UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

Segurança da informação e a proteção contra a violação de dados pessoais: A confidencialidade no Direito do Consumidor

Guilherme Damasio Goulart

Porto Alegre, Dezembro de 2012

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

Segurança da informação e a proteção contra a violação de dados pessoais: A confidencialidade no Direito do Consumidor

Guilherme Damasio Goulart

Dissertação apresentada no Programa de Pós-Graduação em Direito da UFRGS, como requisito parcial para a obtenção do grau de Mestre em Direito.

Orientação:
Prof. Dr. César Viterbo Matos Santolim

Porto Alegre, Dezembro de 2012

AGRADECIMENTOS

Agradeço, inicialmente, à Universidade Federal do Rio Grande do Sul e ao Programa de Pós-Graduação em Direito, que representam a excelência no estudo do Direito no Brasil, principalmente por meio da dedicação e competência de seus professores.

Esse trabalho só foi possível de ser realizado em função da orientação do Professor Doutor César Viterbo Matos Santolim, pioneiro na pesquisa do Direito relacionado ao fenômeno informático. Suas lições foram muito valiosas, especialmente por meio da disciplina de "Direito da Informática", a qual leciona com maestria no PPGD da UFRGS. Foi uma honra e alegria assisti-la por duas ocasiões: primeiro como aluno ouvinte e, após, já como mestrando. Agradeço por suas lições, pela paciência e pela compreensão.

Agradeço a Deus por ter colocado em minha vida pessoas tão especiais. Elas foram fundamentais para a realização de meu trabalho. Meus agradecimentos: ao amigo e professor Vinícius Serafim, meu irmão por escolha, que contribuiu com suas conversas, com o apoio intelectual e com suas lições de Tecnologia da Informação; ao professor Bruno Miragem que, antes mesmo de meu ingresso no PPGD da UFRGS, deu importantes conselhos; a todos os colegas de Pós-Graduação, principalmente a Fabiano Koff Coulon, João Pedro Scalzilli, Cássio Cavalli e José Rodrigo Dorneles Vieira. Agradeço especialmente ao último pelo grande apoio e pelas palavras de incentivo nas horas difíceis: fico feliz de tê-lo como amigo; ainda a Marcel Leonardi, Aila Corrent, Clemilson Dias, Guilherme Bertoni Machado, Kurt Rieck, André Fávero, André Peres e William Keffer.

Agradeço aos meus pais pela compreensão e pelo apoio. Agradeço à minha irmã pelo incentivo, e por ter presenteado-me com obras importantes para o meu trabalho. Agradeço, por fim, à minha esposa Tatiane, amiga e companheira, por entender minhas ausências, pelo apoio incessante e pelo imenso carinho.

Dedico esse trabalho ao meu avô, Vicente Silva Goulart (*in memorian*).

SUMÁRIO

RESUMO

O presente trabalho aborda a relação da proteção de dados pessoais e sensíveis com a proteção da privacidade no direito do consumidor. O amplo recolhimento de dados dos usuários, principalmente no comércio eletrônico e nas relações de consumo, permitem a violação de direitos. Nesse sentido, os fornecedores de serviços informáticos devem cumprir um dever geral de confidencialidade de dados, principalmente no armazenamento de dados dos usuários nos chamados "bancos de dados de informações de consumidores". Os danos causados pela violação da confidencialidade de dados também são abordados, com a consideração, inclusive, das situações de cruzamento de dados. Por fim, são abordadas, também, as causas de exclusão de responsabilidade na falha de proteção de dados.

Palavras Chave – Privacidade - Dados pessoais e dados sensíveis - Segurança da informação - Direito do consumidor - Violação da privacidade e confidencialidade – Internet e Sociedade da Informação.

ABSTRACT

This study examine the relationship between the personal and sensitive data protection with the privacy protection in information society and in consumer law. The user data collection, especially in e-commerce and consumer relations, allows a broader rights violation. In this way, computer services providers must comply with a general duty of confidentiality, mainly in the storage of user data in so-called "databases of consumer information". Caused harms in confidentiality breach is also discussed, considering the data correlation. Finally, will be discussed causes of liability exclusion in data protection failures.

KeyWords - Privacy - Personal and sensitive data - Information Security - Consumer Law - Privacy and Confidentiality breach - Internet and Information Society.

INTRODUÇÃO

Um dos aspectos relevantes acerca da sociedade da informação diz respeito à proteção da confidencialidade de dados pessoais e sensíveis. As novas tecnologias proporcionam, de uma forma ampla e frequente, a violação da privacidade dos usuários. Isso pode ocorrer tanto na forma da violação de sigilo de comunicações ou correspondência, ou ainda por meio do monitoramento de hábitos e também por intermédio da coleta de vários tipos de informações sobre as pessoas.[1]

Para esse trabalho será estabelecida a ligação da ideia de proteção de dados pessoais com o conceito de segurança da informação e confidencialidade. Um dos atributos da segurança da informação, como será visto, é justamente a confidencialidade. O ponto relevante, portanto, é que um dos efeitos do descumprimento do dever de confidencialidade de dados ocorre à medida que seu não cumprimento, via de regra, tem como consequência a violação da privacidade e da intimidade dos usuários.

A sensibilidade e a confidencialidade das informações armazenadas em bancos de dados de consumo também merecem estudo. O vazamento, o acesso e a alteração não autorizados de tais informações podem afetar não somente os direitos fundamentais dos usuários bem como a própria atividade das empresas.

O atual armazenamento indiscriminado e constante de informações dos consumidores, principalmente aquele realizado por meio de bancos de dados de

1 CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. Revista de Direito do Consumidor, São Paulo, n. 46, abr.-jun./2003, p. 78.

consumo, constitui uma grave ameaça à privacidade. Além do mais, a disposição do § 2º do art. 43 do CDC, no que se refere à comunicação da abertura dos referidos cadastros, muitas vezes não é cumprida. Ainda, muitos ilícitos iniciam-se com a coleta de dados pessoais para a sua futura utilização em falsificações de documentos, compras fraudulentas de produtos e operações bancárias.

Se, por um lado, é possível notar um certo descontrole no tratamento de dados pessoais por parte das empresas, por outro, há uma banalização da privacidade na Internet. Cada vez mais, os indivíduos abdicam voluntariamente de sua intimidade e privacidade para fazerem parte de certos grupos e de redes sociais. É requisito para a participação em tais ambientes que o indivíduo exponha sua privacidade, em um comportamento praticamente performático.

As empresas têm nos dados pessoais de clientes, por sua vez, um valoroso ativo informacional. Com eles é possível verificar tendências, projetar cenários, prever potenciais variações de estoques, iniciar campanhas personalizadas de venda, realizar campanhas geograficamente adaptadas, etc. Igualmente a combinação cruzada dos dados pessoais, pode indicar informações e tendências até então desconhecidas. O armazenamento e o processamento de um número cada vez maior de informações pessoais gera, por consequência, o risco sempre presente de perda e acesso não autorizado de tais informações[2]. A informação passa a ser vista, inclusive, como uma *commodity*.

Diante desse panorama, o trabalho versará, na primeira parte, sobre uma ideia de risco na sociedade da informação, com a consideração de questões envolvendo a tomada de decisões nesse ambiente além da regulação do espaço virtual. Serão visitados alguns conceitos atinentes aos atributos de segurança da informação, bem como ao controle acesso. Após, o problema da privacidade nos

2 Neste sentido ver CADKIN, John; COURSON, J. Zachary; SOMA, John T. Corporate privacy trend: the "value" of personally identifiable information ("PII") equals the "value" of financial assets. *Richmond Journal of Law & Technology*. Volume XV, Issue 4. 2009. Disponível em <http://law.richmond.edu/jolt/v15i4/Article11.pdf>. Acesso em: 15 jun. 2009, p. 5-6.

meios digitais será tratado, com a consideração da vulnerabilidade geral dos usuários, a diferenciação entre dados pessoais e sensíveis além do controle de dados pelos próprios usuários.

Na segunda parte do trabalho será relacionada a proteção de dados pessoais com o atendimento de um dever geral de confidencialidade no direito do consumidor. Será abordada a importância da boa-fé e da confiança despertada nos usuários, bem como a importância dos termos de uso dos serviços e o armazenamento de dados nos bancos de dados de informações de consumidores. Após, o dever de confidencialidade de dados será entendido com a consequente consideração dos danos provenientes de sua violação para, após, verificar os casos de exclusão da responsabilidade pela não proteção de dados pessoais.

Parte I - O valor da informação digital para a sociedade da informação

A sociedade da informação, baseada na massificação do uso e na transmissão da informação digitalizada, influenciou, e ainda influencia, diretamente a ciência jurídica. Roberto Senise Lisboa faz um paralelo interessante acerca da evolução do direito entre a sociedade industrial e a sociedade da informação[3]. A evolução da fábrica e da economia, baseada nesses meios de produção, provocou diversos impactos jurídicos, dentre os quais, os mais importantes são citados por ele: o aparecimento e a evolução do contrato de prestação de serviços civis predisposto e de adesão; a repersonalização da família moderna; a maior participação popular no processo político, social e econômico; o advento de normas jurídicas de ordem pública e de cláusulas gerais de contratação; o advento do contrato coletivo de trabalho; a insuficiência do sistema de responsabilidade civil fundada na culpa; a insuficiência dos vícios redibitórios para a defesa do consumidor. [4]

Entre as diversas modificações no direito apontadas pode-se citar: a transnacionalização[5] e o surgimento de blocos econômicos; o *e-commerce*; a economicidade da informação; a formação de bancos de dados; a transferência eletrônica de dados e o estabelecimento de normas comunitárias para uniformização legislativa.[6] O fenômeno da massificação do uso da tecnologia da informação e também da Internet, influenciou todos os ramos do direito.[7]

3 LISBOA, Roberto Senise. Direito na Sociedade da Informação. *Revista dos Tribunais*. São Paulo, v. 95, n. 847, p. 78 – 95, maio/2006, p. 78

4 Idem, Ibid, p. 79.

5 Santolim aponta o caráter transnacional da rede, uma vez que "*qualquer pessoa possa estabelecer contato, inclusive de natureza negocial, com outra, pelo simples fato de estar conectado à rede, sem qualquer relação antecedente.*" SANTOLIM, Cesar Viterbo Matos. Os princípios de proteção do consumidor e o comércio eletrônico no direito brasileiro. *Revista de Direito do Consumidor*, São Paulo, n. 55, jul.-set./2005, p. 65.

6 LISBOA, Roberto Senise. Ibid, p. 84-85

7 Como exemplos, no Direito Penal, há a questão dos crimes digitais; no Direito Tributário a questão

A informação passa a ser o vetor dessa nova revolução. As empresas passam a ter nos ativos informacionais seus ativos mais valiosos. Se, antes, na revolução industrial[8], os bens físicos tinham maior valor para os negócios, na revolução informacional[9] esse papel passa a ser desempenhado pela informação. Nesse paradigma, a informação passa a ser um bem da vida a ser tutelado pelo direito[10].

---

da reavaliação dos fatos geradores; no Direito Comercial a questão do estabelecimento virtual, dos contratos comerciais e a própria reavaliação dos títulos de crédito; no direito do consumidor, a sua relação deste com todos os novos serviços e produtos oferecidos na Internet; no Direito Processual a questão das provas digitais e também do processo eletrônico; no Direito do Trabalho toda a questão do monitoramento de comunicações pelos empregadores e também do teletrabalho; no Direito Constitucional toda a ampla e vasta questão da proteção e extensão dos direitos e liberdades individuais, principalmente no que se refere à proteção da liberdade de expressão; no Direito da Propriedade Intelectual a proteção de marcas, softwares e também de filmes e músicas, hoje tão acessados pela Internet por grande parte dos usuários; no Direito Eleitoral também há a interessante questão da possibilidade das manifestações das pessoas nas redes sociais em período eleitoral bem como da regulamentação da propaganda além do próprio fato das eleições, no Brasil, terem todo o seu processo realizado em meios digitais e assim por diante. Sobre a influência da chamado Direito Virtual com os ramos do Direito ver a belíssima lição de ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Belo Horizonte: Del Rey, 2005, p. 40 a 48. Ver também LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 35, quando diz que seriam oito as grandes áreas do Direito da Informática: regulação dos bens de informação, proteção de dados pessoais, regulação jurídica da Internet, propriedade intelectual e informática, delitos informáticos, contratos informáticos, aspectos trabalhistas da informática e valor probatório dos suportes atuais de informação. No mesmo sentido ver RUIZ, Carlos Barriuso. *Interacción del derecho y la informática*. Madrid: Dykinson, 1996, p. 64.

8 Cláudia Lima Marques destaca também que a "*a primeira crise do contrato nasceu, na Revolução Industrial, com a massificação da produção e da distribuição indireta, depois do primeiro contrato standard e foi respondida pelo direito do consumidor.*" Já a segunda crise do contrato, teria ocorrido desde o fim da 2ª Guerra Mundial, em que "*os bens juridicamente relevantes, ou a riqueza econômica, passaram a ser os bens móveis imateriais e os fazeres ou serviço de massa*". Como consequências há a diminuição da "*intervenção protetiva estatal*" e ao mesmo tempo uma deslegitimação dos poderes estatais culminando no "*renascimento da autonomia da vontade, dos árbitros e dos meios alternativos de solução de controvérsias, legitimando as chamadas regras do mercado e da lei dos mercadores (lex mercatoria), concentrando ainda mais o poder nas empresas mundiais e acompanhado da revolução das relações virtuais da sociedade da informação*". (*grifo nosso*). MARQUES, Cláudia Lima. A chamada nova crise do contrato e o modelo de direito privado brasileiro: crise de confiança ou de crescimento do contrato. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual*. São Paulo: RT, 2007, p. 22 a 24.

9 Também chamada por Vittorio Frosini de segunda revolução industrial. FROSINI, Vittorio. *Cibernética, Derecho y Sociedad*. Madrid: Tecnos, 1978, p. 97.

10 Os estudos envolvendo a relação entre Direito e Informática ou Direito e Cibernética não são novos. Na Europa, na segunda metade do século XX, iniciam-se os estudos do chamado "Direito

Nas palavras de Lorenzetti, na economia digital a informação passa a ser um bem comercializável. [11]

Nesse rumo, é inafastável a lição de Santolim, ao afirmar que o estudo de um "Cyberlaw" não pretende que sejam refeitas todas as categorias, os conceitos e os princípios. Ressalta ele que "*Esta solução somente seria aceitável se restasse demonstrada a incapacidade dos modelos jurídicos vigentes em assentar as condições para sua funcionalização em relação às novas tecnologias da informação*".[12] Vê-se que o problema é por demais complexo, não existindo uma resposta única e clara na atualidade.[13]

A pós-modernidade[14] causa uma inquietação nos juristas à medida que a eficiência das categorias jurídicas parece estar em xeque. O desafio já foi sentido por Cláudia Lima Marques ao afirmar que a pós-modernidade traz o ceticismo no que diz respeito *"à capacidade da ciência do direito de dar respostas adequadas e gerais aos problemas que perturbam a sociedade atual e modificam-se com uma velocidade assustadora".* É necessária a proposição de *"uma nova jurisprudência*

Artificial" em oposição a um "Direito Natural". O Direito Artificial estaria vinculado ao estudo da filosofia matemática, da lógica simbólica e que levaria o jurista a efetuar um trabalho de "*redução do problema jurídico a sua dimensão lógica."* cf. FROSINI, Vittorio. Ibid, p. 24-26. Da mesma forma, o estudo da cibernética (vista como a ciência de controle e da comunicação entre os animais e as máquinas) foi utilizado por Wiener como modelo para a criação de um "*esquema geral de interpretação que pode ser aplicado também à compreensão de estruturas sociais...*". Outros estudos nesta linha apareceram com a chamada Jurimetria, principalmente a partir do artigo de Lee Loevinger "*Jurimetrics: The Next Step Forward*" publicado na Minesota Law Review de 1949. A jurimetria tinha, conforme destaque de Frosini, a intenção de aplicar métodos da ciência no campo do Direito, principalmente, as novas tecnologias de automatização e da eletrônica. Idem, p. 29-31.

11 LORENZETTI, Ricardo L.. *Comércio Eletrônico*. São Paulo: RT, 2004, p. 54-55

12 SANTOLIM, Cesar Viterbo Matos. Ibid, p. 54.

13 LORENZETTI, Ricardo L.. Ibid, p. 79.

14 Ao falar sobre a pós-modernidade, Roberto Senise Lisboa ensina que: "*A pós-modernidade, impulsionada pelo desenvolvimento tecnológico que trouxe a chamada "globalização", consequência de uma contratação massiva transnacional realizada por diversos meios, inclusive o eletrônico, continua por trilhar caminhos que levem a uma maior segurança nas relações negociais (o meio da operação tornou-se complexo para todos e, sobretudo, um grande "desconhecido" sob a perspectiva do conhecimento do leigo) e a minoração da desconfiança decorrente de atos externos à contratação que acabam por influir decisivamente no equilíbrio jurídico...*" LISBOA, Roberto Senise. Tecnologia, confiança e sociedade. Por um novo solidarismo. In: PAESANI, Liliana Minardi (coord). *O Direito na Sociedade da Informação II*. São Paulo: Atlas, 2009. cap III, p. 63.

dos valores, uma nova visão dos princípios do direito civil, agora muito mais influenciada pelo direito público e pelo respeito aos direitos fundamentais dos cidadãos".[15] A chamada *"crise da pós modernidade"* também é assim vista como uma *"crise de desconfiança do direito",* sendo que a reação deve vir *"por meio do direito privado como instrumento de realização das expectativas legítimas do homem comum, o leigo, o consumidor."*[16]

Cláudia Lima Marques propõe também que a chamada crise da pós-modernidade é entendida por alguns como uma crise de *"desconstrução, de fragmentação, de indeterminação, à procura de uma nova racionalidade, de desregulamentação e de deslegitimação de nossas instituições, de desdogmatização do direito; para outros, é um fenômeno de pluralismo e relativismo cultural arrebatador a influenciar o direito."*[17]

e formas, do direito à diferença, da 'euforia do individualismo e do mercado', da globalização e da volta ao tribal, é também a realidade da substituição do Estado pelas empresas particulares, de privatizações, do neoliberalismo, de terceirizações, de comunicação irrestrita, de informatização e de um neoconservadorismo. […] Realidade de perda dos valores modernos, esculpidos pela revolução burguesa e substituídos por uma ética meramente discursiva e argumentativa, de legitimação pela linguagem, pelo consenso momentâneo e não mais pela lógica, pela razão ou somente pelos valores que apresenta." p. 168.

Se a informação é o ativo mais valioso na pós-modernidade[18], a proteção de sua confidencialidade passa a ser igualmente relevante.[19] A proteção da confidencialidade das transações realizadas na Internet é peça fundamental para o desenvolvimento dos negócios neste ambiente e para garantir também a confiança dos envolvidos. Esses argumentos justificam a questão da valorização da segurança da informação como tema a ser estudado. A observância da manutenção de medidas de segurança da informação, principalmente no que diz respeito à proteção de dados pessoais e sensíveis, atende também ao interesse de estabilidade e organização da sociedade. Ambientes inseguros, desiguais e desiquilibrados, também do ponto de vista de segurança da informação, fazem com que apareçam conflitos e a insegurança. Com isso, "*esvai-se o horizonte de sustentação da sociedade e suas instituições.*"[20]

Além do mais, a falta de cuidado com segurança da informação pode representar um empecilho para o desenvolvimento. Como os incidentes de segurança da informação também representam perdas financeiras, mesmo quando

---

18 Vittorio Frosini, em 1978, já afirmava: "*Como hemos sostenido, la simple presencia física, em continuo proceso de multiplicación de los computers em el sistema productivo estadounidense es por sí misma el sintoma de una transformación económica, tecnológica y social de una importância quizás sin precedentes, que señala el advenimiento de una nueva dimensión de la actividad humana y no solo su reducción a una dimensión única, como há sido proclamada por Marcuse.*" FROSINI, Vittorio, Ibid, p. 100.
No mesmo sentido, e mais recentemente, ver MARQUES, Cláudia Lima. Ibid, p. 174. "*Se, na Idade Média, os bens economicamente relevantes eram os bens imóveis, na idade moderna, o bem móvel material indiscutível que hoje, na idade atual pós-moderna, valorizado está o bem móvel imaterial (software, etc) ou o desmaterializado "fazer" dos serviços, da comunicação, do lazer, da segurança, da educação, da saúde, do crédito*". No mesmo sentido

19 Sem perder de vista que "*O ponto de referência para uma análise pós-moderna dos institutos jurídicos passa a ser, portanto, o sujeito e, nesse sentido, abre-se espaço para a proteção daquilo que lhe é mais caro, como forma de assegurar a sua dignidade, valor supremo. Mais do que liberdade e igualdade, busca-se a dignidade como valor fonte, a qual garantirá liberdade e igualdade efetivas*". BARBOSA, Fernanda Nunes. *Informação: direito e dever nas relações de consumo*. São Paulo: RT, 2008, p. 75.

20 Ver JUCÁ, Francisco Pedro. Responsabilidade social e sustentabilidade. In: MESSA, Ana Flávia; THEOPHILO NETO, Núncio; THEOPHILO JÚNIOR, Roque (coord.). Sustentabilidade ambiental e os novos desafios na era digital: Estudos em homenagem a Benedito Guimarães Aguiar Neto. São Paulo: Saraiva, 2011, p. 29: "*Neste tempo de relativização de direitos decorrente de restrições em favor dos interesses gerais, assistimos à elevação de princípios fundados na solidariedade, não mais como decorrência da genorosidade dos espíritos, mas no interesse da estabilidade da organização e do processo da sociedade.*"

se trate violações de dados pessoais, medidas de segurança também representam medidas em direção ao desenvolvimento[21].

A Internet é comumente relacionada com o chamado “espaço virtual”. E esse “espaço virtual” - ou ciberespaço -, segundo Ricardo Lorenzetti, possui características que merecem destaque, tais como:

> “*autônomo, no sentido de que funciona segundo as regras de um sistema auto-referente, como já assinalamos. Também é “pós-orgânico”, uma vez que não é formado por átomos, nem segue as regras de funcionamento e de localização do mundo orgânico: tratam-se de bits. Tem uma natureza “não territorial” e comunicativa, um “espaço movimento”, no qual tudo muda a respeito de tudo, ou seja, o “espaço virtual” não é sequer assemelhado ao espaço real, porque não está fixo, nem é localizável mediante o sentido empírico como, por exemplo, o tato*”.[22]

Esse “*espaço*” desterritorializado - não-lugar – também é notado pelo autor, quando destaca seus aspectos transnacionais[23] e atemporais.[24] A Internet, por ser

21 DALLARI JÚNIOR, Hélcio De Abreu; GARCEZ, Robson do Boa Morte. Desenvolvimento sustentável e o direito baseado em evidências. In: MESSA, Ana Flávia; THEOPHILO NETO, Núncio; THEOPHILO JÚNIOR, Roque (coord.). Sustentabilidade ambiental e os novos desafios na era digital: Estudos em homenagem a Benedito Guimarães Aguiar Neto. São Paulo: Saraiva, 2011. Os autores destacam, entre as Metas de Desenvolvimento do Milênio, definidas em 2000 pela ONU, justamente o “*estabelecimento de uma parceria mundial para o desenvolvimento*”, p. 258. A questão de parcerias globais são necessárias em função do aspecto global da segurança da informação.

22 LORENZETTI, Ricardo Luis. Ibid, p. 30.

23 Sobre a utilização do termo “transnacional” ele é semanticamente ambíguo e abrangente, segundo Marcelo Neves. Ele poderia ser usado não só para referir-se a ordens, instituições e problemas transnacionais (em sentido estrito e amplo) mas também a ordens, instituições e problemas internacionais ou supranacionais. O conceito está baseado principalmente na ideia de questões que “ultrapassam as fronteiras do Estado”. Igualmente o termo também refere-se a ordens normativas “*privadas ou quase públicas que surgem e se desenvolvem no plano global independentemente tanto do Estado e de suas fronteiras*”. Cf. NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: Wmf Martins Fontes, 2009, p. 84.

24 LORENZETTI, Ricardo Luis. Ibid, p. 31. A não territorialidade é uma característica comum citada por aqueles que escrevem sobre o ciberespaço. O filósofo francês Pierre Levy diz que mesmo em uma abordagem limitada os problemas principais do ciberespaço perante os estados seriam referentes à soberania e territorialidade, uma vez que nas palavras do autor “*o Estado moderno*

uma rede transnacional, compõe uma verdadeira "*ordem cibernética*". Ela pode ser considerada, inclusive, como um ordenamento transnacional, pela sua natureza e principalmente por, em alguns casos, ficar imune à legislação de alguns países[25]. Pela sua natureza transnacional, há a possibilidade do ordenamento jurídico de um país não possuir alcance nos fatos nela [na Internet] ocorridos, mesmo que os efeitos venham a ocorrer dentro do próprio território do país em questão.[26]

Apoiando essa ideia, Têmis Limberger e Ricardo Mena Barreto apontam o que chamam de "triplos obstáculos" surgidos no âmbito do comércio eletrônico: os "obstáculos 3-D" representados pela desmaterialização, desterritorialização e despersonalização.[27]

Sobre o uso das Novas Tecnologias da Informação e Comunicação (TIC) no Brasil, anualmente, o Comitê Gestor da Internet realiza uma pesquisa sobre o assunto[28]. A pesquisa, publicada em 2011, abrange os dados de 2010 e levanta

---

baseia-se, sobretudo na noção de território" em LEVY, PIERRE. *Cibercultura*. São Paulo: Editora 34, 1999, p. 204. Mais adiante o autor destaca que o ciberespaço *"possibilita que as leis que dizem respeito à informação e à comunicação (censura, direitos autorais, associações proibidas etc), sejam contornadas de forma muito simples. […] Como os sujeitos de um Estado podem conectar-se a qualquer servidor do mundo, contanto que tenham um computador ligado à linha telefônica, é como se as leis nacionais que dizem respeito à informação e à comunicação se tornassem incompatíveis*", p. 204. Sobre toda a abordagem filosófica do ciberespaço ver esta obra e também "O que é virtual", do mesmo autor.

25 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva. 2012, p. 32, "*Apenas isso, porém não bastaria para justificar o estudo do tema. É evidente que a Rede modificou o modo como vivemos e interagimos. O mesmo, no entanto, pode ser dito telégrafo, do telefone, do rádio e da televisão. A questão fundamental é que, ao contrário dessas outras tecnologias, a Internet desafia de modo único a capacidade de controle por parte dos estados.*"

26 MARQUES, Cláudia Lima. *Contratos..., p.* 187. A autora entende que a crise do contrato na pós-modernidade tem entre suas características a desterritorialização e a diminuição da intervenção estatal o que causa o "*aumento da internacionalidade e da regulamentação paraestatal e não cogente das relações*".

27 BARRETO, Ricardo Menna; LIMBERGER, Têmis. Ciberespaço e obstáculos 3-D: Desafios à concretização dos direitos do consumidor. *Revista de direito do consumidor*, São Paulo, n 79, jul.-set./2011, p. 103. Anteriormente, FROSINI, Vittorio. Ibid, p. 100-101, já afirmara que: "*Esta nueva dimensión está marcada, sin duda alguna, por una despersonalización em el aspecto decisorio dentro del proceso productivo. Con la nueva capacidad de cálculo, abierta por el análisis electrónico de los datos de venda, de demanda y de beneficio, el flujo de mercaderías queda regulado de acuerdo con un principio de rigor racional, que ua no es el de lá intuición general y de lá dedicación infatigable del dirigente de empresa individual.*"

28 COMITÊ GESTOR DA INTERNET NO BRASIL. *TIC Domicílios e Empresas 2010. Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo, 2011. Disponível em:

questões interessantes sobre a amplitude e o alcance das TIC no Brasil. O Brasil possui 35% dos domicílios com computadores, sendo que 27% dos domicílios possui acesso à Internet. Entre os motivos que indicam a falta de computador nos domicílios, 74% das pessoas apontam o seu custo elevado. Foi apontado também, por 38% das pessoas, a não necessidade/não interesse e 26% disseram não saber usar o computador.[29] Naturalmente o custo é um grande problema. No entanto, praticamente um terço das pessoas também apontaram a falta de informação sobre o uso. Isso destaca a grande vulnerabilidade técnica nos futuros usuários da rede. Essa questão motiva também a necessidade das empresas que oferecem serviços na Internet, realmente ficarem atentas para o nível e a qualidade das informações que fornecem.

A pesquisa também apresenta dados sobre o uso do comércio eletrônico. A cada ano, nas classes mais altas, aumenta o número de pessoas que compram pela Internet. Na classe A, em 2009, 59% das pessoas realizavam compras no comércio eletrônico enquanto o número apurado para 2010 foi de 63%. No lado oposto, apenas 4% das pessoas nas classes D e E compraram pela Internet. Entre os motivos expostos pelas pessoas para não fazerem compras pela Internet, a pesquisa aponta que 29% dos entrevistados demonstraram preocupação com a proteção da segurança e privacidade, inclusive apontando "*terem receio de fornecer informações pessoais ou de usar o cartão de crédito pela Internet.*"[30] Esse último dado também justifica um estudo mais aprofundado dos problemas relacionados à segurança na Internet, uma vez que ela está diretamente relacionada com o nível de confiança que as pessoas depositam nos serviços.

A) Risco na Sociedade da Informação

<http://www.cgi.br/publicacoes/pesquisas/index.htm>. Acesso em: 10 Jan. 2012.

29 Evidentemente aqui as pessoas deram mais do que uma resposta.

30 COMITÊ GESTOR DA INTERNET NO BRASIL. Ibid, p. 168.

São ingênuos aqueles que pensam que o avanço da tecnologia é sempre livre de riscos. Atualmente, há quem diga que existe uma "*cegueira econômica dos riscos*"[31]. Em uma ânsia de aumentar mais e mais a produtividade é comum que se abstraiam os riscos vinculados a uma determinada tecnologia. Segundo Ulrich Beck "*A primeira prioridade da curiosidade técnico-científica é a utilidade da produtividade sendo que só depois - e com frequência ainda nem sequer em segundo lugar - pensa-se nos perigos vinculados a ela*"[32]. Com isso, mesmo que se tenha ciência dos riscos do progresso há, cada vez mais, "*a consciência da impossibilidade de deter tal progresso, mesmo se este não se apresenta mais com os prognósticos somente positivos*"[33].

Uma das questões que merecem reflexão é até que ponto o direito, com o seu tempo de evolução próprio, deve alinhar-se com a rápida evolução da tecnologia. O desafio não é simples[34]. Na verdade, a evolução tecnológica pode trazer aspectos imprevisíveis de adequação entre as categorias legais existentes e o fato jurídico advindo das relações tecnológicas.[35] Nas palavras de Ronaldo Lemos "*a questão começa a tornar-se relevante quando se inicia a partir do ponto em que a chave é se a nova realidade deve adaptar-se ao velho direito ou se o velho direito deve adaptar-se à nova realidade*".[36]Da mesma forma, o chamado "Direito Virtual" ou "Direito da

31 BECK, Ulrich. *La socied del riesgo: Hacia una nueva modernidad*. Barcelona: Editorial Paidós, 1998, p. 67.

32 BECK, Ulrich. Ibid, p. 67

33 RODOTÀ, Stefano. A vida na sociedade da vigilância: A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 41.

34 MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 179. A autora destaca que nos tempos pós-modernos "*é necessária uma visão crítica do direito tradicional, é necessária uma reação da ciência do direito, impondo uma nova valorização dos princípios, dos valores de justiça e equidade e, principalmente no direito civil, do princípio da boa-fé objetiva, como paradigma limitador da autonomia da vontade.*"

35 Neste sentido observar a lição de MANDEL, Gregory N. History Lessons for a General Theory of *Law and Technology.* Minnesota Journal of Law, Science & Technology, Vol. 8, n. 20, Minneapolis, p. 552, 2007. Disponível em: <http://ssrn.com/abstract=1012612>. Acesso em: 12 Fev. 2012.

