se verifica é que a navegação completa em grande número de páginas somente é possível mediante a coleta de dados pessoais. Proibida essa coleta, alguns recursos da página se tornam indisponíveis, cerceando seus usuários.

3. Coleta, gestão e armazenamento de dados de outrem e os novos contornos da privacidade na sociedade da informação.

O simples ato de efetuar uma busca no Google¹² colabora para a formação de um imenso banco de dados¹³. Ao procurar determinado *site*, a pessoa acaba revelando aspectos de sua personalidade, como preferências políticas, religiosas, desportivas, gastronômicas, etc. Devidamente sistematizadas, tais informações adquirem valor econômico:

“(...) na chamada new economy, cresce de forma exponencial a importância econômica do conhecimento de dados pessoais dos usuários porque essas informações permitem a empresas atuantes em determinados setores

¹⁰ ROHRMANN, Carlos Alberto. Notas acerca do Direito à Privacidade na Internet: A perspectiva comparativa. *Revista da Faculdade de Direito Milton Campos*. Belo Horizonte, v. 9, 2002. p. 25.

¹¹ Por exemplo, proibindo os *cookies*, como se verá adiante.

¹² O Google é um renomado mecanismo de busca na *internet*. Disponível em <<http://www.google.com.br>>. Consultado em 22.02.2009. Note-se que cada país possui um *site* local para buscas, como o [google.com](http://www.google.com) para os Estados Unidos, [google.ar](http://www.google.ar) para a Argentina, [google.it](http://www.google.it) para a Itália, etc.

Sobre os motores de busca na *internet*, confira-se a seguinte conceituação: ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Belo Horizonte: Del Rey, 2005. p. 202-203. “Uma forma de facilitar a localização de *web sites* ‘perdidos’ na grande quantidade de informação disponível na Internet é a utilização dos chamados ‘mecanismos de busca’ ou ‘motores de busca’ (expressão que corresponde à tradução do termo usado na língua inglesa, qual seja, ‘search engines’).

Cada um dos muitos *web sites* de busca na rede pode ter um programa de computador próprio com um algoritmo específico para a localização de outros *sites* na Internet. Normalmente, a pessoa que quer localizar algum *web site* sobre determinado assunto digita a palavra que se relaciona com o assunto (ou com o produto, caso esteja à procura de um fornecedor). O algoritmo do programa de computador do buscador gera uma lista indexada de *web sites* que se relacionam com a palavra que foi o objeto da busca. A lista gerada pelo buscador costuma colocar em primeiro lugar aquele *web site* que mais relação teria com a palavra que foi objeto da busca.”

¹³ BATTELLE, John. *A Busca: como o Google e seus competidores reinventaram os negócios e estão transformando nossas vidas*. Tradução: Nivaldo Montingelli Jr. Rio de Janeiro: Elsevier, 2005. p. 02.

delinear o mercado de determinado produto ou serviço. De fato, as informações que permitem identificar o perfil de um consumidor-usuário viabilizam a criação de oferta de determinado produto ou serviço bastante próxima daquilo que ele está propenso a adquirir ou a fruir. Assim, essas informações assumem valor socioeconômico para as empresas interessadas, que utilizam a tecnologia telemática para o tratamento e a gestão desses dados, promovendo uma divulgação comercial ágil, eficaz e bem mais econômica do que qualquer campanha publicitária realizada nos moldes tradicionais.”¹⁴

Para se ter uma idéia da dimensão e confiabilidade desse banco de dados *online*, a equipe do Google descobriu que ao monitorar o número de buscas relacionadas ao assunto gripe na *internet*, é possível antecipar a chegada de epidemias dessa doença com até quinze dias de antecedência em relação às fontes oficiais¹⁵.

Nesse ambiente pluralista, a coleta eletrônica de dados pessoais pode se dar sem o consentimento do interessado – o que é mais comum –, ou de forma consentida. No primeiro caso, sua obtenção é comumente realizada por meio de um arquivo de computador denominado *cookie*¹⁶. Pesquisa realizada por uma organização norte-

¹⁴ PASQUINO, Teresa. Serviços da Sociedade de Informação: Tutela dos Dados Pessoais e Regras de Conduta. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2. p. 699-700.

Note-se que a informação, ou seja, um conjunto de dados inter-relacionados constitui bem jurídico, objeto de tutela jurisdicional, como adverte o jurista italiano Pietro Perlingieri: PERLINGIERI, Pietro. *Perfis do Direito Civil: Introdução ao Direito Civil Constitucional*. Tradução: Maria Cristina de Cicco. Rio de Janeiro: Renovar, 1999. p. 237 a 241.

¹⁵ GOOGLE USA BUSCAS PARA MONITORAR EPIDEMIAS DE GRIPE NOS EUA. Site IDG NOW!, 12 nov. 2008. Disponível em <<http://idgnow.uol.com.br/internet/2008/11/12/google-usa-buscas-para-monitorar-epidemias-de-gripe-nos-eua/>>. Consultado em 22/02/2009. “O Google descobriu que, ao analisar as buscas relacionadas com gripe feitas em seu site, é possível antecipar possíveis epidemias da doença até duas semanas antes que os sistemas de monitoramento governamentais.

Os resultados da pesquisa foram publicados nesta semana em um *hotsite* chamado *Google Flu Trends*, que revelaram uma relação entre as buscas por tópicos sobre gripe e a quantidade de pessoas realmente contaminadas pela doença.

De acordo com a empresa, algumas pesquisas se tornam mais comuns quando as pessoas estão gripadas. A vantagem do Google é que ele consegue filtrar a pesquisas e obter dados automática e instantaneamente, enquanto os sistemas de monitoramento do governo norte-americano levam até duas semanas para obter dados semelhantes.”

¹⁶ SAWAYA, Márcia Regina. *Dicionário de Informática e Internet*. 3. ed. São Paulo: Nobel, 1999. p. 101. “Um arquivo é remetido, automaticamente, pelo servidor de rede ao disco rígido do usuário quando este entra em certos *sites* da WWW (*Word Wide Web*) alojados no servidor. Este arquivo, chamado de *cookie*, é usado pelos servidores para manter rastros, padrões e preferências dos usuários.

A finalidade desses arquivos é criar uma identificação individual, para quando o usuário acessar o *site* novamente, ele possa identificar que aquele usuário já o visitou anteriormente, além de saber que tipo de coisa procurou, comprou ou olhou no site, bem como o valor que gastou com algo que tenha adquirido neste *site*.

Portanto, os ‘*cookies*’ funcionam como um banco de dados, onde constam as preferências e disposições do usuário do site (...).”

Definição um pouco mais dilatada de *cookie* é dada por Newton de Lucca: LUCCA, Newton de. *Aspectos Jurídicos da Contratação Informática e Telemática*. São Paulo: Saraiva, 2003. p. 120. “Consistem os *cookies* num tipo de programa que monitora todos os procedimentos executados pelo internauta a partir

americana, denominada Centro de Informações acerca da Privacidade Eletrônica, concluiu que dentre os 100 (cem) *sites* mais visitados do mundo cerca de 24% utilizavam-se de *cookies* para captar dados pessoais dos usuários, sem informá-los a respeito¹⁷.

Além dos *cookies*, existem outros mecanismos subliminares de obtenção de dados. Um deles é a prática conhecida como *phishing*¹⁸. Esta palavra da língua inglesa significa pesca e consiste numa estratégia artilosa por meio da qual um sujeito, denominado *phisher* (pescador), busca iludir sua vítima, fazendo com que ela lhe forneça dados pessoais, sobretudo senhas bancárias e números de cartão de crédito. Existem vários outros mecanismos ilícitos com o mesmo propósito. Porém, tendo-se em mente o limite máximo de páginas definido pela organização do Congresso¹⁹ ao qual este texto é apresentado, bastam as referências feitas acima. O importante é destacar que, seja em virtude dos *cookies*, seja por meio de *phishing*, o titular dos dados não tem ciência de sua coleta nem, tampouco, da maneira como serão utilizados²⁰.