36 LEMOS, Ronaldo. *Direito, tecnologia e cultura*. Rio de Janeiro: FGV Editora, 2005, p. 13. Igualmente, Bruno Miragem nota que "*Na ciência do Direito, o exame do fenômeno da Internet concentra-se, sobretudo, pela preocupação com a efetividade das normas jurídicas de direito positivo às relações da vida estabelecidas por intermédio da Internet.*" MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009.

Tecnologia da Informação", lida com um (entre vários) desafio: "*apresentar soluções para as novas situações de conflitos trazidas pela virtualização de grande número de atos jurídicos*".[37] Assim, "*a nova realidade não se adaptará ao velho direito mas sim continuará a criar novos desafios, dilemas e problemas.*"[38] Todavia, é inegável que os juristas inclinam-se a analisar os problemas baseando-se em conceitos jurídicos herdados do passado, sentindo-se "*mais habituados a operar com materiais dados ou estabelecidos (de lege data) do que avançar na perspectiva de lege ferenda*"[39].

O fenômeno informático pode seduzir demais o estudioso do fenômeno jurídico. Estender-se demais em temas tecnológicos é bastante comum na doutrina quando se trata do Direito aplicado à Tecnologia da Informação. Tal erro ofusca e desvia o foco do estudo jurídico. Essa inquietação foi percebida por Ricardo Luiz Lorenzetti:

> "*Não é raro escutar a um civilista que fale sobre dano genético estender-se amplamente sobre temas médico-genéticos; a outro, que trate de temas empresariais enveredar nos aspectos econômicos; e quem trata de contratos por computador, iniciar um desenvolvimento técnico sobre informática. Este civilista teve contacto com outra ciência, talvez não muito claro, e fica assombrado com a quantidade de novas coisas que aprendeu e que poderia aplicar ao Direito Privado.*"[40]

---

37 ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Belo Horizonte: Del Rey, 2005, p. 9.

38 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 42. O autor continua afirmando que "*E tais questões não podem ficar sem solução jurídica adequada. O papel do Direito é a consecução da Justiça entre os homens, fator fundamental do convívio social e a realização do individual comum, pouco importando que as relações ocorram por meio de uma ferramenta tecnológica que pareça separada da realidade. O que interessa é que as consequências são sentidas no mundo real - e precisam de uma resposta eficiente.*"

39 Cf. LUÑO, Antonio-Enrique Pérez. *Manual de informática y derecho*. Barcelona: Ariel, 1996, p. 17. Continua o autor afirmando que "*Entre los aspectos novedosos de las nuevas tecnologías que reclaman la capacidad programadora del jurista, ocupa un lugar destacado la necesidad de establecer nuevos marcos teóricos en los que alojar los problemas y cuestiones surgidos de la interacción entre el Derecho y la Informática.*"

40 LORENZETTI, Ricardo Luis. *Fundamentos do Direito Privado*. São Paulo: RT, 1998, p. 56

A lição de Lorenzetti é semelhante a de Gregory N. Mandel quando este diz que:

> "*A segunda lição história a respeito das questões da lei e tecnologia, é a necessidade dos decisores verem além da tecnologia envolvida na disputa e focar nos aspectos legais da questão. Algumas vezes os decisores têm a tendência de ficarem ofuscados pelas conquistas tecnológicas espetaculares.*"[41]

A informatização da sociedade e a sua consequente dependência da Internet fazem com que seja necessário manter a grande infra-estrutura tecnológica que sustente a chamada Sociedade da Informação. Acerca disso, José de Oliveira Ascensão destaca o movimento crescente de concentração dos responsáveis pelas infraestruturas de telecomunicações e seus operadores. Haveria, nas palavras do autor, a possibilidade de formação de *"grandes oligopólios horizontais e grandes conglomerados globais"*[42]. A concentração de poder nas grandes empresas pode representar um aspecto prejudicial à proteção dos direitos do consumidor, seja pelo seu caráter transnacional, seja pela dificuldade de aplicação das normas legais nesse contexto[43]. Além do mais, tais empresas possuem um potencial muito grande de armazenamento de informações pessoais e sensíveis de seus usuários, o que expõe todos a um risco em casos de vazamentos de dados pela concentração de muitos dados em poucos locais.

Para fins desse trabalho, é possível apontar dois conceitos de riscos, sendo o primeiro:

---

41 MANDEL, Gregory N. Ibid, p. 650.

42 ASCENSÃO, José de Oliveira. Ibid, p. 70. Tal observação é apoiada, atualmente, pelo impressionante crescimento da empresa Google, que concentra o mercado de buscas na Internet e em 2010 foi considerada a marca mais valiosa do mundo, conseguindo ultrapassar marcas há muito tempo consolidadas. Ver RANKING APONTA GOOGLE COMO MARCA MAIS VALIOSA DO MUNDO. *Idg Now*. 29 de Abril de 2010. Disponível em: <http://idgnow.uol.com.br/mercado/2010/04/29/ranking-aponta-google-como-marca-mais-valiosa-do-mundo/>. Acesso em: 29 Abr. 2010.

43 Ver RUIZ, Carlos Barriuso, Ibid, p. 148, quando afirma que "*La información, como decimos, confiere poder y por tanto, no puede ser monopolizada o detendata sin los debidos controles.*"

> "*quando um ator sabe das consequências de seu agir e procede na consciência tanto do possível sucesso de sua ação como dos possíveis danos. O segundo conceito, que podemos chamar de conceito amplo de risco, vai mais além e inclui aquilo que Luhmann chamaria de perigo.*"[44]

Bruseke, ao avaliar o risco, ensina que:

> "*esta categoria de eventos é sempre, para o homem, uma ameaça hipotética. Existem outros eventos avaliados como chances, sorte, bênção, graça, etc., que apesar de ter a mesma estrutura contingente como o risco, ocultam, facilmente, seu caráter, porque são vividas de forma positiva. O homem tem a compreensível inclinação de atribuir as contingências positivas a seu próprio mérito e buscar a culpa para as contingências negativas fora da própria responsabilidade.*"[45]

A ideia de uma sociedade de risco é baseada também em uma sociedade que tende a evitar o risco. O homem passa a se preparar para novos "*padrões de possibilidades relevantes*". A sociedade prepara-se para enfrentar o risco com uma série de estudos e ferramentas de previsão, justamente, na intenção de evitar os efeitos negativos da concretização de um risco.[46] Na relação específica com o ambiente digital, nos dizeres de Lorenzetti, "*a rede dilui a potencialidade dos processos de identificação e de autoria*"[47], o que amplia a ideia de risco nesse ambiente.[48]

---

44 BRÜSEKE, Franz Josef. Ibid. p. 86-87.

45 Idem. Ibid, p. 87. Sobre a noção de risco e de possibilidade-previsibilidade dos acontecimentos, Brüseke diz também que "*Nem tudo é possível, mas muito mais do que comumente imaginamos. Sabemos, na verdade, muito pouco sobre o possível. Este acontecimento incipiente leva-nos a esperar demais e, às vezes, a esperar menos ou, em outros momentos, esperar coisas impróprias.*", p. 100.

46 Idem. Ibid, p. 100.

47 LORENZETTI, Ricardo L.. *Comércio Eletrônico*. São Paulo: RT, 2004. p 46.

48 Pelo perigo constante de não ser possível identificar os autores dos danos.

É necessário destacar que todos os produtos e serviços possuem riscos sendo necessária uma análise acerca do custo de correção desses riscos. Tomando um carro como exemplo, alguém poderia defender que seja priorizada totalmente a segurança desse produto, transformando-o em um tanque de guerra. Se isso fosse feito, o custo dessa operação seria muito alto além do produto final ser pouco funcional. Por isso, os fornecedores fazem um balanço de risco-benefício que "*deve considerar as expectativas criadas no consumidor.*"[49]

Na sociedade da informação e no comércio eletrônico também são analisados os aspectos de risco, benefício e funcionalidade dos produtos e serviços. Os dados estariam, por certo, muito mais seguros em computadores fechados em cofres de banco e desconectados da Internet. Porém, funcionalmente, seria muito mais difícil acessar e processar esses dados. Nesse sentido, há que se considerar o balanceamento entre a segurança e a produtividade, ou ainda, entre segurança e funcionalidade.

Por outro lado, sabe-se que em certas situações há uma supervalorização do risco digital, inclusive com pesquisas utilizando metodologias pouco científicas e com constatações incorretas. Um dos exemplos vem de uma declaração de um conselheiro de segurança cibernética do governo americano, no qual foi dito que "*digital Pearl Harbors are happening every day*." Paul Ohm, ao discorrer sobre o tema, destaca que:

> *"mesmo que a frase "Pearl Harbor digital" possa ser referida a diferentes coisas - os ataques com efeitos psicologicamente danosos, perdas horríveis de vidas, surpresa terrível [...] ou perdas financeiras do evento de 7 de Dezembro de 1941 - a afirmação representa um terrível exagero, independentemente do significado*

49 LORENZETTI, Ricardo L.. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 130. Continua o autor dizendo que "*el deber de seguridad se relaciona com los bienes del consumidor y con la persona*."

pretendido por Clarke." [50]

Isso denota o fato de que há uma relação psicológica entre o medo e a avaliação de riscos tecnológicos. É a chamada tecnofobia, sofrida por pessoas que sustentam um medo excessivo da tecnologia da informação[51]. É possível ver essa circunstância em uma pesquisa realizada na Inglaterra onde o medo do crime digital foi mais citado do que o medo de assaltos e roubos a carro. Nesse estudo mais de 21% das pessoas sentia-se mais vulnerável às ameaças digitais do que a outros tipos de ameaças físicas.[52]

Da mesma forma, o aumento do uso da tecnologia e a sua complexidade natural demonstra outra fragilidade: a de que caso o mundo fique "desplugado", perca-se o acesso a uma série de serviços essenciais que foram migrados para o mundo digital[53]. Ademais, sabe-se que há uma ansiedade em relação ao uso de tecnologia por algumas pessoas menos preparadas ou com menos conhecimento de tecnologia da informação. Todos que utilizam um computador já passaram por situações preocupantes como a perda de dados importantes, infecção por vírus de computador, caixas lotadas por *spams*, programas que param de funcionar repentinamente, etc. Essa ansiedade pode fazer com que se reaja desproporcionalmente, em alguns casos, às reais ameaças digitais, além do julgamento incorreto acerca da probabilidade de ocorrência de tais eventos.[54]

Diante de todo um novo panorama de risco, foi cunhada a expressão e-Compliance, que significa um novo padrão de conformidade legal que as empresas

50 OHM, Paul. The Myth of the Superuser: Fear, Risk, and Harm Online. *University of Colorado Law Legal Studies Research Paper* No. 07-14; UC Davis Law Review Vol. 41. No. 4. Apr., 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372>. Acesso em: 12 Fev. 2012, p. 1347-1348.

51 Idem. Ibid, p. 1364.

52 Claro que esta pesquisa deve ser encarada dentro da realidade do país pesquisado, bem como considerando o acesso às tecnologias. Sobre isso ver CARTER, Helen. Internet Crime Eclipses Burglary in Survey of Perceived Risks. *The Guardian*, 9 de Outubro de 2006. Disponível em: <http://www.guardian.co.uk/technology/2006/oct/09/news.crime>. Acesso: 10 Ago. 2011.

53 OHM, Paul. Ibid, p. 1365.

54 Idem. Ibid, p. 1367

precisam sustentar em função das mudanças nos sistemas legais, diante do que Gasser e Hauserman chamam de "digitalização".[55] Segundo esses autores seriam cinco[56] as principais áreas de risco sobre as quais o direito deve preocupar-se perante esse novo panorama. São elas:

a) Segurança - As questões de segurança são analisadas em relação à proteção de ameaças como vírus, worms, spyware, hackers e crackers bem como a perda e o furto de dados em dispositivos móveis. Existem múltiplos meios para a proteção da informação, sendo tais meios técnicos, administrativos e pessoais. Nesse sentido, esses meios devem estar adequados com requisitos legais e também com as regras regulatórias (políticas de uso de tecnologia e privacidade, por exemplo) assim impostas pelas próprias empresas.

b) Privacidade de dados - É um tema relacionado com segurança e deve observar todas as diretrizes regulatórias de privacidade atuais. Na Europa e nos EUA, por exemplo, as organizações precisam respeitar uma série de regulamentos em relação à privacidade, envolvendo desde deveres das empresas em respeitar a privacidade de seus empregados até a proteção de dados dos consumidores.

c) Proteção do consumidor - Abrange toda a questão da proteção do consumidor no comércio eletrônico e esbarra em problemas como a lei de qual país é aplicável em compras internacionais, além de toda a problemática sobre a formação e execução de contratos.

d) Propriedade intelectual – Por meio de novas tendências de colaboração e de uma cultura participativa, os modelos de negócios on-line passam a contar com uma massiva participação dos usuários na produção de conteúdos: é a chamada Web 2.0. Como consequência há a clara violação de direitos autorais, bem como os problemas relativos à responsabilização de intermediários pelas violações realizadas pelos seus usuários.

---

55 GASSER, Urs; HAUSERMAN, Daniel. E-Compliance: Towards a Roadmap for Effective Risk Management. *Berkman Center for Internet & Society at Harvard University*. 2007. Disponível em: <http://cyber.law.harvard.edu/publications/2007/ECompliance>. Acesso em: 12 Fev. 2012.

56 Sobre toda esta explicação ver GASSER, Urs; HAUSERMAN, Daniel. Ibid, p. 5 a 9.

e) Governança de conteúdo - Os provedores possuem um grande desafio em respeitar uma série de normas de diversos países que regulam a produção de conteúdo on-line. Os autores destacam, por exemplo, que na Suíça não são claras as questões de responsabilidade civil e criminal dos provedores acerca de publicação de conteúdos.[57]

Como o termo “cracker” já foi usado nesse trabalho, na referência aos riscos digitais, é necessário estabelecer seu conceito e sua diferença do termo “hacker”. O “Hacker” é uma palavra que representa a classificação objetiva, em relação ao nível de conhecimento técnico do agente sobre questões informáticas.[58] Já o termo “cracker” é relacionado com a motivação do agente, ou seja, são aquelas pessoas que possuem um alto nível de conhecimento técnico em informática; porém, possuem uma motivação de causar danos ou realizar ações maliciosas (como apropriação de senhas, invasão de sistemas, invasão de sites, etc).[59] Essa ressalva é feita pois é comum utilizar o termo hacker para indicar agentes que realizam ações criminosas ou que causam danos; no entanto, tal utilização é incorreta.

Toda a ideia de risco proporcionada pelas novas tecnologias, portanto, não deve ser desconsiderada. O conceito de risco, para o direito, é assim entendido por De Plácido e Silva:

---

57 Adiante, no item C.1, serão trazidos alguns elementos sobre o papel dos provedores.

58 Cf. VIANNA, Túlio Lima. Ibid. p 32. Ver também GELBSTEIN, Eduardo e KAMAL, Ahmad. Information *Insecurity: A survivel guide to the uncharted territories of cyber-threats and cyber-security*. New York: United Nations ICT Task Force and United Nations Institute for Training and Research, 2002, p. 25: “*Hackers are technically knowledgeable people who understand and write software, and know how to identify security weaknesses in products. This enables them to make other peoples’ software perform undesired functions, as well as to create tools to facilitate their exploits.*” No mesmo sentido ver a definição de cracker em ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. *Glossário da Sociedade da Informação*. APDSi: Lisboa, 2005. Disponível em: <http://www.apdsi.pt>: “*Pessoa que explora as falhas da segurança de um sistema com o intuito de violar a sua integridade, destruindo ou alterando a informação ali residente, ou ainda de copiar fraudulentamente os seus ficheiros. Nota: O pirata informático (cracker) é um entusiasta da informática (hacker) que usa os seus conhecimentos para fins indevidos.*”

59 Cf. VIANNA, Túlio Lima. Ibid. p 33. Ele ainda classifica os crackers como: Crackers de sistemas; crackers de programas; desenvolvedores de vírus, worms e trojans e por fim, os distribuidores de warez. No entanto, para este trabalho, como se disse, basta apenas a diferenciação entre os termos hacker e cracker.

> "*Na linguagem jurídica, o vocábulo exprime simplesmente o sentido de perigo ou do mal receado: é o perigo de perda ou de prejuízo ou o receio de mal, que cause perda, dano ou prejuízo. […] Mas, em sentido especial, fundado no perigo de perda, risco também exprime a própria responsabilidade ou o encargo acerca da perda ou do dano, trazido pelo risco.*"[60]

O direito reconhece a importância da análise do risco já há muito tempo. Alvino Lima, em seu trabalho clássico, ao comentar sobre a inovação da teoria da responsabilidade sem culpa, coloca como justificativas para esta, entre outras:

> "*a necessidade imperiosa de se proteger a vítima, assegurando-lhe a reparação do dano sofrido, em face da luta díspar entre as empresas poderosas e as vítimas desprovidas de recursos; as dificuldades, dia a dia maiores, de se provar a causa dos acidentes produtores de danos e dela se de deduzir a culpa, à vista dos fenômenos ainda não bem conhecidos na sua essência, como a eletricidade, a radioatividade e outros, não podiam deixar de influenciar no espírito e na consciência do jurista*".[61]

A doutrina da responsabilidade objetiva baseia-se na "necessidade de segurança da vítima"[62], principalmente quando ela não concorre para o resultado,

60 SILVA, De Plácido. *Vocabulário Jurídico*. Rio de Janeiro: Forense, 1987, p. 149.

61 LIMA, Alvino. *Culpa e Risco*. São Paulo: RT, 1960, p. 117-118. Traz ainda, mais adiante, como justificativas, "*o desequilíbrio flagrante entre os "criadores de risco' poderosos e as suas vítimas; os princípios de equidade que se revoltavam contra esta fatalidade jurídica de se impor à vítima inocente, não criadora do fato, o peso excessivo do dano muitas vezes decorrente da atividade exclusiva do agente, vieram-se unir aos demais fatores, fazendo explodir, intenso, demolidor, o movimento das novas ideias, que fundamentam a responsabilidade extracontratual tão somente na relação de causalidade entre o dano e o fato gerador;*"

62 A proteção contra a insegurança que a modernidade traz é um dos justificadores da teoria do risco. LIMA, Alvino. Ibid, p. 208-209. "*A teoria do risco, embora partindo do fato em si mesmo, para fixar a responsabilidade, tem raízes profundas nos mais elevados princípios de justiça e equidade. Ante a complexidade da vida moderna, que trouxe a multiplicidade dos acidentes que se tornaram anônimos, na feliz expressão de JOSSERAND, a vítima passou a sentir uma insegurança absoluta ante a impossibilidade de provar a culpa, em virtude de múltiplos fatores […] foi, pois, em nome dessa insegurança da vítima, cada vez mais evidente e alarmante, desta maioria dos indivíduos expostos aos perigos tantas vezes a serviço da cobiça humana...".*

quando agentes, criadores de risco, tiram proveito dessa atividade. Se os agentes colhem proventos de uma atividade arriscada é justo que se responsabilizem pelos encargos.[63] Na lição de Alvino Lima, ao definir a teoria do risco[64]-proveito:

> "*A questão da responsabilidade, que é mera questão de reparação dos danos, de proteção do direito lesado, de equilíbrio social, deve, pois, ser resolvida atendendo-se somente àquele critério objetivo; quem guarda os benefícios que o acaso de sua atividade lhe proporciona, deve inversamente, suportar os males decorrentes desta mesma atividade.*"[65]

O risco nas novas tecnologias é ampliado, em alguns casos, em face da sociedade ser, cada vez mais, praticamente obrigada a utilizá-las. A própria atividade bancária hoje é inimaginável sem o uso da Internet. Os clientes dos bancos praticamente não precisam mais comparecer às agências, em virtude da praticidade proporcionada pelas novas tecnologias. Quem possui um computador com acesso à Internet dificilmente deixará de utilizá-lo para acesso bancário, mesmo diante dos riscos da atividade. Nesse sentido, "*para novos inventos que surgem, criadores de atividades perigosas, que põem em risco a segurança individual, a consciência jurídico-social reclama um novo preceito.*"[66]

A.1 - Análise do Risco Digital

Dentro da atividade tecnológica de segurança da informação é muito comum que as empresas realizem a chamada "Análise de Risco Digital". Segundo Garfinkel

63 LIMA, Alvino. p. 124.

64 José de Aguiar Dias critica o termo "teoria do risco" dizendo que ela "*não compreende o que pretende exprimir. Muito mais precisa, se bem que limitada ainda pela relativa pobreza da linguagem técnica, é a expressão teoria do risco criado.*" DIAS, José de Aguiar. *Da responsabilidade Civil*. 8ª Ed. Rio de Janeiro: Forense, 1987, p. 85.

65 Idem. Ibid, p. 124.

66 LIMA, Alvino. Ibid, p. 345.

e Spafford, o foco de uma análise de risco digital abrange: a verificação do que se está tentando proteger; contra o que se está protegendo e quanto tempo, esforço e dinheiro será necessário para a implementação das proteções.[67]

Esse processo envolve a identificação dos ativos informacionais envolvidos em uma infraestrutura, a identificação das ameaças que atingem os ativos e suas vulnerabilidade, e o cálculo da probabilidade do risco – incluindo-se aqui o cálculo do custo financeiro de controle do risco[68]. As ameaças podem estar nas mais variadas formas envolvendo, entre outras: ameaças ambientais (fogo, terremotos, explosões); perda e avaria em computadores; epidemias e doenças; perda de infraestrutura básica (telefone, energia elétrica); furto e roubo de equipamentos; ataques de vírus informáticos; falhas em softwares; ataques de crackers, etc.[69]

Com a referida análise das ameaças e a probabilidade de sua ocorrência, são decididas quais medidas de controle de risco devem ser tomadas. É possível dar um exemplo prático, em relação ao ativo "energia elétrica", ativo técnico fundamental para o funcionamento de qualquer sistema. Identifica-se esse ativo e verifica-se que toda a infraestrutura de tecnologia depende de energia elétrica. Igualmente, sabe-se que na falta do fornecimento de energia elétrica, a infraestrutura de tecnologia deixará de funcionar, causando a interrupção dos serviços que dependerem daquela estrutura. Assim, como controle desse risco, investe-se em unidades de contingenciamento de energia (como geradores e nobreaks).

O processo de estabelecimento periódico de análise e gerência de risco, também é conhecido como Sistema de Gerência de Segurança da Informação (SGSI). [70] Há inclusive uma norma técnica para as empresas que desejam certificar-

67 GARFINKEL, Simson; SPAFFORD, Gene. *Practical Unix and Internet Security*. Sebastopol: O'Reilly, 2006, p. 27

68 Por vezes, o custo da medida de controle de um determinado risco é muito mais cara do que suportar a ocorrência do próprio incidente a ser controlado. Nestes casos, diz-se que o risco é “aceito” pela organização, em vez de ser “controlado” ou “eliminado”.

69 Idem. Ibid, p. 27-29.

70 Do inglês ISMS ou *Information Security Management System*.

se nesse processo: é a norma NBR ISO/IEC 27001[71]. Essa norma é usada em conjunto com a norma NBR ISO/IEC 27002[72]. A primeira estabelece como é realizado o sistema de gerência de segurança, enquanto que a segunda estabelece as melhores práticas de segurança a serem implementadas.

A implementação do processo repetitivo de gerenciamento e análise de risco, está diretamente vinculada à natureza do risco e das ameaças a que uma infraestrutura técnica está exposta. Não há razão para uma empresa empreender grandes esforços com equipes de guardas armados em um prédio onde está a infraestrutura de informática se a análise de risco demonstrar que as maiores ameaças são de acesso indevido via Internet. Por outro lado, a implementação de grandes mecanismos de segurança para impedir acesso não autorizado via Internet pode não ser tão eficiente, se a maior ameaça estiver vinculada a funcionários da empresa que não têm seus acessos às informações internas adequadamente controlados.

Por meio da análise de risco, os fornecedores de serviços informáticos encontram uma forma de cumprir o seu dever de segurança das infraestruturas que controlam. Deve-se ter em mente aqui que "*embora seja possível minimizar o risco de invasão de rede, não é possível eliminá-lo por completo*".[73] Afirma-se, inclusive, que a atividade ampla de gestão de riscos está vinculada, inclusive, ao próprio princípio da precaução[74].

---

71 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*. Tecnologia da informação. Técnicas de segurança. Sistemas de gerência da segurança da informação. Rio de Janeiro, 2005

72 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2005.

73 CARVALHO, Ana Paula Gambogi. Ibid, p. 110.

74 Cf. COSTA, Luiz. Privacy and the precautionary principle. Computer Law & Security Review, n. 28, 2012, p. 17 e 22: "*the precautionary principle works together with risk assessment in a rational approach of threats. Precaution is related with rational choices with regard to risk-taking. While prevention relates to identifiable risks, precaution concerns hypotheses that have not been scientifically confirmed. [...] Risk assessment and the precautionary principle go together. They are instruments that jointly determine the allocation of the evaluation of risks and the cost of damages caused by producers of goods and services rather than on citizens themselves. Risk assessment values transparency and readiness with regard to identifiable threats: a complete analysis of risks and the adoption of measures to avoid them shall be done. The precautionary principle*

Ressalte-se aqui, no que se refere à análise de risco, que ela é prevista no documento "*Guidelines for the Security of Information Systems and Networks - Towards a culture of security" editado pela Organisation for Economic Co-operation and Development (OECD)*[75]. Como a sociedade passa por um aumento da chamada "interconectividade", os sistemas e redes ficam expostos a uma crescente e ampla variedade de ameaças e vulnerabilidades.[76] Esse documento serve como um guia de recomendações e estabelece, também, nove princípios de segurança a serem seguidos. De forma sumária, os princípios são:[77]

1) Conscientização - Os participantes devem estar conscientes da necessidade da segurança da informação em sistemas e redes, bem como o que deve ser feito para o seu aprimoramento.
2) Responsabilidade - Os participantes são responsáveis pela segurança da informação dos seus sistemas e redes.[78]
3) Resposta - Os participantes devem agir prontamente, e de forma cooperativa, para prevenir, detectar e responder aos incidentes de segurança.
4) Ética - Os participantes devem respeitar os interesses legítimos dos outros.
5) Democracia - A segurança da informação dos sistemas e das redes deve ser compatível com os valores essenciais de uma sociedade democrática.[79]
6) Avaliação de risco - Os participantes devem conduzir avaliações de risco.[80]
7) Implementação e *security design* - Os participantes devem incorporar a segurança como um elemento essencial nos sistemas de informação e nas redes.

---

establishes that, despite the readiness, if something goes wrong, those responsible shall not invoke scientific uncertainty to exempt their liability." O princípio da precaução será tratado mais adiante no item C.2.

75 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Guidelines for the Security of Information Systems and Networks - Towards a culture of security*. Paris: OECD. 2002. Disponível em: <http://www.oecd.org/>. Acesso em: 15 Dez. 2011.

76 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Ibid, p. 7.

77 Idem. Ibid, p. 9 a 12.

78 Destaca-se aqui a responsabilidade [*accountability*] dos participantes com base nos seus papeis de segurança).

79 Esse princípio relaciona-se, de certa forma, com a proteção geral da liberdade e, consequentemente, dos direitos fundamentais.

80 Esse princípio, em conjunto com o de número oito e nove, é diretamente relacionado com a ideia de gerenciamento de risco entendido como um processo repetitivo.

8) Gerenciamento de segurança - Os participantes devem adotar uma abordagem abrangente do gerenciamento de segurança.
9) Reavaliação - Os participantes devem rever e reavaliar os sistemas de informação e rede, e realizar modificações apropriadas nas políticas, práticas e procedimentos de segurança.

Mais recentemente o Brasil passou a contar com o Decreto 7.829/2012 que, entre outras questões, trata sobre aspectos técnico-operacionais acerca do chamado Cadastro Positivo, assim estatuído pela lei 12.414/2011. Entende-se que esse decreto exemplifica e legitima algumas questões relativas à análise de risco expostas até aqui pois exige da empresa que vá atuar na atividade de banco de dados de informações de adimplemento o cumprimento de alguns requisitos, a saber, principalmente, o do art. 1º, inc. II, alínea a:

> *a) certificação técnica emitida por empresa qualificada independente, renovada, no mínininimo, a cada dois anos, que ateste a disponibilidade de plataforma tecnológicca apta a preservar a integridade e o sigilo dos dados armazenados, e indique que as estruturas tecnológicas envolvidas no fornecimento do serviço de cadastro seguem as melhores práticas de segurança da informação, inclusive quanto a plano de recuperação de desastre, com infraestrutura de cópia de segurança para o armazenamento de dados e informações;*

Conforme pode ser visto essa “certificação técnica” relacionada com as melhores práticas de segurança da informação outra coisa não é que a própria atividade de análise de risco digital baseada, principalmente, na norma NBR ISO/IEC 27002 que trata das melhores práticas.

Após essa breve exposição sobre a análise do risco, será realizada agora a análise do uso das heurísticas na tomada de decisões.

A.2 - As heurísticas na tomada de decisões

Sobre os julgamentos relacionados ao risco e às ameaças digitais, há que se considerar o uso das chamadas heurísticas. Heurísticas podem ser definidas como:

> "*regras gerais de influência utilizadas pelos sujeitos para chegar aos seus julgamentos em tarefas decisórias de incerteza e cita, como vantagens de utilização, a redução do tempo e dos esforços empreendidos para que sejam feitos julgamentos razoavelmente bons. As heurísticas reduzem a complexidade das tarefas de acessar probabilidades e predizer valores a simples operações de julgamento. Geralmente, as heurísticas são úteis, mas, por vezes, podem levar a erros severos e sistemáticos .*"[81]

Os usuários, e algumas vezes até as empresas, não possuem informações completas sobre como lidar com os riscos de tecnologia. No entanto, quando possuem, é comum tomarem decisões que racionalmente não seriam as mais adequadas. São estes "erros", ocasionados pelo uso de algumas heurísticas, que merecem estudo. Assim, o julgamento de uma situação perigosa[82] (e aqui incluem-

81 MELO, Wilson Viera; KALIL, Lisiane Lindenmeyer; et al. O papel das heurísticas no julgamento e na tomada de decisão sob incerteza. *Estudos de Psicologia*, Campinas, n. 23(2), p. 181-189, abr – jun/2006. Disponível em: <http://www.iders.org/textos/o_papel_das_heuristicas_na_tomada_de_decisao.pdf>. Acesso em: 12 Fev. 2012, p. 182.

82 Um outro exemplo interessante é trazido por Ian Ayres: "*The human mind tends to suffer from a number of well documented cognitive failings and biases that distort our ability to predict accurately. We tend to give too much weight to unusual events that seem salient. For example, people systematically overestimate the probability of 'newsworthy'" deaths (such as murder) and underestimate the probability of more common causes of death. Most people think that having a gun in your house puts your children at risk. However, Steve Levitt, looking at statistics, pointed out that 'on average, if you own a gun and have a swimming pool in the yard, the swimming pool is almost 100 times more likely to kill a child than the gun is.'*" AYRES, Ian. *Super Crunchers: Why thinking-by-numbers is the new way to be smart*. New York: Bantam Dell, 2007, p. 112.

se os riscos digitais) passa pela frequente utilização da “heurística da disponibilidade”. Esta é fundamentada no fato de que a:

> “*facilidade com que um determinado fato é lembrado ou imaginado pelo indivíduo pode determinar uma hiper ou subestimação da probabilidade ou frequência desse evento ocorrer. Dessa forma, as pessoas julgam essa probabilidade pela facilidade de evocar exemplos em suas memórias.* ”[83]

O exemplo trazido pelos autores envolve alguém que já foi vítima de um assalto (ou assista frequentes programas de TV sobre a violência urbana). Quando essa pessoa é questionada sobre o nível de violência em sua cidade, irá responder com mais intensidade do que os que não foram vítimas de um assalto. O mesmo aplica-se ao ambiente digital: a assimetria informacional faz com que os usuários subestimem os riscos, atuando de acordo com a heurística acima mencionada. Quem, por sua vez, passou por um recente incidente de segurança da informação (conta bancária invadida, computador invadido, conta da rede social invadida), tenderia, conforme a lição acima citada, a ficar mais sensível a riscos digitais[84].