Ao lado da obtenção clandestina, existem também hipóteses nas quais é o próprio interessado quem fornece dados pessoais a um terceiro. Algumas sociedades empresárias, inclusive, têm por objeto precipuamente coletá-los, geri-los e armazená-los. É o caso, por exemplo, da *Recall*, sociedade que atua no Brasil e em mais de 20 países, com cerca de 80.000 clientes. Sua atividade empresarial consiste em gerenciar os

do momento em que ele acessa a *internet*. Agem como se, na vida real, fossem espíões de todos os nossos passos, registrando-os para futura utilização, de cunho mercadológico.”

¹⁷ SURFER BEWARE: PERSONAL PRIVACY AND THE INTERNET, *Electronic Privacy Information Center*, jun. 1997. Disponível em <<http://epic.org/reports/surfer-beware.html>>. Consultado em 14/02/2009. “We were interested to see how many of the top 100 web sites enabled the cookies feature. We visited each web site and then checked our cookies file to see if a new line was added. We did not, of course, visit every page or every linked site at each site we visited, so we may have missed some pages that generate cookies.

Of the 100 sites, 24 enable cookies.

(...) none of the sites that enabled cookies told the user that information about the user was being placed on the user's system.

Even though privacy is one of the top concerns among Internet users, few webs sites today actually have privacy policies or provide users with information about privacy practices. This makes it almost impossible for users to make informed decisions about their on-line activities.

(...)

In the absence of meaningful privacy policies, net surfers today also have little assurance that personal information that is provided at a web site might not be misused. Not surprisingly, many users are reluctant to disclose personal information and some provide false information when asked.”

¹⁸ Sobre as diversas fraudes perpetradas via *internet*, dentre elas o *phishing*, consulte-se: FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2. p. 418.

¹⁹ Trata-se do I Congresso Internacional sobre “Os desafios do Direito face às novas tecnologias”, realizado pela Faculdade de Direito da USP - Ribeirão Preto, no ano de 2010, e Coordenado pelas Doutoras Cintia Rosa Pereira de Lima e Lydia Neves Bastos Telles Nunes.

²⁰ BESSA, Leonardo Roscoe. *Relação de Consumo e Aplicação do Código de Defesa do Consumidor*. 2. ed. São Paulo: Revista dos Tribunais, 2009. p. 31. “O avanço da tecnologia conduz ao oferecimento de serviços e bens cada vez mais complexos, gerando um déficit informacional e, conseqüentemente, dificuldades para uma escolha madura e consciente do consumidor. Na área informática, o rápido progresso da tecnologia permite um absoluto controle dos dados pessoais do consumidor, possibilitando, em ofensa ao valor privacidade, traçar a rotina, hábitos e gostos do cliente e, ainda, desenhar um perfil digital do consumidor – que pouco se aproxima da realidade –, ensejando ofensa à honra e condutas discriminatórias.”

dados de seus clientes durante todo o processo, desde o armazenamento e recuperação de documentos, até a conversão digital, proteção e destruição segura²¹.

4. A responsabilidade objetiva como garantia para a vítima.

A responsabilidade civil *objetiva* recebe esta denominação pelo fato de que a ela não interessa o elemento subjetivo, ou seja, a ação ou omissão voluntária, negligência, imperícia ou imprudência. Bastam a demonstração do dano e o nexo de causalidade entre ele e o sujeito causador, desde que inexista qualquer causa excludente, como a culpa exclusiva da vítima.

Como destaca Orlando Gomes, a responsabilidade civil objetiva tem uma *função garantista*²², pois visa a evitar que um dano deixe de ser ressarcido em virtude da dificuldade de se provar o dolo ou a culpa de quem o causou. Em regra, o *fundamento* dessa garantia é o fato de que algumas atividades, por sua própria natureza, geram um risco de lesão aos direitos de outrem. Assim, quem exerce tais atividades deve assumir os danos dela decorrentes, ainda que não atue com dolo ou culpa. Este é o fundamento do art. 927, parágrafo único, do Código Civil.

5. Excludentes de responsabilidade civil.

Em apertada síntese, são quatro as causas excludentes de responsabilidade civil: caso fortuito, força maior, culpa exclusiva da vítima e culpa exclusiva de terceiro. Tratando-se de conceitos comumente conhecidos, e tendo em vista os estreitos limites fixados para este texto²³, não será detalhado em que consiste cada uma destas excludentes. Basta dizer que elas *afastam o nexo de causalidade*, eliminando a própria responsabilidade civil (e não apenas a ilicitude do ato)²⁴.