A heurística da disponibilidade pode afetar não apenas os envolvidos em um incidente, mas também os juízes envolvidos no julgamento de uma ação. Esse problema pode influir diretamente na consideração da limitação ou estipulação de um dever legal. A verificação das probabilidades e do grau de cuidado esperado advindo de um dever legal, podem sofrer também a influência dessas heurísticas. A má-avaliação dessa situação pode levar à definição, em um julgamento, de que

---

83 MELO, Wilson Viera; KALIL, Lisiane Lindenmeyer; et al. Ibid, p. 184.

84 Ainda que estatísticamente o risco seja o mesmo. Neste sentido ver o contraponto de HARTMANN, Ivar Alberto Martins. O princípio da precaução e sua aplicação no direito do consumidor: dever de informação. *Direito & Justiça*. v. 38, n. 2, jul.-dez./2012, p. 161-162: “*Na verdade, não temos problema algum em gerenciar riscos, mesmo riscos de vida. O que o indivíduo não aceita é que um risco de dano a ele seja gerenciado por outrém, sem seu devido conheci- mento e sua completa compreensão. E este é o ponto onde surgem as controvérsias, pois nosso sistema requer que deleguemos a administração de aspectos de nossa existência a outros...*”

deveria ser esperado do agente um nível de cuidado muito maior do que o realmente necessário naquele momento.[85]

Bruce Schneier afirma que a heurística da disponibilidade está ligada também à chamada "*probability neglect*"[86]. Nesse fenômeno, as pessoas tendem a ignorar as probabilidades da ocorrência de algo, quando estiver ligado a um conteúdo altamente emocional (como as ameaças de terrorismo, por exemplo). Enfim, a heurística da disponibilidade faz com que as pessoas superestimem riscos raros e subestimem riscos mais comuns.[87]

Já se disse que as pessoas reagem de formas diferentes frente às ameaças. Muitas vezes, os diversos comportamentos contrariam completamente as disposições matemáticas e estatísticas frente ao risco enfrentado[88]. De fato, há várias ponderações que podem ser feitas acerca da consideração de ocorrência de um risco digital: a severidade do risco, a probabilidade do risco, a magnitude do risco, o quão efetivas serão as medidas para mitigar os riscos e como os riscos e os custos podem ser comparados. A falta de informações e o erro em cima dessas escolhas afasta cada vez mais o agente da avaliação eficaz do risco.[89]

Há situações interessantes, envolvendo a maneira incorreta como são avaliados riscos e perigos. Em 2001, mais pessoas morreram em função de comida estragada do que em função dos atentados de 11 de Setembro (5000 contra 2973) e ainda assim os EUA gastaram dezenas de bilhões de dólares em segurança contra U$ 1.9 bi no orçamento inteiro da *Food and Drug Administration* (FDA) americana. A psicologia explicaria essas escolhas[90] como absolutamente irracionais .[91]

---

85 FAURE, Michael G. Calabresi and Behavioural Tort Law and Economics. *Erasmus Law Review*. Volume 01 , Issue 04, p. 77

86 O termo é de difícil tradução, mas pode representar “a negligência na probablidade”.

87 SCHNEIER, Bruce. *The Psychology of Security*. Disponível em: <http://www.schneier.com/essay-155.html>. Acesso em: 12 Fev. 2012, p. 16

88 Idem. Ibid, p. 1.

89 Idem. Ibid, p. 3.

90 Ou *trade-offs*

91 SCHNEIER, Bruce. Ibid, p. 4.

Situações como essa podem levar a uma atividade de produção de normas que pretenda controlar riscos cuja probabilidade é baixa ou cientificamente não comprovada de acontecer. Nos EUA, são conhecidos exemplos de leis que, inicialmente criadas para o combate de potenciais cibercriminosos ou para a defesa de ameaças digitais, são usadas contra pessoas fora desse contexto.[92]

Schneier também menciona a lição de David Ropeik e George Gray, que enumeram algumas dessas irracionalidades, cujas mais importantes são: [93]

a) As pessoas temem mais riscos novos do que riscos que elas já conhecem e convivem há mais tempo. Um exemplo recente diz respeito à gripe suína que mata menos do que outras doenças mais antigas, mas tem gerado reações absolutamente exageradas da sociedade.
b) As pessoas temem mais riscos advindos do próprio homem do que riscos naturais. Os autores dizem que a população teme mais situações envolvendo a radiação nuclear do que a radiação solar, embora esta atinja bem mais pessoas na atualidade.
c) As pessoas temem menos situações de risco que, no entanto, conferem benefícios. O exemplo trazido pelo autor envolve algumas pessoas que moram em São Francisco – EUA, as quais, mesmo com os riscos de terremotos, preferem permanecer por gostarem do local ou por terem mais oportunidades de empregos.
d) As pessoas temem mais situações de risco que possam matá-las ou afetá-las de formas terríveis. Teme-se mais, por exemplo, tubarões do que abelhas, embora mais pessoas morram no mundo por ataques de abelhas.
e) As pessoas temem menos as situações de risco da qual elas têm algum tipo de controle. Teme-se mais viajar de avião do que viajar de carro enquanto se está dirigindo, embora esta situação traga mais riscos.

92 OHM, Paul. Ibid, p. 1348-1349.

93 SCHNEIER, Bruce. Op. Cit, p. 4. apud David Ropeik and George Gray, Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You, Houghton Mifflin, 2002. Ao mesmo tempo, o já citado texto de Paul Ohm também retrata a questão das heurísticas e de tomadas de decisões aparentemente racionais em OHM, Paul. Ibid, p. 1364.

f) As pessoas temem menos situações de risco provenientes de lugares, pessoas, governos ou empresas conhecidas ou que elas confiem, mesmo que isso por si só, não altere em nada a probabilidade do risco.

Nesse sentido, cita-se o conceito de Fauare sobre racionalidade limitada, que resume, de certa forma, a preocupação sobre a tomada de decisões acerca de riscos:

> *"a noção de 'racionalidade limitada' não é nova no direito e economia comportamental. Foi introduzida por Herbert Simon para mostrar que os atores, muitas vezes, tomam atalhos na tomada de decisões que frequentemente resultam em escolhas que falham em satisfazer a previsão de maximização da utilidade*
>
> *...*
>
> *pequenas probabilidades podem ser superestimadas como resultado de grandes medos de desfechos negativos ou na esperança de desfechos positivos. As pessoas tendem, portanto, a se concentrar mais em resultados absolutos em vez da probabilidade de que um evento adverso possa ocorrer.*[94]

Pelo que se pode perceber em relação às heurísticas e às nuances sobre a tomada de decisões acerca de controle de riscos, entende-se que ela aplica-se perfeitamente ao ambiente e aos riscos informáticos. O uso da Internet (que traz uma série de riscos digitais, muitas vezes negligenciados) é uma atividade bastante agradável para muitas pessoas. Como se pontuou anteriormente, o fato de uma atividade ser realizada com prazer, diminui a capacidade de as pessoas lidarem com os riscos advindos do seu uso.[95] Essas questões afetam diretamente as decisões tanto das empresas responsáveis pela infraestrutura de informática, como dos usuários das tecnologias.

---

94 FAURE, Michael G. Ibid, p. 77.

95 Idem. Ibid, p. 87.: "*One reason is the well-known affect heuristic: if an individual considers a certain activity to be useful and pleasant, the likelihood that he/she will realise that the consequences of the activity are damaging will be lower than if he/she dislikes or disapproves of the activity.* "

A.3 - A regulação do espaço virtual

Ronaldo Lemos, na introdução de seu livro Direito, Tecnologia e Cultura, ensina que "*há muito a lei deixou de ser o único fator que contribui para a maior ou menor liberdade individual, ou para a regulamentação da sociedade da informação*". Ao discorrer sobre as formas de regulação no ambiente informacional, Lemos menciona que elas seriam quatro[96]: a lei, as normas sociais, o mercado e a arquitetura ou código.[97] Em breve síntese, a lei, forma mais conhecida de controle, é representada pelas normas estatais. Já as normas sociais representam os usos e costumes além de qualquer "*postulação normativa compartilhada por comunidades ou inerente à determinadas situações e circunstâncias*"[98]. O mercado também é considerado à medida em que regula o acesso e o desenvolvimento das novas tecnologias. Por fim, a arquitetura – ou código – assim colocado por Lemos, e baseado na conhecida lição de Lessig em sua obra Code, é entendido pela "*estrutura inerente de como as coisas são construídas e ocorrem. Esta última torna-se um fator regulador cada vez mais importante na sociedade da informação ...*".[99]

---

96 Marcel Leonardi, ao analisar com profundidade a obra de Lessig, faz um paralelo interessante em relação às referidas formas de interação com a conhecida teoria tridimensional do direito de Miguel Reale. Diz ele que: "*É possível traçar um paralelo entre as quatro modalidades de regulação propostas por Lawrence Lessig e a teoria tridimensional do Direito de Miguel Reale. Há uma aproximação, nas duas teorias, dos conceitos de direito e de norma, assim como das ideias de normas sociais e de valores; por sua vez, o mercado e a arquitetura representam um desdobramento da dimensão dos fatos. O modelo de Lawrence Lessig é, sem dúvida, uma simplificação; apesar disso, é útil por chamar a atenção para a possibilidade de utilização do sistema jurídico para regular indiretamente certas condutas que, de modo geral, costumam ser reguladas diretamente pelas outras modalidades."* LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 166

97 LEMOS, Ronaldo. Ibid, p. 21.

98 Enquadram-se aqui as normas comuns, mesmo que não escritas, das comunidades digitais, a chamada Netiqueta. Sobre isso ver LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 192.

99 LEMOS, Ronaldo. Ibid, p. 21. O autor coloca como exemplo acerca das formas de regulação, o controle do ato de fumar. Legalmente é possível regular a atividade de fumar, através da proibição do fumo em locais públicos. Igualmente, as normas sociais também possuem um papel importante na medida em que o bom senso e as boas maneiras, geralmente, impedem que alguém fume na casa de alguém que não fuma, no carro de quem não fuma e também perto de crianças. O mercado influencia a atividade de fumar à medida que o aumento do preço de cigarro

No ciberespaço, a estrutura da própria tecnologia possui, via de regra, um papel preponderante sobre as outras formas de controle. Os exemplos claros podem ser vistos nas áreas de propriedade intelectual e direitos autorais na Internet. Mesmo que a lei proteja filmes e músicas em suas modalidades digitais, sabe-se que é grande o acesso e a reprodução ilegais de obras na Internet. A própria arquitetura da Internet, que permite o acesso fácil às obras digitais, aliada à questão mercadológica – do custo praticamente zero de reprodução das obras no suporte digital – sobrepõem-se ao controle legal. [100]

Quando a técnica passa a determinar a direção da regulação, surge a importância de se estudar a questão da vontade da técnica.[101] Segundo Pierre Levy:

> "*as técnicas carregam consigo projetos, esquemas imaginários, implicações sociais e culturais bastante variados. Sua presença e uso em lugar e época determinados cristalizam relações de força sempre diferentes entre seres humanos. […] por trás das técnicas agem e reagem ideias, projetos sociais, utopias, interesses*

---

faz com que o acesso ao cigarro seja potencialmente diminuído. Por fim, a própria arquitetura do cigarro também regula seu uso. As características dos cigarros possuírem mais ou menos nicotina, sabores diferentes e ter ou não filtro influenciam na escolha do fumante.

100 Carlos Alberto Rohrman, ao opinar sobre a obra de Lessig, ressalta que este "*não advoga a tese de que se deve deixar a cargo dos entes privados a determinação da arquitetura da Internet. Insista-se, ele afirma que tal ausência de intervenção do Estado acabaria por acarretar controle maior que seria nocivo para os interesses da maioria, em benefício das necessidades e dos interesses próprios das grandes empresas. Assim, em seu livro Code, Lessig alerta para a necessidade de o Estado intervir para determinar a natureza que o espaço virtual deve seguir.*" ROHRMANN, Carlos Alberto. Ibid, p. 24-25.

101 Nesse sentido DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 16: "*Entra em cena, portanto, a técnica como elemento dotado de características próprias e, consequentemente, inicia-se a discussão em torno do que seria a 'vontade da técnica'*."
Ver também LEVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999, p. 22. Segundo ele, acerca da vontade da técnica "*um ângulo de análise dos sistemas sócio-técnicos globais, um ponto de vista que enfatiza a parte material e artificial dos fenômenos humanos, e não uma entidade real, que existiria independentemente do resto, que teria efeitos distintos e agiria por vontade própria. [...] não podemos separar o mundo material - e menos ainda sua parte artificial - das ideias por meio das quais os objetos técnicos são concebidos e utilizados.*"

> *econômicos, estratégias de poder, toda a gama dos jogos dos homens em sociedade.*"[102]

Como a técnica é, portanto, produzida dentro de um meio cultural e social, ela é condicionada pelo meio. Da mesma forma, ela também "condiciona" e "*abre algumas possibilidades, que algumas opções culturais ou sociais não poderiam ser pensadas a sério sem sua presença.*"[103]

Dessa maneira, segundo o autor, a ideia de que as técnicas seriam neutras não é correta. Afirma ele que:

> "*uma técnica não é nem boa, nem má (isto depende dos contextos, dos usos e dos pontos de vista), tampouco neutra (já que é condicionante ou restritiva, já que de um lado abre e de outro fecha o espectro de possibilidades. Não se trata de avaliar seus "impactos", mas de situar as irreversibilidades às quais um de seus usos nos levaria …"*[104]

Ainda, segundo Danilo Doneda*, "tudo em acordo com o que poderíamos denominar um verdadeiro "postulado" da vontade da técnica: o que pode ser feito, será feito".*[105]

Se a técnica proporciona claras vantagens como maior eficiência, rapidez e infalibilidade, ao mesmo tempo, há desvantagens e problemas, tanto patrimoniais quanto não patrimoniais. Com a queda do mito de relação entre progresso tecnológico e bem-estar "*abriu-se o leque de situações não patrimoniais sobre as quais a tecnologia poderia ter fortes implicações, originando primeiramente insegurança.*"[106]

102LEVY, Pierre. Ibid, p. 23-24.
103Idem. Ibid, p. 25.
104 Idem. Ibid, p. 26.
105 DONEDA, Danilo. Ibid, p. 17.
106 Idem. Ibid, p. 17.

Embora, em muitas situações, a arquitetura técnica sobreponha-se aos controles legais estabelecidos, a lei também possui o condão de regular uma determinada arquitetura técnica. Assim ocorre no Brasil no que diz respeito à Assinatura Eletrônica. Aqui, a lei (por meio da Medida Provisória n. 2.200-2 de 24 de Agosto de 2001) estabelece a Infraestrutura de Chaves Públicas Brasileira – a ICP Brasil). Dessa forma, a emissão e utilização de certificados digitais para fins de garantia de autenticidade, integridade e validade de documentos eletrônicos (atividade técnica, representada por uma arquitetura técnica) devem respeitar as disposições da referida medida provisória.[107]

Ao realizar uma classificação e divisão dos ordenamentos não estatais, Norberto Bobbio ensina que eles estariam fracionados em quatro tipos assim definidos: os ordenamentos acima do Estado (como o ordenamento internacional, no exemplo de Bobbio abrangendo a igreja católica); ordenamentos abaixo do Estado (estes limitados e absorvidos pelo Estado); ordenamentos ao lado do Estado (em outras concepções também são colocadas ao lado do Estado a igreja católica e os ordenamentos internacionais) e por último os ordenamentos contra o Estado (assim como seitas secretas ou instituições criminosas como a Al-Qaeda e a Máfia).[108]

Para esse autor os ordenamentos, assim considerados, relacionam-se naturalmente entre si. Essa relação, entendida sob um ponto de vista amplo, pode ser classificada em uma relação de coordenação ou subordinação. Além dessa classificação, há também a que leva em consideração a extensão recíproca dos níveis de validade dos ordenamentos, tratando de relações de exclusão total, inclusão total e exclusão (ou inclusão) parcial.[109]

---

107 Sobre o assunto ver a obra de referência no Brasil: MENKE, Fabiano. *Assinatura eletrônica no Direito Brasileiro*. São Paulo: RT, 2005.

108 BOBBIO, Norberto. *Teoria do Ordenamento Jurídico*. Brasília: UnB, 1996, 6ª Ed, p. 164. A descrição de ordens jurídicas "contra o estado", também podem ser encontradas em NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: Wmf Martins Fontes, 2009, p. 214-216.

109 BOBBIO, Norberto. Ibid, p. 165-166.

As regras específicas do ciberespaço (visto como uma instituição), assim colocadas como um ordenamento transnacional, pela sua natureza e pelas características expostas, fazem uma relação de exclusão parcial (ou inclusão parcial) do ordenamento jurídico estatal. Essa exclusão parcial pode ser considerada, inicialmente, pela fato de a própria arquitetura técnica de construção do ciberespaço permitir a inclusão e a exclusão automática de regras em sua própria arquitetura informática. A exclusão automática de regras, na própria estrutura do ciberespaço, poderia fazer que, ao arrepio das leis dos ordenamentos estatais, sejam implantadas regras técnicas que, automaticamente, teriam o caráter de permitir ou impedir condutas juridicamente relevantes. O ciberespaço é, ainda, seletivo no que diz respeito à recepção de leis estatais. Há outra dialética em que a "norma suprema" aplicada nesse espaço passa a não ser mais uma norma escrita fundamental, mas sim a própria arquitetura do ambiente.

Diante disso, a já referida autonomia do espaço cibernético mencionada por Lorenzetti merece ser ressaltada. Essa autonomia seria caracterizada por tratar-se de um sistema autorreferente, ou seja, ele se auto-organiza em função de suas próprias regras. A ordem interna desse sistema é criada, segundo o autor, "*a partir da interação de seus próprios elementos que reproduzem a si mesmo, são funcionalmente diferenciados e buscam uma estabilidade dinâmica"*.[110]

A menção ao ciberespaço, como um espaço desterritorializado, pode ser encontrada também na lição de Marcelo Neves. Para ele, a sociedade moderna nasce como uma sociedade mundial, "*apresentando-se como uma forma social que se desvincula das organizações políticas territoriais...*"[111] A ligação dessa lição com o conceito de ciberespaço pode ser feita à medida que, na sociedade moderna, há a predominância da informática e da comunicação rompendo as fronteiras territoriais do Estado. O autor defende ainda que entender a territorialidade delimitada como característica fundamental de uma sociedade ou ordem "*implica desconhecer até*

110LORENZETTI, Ricardo Luis. Ibid, p. 30.
111 NEVES, Marcelo. Ibid, p. 26.

mesmo a existência de sociedades nômades no passado".[112]

As fronteiras nacionais, em uma ordem policêntrica, passam a ficar mais permeáveis à medida que, entre outras razões[113], as tecnologias permitem uma transcendência dessas fronteiras.[114] Nesse aspecto, a transnacionalidade do ciberespaço permite que diversos ordenamentos estendam sua jurisdição para os atos nele praticados. Dentro do ciberespaço não é mais possível excluir a ação de atores internacionais como fontes de autoridade efetiva. Muitos dos assuntos que eram tradicionalmente tratados dentro de um processo legal nacional estão passando para um campo de decisão supranacional.[115] Têmis Limberger observa esses efeitos, inclusive, com uma revisão dos próprios elementos referenciais do Estado Moderno. Observa a autora que "*Os típicos elementos referenciais de Estado não subsistem. A Internet muda o clássico conceito de território, e a noção de soberania também sofre transformações.*"[116]

Carlos Alberto Rohrman relata que as primeiras pesquisas, do que chama de "Direito da Rede", foram justamente associadas à questão do fenômeno da desterritorialização. Essa preocupação teria ocorrido, justamente, pois o direito é uma ciência "*essencialmente territorial*".[117] Há uma intensa organização de pessoas em torno do ciberespaço. Nele as pessoas consomem, relacionam-se, manifestam opiniões, etc. Essas ações, pela sua natureza, envolvem a observância e aplicação de regras constitucionais, o que faz que, pela sua não-territorialidade e transnacionalidade, seja, o ciberespaço, um motivo de conflito de regras e princípios constitucionais entre os Estados.

---

112 Idem. Ibid, p. 26.

113 Para esse trabalho a razão tecnológica que está sendo abordada.

114 FABRI, Hélène Ruiz; HAMMAN, Andrea. Transnational networks and constitutionalism. *International Journal of Constitutional Law*, Volume 6, Número 3 & 4. pp. 481-508. Disponível em: <http://icon.oxfordjournals.org/cgi/content/abstract/mon024> Acesso em: 12 Fev. 2012, p. 484.

115 NEVES, Marcelo. Ibid, p. 481 e 483.

116 LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007, p. 200.

117 ROHRMANN, Carlos Alberto. Ibid, p. 11.

Acerca da técnica, é importante lembrar que ela:

> "*transcende a racionalidade de fins, que não deixa de existir, para fazer surgir meios que buscam posteriormente seus fins. Nosso velho serrote somente sabe serrar, ele é um meio para um único fim. Nosso computador é polivalente, edita livros, dirige submarinos e admite que brinquemos com ele, admite ou exige que procuremos algo que ele possa fazer; buscamos fins porque temos um meio.*"[118]

A técnica moderna implica na perda de seu caráter finalístico, "*com a prevalência da técnica com o um meio aberto*". Essa característica permite que o uso da técnica adentre no "*mundo do imprevisível, onde a trajetória linear está sendo substituída pelos saltos quânticos...*"[119]. Como se verá adiante, essa característica de vulnerabilidades, de certa forma natural para a técnica moderna, é de fundamental importância para o entendimento da problemática envolvendo o dever de confidencialidade.

Bruno Miragem destaca a questão da regulação e a necessidade do alto grau de uniformidade para a manutenção da eficácia em relação ao regramento das relações na Internet. Aponta o autor que:

> "*Essa necessidade, muitas vezes, induz a um certo ceticismo quanto às vantagens da regulamentação estatal, face à conveniência de se adotarem outras iniciativas mais flexíveis, como as leis-modelo e as diretrizes gerais. Além dessas, existe o recurso genérico às denominadas lex mercatoria ou lex informatica, uma vez constatada a impossibilidade de efetiva regulação dessas relações estabelecidas pelo ambiente virtual*".[120]

---

118 BRÜSEKE, Franz Josef. Risco e contingência. In: VARELLA, Marcelo Dias. *Direito, Sociedade e Riscos: A sociedade contemporânea vista a partir da ideia de risco*. Brasília: UNICEUB, 2006, p. 102.

119 Idem. Ibid, p. 102.

120 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*,

Em função das próprias características do ciberespaço e seus desafios regulatórios, é possível afirmar que os princípios que governam o ciberespaço devem manter uma estabilidade e uma previsibilidade para que esse sistema funcione e que os participantes tenham a confiança suficiente nele.[121] Na lição de Reindenberg "*Para ambientes de rede e para a sociedade da informação, contudo, a lei e a regulamentação governamental não são as únicas fontes da produção de normas.*"[122]

Esse conjunto de regras que orientam o fluxo de informações e de ações praticadas no ciberespaço, (algumas destas fixadas na própria tecnologia), compõem a chamada Lex Informatica.[123] Se no fluxo tradicional de criação de leis há a intervenção estatal, no ciberespaço, "*as soluções técnicas começam a ilustrar que a própria tecnologia de redes impõe regras para o acesso e o uso da informação.*"[124] Essas regras tecnologicamente criadas fazem com que a *Lex Informatica* seja um sistema de regime de regras paralelo ao sistema legal estatal.

É possível realizar uma comparação entre a *Lex Informatica* e a legislação estatal[125]. Alguns critérios podem ser assim colocados: enquanto a legislação estatal baseia-se na lei, a *Lex Informatica* baseia-se em padrões de arquitetura informática da rede; enquanto a jurisdição da legislação estatal encontra-se limitada pelo território físico, a *Lex Informatica* ocorre dentro do ciberespaço; enquanto a legislação estatal tem como fonte o Estado, a *Lex Informatica* tem como fonte principais normas provenientes dos tecnólogos da informação e do próprio ambiente tecnológico; se na legislação estatal o processo de regras customizadas ocorre por meio do contrato, com a *lex informatica* esse processo ocorre por intermédio da

São Paulo, n. 70, abr.-jun./2009, p. 45-46.

121 REIDENBERG, Joel. Lex Informatica: The Formulation of Information Policy Rules Through Technology. Texas Law Review. v. 76, n. 3, Feb. 1998, p. 553-584. Disponível em: <http://reidenberg.home.sprynet.com/lex_informatica.pdf>. Acesso em: 12 Fev. 2012, p. 554.

122 Idem. Ibid, p. 554.

123 Idem. Ibid, p. 554

124 Idem. Ibid, p. 555

125 O termo legislação estatal deve ser entendido aqui em oposição à Lex Informatica.

configuração dos próprios softwares[126] de computador que compõem o ambiente.[127]

Este aspecto, que se refere ao âmbito de cumprimento da *lex informatica,* merece atenção. O cumprimento da legislação estatal tem a característica de ocorrer por provocação e a violação da lei é analisada *ex post*. A *lex informatica* permite, por sua vez, por meio de sua arquitetura e design, um caráter de autoexecutoriedade[128] de suas regras. Caso a técnica informática permita, o ambiente tecnológico pode ser criado de modo a prevenir que certas ações sejam praticadas.[129] Ao mesmo tempo, nesse âmbito, é possível também que sejam estabelecidos mecanismos de monitoramento da conformidade de ações dentro do ciberespaço.[130]

Nas conclusões de Reindeberg,[131] a *lex informatica* seria uma complexa fonte de informações e de regras nas redes globais. Ela permite a coexistência de várias políticas informacionais nesse ambiente heterogêneo. A l*ex informatica* permite também que sejam implantadas, diretamente na arquitetura do ciberespaço, regras imutáveis e auto-aplicáveis, a despeito dos ordenamentos utilizados.[132] Nesse ponto,

---

126 Configuração aqui deve ser entendida como configuração dos programas ou do ambiente informático. Se, por exemplo, uma empresa mantém um site de relacionamentos na Internet, ela pode "configurar" todo o aparato tecnológico que permitirá o formato de relação entre os participantes; enquanto que o cumprimento da lei se dá por meio dos tribunais na legislação estatal, na lex informática esse processo é automático e auto-aplicável.

127 REIDENBERG, Joel. Ibid, p. 566

128 Marcel Leonardi diz que o fato da arquitetura da Internet permitir normas autoexecutáveis representa uma ameaça: "*Essa é, de fato, uma ameaça concreta: pelo fato de ser autoexecutável, o código da Internet representa uma modalidade de regulação que atinge um "nível desumano de perfeição, ameaçando jogar as leis vigentes no "limbo da normatividade abstrata", substituindo o direito estatal por um poder de fato dos detentores da tecnologia.*" LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 176.

129 REIDENBERG, Joel. Ibid, p. 568.

130 Deve haver uma relação de coexistência e transversalidade entre as ordens estatais e informática. No entanto, o autor coloca a possibilidade de, em algumas situações haver a substituição quando a *lex informatica* for mais hábil para resolver alguns conflitos típicos do ambiente. Um exemplo pode ser o controle de conteúdo na Internet. É mais fácil conseguir regrar e controlar o tráfego de conteúdo na Internet por meio de mecanismos tecnológicos do que por meio de leis. Se o mantenedor de uma página na Internet quiser impedir comentários em sua página, pode fazê-lo por meio da arquitetura da rede. No entanto, a legislação estatal, nesse entendimento, pode encorajar o desenvolvimento de controles que ajudem sua implementação *pela lex informatica*. Idem. Ibid, p. 575-577.

131 Idem. Ibid, p. 584.

132 Um dos autores que defenderam de forma pioneira o poder do regulação pelo "código do computador" sobre os "códigos legais", sendo este o meio mais eficiente de regulação é Lawrence Lessig. Sua obra mais importante sobre o assunto é "Code", cujo argumento principal é: Code is

há a necessidade de acoplar as determinações de uma pretensa *lex informatica* dentro dos ordenamentos. Uma possibilidade desse acoplamento pode ser feita a partir do estabelecimento de padrões técnicos a serem seguidos no desenvolvimento das tecnologias. Marcel Leonardi, ao comentar o artigo de Joel Reidenberg, ressalta que a *lex informatica* deve ser usada em complementação e não em substituição às normas jurídicas tradicionais.[133]

O Brasil, ao contrário de outros países, não possui leis específicas tanto para o comércio eletrônico[134] ou mesmo a própria a regulação geral do uso das novas tecnologias. Foi apenas no final de 2012 que o país passou a contar com uma legislação de crimes eletrônicos, a lei 12.737/2012. Merece menção, neste ponto, a análise, mesmo que breve, do projeto de lei 2.126/2011, conhecido como Marco Civil da Internet, que estabelece as bases legais referentes aos princípios, às garantias, aos direitos e aos deveres para o uso da rede mundial de computadores no País. Esse projeto teve um avançado processo de elaboração por meio de um site na Internet[135] que contou com ampla participação da sociedade. Nesse site, foram recolhidas sugestões que motivaram ampla discussão acerca do texto do projeto.

Quanto à defesa do consumidor na Internet, embora não se discuta a aplicabilidade do CDC no comércio eletrônico, o Marco Civil da Internet, estabelece como um dos fundamentos acerca do uso da Internet no Brasil, em seu art. 2º, inc. V "*a livre iniciativa, a livre concorrência e a defesa do consumidor*".

---

law. (código aqui deve ser visto como o código dos programas de computador). Cita-se um excerto dessa obra: "*the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible. The struggle in that world will not be government's. It will be to assure that essential liberties are preserved in this environment of perfect control*.". LESSIG, Lawrence. Code: Version 2.0. Basic Books: New York, 2006, p. 4.

133 LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 147.

134 Há, no entanto, dois projetos de lei (PLS 281/2012 e 289/2012), visando atualizar o CDC para situações envolvendo as novas tecnologias e o comércio eletrônico, que será analisado adiante.

135 Disponível no endereço http://culturadigital.br/marcocivil

Acerca da questão da privacidade e da intimidade, o Marco Civil da Internet é expresso ao considerar acesso à Internet como essencial ao exercício da cidadania em seu art. 7º, assegurando os seguintes direitos:

> "*I - à inviolabilidade e ao sigilo* consentimento *o de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;*
> *IV - a informações claras e completas constantes dos contratos de prestação de serviços, com previsão expressa sobre o regime de proteção aos seus dados pessoais, aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar a qualidade dos serviços oferecidos; e*
> *V - ao não fornecimento a terceiros de seus registros de conexão e de acesso a aplicações de Internet, salvo mediante consentimento ou nas hipóteses previstas em lei.*"

Retiram-se daí importantes definições acerca da privacidade e do sigilo de dados: a reafirmação do princípio de inviolabilidade e o sigilo de comunicações; um dever de informação ampliado que os fornecedores possuem e também o não fornecimento de registros de conexão e acesso à Internet, salvo por consentimento ou ordem judicial.

Após, no art. 8º, é imposta como condição para o pleno exercício do direito de acesso à Internet a "*garantia do direito à privacidade e à liberdade de expressão nas comunicações*". Igualmente, o parágrafo único do art. 9º veda o monitoramento, a análise, ou a fiscalização de pacotes de dados na provisão de conexão à Internet.

Além disso, há uma disposição interessante sobre a guarda de registros de conexão e de acesso dos usuários. No art. 10 é estipulado que a guarda de tais

registros "*devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas*".

No mesmo art. 10 é determinado um dever de informação dos responsáveis pelos serviços ao estabelecer que "*as medidas e procedimentos de segurança e sigilo devem ser informados pelo responsável pela provisão de serviços de conexão de forma clara e atender a padrões definidos em regulamento*". Como se vê, a lei, se aprovada, deixará a cargo de um regulamento específico a questão de medidas de segurança e de sigilo de dados.

Há uma vedação específica ao armazenamento de registros (logs) de acesso a aplicações de Internet, realizados pelo serviço de provisão de conexão (art. 12). Essa disposição impede que os provedores de acesso à Internet filtrem e registrem o que o usuário de seu serviço está acessando na Internet.

Curiosamente, mesmo que não aprovado, há um julgado do Tribunal de Justiça do Rio de Janeiro, em que o Marco Civil da Internet – à época ainda em fase de discussão - foi invocado e utilizado de forma a orientar uma decisão, justamente pela falta de legislação a respeito.[136]

136 TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. 20ª Câmara de Direito Civil. Agravo de Instrumento n. 0013822-08.2010.8.19.0000. Wanderlei de Carvalho Rego X Net Serviços de Comunicação S/A. Relator: Des. Letícia Sardas. Rio de Janeiro, 30 de Junho de 2010. AGRAVO DE INSTRUMENTO. CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS. SIMPLES ALEGAÇÃO DE IMPOSSIBILIDADE TÉCNICA DE CUMPRIMENTO DA DECISÃO QUE NÃO MERECE PROSPERAR. SÚMULA 372 STJ. APLICABILIDADE. MULTA DIÁRIA EXCLUIDA. PARCIAL PROVIMENTO DO RECURSO. 1. No caso dos autos, alegando violação de sua conta de e-mail, o agravado quer que a agravante lhe forneça os dados necessários para identificação dos invasores de sua conta de e-mail. 2. Haja vista a fase embrionária jurídica em relação ao assunto, ainda não se concretizaram definitivamente as posições no tocante à matéria. 3. Contudo, ainda que existam muitos nichos desconhecidos em relação à Internet, esse mesmo argumento não pode servir para justificar ou escusar a não aplicação da legislação que se tem a mão. 4. O Marco Civil da Internet no Brasil, submetido à segunda consulta pública, estabelece os direitos dos cidadãos brasileiros na Internet.5. Ponto muito importante e positivo do Marco Civil é a forma como propõe regular os direitos e deveres relativos aos vários dados gerados pelo usuário quando navega. 6. Os registros relativos à conexão (data e hora do início e término, duração e endereço IP vinculado ao terminal para recebimento dos pacotes) terão que ser armazenados pelo provedor de acesso à Internet. 7. Em relação ao registro de acesso aos serviços de Internet (e-mails, blogs, perfil nas redes sociais etc.), o provedor não tem obrigação de armazenar os dados. Mas, se o fizer, terá que informar o usuário, discriminando o tempo de armazenamento. 8. Assim, resta claro que a simples alegação de impossibilidade técnica de

De igual importância, é necessário ressaltar também os recentes projetos de lei que visam a alteração e a inclusão de novos dispositivos no Código de Defesa do Consumidor: tratam-se dos PLS 281 e 289 ambos de 2012. Ele são fruto de um estudo realizado por uma Comissão de Juristas, entre os quais, a professora Cláudia Lima Marques. O referido projeto traz alguns avanços muito importantes em relação ao comércio eletrônico bem como em relação à questão da privacidade de dados dos consumidores[137].

No artigo 6º, no qual encontram-se os direitos básicos do consumidor, há a inclusão do inc. XI e XII, respectivamente estabelecendo como direitos básicos:

> *XI - a autodeterminação, a privacidade e a segurança das informações e dados pessoais prestados ou coletados, por qualquer meio, inclusive o eletrônico;*
> *XII - a liberdade de escolha, em especial frente a novas tecnologias e redes de dados, sendo vedada qualquer forma de discriminação e assédio de consumo*

Sobre a interpretação do art. XI, Cesar Santolim leciona que a menção dos termos “autodeterminação, privacidade e segurança” das informações indica que o

---

cumprimento à decisão, tendo em vista não mais possuir armazenados os logs de acesso com as informações das operações realizadas no mês de setembro de 2009 não tem o condão de afastar a determinação judicial concedida nos autos da Medida Cautelar. 9. Além disso, medida não trará nenhum prejuízo ao agravante já que este estará apenas fornecendo os dados necessários para identificar os possíveis violadores da conta de e-mail do autor da ação. 10. Por outro lado, em se tratando de ação de exibição de documentos, aplica-se ao caso a S. 372, STJ. 11. Mantém-se, contudo, a decisão recorrida que determinou o fornecimento dos nomes, endereços e todos os dados que a NET tiver em seus arquivos, relativos a seus contratantes que das 22:00 horas do dia 19.09.2009 às 00:44 horas do dia 20.09.2009, se utilizaram dos IPs indicados no item 1 da petição inicial (cf. fls. 60), especificando os horários de inicio e fim da utilização, bem como os sites na Internet que foram acessados no curso da utilização. 12. Parcial provimento do agravo de instrumento para excluir a imposição da multa diária para caso de descumprimento.

137 Sobre o assunto ver o também recente artigo SANTOLIM, Cesar Viterbo Matos. Anotações sobre o anteprojeto da comissão de juristas para a atualização do código de defesa do consumidor na parte referente ao comércio eletrônico. *Revista de Direito do Consumidor*, São Paulo, v. 83, p. 73-82, jul.-set./2012.

projeto "*foca exatamente a perspectiva dinâmica da utilização, pelo fornecedor, das informações obtidas.*"[138]

Tais princípios já são previstos pela doutrina acerca do tema privacidade, como será visto adiante. No entanto, vê-los fixados no texto legal permite a real ampliação da proteção à privacidade e à autodeterminação informativa.

Nesse âmbito, é incluída uma seção inteira que trata do Comércio Eletrônico, englobando os arts. 45-A até 45-E. Importa, para esse trabalho, destacar:

> *Art. 45-A. Esta seção dispõe sobre normas gerais de proteção do consumidor no comércio eletrônico, visando a fortalecer a sua confiança e assegurar tutela efetiva, com a diminuição da assimetria de informações, a preservação da segurança nas transações, a proteção da autodeterminação e da privacidade dos dados pessoais.*
> *[...]*
> *Art. 45-C. É obrigação do fornecedor que utilizar o meio eletrônico ou similar*
> *[...]*
> *IV - dispor de meios de segurança adequados e eficazes;*

Igualmente, a doutrina reconhece a proteção da confiança despertada nos consumidores e também o dever ampliado de informação a cargo do fornecedor. No entanto representa importante avanço legislativo, se a aprovado o projeto, a fixação de tais regras no texto legal.

A nova proposta, reconhecendo a suma importância da proteção dos dados privados, amplia a proteção contra o tratamento inadequado de dados pessoais ao criar um tipo penal específico sobre o tema, no art. 72-A:

---

138 Idem. Ibid, p. 75. O autor indica ainda que "*qualquer aplicação destas informações para a produção de novas informações deve ser objeto de prévia autorização do consumidor.*" Sobre esse assunto ver o item B.2 deste trabalho.

> *Veicular, hospedar, exibir, licenciar, alienar, utilizar, compartilhar, doar ou de qualquer forma ceder ou transferir dados, informações ou identificadores pessoais, sem a expressa autorização de seu titular e consentimento informado, salvo exceções legais.*
> *Pena – Reclusão, de um a quatro anos, e multa.*[139]

As disposições do Marco Civil da Internet e do projeto de lei de atualização do Código de Defesa do Consumidor trarão um importante avanço tanto na proteção do consumidor no comércio eletrônico assim como na proteção de seus dados pessoais.

B) Atributos de Segurança da Informação

Uma das raízes do problema, envolvendo a segurança da informação aplicada à Internet, consiste no fato de que a arquitetura da Internet não foi construída pensando-se em segurança[140]. O foco básico da Internet era, à época de sua criação, a manutenção da sua disponibilidade em caso de ataques militares. À época, os atributos de confidencialidade, autenticidade e integridade não foram devidamente observados, valorizando-se mais as questões de disponibilidade.[141]

Mesmo assim, é possível afirmar que, em relação à segurança da informação, há certos atributos que são protegidos: a confidencialidade, a

---

139 Acerca da tutela penal, ressalte-se que o crime de Invasão de Dispositivo Informático, do art. 154-A do CP atualizado pela lei 12.737/2012, possui duas situações de aumento de pena, respectivamente, nos casos de obtenção e divulgação de informações sigilosas, nos parágrafos 3º e 4º,

140 KURBALIJA, Jovan. *An Introduction to Internet Governance*. Genebra: DiploFoundation, 2008, p. 55.

141 Como se verá adiante, os atributos de segurança da informação envolvem a autenticidade, integridade, confidencialidade e disponibilidade.

integridade/autenticidade[142] e a disponibilidade. Eles podem ser conceituados da seguinte forma:

> ***"****Confidencialidade: garantia de que o acesso à informação é restrito aos seus usuários legítimos.*
> *Integridade: garantia da criação legítima e da consistência ao longo de seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações. O objetivo de autenticidade da informação é englobado pelo de integridade, quando se assume que este visa a garantir não só que as informações permaneçam completas e previsas, mas também que a informação capturada do seu ambiente externo tenha sua fidedignidade[143] verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo.*
> *Disponibilidade: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna."* [144]

Patrícia Peck Pinheiro trata, de forma sumária, os atributos de segurança:

> *"Quanto aos seus objetivos, a Segurança da Informação visa a três pontos: a) confidencialidade - a informação só deve ser acessada por quem de direito; b) integridade - evitar que os dados sejam apagados ou alterados sem a devida autorização do proprietário; e c) disponibilidade - as informações devem sempre estar disponíveis para acesso. [...] A autenticidade é a capacidade de identificar e reconhecer formalmente a identidade dos elementos de uma comunicação eletrônica ou de comércio."* [145]

---

142 Quanto ao atributo da integridade-autenticidade a maior parte dos autores coloca-os como sendo apenas um atributo por entenderem que a autenticidade é englobada pela integridade.
143 Talvez aqui o termo correto deva ser "autoria".
144 BEAL, Adriana. *Segurança da Informação*. São Paulo: Ed. Atlas. 2005, p.1
145 PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2007, p. 133

A importância de estudo dos atributos de segurança da informação ocorre à medida que, quando há situações de dano à informações em meio digital, haverá, por sua vez, a violação de algum dos atributos. Se, por exemplo, dados pessoais em meio digital forem acessados de forma não autorizada, houve a violação da confidencialidade da informação. Se um dado foi apagado de forma não autorizada, houve a violação da disponibilidade e da integridade da informação. Por sua vez, se houve a alteração indevida de dados protegidos, houve a violação da integridade (ou da autenticidade) da informação.

Em um contexto técnico, a confidencialidade – atributo que mais interessa para esse trabalho - pode ser vista também como a capacidade de um sistema de informação de evitar o acesso não autorizado às informações.[146] Esse atributo é necessário mas não suficiente pois a privacidade pode ser violada pela ação direta de pessoas que possuem o acesso ao recurso. Aquele que possui acesso à informação pode, por sua vez, utilizá-la de forma incorreta.

Pode-se conceituar segurança da informação como "*o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade.*"[147] A segurança da informação pode ser entendida, ainda, como dispõe a norma técnica NBR ISO/IEC 27002 :

> "*Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.*
> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e de hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados,*

146 MERRIL, Charles R. Ibid, p. 10.
147 BEAL, Adriana. *Segurança da Informação*. São Paulo: Ed. Atlas. 2005, p.1

> *onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos* ."[148]

O conceito de segurança da informação, assim retirado da norma ISO 27002, representa o aspecto interno da segurança, esse em relação aos procedimentos técnicos adotados pelas empresas. No entanto, as práticas de segurança da informação internas servem para a instrumentalização do dever geral de segurança aplicado às relações de consumo no comércio eletrônico.

Dentro dessas abordagens é preciso entender a segurança da informação conforme os seguintes aspectos: a) Dever de segurança como dever jurídico[149] b) Disciplina tecnológica, que oferece subsídios para este trabalho, principalmente no que diz respeito aos atributos de segurança que são absorvidos pelo direito, tornando-se aspectos do dever de segurança da informação e c) Segurança da informação como contra-medidas ou inteligência cibernética estatal, visando à proteção contra atividades danosas (sejam criminosas ou não).[150]

Outra abordagem bastante interessante e inteligente é a compreensão da segurança da informação – e seus atributos - como direito fundamental. Essa ideia pode ser encontrada nos estudos de Ahti Saarenpää e Fabiano Menke. O primeiro

---

148 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: Tecnologia da informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação. 2. ed. Rio de Janeiro, 2005, p. 9.

149 Se há um dever geral de respeito à segurança por parte do fornecedor em relação ao consumidor, há consequentemente, um direito subjetivo à segurança. Ver MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais. 6ª Ed. São Paulo: RT, 2011, p. 764. "*Dever jurídico é uma ordem ou comando dirigido pelo ordenamento jurídico ao indivíduo, que ele tem de observar como um imperativo, visando orientar seu procedimento. Ao dever jurídico imposto a um indivíduo (devedor: lado passivo) corresponde um direito subjetivo assegurado a outro indivíduo ou ente (credor:lado ativo).*
O estado de sujeição é o correlativo passivo dos direitos potestativos, assim como o dever jurídico o é dos direitos subjetivos propriamente ditos. A sujeição traduz-se na impossibilidade de querer com eficácia em sentido contrário ao que já foi determinado pelo ordenamento jurídico. É uma subordinação irresistível que consiste na necessidade de suportar as consequências jurídicas da atuação do outro que titula um poder potestativo, enquanto o dever jurídico consiste na necessidade subjetiva de obedecer ao comando jurídico, sob pena de sanção do ordenamento jurídico."

150 Sobre esse aspecto, no Brasil, ver MANDARINO JR., Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Cuzbac, 2010.

autor parte do pressuposto da grande dependência das infraestruturas informáticas[151] e da necessidade de considerar um direito fundamental à segurança em tais "supervias"[152]. Segundo ele, "*o direito à segurança da informação é um direito que todos os cidadãos gozam quando dados relativos a eles – e não apenas dados sensíveis – são processados"*[153]. Já Fabiano Menke considera a proteção de dados e o novo direito fundamental à garantia da confidencialidade e integridade, com base na jurisprudência alemã[154].

É certo que esses aspectos relacionam-se. Porém, o que interessa aqui é a análise do primeiro com o apoio – em alguns casos – da disciplina tecnológica, que é impossível de ser afastada. No entanto, é verdade que é mais comum ver o termo "Segurança da Informação" vinculado aos seus aspectos tecnológicos[155].

A segurança da informação também pode ser vista como o objeto principal de um contrato. Isso ocorre, por exemplo, por intermédio de um contrato em que uma empresa contrata o serviço de segurança da informação para os seus ativos informacionais; um consumidor que contrata de um provedor de acesso um serviço de *firewall* ou ainda em um contrato de compra de um certificado digital.

---

151 Observando que essa dependência também ocorre em relação aos governos que, muitas vezes, disponibilizam serviços essenciais por meio das redes informáticas. Além do mais as discussões acerca de uma ciberdemocracia só podem ocorrer considerando-se medidas de segurança da informação como um direito subjetivo.

152 SAAREPÄÄ, Ahti. Ibid, p. 8: "*Information security for the new infrastructure is thus a significant issue in the realm of fundamental rights: We should have access to a secure information superhighway. Yet this is but one, albeit important, component of legal information security. We must take a look at the other aspects of information as well.*"

153 Idem. Ibid, p. 9-10. O autor afirma ainda que "*given that the right to privacy is a fundamental right, information security can be seen as a right safeguarding a fundamental right. Information security has changed – or at least is in the process of changing – from a technical aid to a legal value. This change is a crucial development*.

154 De acordo com o belíssimo estudo de MENKE, Fabiano. *A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. No prelo.

155 Essa visão (de valorizar mais os aspectos tegnológicos do que jurídicos da disciplina) coloca o próprio direito em perigo, cf. SAAREMPÄÄ, Ahti. The importance of information security in safeguarding human and fundamental rights. *e-Stockholm 2008 Legal Conference*. p. 1-15. Disponível em: <http://www.juridicum.su.se/Iri/e08/documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf>. Acesso em: 20 Dez. 2012, p. 5: "*Where attention is trained exclusively on the changes in IT in society, law is in danger of becoming a lower-level – if still well selling – planning technique. Only a deeper-going assessment of changes in a state and society can fulfil the criteria for good science.*"

A questão da segurança da informação, como dever principal de um contrato, deve ser entendida também considerando-se a possibilidade de contratar apenas alguns aspectos de segurança. É possível contratar apenas a proteção de alguns ativos informacionais deixando outros descobertos da proteção contratada.

O foco principal nesse trabalho será dado ao dever de confidencialidade, principalmente no que diz respeito à proteção de confidencialidade de dados pessoais nos bancos de dados de informações de consumidores.

Em função de defender-se aqui a ligação da proteção dos atributos ao conceito de segurança, sempre que se falar em um dever geral de segurança da informação, estar-se-á falando sobre a proteção de um, ou de todos os referidos atributos.

C) Controle de acesso e identificabilidade

A forma de interação proporcionada pela Internet é muito mais abrangente do que as formas de interação proporcionadas por outros meios de comunicação. José de Oliveira Ascensão observa essa forma de comunicação dispondo que esse meio de comunicação funciona "*não apenas de um para vários, sem interatividade, como na rádio-difusão; ou de um para um com interatividade como no telefone; mas de todos para todos, com interatividade*"[156].

O aspecto de existirem ao mesmo tempo milhões de emissores e receptores na Internet (ao contrário das mídias tradicionais em que há um único emissor para muitos receptores) traz diversos problemas em relação ao controle do fluxo de

156 ASCENSÃO, José de Oliveira. *Direito da Internet e da Sociedade da Informação: Estudos*. Rio de Janeiro: Forense, 2002, p. 68. É o aspecto anárquico da comunicação de muitos para muitos que dificulta (ou até impossibilita) o controle do que pode ser publicado na Internet.

informações. Em uma emissora de televisão, pode ser viável, tanto técnica quanto economicamente, realizar um controle prévio de conteúdo, visando impedir a publicação de materiais que possam representar ofensa a um bem jurídico de quem quer que seja. No entanto, em um ambiente em que todos são emissores e receptores há uma dificuldade, ou até mesmo a impossibilidade de implementarem-se ações de controle, quer pela sua dificuldade técnica ou quer pela alto custo financeiro de ações nesse aspecto.

De outra forma, o fato de existirem tantos emissores quanto receptores dificulta também a identificabilidade geral nesse ambiente. É certo que se aplica ao ambiente digital, sem qualquer dúvida, a regra constitucional a respeito da vedação do anonimato[157]. Portanto, como será melhor explicado adiante, surge aí então o dever do mantenedor de uma estrutura tecnológica de proporcionar meios hábeis a identificar as pessoas que utilizarem a referida estrutura. Ao mesmo tempo, embora exista a previsão constitucional de vedação ao anonimato, sabe-se que há meios tecnológicos de realizar a prática de ações no meio digital de forma anônima, o que aumenta o caráter inseguro da própria Internet.[158] A Internet, vista como meio aberto que é, e em função de uma série de vulnerabilidades técnicas[159] e ameaças, além da própria imaterialidade das relações, é um meio sabidamente inseguro. Em função disso, é visível a circunstância de que aqueles que decidem realizar operações pela Internet devem reforçar o dever de segurança.[160]

---

157 Art. 5º, inc. IV da Constituição Federal.

158 MARTINS, Guilherme Magalhães. Confiança e aparência nos contratos eletrônicos de consumo via Internet. *Revista de Direito do Consumidor*, São Paulo, n. 64, out.-dez./2007, p. 55. "*O fator segurança aparece agravado pela possibilidade de anonimato do autor das operações, ainda que fortemente relativizado em face das modernas técnicas de rastreamento*".

159 Ver a definição de vulnerabilidade de segurança por DE VILLIERS, Meiring. Reasonable Foreseeability in Information Security Law: A Forensic Analysis. University of New South Wales Faculty of Law Research Series, Sydney, p. 102-160, Abr. 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1158165>. Acesso em: 12 Fev. 2012, p. 117: "*A security vulnerability is an error in an information system that an intruder can exploit to violate the system's security policy. A system's security policy protects the confidentiality, integrity, and availability of information contained in the system by controlling access to the system.*"

160 Conforme o correto magistério de MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da Internet. *Revista de direito do consumidor*, São Paulo, n. 40, abr.-jun./2009. p. 63.

Assim, as técnicas de controle de acesso são as medidas utilizadas para garantir, ou não, o acesso de alguém a um recurso de tecnologia. [161]

Antes da existência e utilização maciça da Internet, a questão do controle de acesso era simples: só quem possuía o acesso físico ao computador é que conseguia aceder às informações ali armazenadas. Bastava, portanto, apenas medidas de segurança física[162] para controlar o acesso aos recursos computacionais. Com a popularização do uso da Internet e a consequente ligação de computadores em rede, e também com o compartilhamento e armazenamento maciço de dados, a disciplina do controle de acesso ganhou maior relevância.

Adiante, será abordada a questão do papel dos intermediários nas comunicações informáticas, mais especificamente, os tipos de provedores e suas funções. Após, tratar-se-á da autenticação e autorização, bem como situações de acesso autorizado e não autorizado.

C.1 - O papel dos provedores de serviços na comunicação informática

Para a compreensão do direito aplicado às novas tecnologias é necessário destacar, mesmo que de forma sumária, o papel dos provedores de serviços informáticos. Segundo Marcel Leonardi, provedor de serviços de internet "*é o gênero do qual as demais categorias (provedor de backbone[163], provedor de acesso, provedor de correio eletrônico, provedor de hospedagem e provedor de conteúdo) são espécies.*"[164] Basicamente um provedor de serviços é a "*pessoa natural ou*

161 Recurso aqui deve ser entendido como computador, rede, sistemas tecnológicos em geral, etc.

162 Ou seja, qualquer pessoa que tivesse acesso físico ao computador (pudesse ligá-lo, tivesse acesso à sala onde estava localizado) poderia acessá-lo.

163 Também chamado por Bruno Miragem como "provedores de rede". MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009, p. 49.

164 LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 19.

jurídica que fornece serviços relacionados ao funcionamento da Internet, ou por meio dela".[165]

O provedor de *backbone*[166] possui o papel de fornecer aos provedores de acesso ou de hospedagem a infraestrutura técnica de conectividade à Internet.[167] Um usuário comum de Internet não possui contato direto com o provedor de *backbone*, funcionando ele apenas como um meio de acesso à internet para outros provedores.

O provedor de acesso é aquela empresa que fornece acesso à Internet ao usuário final.[168] Esse acesso pode ocorrer via acesso discado, ADSL, cabo ou ainda via 3G. Qualquer pessoa que acesse a Internet necessita, obrigatoriamente, de um provedor de acesso. São estes os provedores que possuem condições de apontar, dentro do universo de seus clientes, que determinado usuário esteve conectado à Internet em determinado dia e horário. Isso é possível pois são eles que fornecem um endereço IP aos usuários.[169]

Já o provedor de correio eletrônico fornece um serviço que permite ao usuário o envio, recebimento e armazenamento de mensagens eletrônicas. É comum que estes provedores prestem serviços gratuitos o que não afasta a circunstância de constituir uma relação de consumo entre ele e o usuário.[170] Esse provedor possui um dever geral de confidencialidade[171] sobre as mensagens enviadas, recebidas e

---

165 Idem. Ibid, p. 19.
166 Ou "espinha dorsal".
167 Idem. Ibid, p. 19-20.
168 LEONARDI, Marcel. Ibid, p. 21.
169 Cf. BARBAGALO, Erica B.. Aspectos da responsabilidade civil dos provedores de serviços na Internet. In: LEMOS, Ronaldo; WAISBERG, Ivo. (org.) *Conflitos sobre nomes de domínio e outras questões jurídicas da Internet*. São Paulo: RT, 2003, p. 344.
170 LEONARDI, Marcel. Ibid, p. 23. Esta aparente gratuidade, segundo o autor, ocorre "*mediante remuneração indireta, como a venda de dados cadastrais do usuário a empresas interessadas, anúncios inseridos no início ou final das mensagens, envio de propaganda pelo correio eletrônico, entre outras práticas comuns no fornecimento de tais serviços.*"
171 Dever este baseado na regra geral de sigilo de correspondência estabelecida na Constituição Federal, no art. 5º, inc. XII.

armazenadas pelos usuários, devendo empregar todos os meios técnicos ao seu alcance para a proteção dessas informações.

O provedor de hospedagem, por sua vez, oferece o serviço de armazenamento de arquivos em um servidor e a disponibilização de acesso a estes arquivos na Internet. Trata-se de um serviço de "*cessão de espaço em disco rígido remoto*".[172] É através de um provedor de hospedagem que uma pessoa ou empresa consegue disponibilizar um site na Internet.[173] A relação entre os contratantes e os provedores de hospedagem é uma relação de consumo, independente do serviço ser, ou não, gratuito.[174] Via de regra, no serviço de hospedagem, o provedor de serviços "*não interfere no conteúdo dos sites, pois para tanto dá ao proprietário de cada site que hospeda acesso à sua página para criá-la, modificá-la ou extingui-la.*"[175]

Por fim, o provedor de conteúdo disponibiliza na Internet informações "*criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem.*"[176] O provedor de informação é aquele que produz as informações, ou seja, o real autor da informação.[177] No Brasil, a jurisprudência do STJ[178] reconheceu a irresponsabilidade

172 LEONARDI, Marcel. Ibid, p. 23.

173 Entenda-se aqui "site" em seu sentido amplo. Um site pode conter diversos elementos dinâmicos que permitem a realização das mais variadas funções, desde a apresentação de conteúdo até a venda de produtos. Um site não deixa de ser um software.

174 É o conhecido contrato de hosting cf. Indicação de BARBAGALO, Erica B.. Ibid, p. 347.

175 BARBAGALO, Erica B.. Ibid.

176 LEONARDI, Marcel. Ibid, p. 22.

177 Idem, Ibid.

178 SUPERIOR TRIBUNAL DE JUSTIÇA. 3ª Turma. REsp. n.1193764/SP. I.P da S.B X Google Internet Brasil Internet Ltda. Relator: Min. Nancy Andrighi. Brasília, 14 de Dezembro de 2010.
Ementa: DIREITO CIVIL E DO CONSUMIDOR. Internet. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA. 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração" contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. A

do provedor de conteúdo pelo conteúdo gerado pelos seus usuários, além de não exigir um dever de monitoramento por parte daqueles na falta de uma lei específica sobre o assunto.[179] Basicamente os provedores de serviços não precisam monitorar preventivamente as operações de seus usuários.[180] Apenas quando devidamente notificado acerca de uma operação ilícita realizada pelos usuários é que deve tomar uma providência envolvendo a retirada de conteúdo. Igualmente, realizar um controle prévio das informações armazenadas pelo provedor de conteúdo representaria uma ação de censura prévia.[181]

Ainda, acerca da notificação e retirada de conteúdo, é possível sustentar que há três tipos de situações: a retirada após uma simples notificação extrajudicial da parte (o chamado *notice and take down*); a retirada com base em uma ordem judicial provisória e ainda a retirada após o trânsito em julgado de uma sentença. Esse

---

fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos. 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02. 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo. 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na Internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet. 8. Recurso especial a que se nega provimento.

179 Sobre este assunto, o Marco Civil da Internet - PL 2.126/2011 - em seu art. 14, estabelece que "*Salvo disposição legal em contrário, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.*"

180 Marcel Leonardi afirma que "*do mesmo modo, um provedor de hospedagem não exerce controle direto sobre as atividades de seu usuário, assim como o proprietário de um imóvel não controla diretamente o que faz seu inquilino, ocorrendo a mesma situação com provedores de conteúdo que disponibilizam espaço para divulgação de mensagens sem exercer controle editorial prévio sobre o que é publicado*." LEONARDI, Marcel. Ibid, p. 71.

181 Cf. TEIXEIRA, Tarcísio. *Direito Eletrônico*. São Paulo: Juarez de Oliveira, 2007, p. 167.

assunto já foi tratado pelo STJ que entendeu que após uma notificação extrajudicial do usuário[182], o provedor deve retirar o conteúdo do ar, de forma preventiva, em até 24 horas[183]. Após esse prazo teria que apreciar a "*veracidade das alegações, de modo a que, confirmando-as, exclua definitivamente o perfil ou, tendo-as por infundadas, restabelece o seu livre acesso*". A crítica que se faz à decisão é justamente transferir para uma empresa privada a decisão sobre a (i)licitude de conteúdos, tarefa que, salvo melhor juízo, deve ser do judiciário[184] e também definir um prazo tão pequeno para a retirada do conteúdo.[185] Os provedores, nesta situação, "julgariam" o que representa um conteúdo ilícito ou desabonador. Dependendo dos interesses econômicos do provedor, sua decisão pode afetar gravemente a própria liberdade de expressão[186].

182 O julgado refere que a notificação foi feita por meio de uma ferramenta disponibilizada pelo próprio provedor chamada de "denúncia de abusos". Esta questão certamente foi definitiva para a decisão pois se o próprio provedor disponibiliza ferramenta específica para o fim de denúncias deve agir com rapidez. Se não houvesse este tipo de ferramenta na presente situação, talvez, a decisão fosse outra.

183 SUPERIOR TRIBUNAL DE JUSTIÇA. 3ª Turma. REsp. n.1.323.754/RJ. Google Internet Brasil Internet Ltda. X Grasiele Salme Leal. Relator: Min. Nancy Andrighi. Brasília, 19 de Junho de 2012. Ementa: RESPONSABILIDADE CIVIL. INTERNET. REDES SOCIAIS. MENSAGEM OFENSIVA. CIÊNCIA PELO PROVEDOR. REMOÇÃO. PRAZO. 1. A velocidade com que as informações circulam no meio virtual torna indispensável que medidas tendentes a coibir a divulgação de conteúdos depreciativos e aviltantes sejam adotadas célere e enfaticamente, de sorte a potencialmente reduzir a disseminação do insulto, minimizando os nefastos efeitos inerentes a dados dessa natureza. 2. Uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, o provedor deve retirar o material do ar no prazo de 24 (vinte e quatro) horas, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 3. Nesse prazo de 24 horas, não está o provedor obrigado a analisar o teor da denúncia recebida, devendo apenas promover a suspensão preventiva das respectivas páginas, até que tenha tempo hábil para apreciar a veracidade das alegações, de modo a que, confirmando-as, exclua definitivamente o perfil ou, tendo-as por infundadas, restabeleça o seu livre acesso. 4. O diferimento da análise do teor das denúncias não significa que o provedor poderá postergá-la por tempo indeterminado, deixando sem satisfação o usuário cujo perfil venha a ser provisoriamente suspenso. Cabe ao provedor, o mais breve possível, dar uma solução final para o conflito, confirmando a remoção definitiva da página de conteúdo ofensivo ou, ausente indício de ilegalidade, recolocando-a no ar, adotando, nessa última hipótese, as providências legais cabíveis contra os que abusarem da prerrogativa de denunciar. 5. Recurso especial a que se nega provimento

184 Mesmo assim o assunto é delicado pois há situações de conteúdos flagrantemente ilícitos – como a pornografia infantil – que não exigem a manifestação do poder judiciário para ordenar a retirada do ar. No entanto, este exemplo é mais simples pois a ilicitude da publicação deste tipo material é definida em lei penal.

185 Além do mais, o provedor é incentivado a sempre retirar conteúdos do ar com receio de ser responsabilizado solidariamente mesmo em situações que o conteúdo não é ilícito. Assim, parece que a liberdade de expressão pode ser afetada.
De outra forma a decisão contraria as disposições do próprio Marco Civil que, em seu art. 14, impõe a necessidade de ordem judicial específica para a retirada conteúdo.

186 Igualmente as próprias empresas que se sentirem atingidas por comentários desabonatórios

Além do mais, a própria decisão menciona que o provedor deve tomar as medidas legais cabíveis contra aqueles que "*abusarem da prerrogativa de denunciar*". Parece inadequada essa disposição pois o provedor, em princípio, não teria nenhum interesse em coibir abusos na denúncia, até porque ele não sofre dano em tal situação. Quem sim tem a legitimidade de propor eventual medida contra o abuso na denúncia é a parte que fez a publicação e que sofre o dano pela publicação indevida.