O que se discute não é a existência de tais excludentes, mas os *limites de sua aplicação*, sobretudo em face da responsabilidade objetiva que, como já alertado, constitui mais uma *garantia da vítima* do que propriamente uma forma de responsabilização. Sua função, repita-se, é evitar que um dano deixe de ser ressarcido em virtude da dificuldade de se provar o dolo ou a culpa de quem o causou.

Assim, *em relação à responsabilidade objetiva, as excludentes devem ser aplicadas com parcimônia*, sob pena de subverterem a própria finalidade desse regime especial²⁵. A jurisprudência consolidou este aspecto ao considerar que certas atividades,

²¹ Informações detalhadas disponíveis em <<http://www.recall.com/recall/br/pt/home>>. Consultado em 23/02/2009.

²² GOMES, Orlando. *Obrigações*. 14. ed. Rio de Janeiro: Forense, 2000. p. 307.

Sobre os fundamentos da responsabilidade objetiva, aprecie-se a seguinte decisão: STF, Decisão Monocrática, AI. n.º 455.846/RJ. Data da decisão: 11/10/2004. Publicação: DJ Data: 21/10/2004. Relator (a) Ministro (a): Celso de Mello.

²³ A chamada de artigos para o Trata-se do I Congresso Internacional sobre “Os desafios do Direito face às novas tecnologias” impõe limite de 10 páginas para os artigos.

²⁴ Tal conclusão é partilhada até mesmo pelos autores que conferem máxima extensão à responsabilidade objetiva, como é o caso de Nelson Nery Júnior: LIMA, Alvinio. *A Responsabilidade Civil pelo Fato de Outrem*. Atualização: Nelson Nery Júnior. 2. ed. São Paulo: Revista dos Tribunais, 2000. p. 205-212.

²⁵ NETTO, Felipe Peixoto Braga. *Responsabilidade Civil*. São Paulo: Saraiva, 2008. p. 89. “As excludentes de caso fortuito ou força maior devem ser encaradas com temperamento nas hipóteses de responsabilidade objetiva, só podendo ser aceitas em hipóteses altamente excepcionais, uma vez que o risco é do empreendedor, não do consumidor.”

por sua própria natureza, são suscetíveis de causar dano aos direitos de outrem. Por isso, *nelas a responsabilização faz parte do risco natural do negócio, sendo até previsível*, razão pela qual a incidência das excludentes se restringe a casos absolutamente excepcionais.

As atividades bancárias são um bom exemplo. A ocorrência de furtos e roubos no interior das agências²⁶ ou no estacionamento do banco²⁷, a entrega indevida de cartões²⁸, bem como a vulnerabilidade de seus sistemas eletrônicos²⁹, acarretam a responsabilidade objetiva da instituição financeira, sendo inaplicáveis as excludentes de caso fortuito e força maior, porque essas situações são previsíveis e constituem risco inerente à própria atividade, também chamado de *risco interno do negócio*. É justamente isto o que ocorre em relação a quem coleta dados de terceiro. Nestes casos, a possibilidade de perda, adulteração ou divulgação não autorizada de dados faz parte do

Exemplo dessa aplicação restritiva das excludentes encontra-se na súmula 187 do Supremo Tribunal Federal: “A responsabilidade contratual do transportador, pelo acidente com o passageiro, não é elidida por culpa de terceiro, contra o qual tem ação regressiva.”

²⁶ STJ, REsp. n.º 787.124/RS. Órgão Julgador: Primeira Turma. Data da decisão: 20/04/2006. Publicação: DJ Data: 22/05/2006. Relator (a) Ministro (a): José Delgado. Decisão por unanimidade.

“Ementa:

(...) Restando incontroverso nos autos a ocorrência de assalto em agência bancária, que resultou na morte do genitor dos autores da ação indenizatória (...).