No direito comunitário, é possível ver na Diretiva 2000/31/CE[187], que trata de aspectos legais dos serviços da sociedade da informação, algumas diretrizes acerca da responsabilidade de provedores. Sumariamente, o art. 12 estabelece a irresponsabilidade dos provedores, em relação às informações transmitidas, quando prestar atividade de simples transporte, sob certas condições.[188] Já o art. 13 firma a irresponsabilidade do provedor sobre as informações armazenadas, quando armazená-las com o fim de agilizar a transmissão (a chamada atividade de caching). O art. 14 refere-se à situação exposta acima, no julgado do STJ. Essa determinação implica na irresponsabilidade do provedor, no armazenamento de dados, quando ele desconhecer a natureza das informações armazenadas, devendo responder apenas a partir do momento em que obtenha conhecimento da eventual ilicitude do conteúdo. Por fim, o art. 15, fixa a ausência de um dever geral de vigilância sobre as informações que transmitem ou armazenem.

Ressalte-se o fato de que nada impede que um provedor de serviço acumule mais de uma das funções acima elencadas. Por exemplo, um provedor de serviços

---

(porém lícitos, dentro do espaço da liberdade de expressão, como reclamações de consumidores, por exemplo) podem utilizar-se deste precedente para retirar conteúdos da Internet sem a necessidade de um processo judicial.

187 UNIÃO EUROPEA. *Diretiva 2000/31/CE* – Diretiva relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno de 08 de Junho de 2000. Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu.

188 O provedor assemelhar-se-ia a o serviço de correio, que não é responsável pelo conteúdo das correspondências que entrega.

pode acumular a atividade de provimento de acesso e de correio eletrônico ao mesmo tempo.[189]

Para esse trabalho, importa ressaltar que tanto os provedores de acesso, quanto os de hospedagem e de conteúdo[190] possuem um dever específico de confidencialidade acerca dos dados pessoais e sensíveis que trafeguem ou sejam armazenados em suas estruturas.[191] Aplica-se a eles a responsabilidade objetiva em função da relação de consumo estabelecida entre eles e seus usuários.

C.2 - Autenticação e autorização

A Internet padece de problemas específicos de arquitetura técnica: não é possível, *a priori*, saber quem é o usuário, onde o usuário está e o que o usuário está fazendo. O protocolo de comunicação[192], por si só, não identifica os usuários. Dessa maneira, é necessário um mecanismo de identificação e autenticação que permita o acesso controlado dos usuários aos recursos.[193]

---

189 LEONARDI, Marcel. Ibid, p. 25

190 Segundo MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, São Paulo, n. 70, abr.-jun./2009, p. 50, em relação ao provedor de conteúdo, podem ser dois os regimes de responsabilidade: "*tanto podem ser qualificados como fornecedores, quando realizam atividade negocial no fornecimento de conteúdo (mediante pagamento, por exemplo), quanto simples "publicações", a utilizar-se da Internet para exercício da liberdade de expressão ou da liberdade de comunicação social. No primeiro caso, estaria caracterizada a relação de consumo determinante para a incidência das regras de proteção do consumidor; no segundo caso, as hipóteses de responsabilidade do provedor estariam sob a égide das normas do Código Civil.*"

191 O provedor de acesso, por exemplo, deve manter em sigilo os dados cadastrais de seus clientes, bem como os dados envolvendo quais endereços IPs foram utilizados pelos usuários. A informação de qual endereço IP o cliente do provedor de acesso utiliza pode identificar o cliente nas mais variadas situações. Já o provedor de hospedagem, via de regra, registra o IP dos usuários que acessaram as páginas e serviços hospedados por ele. Naturalmente, esta informação também deve ser mantida em sigilo.

192 O protocolo referido é o TCP/IP.

193 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 156-157. Isto não significa que não seja possível identificar os usuários. É necessário, para isso, confiar-se nos bancos de dados e cadastros que identificam os usuários. A questão de onde o usuário está, só é possível pois o provedor de acesso possui um banco de dados com o endereço IP utilizado pelo seu usuário em determinado momento. O endereço IP sozinho não consegue apontar a

A disciplina de determinar a autorização a algum recurso computacional é conhecida como controle de acesso.[194] Três elementos o compõem: a identificação, a autenticação e a autorização.[195]

A identificação é o processo de reconhecer quem terá o acesso a um determinado recurso. Já a autenticação é o processo de verificar as credenciais fornecidas pelo usuário[196]. A diferença entre identificação e autenticação é: a primeira envolve a verificação da identidade de alguém enquanto que a segunda consiste no processo de confirmar se a pessoa que se apresenta é quem de fato alega ser.

A autenticação tem, portanto, a função de determinar se alguém é quem de fato alega ser, diante de um sistema informático. Ela pode acontecer de três formas diferentes:[197]

---

localização da pessoa.

194 Toda a explicação do controle de acesso segue a lição de NOOR, Arshad; PELED, Ariel. Access Control. In: ISOM, David K.; NELSON, Sharon D.; SIMEK. John W.(editores). *Information Security for Lawyers and Law Firms*. Chicaco: American Bar Association Publishing, 2006.
Fala-se aqui do controle de acesso lógico. Há também, o controle de acesso físico, que envolve o controle físico de como as informações são acessadas.

195 Acerca dos processos de identificação e autenticação, Gerson Luiz Carlos Branco afirma: "*Em resumo, o princípio da confiança obriga o fornecedor a garantir condições de identificação das pessoas que participam da relação contratual, assim como obriga a garantir segurança suficiente para que daquela relação resultem benefícios úteis e não danos.*" BRANCO, Gerson Luiz Carlos. A proteção das expectativas legítimas derivadas das situações de confiança: elementos formadores do princípio da confiança e seus efeitos. *Revista de Direito Privado*, São Paulo, n. 12, out.-dez./2002, p. 202.

196 Em NOOR, Arshad; PELED, Ariel. Access Control. In: ISOM, David K.; NELSON, Sharon D.; SIMEK. John W.(editores). Ibid, é possível ver a explicação mais técnica da autenticação, que é aqui trazida no seu original: "*Authentication is the process of verifying the credential presented to computer. This is necessary to ensure that credentials are not being spoofed by masqueraders. Authentication is generally accomplished by the requester responding to a challenge posed by computer. Just as the sentry challenged Patrick Henry to prove his identity by implicitly demanding knowledge of a secret word or phrase that established his identity, the computer typically requires knowledge or possesion of a secret associated with the presented credencial that verifies the credential presented to the computer.*" p. 74.

197 No jargão técnico, os tipos de autenticação são chamado de "fatores". A cumulação de mais de um fator de autenticação é conhecido como "multifactor authentication" e envolve: *something the person knows; something the person possesses; something the person is*. Cf. SMEDINGHOFF, Thomas J.. *Information Security Law: The Emerging Standard for Corporate Compliance*. Ely: IT Governance Publishing, 2008, p. 11-12.

a) Com a utilização de um nome de usuário ou senha. Por meio do fornecimento desses dois dados e da comparação correta entre o par correspondente (senha estabelecida para aquele usuário) é que é feita a autenticação. Essa é a forma mais utilizada de controle de acesso na maioria dos serviços utilizados comumente na Internet, como e-mail, redes sociais, sites de notícias, etc.
b) Com a acumulação de um elemento que o usuário possua, além da senha, como cartões magnéticos, tokens geradores de senha automática ou ainda os certificados digitais utilizados para assinatura eletrônica. O usuário necessitará possuir algo mais, além da senha, para que seja feita a autenticação.
c) A terceira forma de autenticação consiste em analisar alguma característica física que o usuário possua. Nessa forma são utilizados dispositivos de biometria para a análise de impressões digitais, iris, palma da mão, etc.

Essas três formas de autenticação podem ser utilizadas tanto isolada quanto concomitantemente. Se tais formas citadas forem utilizadas concomitantemente, maior será a segurança do processo de identificação. Um exemplo bastante conhecido do duplo nível de identificação diz respeito ao saque de dinheiro em caixas eletrônicos bancários. No saque, é utilizado um cartão (algo que a pessoa possui) e, concomitantemente, é necessário o fornecimento de uma senha (algo que a pessoa saiba). Se a pessoa possuir acesso a apenas um dos meios (a senha sem o cartão, ou o cartão sem a senha), por óbvio, não será liberado o acesso àquele sistema.[198]

A autorização, por fim, consiste em permitir que a pessoa tenha acesso aos recursos dispostos no sistema. A autorização determina, se alguém que foi autenticado pertence a um grupo ao qual é permitido acessar - ou controlar – alguma informação[199]. Caso a autenticação seja bem sucedida, autoriza-se a pessoa a ter acesso aos recursos.

198 A cumulação destas duas formas, pode perder o nível de segurança, caso o cartão possa ser clonado.

199 MERRIL, Charles R.. Terms and Definitions: ISOM, David K.; NELSON, Sharon D.; SIMEK. John W.(edit.). *Information Security for Lawyers and Law Firms*. Chicaco: American Bar Association Publishing, 2006, p.9

Em um resumo: primeiro identifica-se alguém; com a autenticação verifica-se se a identificação fornecida confere com as credenciais armazenadas no sistema; com a autenticação positiva, autoriza-se o acesso.

Reinaldo Demócrito Filho, em relação aos ataques à infraestrutura bancária, entende que a autenticação de usuários deve ser ampliada para impedir a responsabilização dos bancos.[200] O autor entende que devem ser implementadas ações de mais um de nível de autenticação, abrangendo não apenas o uso de senha, mas também dispositivos de geração de senha aleatória (os chamados tokens de geração de senha), ou cartões de senha. Caso o banco não ofereça tal dispositivo, seria ele responsável pelos incidentes digitais, já que o sistema teria um vício de funcionalidade, na medida em que não protege adequadamente a confidencialidade dos dados. Na verdade o que se vê aqui nesse contexto é uma implementação insuficiente de segurança no que diz respeito ao controle de acesso[201].

No caso de um sistema que utilize os três níveis de autenticação, estabelece-se um alto grau de segurança, ficando praticamente impossibilitada a violação ou o acesso não autorizado. Em tal situação (com a utilização de três níveis de identificação/autenticação), é praticamente impossível a violação de acesso. Mesmo

---

200 FILHO, Demócrito Reinaldo. A responsabilidade dos bancos pelos prejuízos resultantes do phishing. *Jus Navigandi*, Teresina, ano 12, n. 1836, 11 jul. 2008. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=11481>. Acesso em: 12 Fev. 2012, p. 27.

201 Em LESSIG, Lawrence. Ibid, p. 41, é possível ver uma referência ao nível de escolha de métodos de identificação e autenticação: "*Obviously, some credentials are better than others. Some are architected to give more confidence than others; some are more efficient at delivering their confidence than others. But we select among the credentials available depending upon the level of confidence that we need.* " É interessante ver a comparação que Lessig faz com ambientes hostis e não hostis, através do exemplo da confiança existente em pequenas cidades: "*We are constantly negotiating these processes of authentication in real life, and in this process, better technologies and better credentials enable more distant authentication. In a small town, in a quieter time, credentials were not necessary. You were known by your face, and your face carried with it a reference (held in the common knowledge of the community) about your character. But as life becomes more fluid, social institutions depend upon other technologies to build confidence around important identity assertions. Credentials thus become an unavoidable tool for securing such authentication.* " p. 42,

assim, isso não impede que a pessoa devidamente autenticada venha a utilizar a informação de forma inadequada[202].

O controle de acesso também pode ser entendido como uma expressão da reidentificação virtual, já que os contatos no ambiente tecnológico possuem alto grau de impessoalidade dificultando a imediata identificação dos envolvidos.[203] Na verdade, a não utilização de métodos de identificação no ambiente virtual faz com que o autor das ações seja comparado a um “homem invisível”.[204]

Os aspectos de acesso autorizado e não autorizadas serão vistos a seguir.

C.3 - Acesso autorizado e não autorizado

Em relação ao controle de acesso, deve ser explicada a diferenciação entre autorização e permissão de acesso. Tulio Lima Vianna expõe de forma bastante didática essa diferença. Segundo o autor, permissões de acesso "*são atributos que controlam o acesso a arquivos e diretórios em um sistema operacional*".[205] A permissão de acesso pode ser de leitura, escrita ou execução. Quando várias pessoas têm acesso a um sistema e, nesse sistema, há diversos níveis de informações (confidenciais, protegidas, públicas, etc), elas podem ter permissões

202 E não impede também que a invasão ocorra em função de outras falhas no sistema que não nos mecanismos de autenticação ou ainda se o titular das credenciais contribuir para a realização de uma fraude.

203 Cf. MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor : (um estudo dos negócio jurídicos de consumo no comércio jurídico)*. São Paulo: RT, 2004, p. 103. A autora ainda destaca que mesmo reidentificando o sujeito virtual, resta o problema da capacidade eletrônica, pois o de usuário da Internet e de uma contratação a distância nem sempre tem sua idade e sua capacidade plenamente identificada.

204 Conforme alegoria proposta por LESSIG, Lawrence. Ibid, p. 45. De outra banda, FROSINI, Vittorio, Ibid. p. 153, falava sobre a alegoria do homem artificial e sua relação com o novo mundo artificial: “*El hombre de hoy, em suma, es efectivamente un hombre artificial, de por sí un hombre-autómata, dotado de una conciencia doble, según que se considere a sí mismo, em su identidad originaria o 'natural' (como se decía alguna vez), o que se observe a sí mismo em su integración com el mundo 'artificial', creado por él mismo, el hombre em su alteridad.*”

205 VIANNA, Túlio Lima. *Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais*. Rio de Janeiro: Forense, 2003, p. 53 .

diferenciadas. Uma pessoa pode ter permissão de leitura de um arquivo, mas pode não ter a permissão de escrita, o que indica que ela não conseguirá alterar o arquivo. O exemplo trazido pelo autor refere-se a uma página de Internet: quando alguém acessa a uma página na Internet possui apenas permissão de leitura, visto que não consegue alterá-la.[206]

O conceito exposto no item anterior sobre autorização refere-se ao mecanismo de controle de autorização do acesso informático. Porém, segundo a interpretação de Vianna, há também o conceito jurídico de autorização. Segundo ele, a autorização significa a "*legitimidade jurídica que alguém possui para acessar determinados dados em um sistema computacional*". [207]

A autorização jurídica pode depender da condição de alguém ser proprietário dos dados; de ter permitido o acesso aos dados; da natureza jurídica da relação existente no contato informático; em virtude de relações de parentesco, etc.

A relação entre a permissão e a autorização pode variar. Quem tem a permissão de acessar um recurso pode não ter a autorização para tanto. Um exemplo simples ocorre no caso de um provedor de serviços de e-mail. O administrador do provedor de e-mails detém a permissão técnica de acesso aos arquivos dos e-mails dos usuários. No entanto ele não possui a autorização para a leitura dos e-mails. O mesmo pode aplicar-se em sistemas bancários: os administradores podem ter permissão de acesso aos dados bancários, mas não têm a autorização de acessá-los. [208]

Ainda acerca desse aspecto, a autorização de acesso pode ocorrer de forma expressa, por meio de políticas de uso dispostas em sites (quando a política afirma o que o usuário pode fazer ou como o provedor de serviço usará os seus dados),

206 O exemplo do autor abrange uma página estática. É evidente que existem páginas em que o conteúdo pode ser alterado pelo usuário, como as redes sociais e um blog pessoal.

207 Idem, Ibid, p. 53.

208 E se assim o fizerem, podem cometer o crime de violação de sigilo bancário, assim disposto na lei complementar 105/2001.

também por meio das políticas de acesso empresariais (que definem qual o uso autorizado dos recursos pelos empregados) e por meio de contrato ou outra forma escrita. Já a autorização tácita[209] ocorre pela natureza do contato entre o proprietário e o autorizado, pela manifestação exterior de concordância do acesso, ou outra circunstância específica. Nesse sentido, a jurisprudência já cuidou de situação em que alguns arquivos foram deletados por quem possuía a permissão técnica para tanto, sem haver, no entanto, a clareza acerca da autorização para a deleção. Foi levado em consideração que a parte possuía a permissão para deletar os arquivos, tanto que conseguiu deletá-los, e isso prevaleceu na falta da certeza da autorização.[210]

209 O conceito de autorização tácita também é importante no âmbito criminal, principalmente após a lei 12.737/2012 que atualiza o Código Penal. Assim, o novo crime de invasão de dispositivo informático do art. 154-A do CP só pode ser cometido se a invasão ocorrer "*sem autorização expressa ou tácita do titular do dispositivo.*"

210 Nessa decisão também foi avaliado o fato de que os arquivos deletados puderam ser recuperados, o que certamente possui impacto na decisão. Porém, mesmo que incidentalmente, foi tratada a questão da permissão de acesso.
TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70019549971. Rádio e TV PortoVisão Ltda X Kapitanski Representações Ltda. Relator: Des. Odone Sanguiné. Porto Alegre, 4 de Julho de 2007. Ementa: APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL POR ATO ILÍCITO. NULIDADE DA SENTENÇA AFASTADA. EXCLUSÃO DE ARQUIVOS DE COMPUTADOR SEM PERMISSÃO. PREJUÍZOS MATERIAIS E MORAIS INDEMONSTRADOS. SENTENÇA MANTIDA. 1. A sentença expõe, de maneira clara, as razões do seu convencimento, com a citação dos indigitados depoimentos testemunhais nos pontos em que entendeu necessários. A ausência de menção a argumentos lançados ao longo da instrução não tem o severo condão de nulificar o ato sentencial, se bem fundamentado, com razões de decidir em consonância com o dispositivo, como no caso vertente. 2. Impende analisar a prova dos autos para aferir a presença dos pressupostos da responsabilidade civil no caso: o ato ilícito, consubstanciado na exclusão de arquivos de computador importantes para a empresa demandada, sem a permissão desta; os danos materiais e morais advindos desta conduta e o nexo de causalidade entre os dois últimos elementos. O depoimento pessoal da ré e testemunhal de pessoas ligadas ao acontecimento não amparam um juízo de certeza sobre a ilicitude da conduta da ré tampouco sobre os prejuízos alegados, motivo pelo qual, adianto o veredicto de manutenção da sentença guerreada. 3. Com efeito, restou sobejamente comprovado que a empresa da demandada prestava serviços de promoção e intermediação na captação de publicidade comercial e de patrocínio, agenciando propostas ou pedidos e encaminhando-os à demandada (contrato de fl. 10). Para tal desiderato, a ré utilizava-se da estrutura material da autora para o seu trabalho, incluindo as suas dependências e os seus computadores. De fato, funcionários da demandada realizavam reuniões no interior do estabelecimento da ré e possuíam senhas pessoais para acessar o sistema de computadores, a exemplo da representante da ré. Portanto, nada houve de ilícito na atitude da preposta da demandada em adentrar na empresa-ré durante a madrugada, como era comum de acontecer, acessar os seus arquivos pessoais, com senha pessoal, apagando alguns. Trata-se de relação terceirizada, e os arquivos estavam à total disposição da representante legal da empresa-ré, tanto que conseguiu deletá-los. Não eram arquivos de uso restrito, tampouco insuscetíveis de recuperação, conforme a própria demandada assume. 4. Para o acolhimento dos danos materiais não é suficiente simples alegação de sua ocorrência. Devem restar sobejamente comprovados, o que não ocorreu no caso vertente. Ao revés, a prova testemunhal indica que não houve prejuízo no trabalho após a exclusão dos

As políticas de uso (ou de privacidade) dos sites e serviços também podem estabelecer ou autorizar o fornecedor de serviços a acessar informações relativas ao serviço prestado.

Quem detém as permissões tecnológicas de acesso mas não possui a autorização jurídica e mesmo assim pratica ações em desacordo com a autorização, realiza o chamado excesso no acesso autorizado. Nas palavras de Vianna:

> "*autorização de acesso que o superusuário tem em relação a todos os arquivos do sistema, não implica um reconhecimento jurídico de poderes arbitrários a ele. Sua autorização de acesso pleno é meramente operacional e se limita às necessidades próprias de administração do sistema. [...] Ainda que tecnicamente ele tenha permissão para acessar qualquer dos dados armazenados no sistema, juridicamente sua autorização está limitada à necessidade e aos fins deste acesso.*"

Diante do exposto, acerca do controle de acesso, entende-se que há um dever geral de controlar o acesso a uma infraestrutura tecnológica que armazene dados. A natureza das informações armazenadas, ou de um sistema, orientam que a medida de controle de acesso seja ou não utilizada. Como exemplo, é possível citar a publicação de um site de notícias na Internet. Se as informações ali disponibilizadas são públicas, não há motivos para limitar o acesso por meio da implementação de medidas de controle de acesso. Por sua vez, caso se trate de um site que disponibilize informações confidenciais, ou protegidas por sigilo[211], ou reservadas ao acesso apenas de algumas pessoas, há a real necessidade de implementação de medidas de controle do acesso.

---

arquivos. 5. A prova testemunhal nada aponta no sentido do acolhimento dos prejuízos extrapatrimoniais, a indenização pleiteada não merece acolhimento. REJEITARAM A PRELIMINAR. DESPROVERAM O RECURSO DE APELAÇÃO. UNÂNIME.

211 O exemplo mais simples é um site de HomeBanking. É possível ver a lição de DE VILLIERS, Meiring. Ibid, p. 134: "*Valuable property is usually secured by measures that require authentication, such as through a valid key, an access card, or proof of identity.*"

O controle de acesso a uma determinada informação protege primeiramente o atributo de confidencialidade da informação. A única maneira de permitir o acesso a uma informação controlada é por meio da identificação do usuário autorizado a acessá-la. Por sua vez, um controle de acesso aplicado incorretamente pode permitir que, erroneamente, alguém não autorizado possua as permissões tecnológicas para a manipulação das referidas informações. Em tais casos a pessoa não autorizada poderia deletar ou alterar os dados.

Utilizando o mesmo exemplo do site de Internet de notícias, levando-se em consideração que as informações a serem acessadas são públicas, não há a necessidade de implementação de medidas de controle de acesso para o acesso de leitura dessas informações. Por sua vez, o fato de as informações serem públicas e, assim, poderem ser acessadas por qualquer pessoa, não significa que qualquer pessoa possa alterar o conteúdo das informações publicadas no site.

O controle de acesso pode servir, nessa situação, para impedir apenas a alteração das informações no site. Além do mais, a própria existência de uma medida de controle de acesso a um determinado sistema informático é uma demonstração que seu administrador dá de que aquele sistema é protegido.

O que se quer afirmar com essa exposição acerca do controle de acesso é que, quando um responsável deixa de cumprir com esse requisito básico de segurança, ou seja, estabelecer a medida de controle de acesso a informações sensíveis ou sigilosas armazenadas em meio digital, descumpre ele o dever de segurança da informação, e acarreta as conhecidas consequências jurídicas do descumprimento de um dever jurídico.[212]

212 Ver, por exemplo, a lição de DE VILLIERS, Meiring. Ibid, p. 135, onde a não tomada de certas medidas de proteção, permite, inclusive a execução de ações criminosas: "*Situations such as an unlocked door, strategically positioned scaffold, or electronic access, are valuable opportunities to a criminal, because they enable a level of access that normally requires authentication. The opportunity also lowers a wrongdoer's transaction cost. A thief can use brute force to break into a house, but exploiting an unlocked door or conveniently placed scaffold requires less physical exertion, produces faster results, and is less likely to attract attention than a more forceful entry.*".

Além do mais, o controle de acesso deve ser eficiente e adequado, cumprindo com eficiência a função de controlar o acesso. Um exemplo de um controle de acesso inadequado é aquele que permite os usuários escolherem senhas fracas, de fácil adivinhação[213]. O sistema informático que realiza o controle de acesso não deve permitir senhas de natureza simples, o que inviabiliza e diminui a eficiência do mecanismo técnico. [214]

Ainda, o próprio sistema de controle de acesso também deve ser configurado de modo a permitir que a senha seja trocada em períodos regulares, impedindo a reutilização de senhas antigas. O sistema deve registrar as tentativas de acesso e também bloquear o acesso àquele nome de usuário, se realizadas diversas tentativas infrutíferas de acesso.[215]

Se há, por sua vez, a responsabilidade do mantenedor pelo serviço em manter uma estrutura adequada e segura de controle de acesso, há, por outro lado,

Especificamente no common law, o autor destaca mais adiante, na p. 143, que: "*The common law pattern shows that enablers foreseeably encourage tortious and criminal behavior when they provide opportunities that are scarce, easily exploitable, aligned with the objectives of the criminal, and that provide the criminal with anonymity, unauthenticated access, and access with low complexity.* "

213 Por exemplo, sequências simples como "*1234*", "*4321*", "*qwerty*" ou palavras comumente usadas como "*senha*", "*password*", "*letmein*", etc. Além do mais, o sistema deve impedir que se utilize o mesmo nome de usuário como senha. A norma técnica NBR ISO/IEC 27002, trata no item 11.3.1 – Uso de Senhas, algumas indicações sobre uso de senhas, indicando que deve ser estabelecido um tamanho mínimo para a senhas e "*2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário; 3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário) ; 4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos*." Ver ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*. Tecnologia da informação. Técnicas de segurança. Sistemas de gerência da segurança da informação. Rio de Janeiro, 2005, p. 69.

214 Sobre isso, ver também GARFINKEL, Simson; SPAFFORD, Gene. Ibid, p. 62-63. Os autores fazem a analogia de que uma senha mal escolhida seria semelhante a "open doors" enquanto que boas senhas seriam "locked doors".

215 Isso é necessário pois há programas com o único fim de "adivinhar" senhas. Baseados em palavras de dicionário e também em combinações mais comuns, estes programas tentam realizar diversas combinações possíveis para conseguirem "adivinhar" as senhas. Sendo assim, com a rapidez que o computador permite, uma senha simples (como 1234) pode ser facilmente descoberta com o uso de tais sistemas. Se, no entanto, o sistema de controle de acesso consegue bloqueà-lo após uma série de tentativas infrutíferas, antecipa-se ao uso de tais sistemas. Quem utiliza sistemas corporativos com frequência certamente já passou por situação semelhante, ou seja, o bloqueio da conta de acesso por excesso de número de tentativas.

o dever do usuário em manter em sigilo suas credenciais de acesso. É requisito básico para a segurança do processo de controle de acesso, que o titular das credenciais, as mantenha em absoluto sigilo. É o sigilo de conhecimento das credenciais que garante a segurança do sistema.

Embora a doutrina reconheça que é do mantenedor do sistema a responsabilidade pelas falhas nos processos de identificação, entende-se que esta pode ser afastada nos casos de desídia do utilizador na manutenção de sigilo de sua senha ou, por óbvio, nos casos de auto fraude.[216] É evidente que nas relações de consumo, as eventuais alegações de auto fraude do consumidor devem ser provadas pelo próprio fornecedor. Isso ocorre, principalmente, pelo fato de o fornecedor possuir todo o controle sobre sua infraestrutura e ser o único capaz de conseguir realizar essa prova (com a produção de logs de acesso e de uso do serviço).[217]

A partir deste momento, analisar-se-á a questão da privacidade na sociedade da informação.

---

216 Ver a lição de Cláudia Lima Marques na apresentação da obra de Fabiano Menke: "*Assim, aquele que se organiza para negociar por meio eletrônico profissionalmente, deve suportar o risco de identificação e imputação errônea de uma vontade negocial. Dessa forma, a jurisprudência alemã tem demonstrado que a utilização de uma senha ou PIN no caixa eletrônico não é – sozinha – indício suficiente de falta de diligência do consumidor-leigo em manter em segredo e em outro lugar sua senha, pois o terceiro pode ter "descoberto" a senha e o risco de segurança das senhas é do profissional*". MENKE, Fabiano. Ibid.

217 Sobre isso ver TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 3ª Turma Recursal Cível. Recurso Inominado n. 71002243293. Maria Elena Abdala Pinheiro X Banco do Estado do Rio Grande do Sul S/A. Relator: Eugênio Facchini Neto. Porto Alegre, 28 de Janeiro de 2010. Ementa: REPARAÇÃO DE DANOS MATERIAIS E MORAIS. TRANSFERÊNCIA DE VALORES E PAGAMENTO DE DOC. BANCÁRIO VIA Internet. ALEGAÇÃO DE FRAUDE. IMPUTAÇÃO DA AUTORIA DA OPERAÇÃO À CORRENTISTA. AUSÊNCIA DE PROVA NESSE SENTIDO. DEMONSTRAÇÃO QUE INCUMBIA AO BANCO. DANOS MORAIS CONFIGURADOS, NA HIPÓTESE CONCRETA. 1. Ao imputar à demandante a responsabilização pelas operações bancárias realizadas via Internet, era do banco, sem dúvida, o encargo de produzir prova cabal nesse sentido, não só por se tratar de relação de consumo, sendo o fornecedor o único detentor de tais dados, mas notadamente porque da parte autora não se pode exigir a produção de prova negativa. 2. Danos morais configurados, no caso concreto, ante a negativa de restituição dos valores, com privação de capital significativo por mais de cinco meses e, especialmente, em razão do constrangimento decorrente da injusta acusação do banco no sentido de que a autora teria contribuído para a efetivação da fraude, ao repassar dados a terceiros não autorizados. Atendimento, também, da função dissuasória da responsabilidade civil. RECURSO DESPROVIDO.

D) A privacidade na sociedade da informação

No Brasil, a privacidade tem status de direito fundamental.[218] Sobre esse assunto, Têmis Limberger, ancorada na lição Peter Häberle, afirma que os direitos fundamentais possuem dupla perspectiva:

> "*de um lado, como garantias da liberdade individual (direitos de defesa), e, por outro, como instituições que fazem operativos os conteúdos dos direitos para a consecução dos fins sociais e coletivos constitucionalmente proclamados.*"[219]

O direito à intimidade e à vida privada tem como núcleo:

> "*a faculdade concedida ao indivíduo, a todos oponível, de subtrair à intromissão alheia e ao conhecimento de terceiros certos aspectos da sua vida que não deseja participar a estranhos, ou seja, de decidir o que vai desnudar aos outros, de que forma e em que circunstâncias.*"[220]

---

218 Cf. RIBEIRO, Luciana Antonini. Ibid, p. 151: "*No Brasil, a Constituição Federal de outubro de 1988, ao dispor sobre a inviolabilidade de correspondência, vedando a interceptação telefônica e a invasão de domicílio, bem como resguardando, expressamente, o direito à intimidade e à vida privada de cada um dos cidadãos brasileiros, deu à privacidade status de direito fundamental.*"
Já na União Europeia, a Carta dos Direitos Fundamentais da União Europeia (2010/ C 83/02), em seu art. 8º fala especificamente sobre a Proteção de dados pessoais, assim estipulando:
1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

219 LIMBERGER, Têmis. *O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007, p. 109-110. Mais adiante, complementa, baseada em Alexy, que o "*o direito à intimidade com relação à informática pode ser denominado como um direito a algo, levando em conta seu objetivo. São direitos a ações negativas (direito a não ser molestado) e positivas (direito de acesso, retificação, etc).*" p. 112

220 CARVALHO, Ana Paula Gambogi. Ibid, p. 83-84. Essa autora entende ainda que não é importante a diferenciação entre as expressões "intimidade e vida privada" assim dispostas na

Tais direitos são considerados como direitos da personalidade,[221] tendo como fundamento principal o art. 1º, inc. II da Constituição Federal que consagra o princípio da dignidade da pessoa humana, "*segundo o qual a pessoa humana é o fundamento e o fim da sociedade, Estado e do Direito.*"[222] Igualmente possuem previsão, como se sabe, nos arts. 11 a 21 do Código Civil.[223] Já a natureza jurídica do direito à intimidade "*possui caráter personalíssimo e ligado à existência do*

Constituição, principalmente pelo fato dos efeitos jurídicos de sua violação, serem os mesmos. p. 85. No mesmo sentido LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 80, que entende essa discussão como meramente acadêmica sem repercussão prática.