Descabido, ainda, o argumento de que houve força maior a ensejar a exclusão da responsabilidade do recorrente. Em diversos precedentes deste Pretório, restou assentada a orientação de que, em razão da previsibilidade, o roubo não caracteriza hipótese de força maior, capaz de elidir o nexo de causalidade, indispensável à configuração do dever indenizatório.”

²⁷ STJ, REsp. n.º 1.045.775/ES. Órgão Julgador: Terceira Turma. Data da decisão: 23/04/2009. Relator (a) Ministro (a): Massami Uyeda. Decisão por unanimidade.

²⁸ STJ, REsp. n.º 703.129/SP. Órgão Julgador: Terceira Turma. Data da decisão: 21/08/2007. Publicação: DJ Data: 06/11/2007. Relator (a) Ministro (a): Carlos Alberto Menezes Direito. Decisão por unanimidade.

“Ementa:

(...) Não é possível identificar a excludente de culpa exclusiva de terceiro sob a égide do Código de Defesa do Consumidor quando o banco entrega cartão de crédito a terceira pessoa que não o titular da conta, considerando que direta ou indiretamente participa da operação por meio de seus sistemas de controle em operações da espécie.”

²⁹ STJ, REsp. n.º 557.030/RJ. Órgão Julgador: Terceira Turma. Data da decisão: 16/12/2004. Publicação: DJ Data: 01/02/2005. Relator (a) Ministro (a): Nancy Andrighi. Decisão por unanimidade.

“Ementa:

(...) Reconhecida a possibilidade de violação do sistema eletrônico e, tratando-se de sistema próprio das instituições financeiras, ocorrendo retirada de numerário da conta corrente do cliente, não reconhecida por este, impõe-se o reconhecimento da responsabilidade objetiva do fornecedor do serviço, somente passível de ser ilidida nas hipóteses do § 3º do art. 14 do CDC.”

No mesmo sentido o entendimento doutrinário: LUCCA, Newton de. Aspectos Atuais da Proteção aos Consumidores no Âmbito dos Contratos Informáticos e Telemáticos. *In*: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2. p. 66-71. “(...) ocorrendo a invasão por um *hacker* ou por um *cracker* no sistema telemático do banco, com prejuízo aos seus correntistas, poderia ser invocada a exclusão de responsabilidade dos bancos com base no art. 12, § 3º, inciso III, do nosso CDC?

(...)

Parece não haver dúvida, assim, no que se refere aos problemas apontados – falhas no equipamento eletrônico ou nos programas de computador e erros no processamento de dados -, de que a responsabilidade civil dos estabelecimentos bancários desponta indeclinável, como já ficou dito anteriormente, quer ela derive da teoria do risco empresarial, num dos caminhos possíveis de raciocínio, quer ela decorra do regime de responsabilidade de nosso Código de Defesa do Consumidor, segundo outro ângulo de análise. Assinale-se que a teoria do risco empresarial – direta ou indiretamente – vem sendo progressivamente acolhida pela jurisprudência pátria, especialmente pelo nosso Superior Tribunal de Justiça (...).”

risco interno do negócio. Aliás, *é justamente para gerenciar esse risco que se costuma contratar sociedades especializadas no armazenamento eletrônico de dados.*

6. Conclusão

Conclui-se, então, que *as excludentes de caso fortuito e força maior não se aplicam à atividade de coleta, gestão e armazenamento de dados de outrem, por se inserirem no risco natural do negócio, sua própria razão de ser.* Por exemplo, um provedor de armazenamento de dados não se furta à responsabilização civil pela perda de tais dados ao alegar que foram destruídos em virtude de incêndio ou inundação que atingiu os computadores nos quais estavam armazenados. Foi justamente para assegurar-se de que não ocorreria a perda que o titular dos dados havia contratado o referido provedor.

Já a *culpa exclusiva da vítima* é suficiente para afastar a responsabilidade civil uma vez que não se concebe possa ela ser ressarcida por dano do qual foi a única causadora. Admitir o contrário seria privilegiar um comportamento contraditório³⁰, propiciando o enriquecimento ilícito da vítima. Assim, imagine-se o exemplo em que um Tribunal de Justiça determina à sociedade empresária por ele contratada para gerenciar seu arquivo processual - por meio da pessoa competente e de acordo com contrato - que elimine completamente determinado processo. Neste contexto, não poderá o Presidente do Tribunal, posteriormente, obter a responsabilização da sociedade, ainda que se verifique que a ordem foi dada por engano.