221 De acordo com PAREDES, Marcos. Violação da privacidade na Internet. *Revista de Direito Privado*, São Paulo, n. 9, jan.-mar./2002, p. 184, "*Os direitos da personalidade são, portanto, direitos subjetivos que têm por objeto o bem jurídico da personalidade, ou seja, a titularidade de direitos e deveres que se consideram ínsitos em qualquer ser humano, no seu aspecto físico, moral e intelectual.*"

Igualmente, Diógenes Ribeiro, ao dissertar sobre as características dos direitos da personalidade, menciona que "*São direitos essenciais. São direitos não patrimoniais, porque a vida, a integridade física e a liberdade não contêm em si uma utilidade econômica. São direitos absolutos, porque são comuns a todas as pessoas, numa relação com a generalidade das outras pessoas. São direitos intransmissíveis, sendo, por isso, inseparáveis do sujeito originário. São indisponíveis, porque não se pode determinar o destino de tais direitos; eles não podem mudar de pessoa nem mesmo pela vontade do titular daquele direito. O exemplo mais claro é o de alguém não poder se tornar escravo vendendo a sua liberdade. São direitos irrenunciáveis, pois o consentimento não constitui uma renúncia, não produzindo a extinção do direito.*" RIBEIRO, Diógenes V. Hassan. *Proteção da Privacidade*. São Leopoldo: Unisinos, 2003, p. 24.

222 Idem. Ibid, p. 185. Em Portugal, a Constituição possui disposição específica acerca da "Utilização da informática" que envolve também a privacidade e a questão de dados pessoais. Assim dispõe seu art. 35:

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

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

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

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

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

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

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

Na Constituição espanhola, no art. 18.4, também é definida a proteção da intimidade quando do uso de recursos informáticos.

223 No Código Civil Italiano, os direitos da personalidade são "previstos parcialmente" fazendo com

indivíduo."[224]

Diógenes Ribeiro afirma que:

> "*O direito à intimidade e à vida privada é considerado, numa classificação oriunda do direito civil, um direito da personalidade. Diversamente, no direito constitucional, está inserido nos direitos humanos [...] Os direitos da personalidade constituem uma parte especial dos direitos fundamentais, pois, se entre tais direitos houver alguma hierarquia, em eventual colisão de direitos, os direitos da personalidade ocupam um lugar privilegiado.*"[225]

Assim, os direitos da personalidade positivados no Código Civil[226] não devem ser lidos "*de forma a excluir outras hipóteses não previstas; na verdade, mais importante que este (aliás tímido) elenco é a sua leitura à luz da cláusula geral de proteção da personalidade presente na Constituição.*"[227]

Se nos países de *Civil Law* o modelo de privacidade tem como principal fundamento a dignidade da pessoa humana, o mesmo não ocorre nos países de *Common Law*. Nestes, o principal fundamento da privacidade é a própria liberdade. Ainda assim, mesmo nos sistemas de *Common Law* do Reino Unido e dos EUA:

> "*há diferenças significativas entre o âmbito de proteção do direito à privacidade. Além disso, ainda que o direito europeu caminhe, por*

---

que o direito italiano tenha positivado um maior número de direitos protegidos. Já o direito brasileiro optou por utilizar uma cláusula aberta. Cf. MIRAGEM, Bruno. Os direitos da personalidade e os direitos do consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 425.
Quanto à previsão no código civil italiano, eles estão nos arts. 5º a 10º: Art. 5º Atti di disposizione del proprio corpo; Art. 6º Diritto al nome; Art. 7º Tutela del diritto al nome; Art. 8º Tutela del nome per ragioni familiari; Art. 9º Tutela dello pseudonimo; Art. 10º Abuso dell'immagine altrui.

224 LIMBERGER, Têmis. *O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007, p. 116.

225 RIBEIRO, Diógenes V. Hassan. *Proteção da Privacidade*. São Leopoldo: Unisinos, 2003, p. 23.

226 Arts. 11 a 21.

227 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 96.

> *meio de diversas diretivas relacionadas à privacidade, para uma uniformização relativa - ao menos no que tange aos padrões mínimos de proteção - há importantes diferenças culturais entre os países membros da União Europeia, aos quais influenciam, por óbvio, a transposição desses padrões mínimos no direito interno de cada nação. Dificuldades similares impedem a adoção de padrões mundiais da privacidade, ainda que não faltem iniciativas nesse sentido.*"[228]

Têmis Limberger ressalta que diante desse novo cenário, a garantia da efetividade dos direitos fundamentais e da própria intimidade "*diante do fenômeno informático, em particular, é a grande questão enfrentada pelos juristas, considerando as invasões que se costumam ocorrer nos bancos de dados*".[229]

Deve ser considerado, nessa realidade de informações massificadas, o amparo e o cuidado aos direitos e às liberdades individuais tanto nas comunicações informatizadas bem como no comércio eletrônico.[230] Não é raro ocorrer, nas redes sociais por exemplo, a mais absurda violação de direitos fundamentais, seja mediante discursos racistas ou violação de privacidade e intimidade, ainda a publicação de materiais protegidos por direitos autorais e também, em países com regimes ditatoriais e não democráticos, há o impedimento da livre manifestação do discurso pela Internet, ou seja a liberdade de comunicação[231].

---

228 LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 49 a 51. Há quem entenda também que "*os princípios que norteiam o direito europeu podem, embora de forma implícita, ser identificados no nosso ordenamento jurídico. Entretanto, a opção pela ausência de disciplina legislativa, no Brasil, acaba, na prática, por transferir para o mercado a tarefa de auto-regulamentar a matéria, interpolada por intervenções estatais, em geral, marcadas pelo recurso às razões de Estado.*", cf. CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito - UFPR*, Curitiba, n. 47, 2008, p. 148.

229 LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007, p. 196.

230 Ver a lição de Cesar Santolim quando ensina que: "*O tema da proteção dos dados referentes aos consumidores, na realidade, está conectado a uma tutela mais ampla, que diz respeito aos direitos fundamentais da pessoa humana, como vêm reconhecendo a doutrina e a jurisprudência.*" SANTOLIM, Cesar Viterbo Matos. Ibid, p 70.

231 Assim ensina Peter Häberle, ao falar sobre a liberdade de comunicação: "*peça de conexão ou transmissão, sem a qual o nexo entre a dignidade humana e a democracia pluralista nem poderia*

Há muito tempo são utilizados dados de consumidores recolhidos nas mais variadas atividades para a criação de perfis. Se em alguns casos há a violação da privacidade e intimidade do usuário, há também, por outro lado, vantagens. É possível, por exemplo, por meio da criação de perfis de consumo ou da análise de conteúdo de mensagens de e-mails dos usuários, a oferta personalizada[232] de produtos, bem como o atendimento

> "*dirigido e personalizado, possibilitando o tratamento de cada consumidor como sujeito único, merecedor de atenção. Em uma sociedade massificada, com atendimento generalizado e atenção individual dispensada ao consumidor próxima a zero, o tratamento personalizado retrata algo há muito perdido na sociedade do consumo.*"[233]

tornar-se realidade: refiro-me às assim chamadas 'liberdades de comunicação' que adquiriram, mormente na época atual das novas tecnologias midiáticas (Pcs de uso doméstico, multimídia, Internet e online banking) possibilidades antes nem pensadas, mas também geraram vários riscos. O conceito de 'liberdades de comunicação' deve ser compreendido aqui nos termos mais amplos imagináveis: principia com a tríade da liberdade religiosa, artística e científica, passa pela liberdade de opinião, informação, imprensa e manifestação, bem como plea liberdade de reunião, também pela liberdade de associação (sem esquecer nesse contexto a liberdade dos partidos políticos) e se estende até as formas precursoras e as instâncias precedentes das competências estatais." HÄBERLE, Peter. A dignidade humana e a democracia pluralista – seu nexo interno. In SARLET, Ingo Wolfgang (org). *Direitos fundamentais, informática e comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007, p 11-28.

232 A oferta personalizada de produtos também é conhecida como a super individualização de produtos e serviços, conforme Ian Ayres: "*This hyper-individualized segmentation of consumers also letes firms offer new personalized services that clearly benefit society.*" AYRES, Ian. Ibid, p. 32.

233 RIBEIRO, Luciana Antonini. Ibid, p.151.

O armazenamento crescente de dados pessoais, por sua vez, faz com que se reavalie o conceito de privacidade. A tradicional ideia do "*right to be let alone*"[234] é insuficiente[235] para a atual realidade[236]. Conforme a lição de Danilo Doneda:

> "*Neste novo panorama, a privacidade deixa de ser um meio de garantir o isolamento de alguns para cumprir também uma outra função, que é reagir contra políticas de discriminação baseadas em opiniões e opções religiosas, políticas e sexuais, bem como de toda sorte de informações privadas […] Pode-se considerar, emblematicamente, uma transformação na definição do direito à privacidade, do "direito a ser deixado em paz" para o "direito a controlar o uso que outros fazem das informações que me digam respeito.*"[237]

Na verdade, a ideia de privacidade vista apenas como o impedimento contra interferências alheias constitui uma visão insuficiente da questão. Em primeiro lugar, por que não são todas as interferências alheias que violam a privacidade. Em segundo lugar, e este é o motivo principal, pois esse conceito falho de privacidade

---

234 BRANDEIS, Louis; WARREN, Samuel. The right to privacy. *Harvard Law Review*, Cambridge, v. IV, n. 5. Dec. 1890. No mesmo sentido ver a ressalva de Lorenzetti: "*En este contexto, la privacidad no es sólo la reserva del "derecho a estar solo", sino un problema de comunicación: el dato ulteriormente utilizado sin consentimiento para construir un perfil del sujeto.*". LORENZETTI, Ricardo Luis. *Tratado de los contratos*. Buenos Aires: Rubinzal y Asociados, 1999. Tomo III, p. 866.

235 Cf. RODOTÀ, Stefano. Ibid, p. 24. O autor ao falar sobre o de controle sobre os próprios dados argumenta que "*não que este último aspecto estivesse ausente das definições tradicionais: nelas, porém, ele servia muito mais para sublinar e exaltar o ângulo individualista, apresentando a privacidade como mero instrumento para realizar a finalidade de ser deixado só; enquanto hoje chama a atenção sobretudo para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados.*"

236 Marcel Leonardi ensina que esse conceito é falho pela sua amplitude. Segundo ele "*definido dessa maneira, seria possível concluir que qualquer conduta direcionada a outra pessoa, quer ilícita ou não – uma agressão física, ou simplesmente pedir informações quando se está perdido, por exemplo – seria uma violação de sua privacidade. Tutelar a privacidade nessa medida significaria aniquilar o convívio humano e a formação de relações sociais; é por isso que se afirma que a intimidade só faz sentido como fenômeno emergente da vida em sociedade, de relações intersubjetivas*". LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 54.

237 Cf. DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em: 12 Fev. 2012, p. 7.

não abrangeria as questões como "*a coleta, o armazenamento e o processamento de dados pessoais que não revelam segredos, não identifiquem imediatamente a pessoa nem perturbem a solidão.*"[238]

Há um argumento utilizado nos EUA pelos defensores da diminuição da defesa da privacidade em nome da segurança[239], que defende a ideia de que quem não tem nada a esconder não deve se preocupar com eventuais violações à privacidade. Aqueles que não promovem atividades ilegais, com base neste argumento, poderiam ficar livres de preocupações.[240] Esse argumento é absolutamente perigoso e promove a formação de um estado policialesco e vigilante. Além do mais, a falha principal desse argumento baseia-se na premissa de que a privacidade consiste apenas em esconder coisas erradas.[241]

A doutrina critica também a ideia de privacidade vista apenas como a proteção do sigilo, com o estabelecimento de um binômio de informações públicas-privadas.[242] Essa também pode ser considerada equivocada pois:

> "*ignora a existência de relações privadas limitadas aos membros de um grupo, e não reconhece que o indivíduo pode querer ocultar*

238 LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 61.

239 Sobre isso a observação de CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito - UFPR*, Curitiba, n. 47, 2008, p. 145. "*Da perspectiva do Estado, notadamente nos países do hemisfério norte, tem-se buscado, sob o fundamento da garantia da segurança pública, incrementar as tecnologias de controle de acessos e saídas a determinados locais e também de circulação de pessoas em lugares públicos pela combinação da tecnologia de codificação de dados biométricos com câmeras de vigilância, do mesmo modo, verificam-se o aumento numérico e a melhoria qualitativa dos bancos de dados de impressões digitais e de DNA à disposição das polícias e outras instâncias estatais de controle social. […] Isso se verifica em países os Estados Unidos e nos países europeus, que justificam essas limitações ante a necessidade de combater o terrorismo.*"

240 Cf. SOLOVE, Daniel J. Ibid, p. 746-747 "*When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remain private. Thus, if an individual engages only in legal activity, she has nothing to worry about. [...] Sometimes the nothing to hide argument is posed as a question: "If you have nothing to hide, then what do you have to fear?" Others ask: "If you aren't doing anything wrong, then what do you have to hide?*"

241 Idem. Ibid, p. 764.

242 LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 62.

> *determinadas informações apenas de pessoas específicas, compartilhando-as com outras.*"[243]

O sigilo não pode ser considerado um segredo absoluto, pois as pessoas podem desejar compartilhar informações privadas apenas com um grupo familiar, por exemplo, não desejando que tais informações saiam deste grupo.[244] É certo, há a necessidade da manutenção da confidencialidade entre informações privadas, pessoais e sensíveis, o que não se discute. Porém, é a questão do binômio público-privado que não parece adequada.

Da mesma forma, um conceito de privacidade visto apenas como o controle de informações e dados pela pessoa parece também ser insuficiente. Marcel Leonardi defende que a privacidade não é apenas aquilo que o indivíduo deseja proteger mas também "*engloba, preponderantemente, aquilo que a sociedade considera apropriado proteger*".[245] Ademais, esse princípio não representa uma limitação razoável sobre o que o indivíduo deseja proteger, parecendo exagerado que o indivíduo possa realizar o controle sobre todas as informações que o identifiquem. O autor afirma ainda que mesmo que fosse limitada a proteção às informações íntimas e sensíveis, isso teria pouca utilidade em função da possibilidade do cruzamento de dados.[246]

Têmis Limberger ensina que a questão dos "direitos sociais" necessita de uma estrutura para sua implementação, pois:

> "*são demandas positivas com cunho prestacional oponível ao poder público, por exemplo: saúde, segurança, educação e cultura, etc. O direito à intimidade começa num aspecto negativo, o direito de não ser molestado, e evolui em direção a um aspecto positivo, o direito a pedir prestações concretas do Estado. Daí resultam a objetividade*

243 Idem. Ibid, p. 64.
244 Idem. Ibid, p. 65.
245 Idem. Ibid, p. 75.
246 Idem. Ibid, p. 76.

> *dos dados, o direito ao esquecimento, a necessidade de prazo para armazenamento de informações negativas e a comunicação de repasse de dados, a fim de favorecer o direito de acesso e retificação de informação.*"[247]

Dessa maneira, quem "*confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente, seja em entidades públicas ou privadas*"[248] Assim, o chamado direito à autodeterminação informativa[249] é visto como o direito do cidadão "*tomar conhecimento sobre o arquivamento e uso de informações suas por terceiros, bem como de controlá-los e mesmo impedi-los.*"[250] Como consequência, há a necessidade da devida autorização do atingido para o armazenamento de informações em bancos de dados, de qualquer tipo de informação de cunho pessoal, abrangendo além dos dados de identificação até dados que tratem de "*seu caráter e a sua reputação, sua família, suas características individuais, sua condição financeira, seus hábitos, suas opiniões políticas, sua crença religiosa, etc*"[251] Esse direito possui uma estreita relação com a

---

247 LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). Direitos Fundamentais, Informática e Comunicação: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007, p. 208. Ver também o art. 43, §4º do CDC, que define que "*Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público*."

248 Idem. Ibid, p. 215.

249 Ver a lição de Danilo Doneda: "*Considerando-se a esfera privada como um conjunto de ações, comportamentos, preferências, opiniões e comportamentos pessoais sobre os quais o interessado deseja manter um controle exclusivo, esta tutela há de basear-se em um novo "direito à autodeterminação informativa", hoje possível de ser identificado em diversos ordenamentos, que estabelece condições para um efetivo controle das informações pessoais em circulação*." DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em: 12 Fev. 2012, p. 14. Segundo Silney Alves Tadeu, na Alemanha, o direito à autodeterminação informativa "*atingiu caráter de direito fundamental quando foi consagrado pelo Tribunal Constitucional alemão, através de uma sentença de 15.12.1982, oriundo de um recurso apresentado contra uma lei, de 25.03.1982, sobre o censo demográfico que havia excedido ao número de informações que solicitava de seus cidadãos...*" TADEU, Silney Alves. Algumas reflexões sobre a proteção da pessoa e o uso informatizado de seus dados pessoais. *Revista de Direito do Consumidor*, São Paulo, n. 79, jul.-set./2011, p. 86.
Esse direito também é chamado de "*libertad informática*" cf. LUÑO, Antonio-Enrique Pérez. *Manual de informática y derecho*. Barcelona: Ariel, 1996, p. 43. O autor afirma que a autodeterminação informativa é uma construção da doutrina jurisprudência e alemãs (*Recht auf informationelle Selbstbestimmung*) com base na clássica decisão do Tribunal Constitucional alemão de 1983. p. 44.

250 CARVALHO, Ana Paula Gambogi. Ibid, p. 93.

251 Idem. Ibid, p. 93.

questão da arquitetura da rede eis que, na prática, devem ser disponibilizados também mecanismos técnicos de controle para os usuários.

O direito à autodeterminação informativa também é representado pela questão da liberdade informática. A doutrina entende tratarem-se de direitos fundamentais de terceira geração que:

> "*em seu aspecto negativo, traduz-se no direito de evitar que certas informações pessoais caiam no domínio público e, em seu aspecto positivo, no direito ao controle dos dados concernentes à própria pessoa que ultrapassando a esfera da privacidade, tornam-se objeto de bancos e cadastros de dados eletrônicos.*"[252]

Da mesma forma, o referido direito merece guarida mesmo nas situações onde os dados não estão protegidos por sigilo "*pois, como os dados se referem à personalidade do cidadão, estão sob a sua esfera de autonomia."*[253]

Ricardo Lorenzetti faz uma interessante relação entre a privacidade, proteção do consumidor e o uso das novas tecnologias. Diz ele que:

> "*O direito à privacidade é de fundamental importância em termos de proteção do consumidor. A invasão do âmbito familiar através da tecnologia, o uso da Internet, a manipulação de dados pessoais em geral, os dados médicos, creditícios e no campo dos seguros. A privacidade de dados nas operações bancárias on-line além de*

252 Idem. Ibid, p. 108. Cabe o mencionar o alerta de DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 399-400. "*A impossibilidade de uma autodeterminação informativa baseada na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e a existência de estruturas destinadas à coleta de seus dados e preparadas a excluí-lo de cartas vantagens caso decida por não fornecê-los – assim, tal tutela singular reproduziria uma tradição algo elitista da privacidade, que não corresponde à sua atual posição na nossa carta constitucional...*"

253 MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, n. 79, jul.-set./2011, p. 62.

> *muitos outros aspectos relacionados com esta temática têm uma relevância de primeira ordem.*"[254]

Danilo Doneda, ao falar ainda sobre a evolução da privacidade, baseando-se na lição de Stefano Rodotà, ressalta que a questão da privacidade evoluiu do eixo "pessoa-informação-segredo" para um novo eixo "pessoa-informação-circulação-controle".[255] Marcel Leonardi, também citando Stefano Rodotá[256], adota o conceito de privacidade deste ao afirmar que ela é "*o Direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada*".[257]

Porém, a questão da privacidade não pode ser totalmente entendida sem a análise dos conceitos de dados pessoais e de dados sensíveis. Passa-se, agora, a essa tarefa.

D.1 - Dados pessoais e dados sensíveis

O direito comunitário, mediante o art. 2º, alínea a) da diretiva 95/46/CE[258] estabelece que dados pessoais podem ser classificados como:

> "*qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo*

254 LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 130.
255 DONEDA, Danilo. Ibid, 2006, p. 23.
256 Ver também RODOTÁ, Stefano, Ibid, p. 93: "*Partindo dessa constatação, pode-se dizer que hoje a sequência quantitativamente mais relevante é "pessoa-informação-circulação-controle", e não mais apenas "pessoa-informação-sigilo", em torno da qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de "circulação controlada", e não somente interromper o fluxo de informações que lhe digam respeito.*"
257 RODOTÁ, Stefano. Tecnologie e diritti. Bologna: Mulino. 1995, p. 122 *apud* LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 83.
258 UNIÃO EUROPEIA. *Diretiva 95/46/CE* – Diretiva Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de Outubro de 1995. Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu.

> *aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;*"

A mesma diretiva, também no art. 2º, alínea b) define a atividade de tratamento como:

> "*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;*"

No Brasil, a definição de dados ou informações pessoais não é específica. Há as disposições constitucionais acerca da privacidade nos art. 5º inc. X[259] e XII[260]. Ao mesmo tempo, acerca da proteção de dados, existem leis que indiretamente tratam da questão, como o próprio Código de Defesa do Consumidor, a Lei da Interceptação Telefônica (lei 9.296/96), a lei que regulamenta o *habeas data* (Lei 9.507/97) além da própria Lei de Quebra de Sigilo Bancário (Lei Complementar n. 105/01).[261] Igualmente o Código Civil, no seu art. 21, consagra a inviolabilidade da vida privada da pessoa natural.

A lei 12.527 de 18 de Novembro de 2011, embora trate de procedimentos de acesso a informações a serem observados pela União, Estados, Distrito Federal e

259 Art. 5º, inc X da CF: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

260 Art. 5º, inc XII da CF: "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;"

261 Conforme LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). Direitos Fundamentais, Informática e Comunicação: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007, p. 196 e 200.

Municípios, traz alguns conceitos importantes relativos ao tratamento de informações. Tais conceitos podem oferecer um apoio para a compreensão da questão de acesso às informações privadas. O art. 4º traz as seguintes definições:

> *I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;*
> *[…]*
> *IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;*
> *[…]*
> *V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;*
> *[…]*
> *IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.*

Na verdade, a noção de dados pessoais é bem ampla. José Antônio Peres Gediel e Adriana Espíndola Correa trazem como exemplos de dados pessoais: nome e endereço; número de telefone; números de documentos de identificação; currículos escolares; dados profissionais, fiscais e bancários; dados envolvendo dívidas e créditos bem como meios de pagamento; endereço eletrônico; imagens recolhidas por câmeras de segurança, fotografias disponibilizadas na Internet, etc.[262] Os dados ou informações pessoais possuem um ”*vínculo objetivo com uma pessoa.*”[263]

---

262 CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito - UFPR*, Curitiba, n. 47, 2008, p. 144.

263 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 156

Destaque-se que, o endereço IP utilizado para acessar a Internet também deve ser visto como um dado pessoal. Isso pois, ele é relacionado com as atividades realizadas pelos usuários na Internet. Assim, quando um usuário acessa uma página, quando posta um comentário em um blog, quando acessa um conteúdo pornográfico ou lê um artigo policial ou, ainda, realiza uma pesquisa sobre como fazer uma bomba, seu endereço IP é registrado.[264] Esses dados ficam armazenados nos provedores de serviços de Internet[265] e podem ser usados para a identificação das ações realizadas pelos seus usuários.

Em geral, os dados de internautas são recolhidos, em primeiro lugar, por meio do fornecimento feito pelo próprio usuário.[266] Basicamente o fornecedor de serviços solicita previamente o fornecimento desses dados. Com frequência, o preenchimento de tais formulários é acompanhado das chamadas políticas de privacidade (*também chamadas de políticas de uso, ou simplesmente de disclaimers*). Há também a possibilidade de recolhimento de informações mediante os chamados *cookies*. Segundo Luciana Antonini Ribeiro, os cookies:

> "*nada mais são do que programas que, uma vez instalados, identificarão aquele computador específico. Assim, quando o consumidor ingressa em um determinado site, o qual, em oportunidade anterior, instalou um cookie no computador do usuário, sua presença será detectada e individualizada.*"[267]

---

264 McINTYRE, Joshua J.. Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information. *DePaul Law Review*, Vol. 60, N. 3, 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621102>. Acesso em: 12 Fev. 2012, p. 3.

265 O endereço IP, sozinho, não significa nada mais do que um número. Para que ele possa ser compreendido é necessário cruzá-lo com outros dados, como por exemplo, o cadastro de clientes do provedor de acesso. Idem. Ibid, p. 18

266 Cf. PAREDES, Marcos. Violação da privacidade na Internet. *Revista de Direito Privado*, São Paulo, n. 9, jan.-mar./2002, p. 197-198. "*Muitas vezes o usuário da Internet é obrigado a preencher questionários pessoais antes de efetivar qualquer aquisição de produtos ou serviços. Outras vezes a mesma exigência é feita ainda que nenhum produto ou serviço seja adquirido. O problema que esta prática representa é a capturação de dados sensíveis e não sensíveis dos diversos usuários conectados na rede. A utilização desvirtuada de tais informações pode acarretar danos aos direitos da personalidade, pois vulneram a intimidade e a privacidade do internauta.*"

267 RIBEIRO, Luciana Antonini. Ibid, p. 157-158.

Na verdade, os *cookies*[268] são arquivos que contêm informações acerca do uso ou acesso a sites e podem ser interpretados pelos fornecedores de serviços na Internet. Os dados armazenados nos *cookies* podem ser "*cruzados com informações presentes em bancos de dados pessoais, possibilitando, assim, uma completa identificação do consumidor, bem como um rastreamento...*".[269] Além do mais, os *cookies* que não são deletados do computador do usuário podem fornecer um histórico completo de onde ele navegou na Internet.[270]

Quanto ao conceito de "dados sensíveis"[271], a recente lei 12.414/2011, ao estabelecer as vedações de anotações nos cadastros de adimplemento[272], traz esta definição no seu art. 3º, inc. II: "*informações sensíveis*[273]*, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas*". O anteprojeto

---

268 Outra explicação sobre os cookies: "*Cookies are simple text files stored on the end user's hard disk and they have many legitimate and beneficial uses, such as customising the content of a web page for an individual. A cookie tells the website that it's you who is looking at it*." Cf. GELBSTEIN, Eduardo; KAMAL, Ahmad. *Information Insecurity: A survivel guide to the uncharted territories of cyber-threats and cyber-security*. New York: United Nations ICT Task Force, 2002, p. 44

269 RIBEIRO, Luciana Antonini. Ibid, p. 158.

270 Cf. GELBSTEIN, Eduardo; KAMAL. Ibid, p. 44.

271 Também chamados pela doutrina de dados "*ultrasensíveis*" cf. RUIZ, Carlos Barriuso. Ibid, p. 145.

272 Ver também a sugestão de alteração do CDC assim proposta por Cláudia Lima Marques, através da criação do art. 43-A. O artigo assim prevê: "*Nos arquivos, coletas e bancos de dados, organizados pelos fornecedores que se utilizarem, seja para conclusão, seja para a execução, total ou parcial, de um meio eletrônico, de telemídia, teleshopping ou meio semelhante de comunicação de massa, os fornecedores somente poderão requerer informações não sensíveis e razoáveis dos consumidores. §1° Neste caso, os fornecedores que organizarem a coleta, o arquivo ou o banco de dados deverão igualmente organizar um meio técnico para que o consumidor possa manifestar sua vontade de que os dados não sejam arquivados e possa ter acesso posteriormente a seus dados, para corrigi-los. §2º Os fornecedores que coletarem, arquivarem, venderem, transmitirem ou organizarem estes dados coletados eletronicamente são responsáveis por qualquer dano deles advindo aos consumidores respectivos, tendo estes fornecidos os dados voluntariamente ou não*". MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 774-775. Acerca da questão dos organizadores serem responsáveis "por qualquer dano", não se sabe se a autora quis estender ao caso a responsabilidade integral pelos danos relacionados às informações armazenadas em banco de dados.

273 A Política de Privacidade do Google, disponível em http://www.google.com/intl/pt-BR/policies/privacy/ refere-se expressamente à coleta destes tipos de dados: "*Ao exibirmos anúncios personalizados, não associaremos cookies de navegador ou identificadores anônimos a determinadas categorias, como aquelas baseadas em raça, religião, orientação sexual ou saúde.*"

brasileiro de lei de proteção de dados pessoais, no seu art. 4º, inc. IV, estabelece uma definição mais completa acerca dos dados sensíveis:

> *dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos e biométricos;*

A doutrina ao caracterizar dados de caráter pessoal e sensíveis, assim define:

> "*Os dados de caráter pessoal contêm informação das pessoas físicas que permitem sua identificação no momento ou posteriormente. Na sociedade tecnológica, os cadastros armazenam alguns dados que possuem um conteúdo especial, e por isso são denominados dados sensíveis. Tais dados podem referir-se a questões como ideologia, religião ou crença, origem racial, saúde, ou vida sexual. Exige-se que os cadastros que os armazenem possuam uma segurança especial, como forma de evitar que sejam mal utilizados.*" [274]

274 LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007, p. 218. Conforme a autora, a lei argentina 25.326 foi uma das primeiras, na América Latina, a legislar sobre o assunto, p. 224. A referida lei conceitua as informações sensíveis (*datos sensibles*), em seu art. 2º: "*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.*"
Conforme DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 350, essa lei "*revela sua sintonia com os preceitos básicos do modelo europeu de proteção de dados pessoais. Ela procura estabelecer uma disciplina de proteção da pessoa, através da tutela de seus dados pessoais. A lei estabelece a obrigação de informação sobre o tratamento de dados pessoais, inclusive sobre sua finalidade e as suas consequências; a lei estabelece também um regime específico para dados sensíveis.*"

A definição do que são dados sensíveis[275] e o afastamento de seu recolhimento nesse contexto[276] representa um grande avanço da lei 12.414/2011. A sistemática de proteção ao consumidor não está limitada apenas na observância do CDC. A regra do art. 7º do CDC prevê expressamente que os direitos estabelecidos no código:

> "*não excluem outros decorrentes de tratados ou convenções de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e eqüidade.*"

Ora, em função do exposto, a proibição de anotações de informações sensíveis do parágrafo 3º do art. 3º da lei 12.414 de 9 de Junho de 2011 pode ser vista de forma ampla, em relação ao armazenamento de dados sensíveis do consumidor. Por outro lado, há a possibilidade do armazenamento de dados sensíveis com o consentimento explícito do usuário; em situações de associação com entidades sem fins lucrativos com finalidades políticias, filosófica, religiosas e sindicais; em situações de proteção da vida e incolumidade física e em situações envolvendo profissionais da área da saúde[277]. É certo que a doutrina e jurisprudência terão a tarefa de elucidar essa questão.

---

275 DONEDA, Danilo. Ibid, 163. Conforme o autor "*a diferenciação conceitual dos dados sensíveis atende à uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior...*".

276 Ver também a lição RODOTÀ, Stefano. Ibid, p. 96: "*A classificação desses dados na categoria de dados "sensíveis", particularmente protegidos contra os riscos da circulação, deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias. Exatamente para garantir plenitude à esfera pública, determinam-se rigorosas condições de circulação destas informações, que recebem um fortíssimo estatuto "privado", que se manifesta sobretudo pela proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação.*"

277 Tais exceções encontram-se no art. 21 do anteprojeto brasileiro de lei de proteção de dados pessoais.

Na mesma direção da lei brasileira, a diretiva 95/46/CE também define a proibição de tratamento de dados sensíveis. Porém, vai mais além ao impor exceções ao tratamento de dados sensíveis, assim dispostas no art. 8º, n. 2. Entre os casos estão o consentimento explícito da pessoa envolvida, o que se realizado de forma consciente e adequada, parece representar uma real exceção. Portanto, no caso de dados pessoais, bastaria o consentimento explícito, e no caso de dados sensíveis, o consentimento inequívoco.[278]

D.2 - O controle do usuário sobre os próprios dados

A privacidade informacional é mais ampla e complexa diante da evolução da tecnologia. O conceito de "ser" ganha um novo sentido. A massiva utilização de ferramentas tecnológicas, redes de relacionamento e serviços tecnológicos dos mais variados tipos pode indicar a tendência do reconhecimento de um "ser virtual", ou uma representação virtual da personalidade.[279] É evidente que a existência desse "ser virtual" deve ser limitada também pela não transformação das pessoas em mercadorias, por meio do processamento indiscriminado de seus dados pessoais.[280] O usuário-consumidor passa a ser um grande produtor de dados.

Nesse aspecto, entre os limites impostos à intimidade e à vida privada estão o interesse público, a publicidade dos atos e o próprio consentimento dos interessados.[281] No direito comunitário, o conceito de consentimento para o

278 LIMBERGER, Têmis. *O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais.* Porto Alegre: Livraria do Advogado, 2007, p. 182.