Por fim, a exclusão da responsabilidade civil objetiva com base na *culpa exclusiva de terceiro* tem lugar apenas quando o dano decorre de conduta absolutamente inevitável e imprevisível, corporificando *risco externo ao negócio*. Sua aplicação à atividade de coleta, gestão e armazenamento de dados de outrem é bastante improvável, pois, como frisado, a possibilidade de perda, adulteração ou divulgação não autorizada de dados faz parte do risco interno desse negócio, sua própria razão de ser, não justificando a aplicação da referida excludente.

Essas, em suma, as principais considerações acerca da aplicação das excludentes de responsabilidade civil à atividade de coleta, gestão e armazenamento de dados de outrem.

7. Referências Bibliográficas.

- BATTELLE, John. *A Busca: como o Google e seus competidores reinventaram os negócios e estão transformando nossas vidas.* Tradução: Nivaldo Montingelli Jr. Rio de Janeiro: Elsevier, 2005.
- BESSA, Leonardo Roscoe. *Relação de Consumo e Aplicação do Código de Defesa do Consumidor.* 2. ed. São Paulo: Revista dos Tribunais, 2009.
- DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais.* Rio de Janeiro: Renovar, 2006.
- GOMES, Orlando. *Obrigações.* 14. ed. Rio de Janeiro: Forense, 2000.
- LIMA, Alvino. *A Responsabilidade Civil pelo Fato de Outrem.* Atualização: Nelson Nery Júnior. 2. ed. São Paulo: Revista dos Tribunais, 2000.

³⁰ SCHREIBER, Anderson. *A Proibição do Comportamento Contraditório.* 2. ed. Rio de Janeiro: Renovar, 2007.

- LUCCA, Newton de. Aspectos Atuais da Proteção aos Consumidores no Âmbito dos Contratos Informáticos e Telemáticos. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2.
- _____. *Aspectos Jurídicos da Contratação Informática e Telemática*. São Paulo: Saraiva, 2003.
- NETTO, Felipe Peixoto Braga. *Responsabilidade Civil*. São Paulo: Saraiva, 2008.
- PASQUINO, Teresa. Serviços da Sociedade de Informação: Tutela dos Dados Pessoais e Regras de Conduta. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2.
- PERLINGIERI, Pietro. *Perfil do Direito Civil: Introdução ao Direito Civil Constitucional*. Tradução: Maria Cristina de Cicco. Rio de Janeiro: Renovar, 1999.
- ROHRMANN, Carlos Alberto. Notas acerca do Direito à Privacidade na Internet: A perspectiva comparativa. *Revista da Faculdade de Direito Milton Campos*. Belo Horizonte, v. 9, 2002.
- ROSA, Mário. *A Reputação na Velocidade do Pensamento: Imagem e Ética na Era Digital*. São Paulo: Geração Editorial, 2006.
- SANTOS, Manoel J. Pereira dos. Princípios para Formação de um Regime de Dados Pessoais. In: LUCCA, Newton de, SIMÃO FILHO, Adalberto (Coord.). *Direito e Internet: Aspectos Jurídicos Relevantes*. São Paulo: Quartier Latin, 2008. v. 2.
- SCHREIBER, Anderson. *A Proibição do Comportamento Contraditório*. 2. ed. Rio de Janeiro: Renovar, 2007.
- SAWAYA, Márcia Regina. *Dicionário de Informática e Internet*. 3. ed. São Paulo: Nobel, 1999.
- SURFER BEWARE: PERSONAL PRIVACY AND THE INTERNET, *Electronic Privacy Information Center*, jun. 1997. Disponível em <<http://epic.org/reports/surfer-beware.html>>. Consultado em 14/02/2009.
- VASCONCELOS, Pedro Pais de. *Direito da Sociedade da Informação: Protecção de dados pessoais e direito à privacidade*. Coimbra: Coimbra Editora, 1999. v. I. p. 245.