279 CADKIN, John; COURSON, J. Zachary. Ibid, p. 6.

280 Cf. Ao mesmo tempo Têmis Limberger faz a importante ressalva da intimidade no âmbito informático é "*não apenas proteger a esfera privada da personalidade, garantindo que o indivíduo não seja incomodado devido à má utilização de seus dados. Pretende-se evitar, outrossim, que o cidadão seja transformado em números, tratado como se fosse uma mercadoria, sem a consideração de seus aspectos subjetivos.*" LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007, p. 217.

281 CARVALHO, Ana Paula Gambogi. Ibid, p. 86.

tratamento de dados é caracterizado como "*qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento.*"[282]

É certo que, vista unicamente sob o prisma da proteção individual, a privacidade tem seu valor diminuído. Ela possui também um valor social: "*Ela molda as comunidades sociais e fornece a proteção necessária aos indivíduos contra diversos tipos de danos e intromissões, possibilitando que desenvolvam sua personalidade e devolvam à sociedade novas contribuições*".[283]

O interessado pode, quando lhe convém, voluntariamente disponibilizar seus próprios dados pessoais. Isso não significa que a intimidade deixe de ser indisponível[284], conforme a lição do art. 11 do Código Civil. Nesse caso, os direitos à intimidade e à privacidade, mediante o consentimento, deixam de ser exercidos temporariamente, sem haver a renúncia do próprio direito.[285] Ao mesmo tempo, a autotutela das informações pessoais também está presente na Internet pois "*é ônus do próprio indivíduo resguardar adequadamente sua privacidade online.*"[286]

Sobre a necessidade de autorização do interessado para o recolhimento e armazenamento de dados pessoais, naturalmente, ela não é necessária [a autorização] quando os dados forem voluntariamente fornecidos pelas pessoas. Um

---

282 UNIÃO EUROPEIA. Diretiva 95/46/CE – Diretiva Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de Outubro de 1995. Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu. Art. 2º, alínea h).

283 LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, p. 120-121. O autor continua, afirmando que: "*Isso significa que não se deve entender a tutela da privacidade como a proteção exclusiva de um indivíduo, mas sim como uma proteção necessária para a manutenção da estrutura social.*"

284 De acordo com MIRAGEM, Bruno. Os direitos da personalidade e os direitos do consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 455-456. "*...não se vai tratar da disposição sobre o direito da personalidade em si, mas ao conteúdo que o consumidor indicará para sua proteção, qualificando-as como informações privadas.*"

285 MORI, Michele Keiko. Ibid, p. 56.

286 LEONARDI, Marcel. Ibid, p. 187-188.

exemplo clássico são as informações voluntariamente fornecidas pelos usuários em redes sociais como Orkut e Facebook.[287]

É evidente que o consentimento deve ser adequado, por intermédio não apenas da coleta lícita e transparente dos dados, bem como através da obtenção, pelo consumidor-usuário, das informações específicas sobre a destinação que seus dados receberão. Além do mais o consumidor, ao fornecer seus dados pessoais, deve ter a exata noção de como eles serão armazenados, utilizados e, em geral, tratados. Nesse sentido, a lição de Danilo Doneda:

> "*O consentimento, ao sintetizar esta atuação da autonomia privada em um determinado momento, há de ser interpretado como o instrumento por excelência da manifestação da escolha individual, ao mesmo tempo que faz referência direta aos valores fundamentais em questão.*"[288]

Acerca do consentimento, observar ainda, o enunciado 404 da V Jornada de Direito Civil do Centro de Estudos Judiciários da Justiça Federal, que assim dispõe:

> *"A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a*

---

287 Idem. Ibid, p. 95. Ao final de sua obra, o autor ainda aponta que, essa característica de abdicação voluntária da própria privacidade e intimidade, permite a reflexão dos próprios limites do direito: "*Não é possível pretender tutelar todas as situações que envolvem problemas de privacidade na Internet, principalmente quando os próprios indivíduos parecem desprezar seu direito a ela.*" p. 368.

288 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 371. O autor continua, afirmando que: "*O consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser verificada a partir dos efeitos de sua concreta aplicação ao caso dos dados pessoais e seus efeitos...*"

> *origem racial ou étnica, as convicções religiosas, filosóficas e políticas."*

O consentimento passa, então, a ser uma expressão da própria autodeterminação em relação aos dados pessoais.[289] Pode ele, inclusive, ser revogado em função de sua ligação com os direitos da personalidade.[290]

Na verdade, em muitas situações, o consentimento do usuário acaba sendo prejudicado à medida que o uso dos serviços só pode ser feito mediante a aceitação de termos de uso, que incluem determinações sobre o uso de dados pessoais. Para que o usuário consiga utilizar os serviços só resta a ele consentir no tratamento de seus dados pessoais. Não há, portanto, uma negociação do usuário com o fornecedor de serviços, o que coloca em xeque a ideia do consentimento.[291]

Acerca do acesso do consumidor aos próprios dados, mesmo que ele disponha da via legal, por meio do *habeas data*, a doutrina entende que:

> "*não deveria ser necessária a lide, a pretensão resistida, o recurso à ação de habes data, da mesma forma não deveria o fornecedor impor exigências exorbitantes e pouco razoáveis, obstáculos desproporcionais, para que o consumidor pudesse chegar a seus dados e à sua modificação...*"[292]

Infelizmente não é o que ocorre, negando quase sempre, os fornecedores de serviços, o fornecimento espontâneo dos dados referentes ao próprio usuário.

O CDC, por sua vez, ao considerar os bancos de dados relativos aos consumidores como entidades de caráter público, no art. 43, § 4º, abre caminho para

289 DONEDA, Danilo. Ibid, p. 378.
290 Idem. Ibid, p. 378.
291 Idem. Ibid, p. 380.
292 BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 2ª ed. São Paulo: RT, 2006, p. 612-613.

a utilização do *habeas data*[293]*, nos termos do art. 5º, LXXII* para a tutela de dados pelos consumidores.[294] Trata-se de "*uma das ações constitucionais que formam um rol de instrumentos para a garantia de direitos individuais e coletivos.*"[295]

D.3 - A vulnerabilidade técnica do consumidor e a privacidade

É certo que há uma grande acumulação de informações recebidas pelos usuários das novas tecnologias. O usuário comum não consegue absorver e acessar todas as informações e alertas dos serviços informáticos atualmente disponibilizados. Em face da complexidade informática, o usuário fica alheio a uma série de detalhes técnicos importantes para a compreensão das funções, limites e riscos dos sistemas.[296] Da mesma forma, podem ocorrer também situações em que os responsáveis não fornecem informações acerca de seus serviços. Os motivos podem ser vários, entre eles a intenção de ocultar condições negociais leoninas e produtos defeituosamente elaborados ou serviços deficientes. Nessas situações, o fornecedor viola o dever de informar quando se omite voluntariamente em fornecer as informações, uma vez que "*a informação é o antídoto do erro*".[297]

---

293 Danilo Doneda ressalta que o *habeas data* apresenta "*evidentes 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.*" DONEDA, Danilo. Ibid, p. 331.

294 DONEDA, Danilo. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em: 12 Fev. 2012, p. 18.

295 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 332. No mesmo sentido LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 200-201. "*O habeas data é, portanto, um mecanismo de tutela à disposição do usuário de Internet que, vinculado a uma relação de consumo com um fornecedor, pretenda fazer valer seu direito de acessar os registros existentes em bancos de dados e em cadastros de consumo, bem como retificar ou apagar registros errôneos e complementar registros insuficientes ou incompletos.*"

296 Ver MARTINS, Guilherme Magalhães. Ibid, p. 45, quando ensina que "*Os dias de hoje trazem a ideia da confiança como uma fé no conhecimento de sistemas tecnológicos e especializados, acompanhada da ignorância do leigo acerca de seu funcionamento. A conduta individual busca a simplificação que a confiança fornece, uma vez que os custos de cada demanda por informação seriam incalculáveis. Um cético, orientado pela necessidade de plena compreensão racional de cada um dos sistemas de que faz uso, dificilmente conseguiria viver nessa sociedade*."

297 LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 171,

A vulnerabilidade do consumidor é assim reconhecida no art. 4º, inc. I do CDC. Via de regra, o usuário também não possui informações técnicas acerca da segurança dos serviços utilizados por ele na Internet. Quase nunca consegue monitorar a qualidade do serviço devendo, apenas, confiar na promessa de segurança e confidencialidade na proteção dos dados feita pelo fornecedor. De uma forma geral "*o comprador não possui conhecimentos específicos sobre o objeto que está adquirindo e, portanto, é mais facilmente enganado quanto às características do bem ou quanto à sua utilidade, o mesmo ocorrendo em matéria de serviços.*"[298]

Em sendo assim, o consumidor fica tecnicamente vulnerável. De acordo com Paulo Valério Dal Pai Moraes a vulnerabilidade técnica ocorre quando:

> "*o consumidor não detém conhecimentos sobre os meios utilizados para produzir produtos ou para conceber serviços, tampouco sobre seus efeitos "colaterais", o que o torna presa fácil no mercado de consumo, pois, necessariamente, deve acreditar na boa-fé com que o fornecedor 'deve estar agindo'.*"[299]

A manifestação da vulnerabilidade técnica pode ocorrer por várias razões, entre elas, a falta de informações ou informações prestadas incorretamente e até mesmo pelo excesso de informações desnecessárias. Neste caso, estas

---

174, 177 e 178. Basicamente o dever precisa englobar, por exemplo, a informação de: fatos suscetíveis a influir sobre a decisão do consumidor; fatos que tornem o contrato inválido; vícios dos bens; funcionalidades dos bens ou serviços, etc. A exceção, segundo o autor, seria a informação sobre fatos notórios e amplamente conhecidos. p. 180.

298 Cf. MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 324. Não é por mero acaso, também, segundo a autora, que o consumidor "*foi o único agente econômico a merecer inclusão no rol dos direitos fundamentais do art. 5º da CF: foi escolhido porque seu papel na sociedade é intrinsecamente vulnerável perante o seu parceiro contratual, o fornecedor. Trata-se de uma necessária concretização do princípio da igualdade, do tratamento desigual aos desiguais, da procura de uma igualdade material e momentânea para um sujeito com direitos diferentes, sujeito vulnerável, mais fraco*". p. 373.

299 MORAES, Paulo Valério Dal Pai. *Código de defesa do consumidor: o princípio da vulnerabilidade no contrato, na publicidade, nas demais práticas comerciais: interpretação sistemática do direito*. Porto Alegre: Livraria do Advogado, 2009, p. 141.

informações desnecessárias impedem que o consumidor tome consciência do que é realmente importante.[300]

O comércio eletrônico possui, ainda, vulnerabilidades específicas. Há muitos produtos que são constituídos puramente por informações. Tais produtos são caracterizados por serem: intangíveis, herméticos (no sentido de serem singulares e dificultada a possibilidade de conhecê-los com base no conhecimento de outros produtos semelhantes), flexíveis e estão sempre se alterando, além de estarem "*inseridos em um sistema de relações complexos, já que apresentam múltiplas interações com outros sujeitos ou outras partes.*"[301] O produto é um verdadeiro desafio para o consumidor![302]

Há uma clara impossibilidade de o consumidor, nesse cenário, conseguir identificar os meandros desses serviços informáticos massificados, ficando ampliado o papel da confiança[303], ou seja, ao consumidor só resta confiar.[304] Em função da complexidade do ambiente, há uma grande assimetria informacional entre os atores e, consequentemente, uma ampliação da vulnerabilidade técnica dos consumidores.[305] Nela, o consumidor não possui "*conhecimentos específicos sobre*

300 Idem. Ibid, p. 253

301 LORENZETTI, Ricardo Luis. Consumidores. Buenos Aires: Rubinzal y Asociados, 2003, p. 41.

302 Idem. Ibid, p. 41.

303 Ricardo Mena Barreto e Têmis Limberger ao comentarem sobre o aspecto da "despersonalização" do ciberespaço, destacam um ponto importante sobre a segurança. "*A segurança advinda da interação presencial (física) é abalada, logo, pela complexidade de um espaço virtual. A interação via computador possui a propriedade de despersonalizar as relações, produzindo novas formas de sociabilidade. O ciberespaço promove e intensifica a efetivação de uma singularidade ordinária, onde é possível escolher um personagem, uma vida e máscaras de agir. A possibilidade de burla de identidade real é, portanto, um dos fatores que aumenta a desconfiança no ambiente virtual.*"

304 LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 62-63. "*No se trata de un problema de negligencia, sino de una necessidad: se tuviera que verificar razonablemente cada acto, sería imposible vivir, y los costos de transacción serían altísimos. Es necesaria la confianza, porque ésta reside en la base del funcionamiento del sistema experto, inextricable y anónimo y es el lubrificante de las relaciones sociales*." O autor faz essa mesma constação em LOREZENTTI, Ricardo Luis. *Tratado de los contratos*. Buenos Aires: Rubinzal y Asociados. 2000. Tomo III, p. 863.
Nesse sentido também BRANCO, Gerson Luiz Carlos. Ibid, p. 190. "*O mesmo não acontece quando o homem contemporâneo entra em um avião. O passageiro só tem uma alternativa: confiar que todo o sistema tecnológico e as pessoas que estão trabalhando vão agir conforme o previsto.*"

305 Idem. Ibid, p. 65. "*Debe tenerse en cuenta también que la tecnologia es cada vez más compleja*

o objeto que está adquirindo e, portanto, é mais facilmente enganado quanto às característica do bem ou quanto à sua utilidade, o mesmo ocorrendo em matéria de serviços".[306]

Bruno Miragem, ao falar especificamente do dever de informar dos fornecedores de serviços na internet, destaca que todos são vulneráveis tecnicamente, à exceção dos especialistas em informática. Ele menciona também três aspectos principais sobre os quais o consumidor não possui domínio:

> "*a) aspectos técnico-informáticos (armazenamento de informações, segurança sobre os dados pessoais transmitidos pela rede, procedimento de acesso a determinadas informações), (b) aspectos decorrentes do caráter imaterial da contratação, ou ainda (c) do fato de ser celebrada à distância, bem como aspectos relativos à defesa e efetividade de seus direitos, como é o caso de contratações celebradas entre consumidores e fornecedores de cidades, Estados ou países distintos...*"[307]

Com isso, é possível relacionar a ideia de vulnerabilidade técnica com a proteção da privacidade. Ela reflete-se no fato das pessoas conseguirem (ou não) entender e prever quais riscos podem estar expostas quando do processamento de seus dados. Há igualmente a ligação da vulnerabilidade com a complexidade do

---

en su diseño, pero se presenta de modo simplificado frente al usuario, ocultando de este modo una gran cantidad de aspectos que permanecen en la esfera de control del proveedor. Puede afirmarse que la tecnologia incrementa la vulnerabilidad de los consumidores, instaurando un trato no familiar."

306 BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno. Ibid, p. 145. Os autores continuam, afirmando que "*A vulnerabilidade técnica, no sistema do CDC, é presumida para o consumidor não-profissional, mas também pode atingir excepcionalmente o profissional, destinatário final fático do bem. Trata-se de exceção e não da regra, pois, como concluiu de forma unânime a 2ª Seção do STJ, citando a doutrina finalista e a ideia de profissionalidade, em relação envolvendo pessoa jurídica, profissional no fornecimento de serviços médicos e de exames, e que compra no exterior (Panamá) equipamento de ponta para exames médicos: "A compra e venda de sofisticadíssimo equipamento destinado à realização de exames médicos – levada a efeito por pessoa jurídica nacional e pessoa jurídica estrangeira – não constitui relação de consumo*""

307 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. Revista de direito do consumidor, São Paulo, n. 70, abr.-jun./2009, p. 74.

ambiente e também com a circunstância de que, muitas vezes, nem ao menos se sabe quais as empresas possuem dados pessoais. Desta maneira, a própria autodeterminação informativa, e a ideia de controle de dados, fica prejudicada em função da vulnerabilidade técnica[308].

308 Sobre isso ver RODOTÀ, Stefano. Ibid, p. 37: "*Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em controle.*"

Parte II - A proteção de dados pessoais e o dever confidencialidade no Direito do Consumidor

O art. 4º do CDC estabelece, como objetivos da Política Nacional de Consumo, entre outros, o respeito à segurança e aos interesses econômicos dos consumidores bem como transparência e harmonia das relações de consumo.[309] Além disso, um dos direitos básicos do consumidor, assim disposto no art. 6º, inc. I do CDC, é justamente a "*proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos*".

A informação, como bem da vida que é, passa a ser também objeto de contratos no comércio eletrônico. Cláudia Lima Marques destaca a "*imaterialidade do objeto*" nos referidos contratos. Ensina ela:

> "*faz-se mister frisar que o comércio eletrônico atualiza a noção de objeto de contrato, pois as prestações contratuais dos contratos informáticos são imateriais, como o fornecimento de software, de jogos, de filmes e de músicas*".[310]

Outro aspecto levantado pela autora, é ideia de fusão de produtos com a prestação de serviços informáticos. Essa questão - da mistura entre produto e serviço - seria em suas palavras um dos grandes desafios do comércio eletrônico.[311]

309 O artigo 4º traz ainda outras referências à segurança no inc. II alínea d; inc. V.

310 MARQUES. Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico)*. São Paulo: RT, 2004 , p. 84.

311 Idem. Ibid, p. 84-85. A autora destaca também em MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 177, que os contratos à distância no comércio eletrônicos possuem a chamada "*desumanização do contrato*", sendo a impessoalidade "*levada a graus antes desconhecidos*".
Já Bruno Miragem, ao comentar sobre os contratos eletrônicos, diz que "*a natureza eletrônica da contratação pode se dar tanto em razão do produto ou do serviço objeto do ajuste, do modo de formação do contrato ou do modo de cumprimento de algumas das prestações*". MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor:

Neste contexto, a regra é de que a responsabilidade pela segurança das informações pessoais dos usuários é objetiva, respondendo o fornecedor independentemente de culpa ainda que:

> "*tenha adotado sistemas de segurança, pela reparação dos danos causados ao consumidor em decorrência da invasão do banco de dados por terceiros. Falhas na segurança do site são, portanto, da responsabilidade do gestor do banco de dados, que deverá, independentemente de ter agido ou não com culpa, reparar quaisquer danos causados aos seus consumidores pelo acesso não autorizado a seus dados confidenciais.*"[312]

Em função disso, passa-se a análise de alguns elementos acerca da proteção de dados pessoais dos consumidores.

A) A proteção de dados e a boa-fé

A boa-fé objetiva é reconhecida como uma cláusula geral. Essas cláusulas gerais possuem função bastante relevante no ordenamento jurídico. Afirma Judith Martins Costa, em obra fundamental para o entendimento do assunto, que as cláusulas gerais:

> "*constituem o meio legislativamente hábil para permitir o ingresso, no ordenamento jurídico, de princípios valorativos, expressos ou ainda inexpressos legislativamente, de standards, máximas de conduta, arquétipos exemplares de comportamento, das normativas constitucionais e de diretivas econômicas, sociais e políticas, viabilizando a sua sistematização no ordenamento jurídico*."[313]

---

desafios atuais da regulação jurídica da Internet. *Revista de direito do consumidor*, São Paulo, n. 40, abr.-jun./2009, p. 46.

312 CARVALHO, Ana Paula Gambogi. Ibid. 111.

313 MARTINS-COSTA, Judith. *A boa-fé no direito privado*. São Paulo: RT, 1999, p. 274.

No mesmo sentido, elucidando também a questão, Bruno Miragem explica que as cláusulas gerais tornaram-se:

> "*veículo de valores ou princípios jurídicos do ordenamento jurídico, provenientes da Constituição e da construção doutrinária e jurisprudencial relativos a comportamentos devidos ou de significados expressivos dos interesses juridicamente protegidos em disputa.*"[314]

Já Gerson Luiz Carlos Branco afirma que:

> "*A materialização do direito privado por meio de cláusulas gerais que concedem ao Juiz um poder maior para a utilização de princípios jurídicos é esforço do próprio Estado para o enfrentamento do problema derivado do algo grau de diferenciação social, que não pode ser coordenado pelo modelo legal lógico-subsuntivo.*"[315]

As cláusulas gerais podem ser de três tipos: restritivas (ao estabelecer "*permissões singulares, delimitando-as, como nos casos da restrição à liberdade contratual...*"), regulativas (quando regula "*através de um princípio, todo um vasto domínio de casos, como corre com a regulação da responsabilidade por culpa*") e por fim, do tipo extensivo (quando amplia "*uma determinada regulação através da possibilidade expressa, de aí serem introduzidos princípios e regras dispersos em outros textos*").[316]

---

314 MIRAGEM, Bruno. Função social do contrato, boa-fé e bons costumes: nova crise dos contratos e reconstrução da autonomia negocial pela concretização das cláusulas gerais. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual*. São Paulo: RT, 2007, p. 188.

315 BRANCO, Gerson Luiz Carlos. Ibid, p. 187.

316 MARTINS-COSTA, Judith. Ibid, p. 295. A autora complementa que um dos exemplos das cláusulas extensivas é justamente "o caso das disposições do Código do Consumidor...". Está ela a referir-se ao art. 7º do CDC.

Por isso, a incorporação de um dever de segurança da informação e de confidencialidade de dados pessoais pode ser alcançado também por meio da observância da boa-fé como um veículo.[317] Não se perca de vista que a boa-fé é um dos princípios orientadores do Direito do Consumidor.[318]

Nota-se também a importância da utilização das cláusulas gerais e dos princípios em função das próprias características de extrema velocidade das mudanças trazidas pelas novas tecnologias e em função da "*impossibilidade de se produzirem leis com a capacidade de tratar minudentemente destes avanços*".[319] Em igual sentido, Antonio-Enrique Perez Luño, ao propor uma metodologia específica para o Direito Informático, leciona que "*a regulamentação jurídica da informática deve adaptar-se à situação de constantes mudanças e inovações...*" e que "*parece mais oportuno que sua disciplina normativa responda a uma técnica legislativa de*

317 Seguindo a lição da autora sobre o delineamento do que o vocábulo "geral" possa significar em relação as cláusulas gerais, ela ensina que "*só se poderá conotar o adjetivo 'geral' às cláusulas gerais se, por este, se estiver compreendendo que esta técnica permite em razão da extensão do seu campo previsivo-estatutivo, uma 'previsibilidade geral' de condutas, ao modo de ensejar o tratamento 'em conjunto' de um vasto domínio de casos.*" . Mais adiante, a autora completa salientando que o fato que caracteriza a cláusula geral é "*o emprego de expressões ou termos vagos no delineamento da 'fattispecie' ou a conferência de um mandato - cujo significado pode ser semanticamente impreciso - ao juiz para que, a partir dele, sejam concretizadas as consequências normativas visadas.*" Da mesma forma, a citada vagueza não lhes retira – das cláusulas gerais - as qualidades essenciais de normas jurídicas, como a coercibilidade e a obrigatoriedade. Idem. Ibid, p. 304, 306 e 312.

318 Sobre as funções da boa-fé, Cláudia Lima Marques ensina que "A expressão atual alemã - função de complementação ou concretização da relação - esclarece que a boa-fé é fonte de deveres, "descobertos" na complementação, na "fotografia" da relação, que realiza o magistrado para bem interpretar a relação de consumo." MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais. 6ª Ed. São Paulo: RT, 2011, p. 917.

No mesmo sentido, BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno, p. 148. "*Segundo dispõe o art. 4º, III, do CDC, todo esforço do Estado ao regular os contratos de consumo deve ser no sentido de "harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170 da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações de consumidores e fornecedores". Poderíamos afirmar genericamente que a boa-fé é o princípio máximo orientador do CDC. Neste trabalho, porém, estamos destacando igualmente o princípio da transparência (art. 4º, caput), o qual não deixa de ser um reflexo da boa-fé exigida aos agentes contratuais.*"

319 SANTOLIM, Cesar Viterbo Matos. Ibid, p. 56. O autor destaca ainda que "*muito antes de se afiançar a ideia de uma "revolução jurídica*" *é importante buscar a correspondência entre estas novas situações e as regras e princípios já conhecidos, especialmente estes, pelo seu caráter "imediatamente finalístico" e "primariamente prospectivo"...*". p. 57.

cláusulas e princípios gerais"[320]. No mesmo sentido, Stefano Rodotà destaca a "*necessidade de invidualizar princípios, de associá-los a tendências de longo prazo*", quando se refere à "*rápida obsolescências das soluções jurídicas*" relacionadas com as novas tecnologias[321].

Na visão de Clóvis do Couto e Silva, aqueles deveres resultantes da incidência da boa-fé são chamados de secundários, anexos ou instrumentais.[322] Entre as características de tais deveres, há uma, por si só bastante importante, que prevê que eles [os deveres] podem subsistir "*mesmo depois do adimplemento da obrigação principal, de modo que, quando se diz que o adimplemento extingue a relação jurídica, se deve entender que se extingue um crédito determinado*".[323] Entre os exemplos trazidos pelo autor poderiam ser citados os "*atos de proteção, como o dever de afastar danos, atos de vigilância, de guarda, de cooperação, de assistência*".[324]

Judith Martins-Costa enumera também os chamados "*deveres instrumentais ou laterais, ou deveres acessórios de conduta, deveres de conduta, deveres de proteção ou deveres de tutela*."[325] Ao exemplificar alguns dos referidos deveres, a autora apresenta um rol, no qual consta os deveres de cuidado, previdência e segurança; os deveres de aviso e esclarecimento; os deveres de informação; o dever de prestar contas; os deveres de colaboração[326] e cooperação; os deveres de

320 LUÑO, Antonio-Enrique Pérez. *Manual de informática y derecho*. Barcelona: Ariel, 1996, p. 20.

321 RODOTÀ, Stefano. Ibid, p. 42. O autor afirma aidna que "*as dificuldades em especificar estes princípios não derivam somente do fato de que se trata de regular uma realidade em contínua transformação. Nascem ainda da necessidade de levar em conta uma multiplicidade de exigências, interesses, valores, frequentemente em conflito entre si".*

322 SILVA, Clóvis V. do Couto. *A obrigação como processo*. Rio de Janeiro: FGV, 2006, p. 91.

323 Idem. Ibid, p. 92.

324 Idem. Ibid, p. 93.

325 MARTINS-COSTA, Judith. Ibid, p. 438

326 Roberto Senise Lisboa sugere sobre um novo princípio de cooperação que se assenta "*no princípio da dignidade pessoal, do respeito, que se presta como conduta que não apenas o outro espera do seu parceiro negocial (expectativa), mas também reflexamente a coletividade, num sentido de comprometimento pela segurança do tráfico mediante a adoção de contratos justos. Garantir segurança (relativa, senão o tráfico deixa de existir) proporciona trazer confiança (relativa, pois a confiança cega não tem valor nenhum)*." LISBOA, Roberto Senise. *Tecnologia, confiança...*, p. 65.

proteção e cuidado com a pessoa e o patrimônio da contraparte e, por fim, os deveres de omissão e de segredo.[327]

Não se considera apenas o que está escrito ou o que foi pactuado entre as partes. A boa-fé tem um papel preponderante na criação dos deveres secundários. A relação obrigacional não é apenas um simples dever de prestar, conforme lição de Couto e Silva. Além disso, ela é constituída, como já dizia Menezes Cordeiro, de "*vários elementos jurídicos dotados de autonomia bastante para, de um conteúdo unitário, fazerem uma realidade composta*.".[328]

Cabe, neste ponto, a menção acerca do papel da confiança[329] nas relações digitais. Cláudia Lima Marques alerta, que em função da nova linguagem da própria Internet:

> "*visual, fluida, rápida, agressiva, pseudo-individual e massificada dos negócios jurídicos de consumo a distância pela Internet propõe desafios sérios para o direito privado, em especial para o direito do consumidor e o seu paradigma moderno da boa-fé nas relações contratuais. Em outras palavras, o uso de um meio virtual, ou a entrada em uma cultura visual leva a uma perda de significado ou eficiência do princípio da boa-fé, que guiou o direito privado e, em especial, o consumidor no século XX. Para alcançar a mesma eficácia em tempos virtuais pós-modernos, pareceu-me necessário evoluir para o uso de um paradigma mais visual (de aparência), de menos fidelidade e personalização (fides),*

---

327 MARTINS-COSTA, Judith. Ibid, p. 439. Continuando, a autora refere que "*ao ensejar a criação desses deveres, a boa-fé atua como fonte de integração do conteúdo contratual, determinando a sua otimização, independente da regulação voluntaristicamente estabelecida.*", p. 440.

328 MENEZES CORDEIRO, António Manuel da Rocha E. *Da boa-fé no direito Civil*. Coimbra: Almedina, 1984. Volume 1, p. 586.

329 Conforme Roberto Senise Lisboa "*A importância do estudo da confiança negocial passou a se tornar ainda maior, em uma sociedade marcada pela despersonalização negocial, que chega ao nível da virtualização.* " LISBOA, Roberto Senise. Ibid, p. 61.

> *de menos eticidade (valoração - bona) e sim de mais socialidade (qualquer forma de declaração vincula o profissional organizador da cadeia de fornecimento) e de coletiva repersonalização (realizar as expectativas legítimas de todo um grupo difuso de consumidores virtuais), a confiança, o modelo-mãe da boa-fé. Esta tese pode ser defendida em matéria de contratos civis, comerciais e de consumo, hoje, após a entrada em vigor do Código Civil de 2002 e suas noções basilares de função social dos contratos, boa-fé objetiva, bons costumes e combate ao abuso nos contratos paritários.*"[330]

No ambiente digital a confiança acaba também por funcionar como "*parâmetro para distribuição dos novos riscos trazidos pela comodidade e facilidade decorrente da evolução tecnológica*".[331] Por sua vez, se há uma crise de desconfiança a resposta deve ocorrer "*através do direito privado como instrumento de realização das expectativas legítimas do homem comum, o leigo, o consumidor*".[332]

A proteção da confiança passa a ser ainda mais relevante, uma vez que, em um mercado eletrônico e altamente sofisticado, os consumidores têm uma sensação de bem-estar ao sentirem-se "*integrados à sociedade high-tech e à cultura contemporânea. Chegam a preferir confiar mais e se assegurar menos.*"[333]

O fato de ser criada uma "situação de confiança", na lição de Menezes Cordeiro, e o consequente aproveitamento dessa situação, para a outra parte, seria o suficiente para "*uma segunda forma de constituir negócios jurídicos,*

---

330 MARQUES, Cláudia Lima. A chamada nova crise do contrato e o modelo de direito privado brasileiro: crise de confiança ou de crescimento do contrato. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual*. São Paulo: RT, 2007, p. 20-21.

331 MARTINS, Guilherme Magalhães. Ibid, p. 46.

332 MARQUES, Cláudia Lima. *Contratos...*, p. 187.

333 LISBOA, Roberto Senise. *Tecnologia, confiança e sociedade*. Ibid, p. 64.

sistematicamente correcta".[334] Ademais, merece proteção a confiança despertada na parte, na formação e cumprimento do contrato, sendo que essa proteção também pode ser realizada por intermédio dos deveres acessórios ou anexos.[335]

Deve ser observado, conforme a lição de Cláudia Lima Marques[336], que as determinações contratuais acerca da boa-fé, assim estabelecidas no Código Civil (arts. 113, 187 e 422) abarcam todos os tipos de contratos[337]. Em função dessa circunstância, é possível a realização do estudo de um dever de segurança da informação, envolvendo a confidencialidade de dados, sendo que sua aplicação ocorre em qualquer tipo de contrato e relação digital. Mais adiante, observa-se igualmente que:

> "*A hora é de especialização e rigor, de atenção e estudo, pois a reconstrução do direito privado brasileiro identificou três sujeitos: o civil, o empresário e o consumidor, mesmo se os princípios do Código Civil de 2002 e Código de Defesa do Consumidor são - em geral - os mesmos*."[338] (grifo nosso).

---

334 MENEZES CORDEIRO, António Manuel da Rocha E. Ibid, p. 561. Também, de acordo com BRANCO, Gerson Luiz Carlos. Ibid, p. 205: *"Entre a teoria da vontade de Savigny e a teoria da declaração, cuja formulação melhor elaborada foi de Oscar Von Bülow, para quem a preponderância é da declaração, a teoria da confiança surgiu como uma terceira via para tentar explicar o papel da vontade na produção dos efeitos do ato, mas ao mesmo tempo para limitar dogmaticamente a importância da vontade na formação e existência do negócio jurídico."* Mais adiante, complementa: "*Os motivos do consumidor são transformados em causa do contrato, pois a expectativa que foi criada e o aproveitamento da confiança do consumidor como elemento determinante da conclusão do contrato, tem por consequência a inclusão de um dever de presença de de tal qualidade na prestação prometida. "* p. 210.

335 MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais.* 6ª Ed. São Paulo: RT, 2011, p. 197. Conforme a autora: "*Daí a importância de se acrescentar, aos já conhecidos princípios contratuais, um paradigma qualificado, valorizando a confiança como eixo central das condutas e como fonte jurídica e dela retirando responsabilidades específicas*".

336 MARQUES, Cláudia Lima. A chamada nova crise do contrato e o modelo de direito privado brasileiro: crise de confiança ou de crescimento do contrato. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual.* São Paulo: RT, 2007, p. 36.

337 No mesmo sentido SANTOLIM, Cesar Viterbo Matos. Ibid, p. 69: "*Não por acaso, o primeiro princípio a ser considerado quando se observam as relações de jurídicas onde há proteção ao consumidor é o da boa-fé objetiva. Isto porque trata-se de diretriz orientadora não apenas no âmbito do microssistema do código de defesa do consumidor mas, na realidade, que atinge todo o sistema jurídico.*"

338 MARQUES, Cláudia Lima. Ibid, p. 54

Menezes Cordeiro ao comentar também sobre os "*deveres acessórios de protecção*" expõe que "*por eles, considera-se que as partes, enquanto perdure um fenómeno contratual, estão ligadas a evitar que, no âmbito deste fenómeno, sejam inflingidos danos mútuos, nas pessoas ou nos seus patrimónios.*"[339] É a visão de que os deveres da boa-fé são "*intrinsecamente bilaterais*", podendo apenas a lei "*transformar esta bilateralidade*".[340]

Os mesmos deveres acabam por transcender o próprio escopo da autonomia privada. Mesmo em casos de nulidades do contrato principal, ainda permaneceriam alguns deveres acessórios, os quais teriam essa característica de autonomia.[341] Essa autonomia incidiria não somente na fase pré-contratual como também na pós-contratual.[342] E, na última, sobressaem-se os deveres de proteção, de informação e de lealdade.

O que se viu acerca da boa-fé, principalmente em relação ao dever de colaboração mesmo na fase pós-contratual, é importante ser ressaltado. Essa questão parece encaixar-se perfeitamente no dever de confidencialidade. Senão vejamos: no caso do comércio eletrônico, mesmo após encerrada a prestação, permanece um dever posterior de manter a confidencialidade dos dados pessoais dos seus consumidores. Não seria lícito imaginar que, após encerrada a prestação, os dados de cartões de crédito, ou ainda dados específicos sobre as compras realizadas fossem publicados livremente na Internet. Portanto, há um dever posterior de "proteção" e também de "afastar danos", por meio de atos de "vigilância" e

339 MENEZES CORDEIRO, António Manuel da Rocha E. Ibid, p. 604.

340 Segundo MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 1135 "*...os deveres de boa-fé são intrinsecamente bilaterais: a boa-fé é "visão" do outro, a proteção "dos interesses do outro" - somente a lei pode transformar esta bilateralidade, imponto o dever de cuidado a um só dos contratantes. É o que o CDC realizou: o dever de cuidado é dever dos fornecedores (arts. 8º, 10, 12, 14, 18, 20, 42, 43, 44, 49, 50), que, descumprido, leva a sanções e poderá levar à nulidade a cláusula que tentar "autorizar' esta prática no contrato (art. 51, I e IV)*"

341 MENEZES CORDEIRO, António Manuel da Rocha E. Ibid, p. 619.

342 Idem. Ibid, p. 625. A responsabilidade pós-contratual também conhecida como culpa *post pactum finitum*. Mais adiante, o autor ressalta que a pós-eficácia coloca-se na área atinente aos deveres acessórios, p. 628. Falando também sobre os deveres laterais ver DIAS, José de Aguiar. *Da responsabilidade Civil*. 8ª Ed. Rio de Janeiro: Forense, 1987, p. 158.

"guarda". Ademais, em casos de incidentes de segurança, como um vazamento, teria o guardião dos dados [a empresa] o dever de "cooperação" e "assistência" perante os prejudicados, visto que ela possui o controle sobre a estrutura.

Verifica-se, na análise do dever de segurança e de confidencialidade, uma proximidade bastante forte do dever geral de informar[343]. Christoph Fabian estabelece diretrizes importantes que apoiam essa ideia. O autor trata dos limites do dever de informar, especificamente dos fatores subjetivos do dever de informar :

> *Um limite inerente ao dever de informar é o conhecimento da informação pelo devedor. A tarefa do dever de informar – sob o ponto de vista geral – é simplesmente a de ampliar o conhecimento do devedor. O conhecimento é, em muitas situações, o fundamento para uma decisão livre.*
> *[...]*
> *A questão do dever de se informar fica em relação estreita com o não-conhecimento por negligência, pois a repreensão do não-conhecimento pressupõe um dever de a outra parte de se informar.*[344]

É demonstrado, no trecho acima, o caráter colaborativo e cooperativo do dever de informar. A ligação, portanto, do dever da segurança da informação com o dever de informar (e ser informado) reside no fato principal de que as partes devem ter conhecimento dos riscos envolvidos na atividade tecnológica. O fato de as atividades tecnológicas serem consideradas de risco, na maior parte dos casos, enseja o nascimento de um dever de informar ampliado, por parte do fornecedor acerca da comunicação dos riscos.[345] Esse dever de informar deve acompanhar o

---

343 Sobre o tema, é trazida a inafastável lição de Menezes Cordeiro, quando diz que "*os deveres acessórios de esclarecimento obrigam as partes a, na vigência do contrato que as une, informarem-se mutuamente de todos os aspectos atinentes ao vínculo, de ocorrências que, com ele, tenham certa relação e, ainda, de todos os efeitos que, da execução contratual, possam advir*". MENEZES CORDEIRO, António Manuel da Rocha E. Ibid, p. 605.

344 FABIAN, Christoph. *O dever de informar no direito civil*. São Paulo: RT, 2002, p. 157 e 158

345 Mesmo que existam produtos de "periculosidade inerente" há situações, em que a periculosidade não é tão evidente, embora exista. No exemplo de Eberlin: "*Há, por outro lado, produtos em que a*

fornecedor que colocou o produto ou serviço no mercado.[346]

Sobre o dever acessório da lealdade, traz ele em seu bojo a abstenção de "*comportamentos que possam falsear o objetivo do negócio ou desequilibrar o jogo das prestações por elas consignado. Com esse mesmo sentido, podem ainda surgir deveres de atuação positiva.*"[347] Nota-se que a consideração da lealdade em relações havidas no meio informático é necessária para a definição do paradigma geral de sigilo acerca dos dados pessoais dos usuários. A proteção do atributo de confidencialidade das informações tem aí um de seus fundamentos. Independentemente de tratar-se de relação contratual ou não, esse dever de impedimento de provocação de dano persiste.

A boa-fé, em uma das suas funções, portanto, cria deveres[348]. A confidencialidade, ou seja o sigilo e o cuidado na preservação das informações da contraparte, pode ser entendida como uma observância dos deveres anexos à boa-fé objetiva.

Um dos efeitos do uso da boa-fé no comércio eletrônico, assim destacado por Lorenzetti, é justamente "*a vedação da utilização de atributos especiais da*

---

obviedade sobre o perigo não é tão clara assim. Os fogos de artifício, por exemplo, exigem certos cuidados no acondicionamento e no manuseio. Alguns remédios possuem contra-indicações. Os fogos e os remédios são, sem dúvida, produtos de periculosidade inerente. No entanto, o fornecedor tem a obrigação de prestar, de forma clara e inequívoca, informações sobre a sua utilização". EBERLIN, Fernando Büscher von Teschenhausen. Ibid, p. 24. Essa ampliação seria, na visão de Hartmann, a expressão (mesmo que implícita) da aplicação do princípio da precaução no direito do consumidor. HARTMANN, Ivar Alberto Martins. Ibid, p. 171.

346 Cf. MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 1266. Destaque-se, oportunamente, a diferença entre a informação e a publicidade, visto que a primeira permite a pessoa a fazer uma escolha consciente a segunda "*pretende exatamente influenciar essa escolha, apelando inclusive para o irracional*", cf. HARTMANN, Ivar Alberto Martins. Ibid, p. 169-170.

347 MENEZES CORDEIRO, António Manuel da Rocha E. Ibid, p. 606. Mais adiante o autor complementa que "*os deveres acessórios de proteção nada têm a ver com a regulação contratual e com a sua execução fiel pelas partes. Visam na verdade, obstar a que, na ocasião do efectivar as prestações e dadas as possibilidades reais de agressão e ingerência provocadas por essa conjuntura, as partes se venham a inflingir danos mútuos.*" p. 615.

348 Cf. BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno. Ibid, p. 149-150, seriam quatro as funções da boa-fé: a) função de complementação ou concretização da relação; b) função de controle e de limitação das condutas; c) função de correção e de adaptação em caso de mudança das circunstâncias; d) função de autorização para a decisão por equidade.

tecnologia para ocultar a identidade ou aspectos essenciais da prestação oferecida."[349]

A consideração da boa-fé nas relações de consumo, também é importante em relação à questão da expectativa de segurança, que será analisada a seguir.

A.1 - Expectativa de segurança, proteção de dados e a confiança despertada

Nas práticas de controle de acesso, o dever de segurança da informação abrange as duas partes envolvidas no acesso: o responsável pelo sistema e também o usuário que tenta acessar o referido sistema. Explica-se: o responsável pelo sistema deve manter um mecanismo para identificar e garantir o acesso apenas pelas pessoas autorizadas; ao mesmo tempo, o usuário deve manter a guarda e o sigilo das informações que ele usa para acessar o sistema. [350]

Cada ambiente informático dá, portanto, ao usuário uma legítima expectativa de segurança da informação. Dependendo do ambiente, e dependendo das informações que o usuário possui sobre o ambiente, sua expectativa quanto à segurança pode ser maior ou menor. As medidas que o responsável pelo sistema utiliza para informar sobre as características do serviço ou do produto gerarão a referida expectativa de segurança no usuário.[351]

Não se discute o fato de que os produtos e serviços colocados no mercado devem corresponder à expectativa de segurança do consumidor.[352] É o que se

349 LORENZETTI, Ricardo L.. *Comércio Eletrônico*. São Paulo: RT, 2004, p. 402.

350 FILHO, Demócrito Reinaldo. op. cit., p. 39. A guarda e sigilo, deve abranger os logins de acesso e as respectivas senhas. Também abrange a guarda sobre os dispositivos como cartões de senha fornecidos pelos bancos, ou tokens de geração de senha aleatória.

351 Idem, Ibid, p. 30. Nas palavras do autor: "*O cliente deste serviço [do home banking] tem uma legítima expectativa de proteção contra fraudes eletrônicas e, se não atende a essa expectativa, não se mostra adequado para realizar a finalidade que razoavelmente que dele se espera.*"

352 Cf. GRINBERG, Rosana. Fato do produto ou do serviço. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011.

depreende, inclusive, da análise do art. 12, §1º, inc II e art. 14, §1º, inc. II do CDC.

Ao mesmo tempo, nas relações de consumo, a integridade moral do consumidor deve ser sempre preservada. A proteção do sigilo e da confidencialidade está englobada, também, na ideia de proteção de integridade moral, principalmente, se o fornecedor desperta a expectativa de privacidade no consumidor.[353]

Se o mantenedor da infraestrutura de tecnologia ou do sistema demonstra sinais exteriores de que é seguro utilizá-la, ele deve promover meios para sustentar essa expectativa de segurança gerada. É consequência da consideração da boa-fé que, se a contraparte dá os referidos sinais de segurança, essa expectativa deve ser suprida. Assim sustenta Gerson Luis Carlos Branco:

> "*O mercado promete oferecer ao consumidor a melhor técnica e a confiança que é forjada dessa promessa, posta na publicidade e no constante e reiterado estímulo para que se utilize cada vez mais de tais meios, impõe a respectiva obrigação de proteger o consumidor contra os riscos derivados do uso da tecnologia.*"[354]

A demonstração dos sinais exteriores de segurança, visa também à:

> "*tutela da confiança do destinatário da declaração, bem como a assegurar o valor real da aparência, sendo tais elementos essenciais ao intercâmbio de bens e serviços*

Vol. V, p. 787-789. A autora afirma ainda que "*O mais inofensivo produto ou serviço, contudo, se utilizado de forma inadequada, ou se estiver potencializado por um defeito, pode vir a causar prejuízo material ou dano físico ou psicológico ao consumidor*".

353 Cf. aponta MIRAGEM, Bruno. Os direitos da personalidade e os direitos do consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 444. O autor afirma ainda que: "*Neste sentido, à medida que a conduta do fornecedor é reconhecida como apta a gerar efeitos decorrentes da legítima expectativa gerada no consumidor, sua frustração, à medida que ofenda à esfera moral do consumidor, tem sido reconhecida como suficiente para determinar o dever de indenizar, conforme as circunstâncias do caso.*"

354 BRANCO, Gerson Luiz Carlos. Ibid, p. 201.

e à segurança das transações."[355]

Se há um dever geral de segurança de proteção de dados que impede o acesso não autorizado a esses dados, há situações em que pode haver a contratação de graus de segurança diferentes. Nada impede que o provedor de serviços deseje oferecer, por um custo maior, certos tipos de serviços de segurança (como serviços de backup ou firewall). Em tais situações o consumidor contrataria um serviço aumentado de segurança objetivando proteger-se de outros riscos que, por óbvio, não estariam cobertos no serviço normal do provedor. [356]

De qualquer forma, quando o consumidor adquire um produto ou serviço, baseado em uma expectativa de que ele seja seguro, essa circunstância deve ser cumprida pelo fornecedor. É a chamada garantia de adequação "*que deriva do princípio da confiança, a garantia de que o produto é adequado aos fins para os quais razoavelmente se pode esperar que o mesmo proporcione*."[357]

A questão da expectativa de segurança e de proteção da confidencialidade de dados também está relacionada aos termos de serviços apresentados pelos fornecedores de serviços na Internet, que será tratado a seguir.

A.2 - A segurança e os termos de serviço

355 MOTA, Mauricio Jorge Pereira da. *A boa-fé objetiva nos contratos de licença de uso de software*. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Software2.pdf>. Acesso em: 2 Dez. 2011, p. 27.

356 Nessa situação, não se afasta o dever de manter a segurança dos dados, dever este implícito à prestação do serviço. O fornecimento de um serviço adicional, portanto, deve englobar apenas o fornecimento de serviços outros, que não a própria segurança esperada no uso do serviço. Um provedor de acesso não possui o dever de monitorar os downloads dos usuários com o objetivo de impedir a infecção por vírus. No entanto, pode, se for o caso, oferecer esse serviço que está além do dever de segurança normalmente esperado para a atividade.

357 BRANCO, Gerson Luiz Carlos. Ibid, p. 211.

Nas relações que ocorrem via Internet, ao lado da lei como forma de regulação, há o importante papel do contrato[358]. Nessas relações, os termos de uso de tecnologia, as políticas corporativas de uso de tecnologia, assim como as regulamentações privadas estabelecidas nos serviços informatizados possuem um caráter contratual e vinculativo, além de representarem uma modalidade importante de controle.[359] Essas regulamentações privadas, consubstanciadas nos termos e políticas de uso de tecnologias apresentadas pelos fornecedores de serviços na Internet, representam também uma forma do fornecedor cumprir o seu dever de informar acerca dos detalhes do serviço e também sobre os riscos pertinentes à atividade. Especificamente, em relação à proteção da privacidade são utilizadas as chamadas “Políticas de Privacidade”.

Assim, a utilização de sistemas informáticos[360] geralmente é precedida de avisos, alertas e termos de uso. Em que pese a natureza de "contratos de adesão” dos referidos termos é inegável que eles possuem um papel importantíssimo no que diz respeito à informação dos riscos e os limites impostos para o utilizador do sistema. Basicamente, na Internet, o dever de informar atende “*em primeiro lugar, uma de suas finalidades básicas no sistema de proteção do consumidor, que é justamente a prevenção de danos.*”[361]

---

358 LORENZETTI, Ricardo L.. Ibid, p 81. Nas palavras do autor: “*É necessário preservar a fluidez, a criação, a democracia interna na rede, e para isso nada melhor que os acordos contratuais com baixos custos de transmissão, mas num marco institucional que preserve os direitos individuais, como já apontamos”.*

359 LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 200. Segundo o autor, os termos de uso também possuem importância “*na prevenção e punição de abusos cometidos por usuários”. Isso pois as atividades e o formato do uso pode ser regrado através desse instrumento.”*

360 É possível dizer que um site é um sistema informático. Um site de uma loja de comércio eletrônico, por exemplo, é apenas a “ponta” de um complexo sistema em que o “site” é a apresentação, o meio de interação da loja com o cliente. O mesmo pode-se dizer de sites de relacionamento, fóruns de discussão, chats, etc.

361 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009, p. 74. No mesmo sentido BARBOSA, Fernanda Nunes. Ibid, p. 120. *“Nesse sentido, o dever de informar, consoante vimos referindo ao longo desta exposição, não se restringe às obrigações contratuais nas quais os interesses em questão são individuais, ou, quando muito, de determinado grupo de pessoas, quando então serão coletivos, mas também a interesses não-contratuais, cujo campo de interessados se alarga para toda a coletividade potencialmente atingida, como ocorre no dever que se fundamenta na prevenção de danos.”*

Em um ambiente como a Internet, de alto risco, a informação fornecida pelos fornecedores, através dos termos de serviço, deve ser clara, precisa, completa, veraz, compreensível e ostensiva, já que a intenção é a prevenção dos danos. Portanto, informações escondidas[362] em links pequenos, no rodapé dos sites[363], com letras pequenas, com linguagem técnica não compreensível ou em língua estrangeira[364], (nos serviços prestados no país) certamente não preenchem os requisitos acima elencados.[365]

O direito à informação do consumidor pode ser visto, inclusive, como um direito fundamental. De acordo com Fernanda Nunes Barbosa

362 FABIAN, Christoph. Ibid, p. 147. "*A instrução deve ser clara, ostensiva e facilmente compreensível para o consumidor. Tais instruções não devem ficar escondidas entre elogios do produto ou alguma propaganda.*" Mais adiante o autor ensina que a instrução é ostensiva "*quando se exterioriza de forma tão manifesta e translúcida que uma pessoa, de mediante inteligência, não tem como alegar ingnorância ou desinformação.*" p. 150.

363 Ver também HARTMANN, Ivar Alberto Martins, p. 171, ao falar sobre a adequação da informação: "*A adequação impõe que esta informação especial seja veiculada no maior número de meios possíveis, contenda linguagem apta a transmitir ao consumidor a situação de incerteza acerca da segurança, reinante sobre determinado produto ou serviço. A suficiência é, por sua vez, também um critério que afigura-se mais exigente que em situações normais. A informação precauciosa deve ser muito mais ostensiva, ampla e presente que a informação normal.*"

364 Acerca do requisito do vernáculo, Fernanda Nunes Barbosa entende que eles podem ser em língua estrangeira, caso o consumidor típico esteja familiarizado. A autora ainda traz como exemplo alguns termos informáticos. No entanto, discordamos desse posicionamento, uma vez que a língua estrangeira, mesmo em atividades informáticas, pode trazer erros de interpretação e compreensão mesmo a um consumidor acostumado com o idioma. Em relação à oferta, não perder de vista o art. 31 do CDC. Além do mais, FABIAN, Christoph. Ibid, p. 84, afirma que a exceção para o uso da língua estrangeira seria o uso de "*palavras estrangeiras que começaram a fazer parte do vocabulário português*".

365 Sobre os aspectos necessários à informação prestada, ver a lição de Fernanda Nunes Barbosa: "*A informação clara seria aquela em que são utilizados os signos qualitativamente mais apropriados, a fim de possibilitar ao receptor interpretar corretamente a mensagem. A informação precisa, por seu turno, seria aquela em que participam também os caracteres da exatidão, pontualidade e fidelidade, o que também se dá mediante a escolha certa dos símbolos pelo emissor da mensagem. Tal requisito responde a um princípio de economia da mensagem. Já a informação completa é aquela em que o emissor, na operação de codificação, utiliza signos (sons linguísticos, sinais gráficos, gestual) e símbolos que representem integralmente a novidade. Veraz é a característica da informação que corresponde à verdade daquilo que se pretende dar a conhecer ao outro. É a correspondência entre o que se quer fazer saber e a realidade objetiva. Por fim, informação compreensível será aquela que mais análise de contexto solicitará, pois requererá do emissor uma apreensão da realidade do receptor, a fim de que a mensagem possa ser por este efetivamente compreendida.*" A autora também destaca os próprios requisitos estabelecidos no CDC, quais sejam a adequação (art. 6º, III, 8º, caput, 12, caput e 14, caput), a necessidade (art. 8º, caput) e a ostensividade (art. 9º e 21º). BARBOSA, Fernanda Nunes. Ibid, p. 61.

> "*correlacionando a disciplina constitucional com o valor da informação na sociedade de consumo pós-moderna antes referido, sem a qual o consumidor não alcança verdadeira proteção, uma vez que a desigualdade informacional potencializa ao extremo a sua vulnerabilidade, não há como deixar de reconhecer o caráter de direito fundamental à informação do consumidor.*"[366]

Se há o dever do fornecedor informar, há igualmente o dever contrário do consumidor informar-se.[367] Há a evidente demonstração aqui do aspecto colaborativo do dever de informar, conforme prescreve o princípio da boa-fé objetiva.[368]

Deve haver também uma relação "*inversamente proporcional entre a quantidade e a qualidade de informação que o fabricante coloca à disposição do público e aquela que o consumidor está disposto a processar...*"[369] Coderch e Gonzalez ensinam que se a saturação de informação é contraproducente é necessário que o fornecedor esteja concentrado em fornecer as informações essenciais sobre o uso do produto ou serviço advertindo, ainda, sobre os riscos mais importantes, baseando-se na sua gravidade e também na frequência com que ocorrem. Não basta informar apenas sobre riscos baseados nos usos apropriados e

---

366 BARBOSA, Fernanda Nunes. Ibid, p. 85.

367 Cf. SANTOLIM, Cesar Viterbo Matos. Os princípios de proteção do consumidor e o comércio eletrônico no direito brasileiro. Revista de direito do consumidor, São Paulo, n. 55, jul.-set./2005, p. 73. "*Ainda, e por outro lado, não se pode desconhecer a circunstância de que a boa-fé objetiva não funciona apenas como mecanismo de proteção do consumidor, mas, paradigma que é da eticidade nas relações obrigacionais, pode ser considerada, eventualmente, também a favor dos fornecedores...*"

368 Respeitando a visão de MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais. 6ª Ed. São Paulo: RT, 2011, p. 925. "*O dever de informar é do fornecedor, e o aplicador da lei deve interpretar toda a relação contratual (publicidade, promessas, pré-contratos, prospectos, contrato, silêncios, adendos, práticas e cláusulas, etc.) sempre a favor do consumidor para só após definir se houve abuso ou não. Indiretamente, cria aqui o CDC, ex vi lege, uma forte exceção à regra da bilateralidade dos deveres de boa-fé...*"

369 CORDERCH, Pablo Salvador; GONZALEZ, Sonia Ramos. El defecto en las instrucciones y advertencias en la responsabilidad de producto. *Latin American and Caribbean Law and Economics Association (ALACDE) Annual Papers*, Berkeley Program in Law and Economics, UC Berkeley. 2007. Disponível em: <http://escholarship.org/uc/item/8xg6n210>. Acesso em: 18 Jun. 2011, p. 8.

corretos, mas também englobando os não apropriados, porém, previsíveis.[370] Dessa forma, crescendo o risco do serviço, cresce também "*a intensidade das advertências*", conforme pode ser extraído da análise do art. 9º do CDC.[371]

O papel dos termos de uso de serviços disponibilizados no comércio eletrônico é importante à medida que podem haver instruções de uso específicas a serem cumpridas pelo consumidor. Ninguém duvida de que o consumidor de um produto perigoso, como um remédio, não deve informar-se lendo a bula para buscar as orientações pertinentes.[372] Nada impede que o fornecedor de serviços informáticos fixe critérios específicos de uso, dentro de uma razoabilidade, visando à manutenção da segurança.[373] A atuação, portanto, dos termos de serviço é relevante na parte das tratativas (art. 6º, II do CDC), na fase de desenvolvimento da relação (art. 6º, III do CDC) bem como na fase pós-contratual, no respeito ao ideal da boa-fé e transparência (art. 4º, *caput*, do CDC).[374]

Da mesma forma, salienta-se que se o fornecedor promete segurança, deve fornecer segurança[375]. Explica-se: própria publicidade, nos termos do art. 30, vincula

370 Idem. Ibid. Os autores destacam ainda que no "*hay deber de advertir sobre riesgos evidentes para consumidores y afectados y generalmente conocidos por ellos, riesgos que son naturalmente previsibles: todo el mundo debería saber que puede magullarse un dedo usando un martillo; cortárselo recogiendo los vidrios de un vaso que ha caído al suelo y se ha roto; fracturárselo al tropezar con su propio pie por no llevar bien acordonados los zapatos, etc. No hay ningún objeto físico que no resulte peligroso en algún sentido. Todos están sujetos, cuando menos, a la ley de la gravedad.*"

371 FABIAN, Christoph. Ibid, p. 150.

372 BARBOSA, Fernanda Nunes. Ibid, p. 126-127. *"Em verdade, mais do que um aumento de clareza, completude e precisão, a potencial nocividade ou periculosidade do produto ou serviço exigirá que o fornecedor alerte o consumidor acerca das precauções a serem tomadas. A advertência nesse caso, irá variar de intensidade conforme se trate de um leigou ou de um profissional especializado."*

373 Sobre o uso de serviços informáticos, Lorenzetti afirma que pode haver a cláusula de uso regular. Diz o autor que "*el uso del programa o de los datos debe ajustarse a las costumbres imperantes en el área, pero las partes pueden establecer criterios específicos, fijando el modo en que se puede usar, los usos prohibidos, con cláusulas penales para el incumplimiento.*" LOREZENTTI, Ricardo Luis. *Tratado de los contratos*. Buenos Aires: Rubinzal y Asociados, 2000. Tomo III, p. 831.

374 Cf BARBOSA, Fernanda Nunes. Ibid, p. 98-99. A autora ressalta também a lição de Clóvis do Couto e Silva no mesmo aspecto.

375 Assim FILHO, Adalberto Simão. Dano ao consumidor por invasão do site ou da rede: Inaplicabilidade das Excludentes de Caso Fortuito ou Força Maior. In: FILHO, Adalberto Simão; DE LUCCA, Newton. (coord.). *Direito & Internet – Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2000, p. 112. "*Assim, se um site se diz seguro para operações comerciais, mencionando que*

o fornecedor a prover a segurança prometida e veiculada[376]. O que parece juridicamente evidente deve ser destacado, à proporção que as políticas de uso de sites da Internet, bem como os *banners* e as informações apostas em tais sites também têm natureza vinculativa. Há uma prática de fornecedores de serviços informáticos descreverem em seus sites, justamente, que o site é totalmente seguro, o que desperta a confiança dos consumidores.

A circunstância acima é comum e vista em alguns sites, principalmente aqueles que ostentam os chamados selos de segurança[377], visando a atestar a segurança de seu ambiente[378]. Uma das empresas que certifica sites, para fins de

dados do cliente são mantidos sigilosos, e o consumidor - por esta razão - passa a efetuar neste ambiente suas aquisições de produtos e/ou serviços, em caso de invasão com resultados danosos ao último, dificilmente será afastada uma responsabilidade de quem explora os serviços dos site ou vende os produtos." No mesmo sentido BINICHESKI, Paulo Roberto. Ibid, p. 264.

376 TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. 11ª Câmara Cível. Apelação n. 2.0000.00.433758-0/000. ProInternet do Brasil Ltda X Websol - Soluções em Informática LTDA. Relator: Des. Teresa Cristina da Cunha Peixoto. Belo Horizonte, 2 de Fevereiro de 2000. Ementa: AÇÃO INDENIZAÇÃO POR DANOS MORAIS- PROVEDORA DE Internet - HOSPEDAGEM DE SITES - INVASÃO DE HACKERS - FOTOS PORNOGRÁFICAS - ABALO NA IMAGEM DA PESSOA JURÍDICA - RESPONSABILIDADE CONTRATUAL - INDENIZAÇÃO. Provado o dano ou prejuízo sofrido pela vítima, a culpa do agente e o nexo causal, surge a obrigação de indenizar, que só será afastada em hipóteses de caso fortuito ou força maior, ou se a responsabilidade pelo evento danoso for exclusiva da parte lesada. Se, por um lado, a conduta dos hackers é considerada previsível e evitável, atualmente, dependendo apenas da evolução tecnológica, não havendo como aplicar-se a excludente de força maior, por outro, a apuração da responsabilidade das empresas prestadoras de serviços de acesso à rede mundial depende do caso concreto. A publicidade amplamente divulgada garantindo segurança aos assinantes da provedora implica responsabilidade da empresa nos exatos termos da oferta apresentada, já que respondem os provedores pelos serviços prestados aos usuários por força de obrigação contratual. Em questão de responsabilização, há de se ter em conta se a empresa veiculou publicidade quanto à existência de segurança para a hospedagem dos sites, ou se comprovou ter informado a seus clientes, de maneira transparente, sobre as questões relativas às invasões dos hackers. (grifo nosso). A ausência de qualquer informação nesse sentido pode dar ensejo à responsabilidade da provedora.

377 É possível ver a questão da chamada "labelização" na tese de Eduardo Silva da Silva. Nela, o autor indica que "*Os processos de labelização atualmente existentes contribuem de forma direta e indireta à eliminação de riscos da sociedade da informação. De forma direta, afastam-se diversos perigos a que se submetem os fornecedores de bens, produtos e serviços pela Internet; de forma indireta, ao gerar um clima geral de maior confiança no próprio comércio eletrônico." p. 125.* Mais adiante o autor reconhece que *"Estas expressões da segurança denotam estabilidade da certificação de sites através de selos. Não se trata mais de experiências acadêmicas ou de exercício de ficção científica, mas, ao contrário, são a consolidação da tendência de unificação de esforços para a mitigação de um crescente implemento dos riscos próprios da Internet e de suas aplicações.*" DA SILVA, Eduardo Silva. Segurança na sociedade da informação: uma visão desde a autonomia privada. 2006. 178 p. Tese apresentada no Programa de Pós-Graduação em Direito da UFRGS, como requisito parcial para obtenção do grau de Doutor em Direito. Porto Alegre.

378 Eduardo Silva da Silva ensina ainda que existem dois tipos de labelização, a externa e a interna. Na externa "*os critérios para a concessão do selo são verificados por um auditor externo – um*

segurança, por meio dos referidos selos é a Site Blindado S/A[379]. Essa empresa realiza uma varredura de vulnerabilidades nas aplicações que o site (no caso analisado, a loja virtual Submarino) disponibiliza aos usuários para a realização das compras. A realização dessa operação abrange as vulnerabilidades que possam ser detectadas de fora, como por exemplo, uma falha conhecida no servidor em que está hospedado o site da loja. No entanto, há uma série de outras variáveis envolvidas que poderiam considerar um site seguro, como por exemplo, o vazamento de informações propagado por funcionários da própria loja virtual. Nesse sentido, é importante trazer as ressalvas técnicas que o próprio Site Blindado S/A faz sobre o serviço prestado:

> "*Os websites protegidos pelo sistema Site Blindado foram submetidos a uma bateria de testes de vulnerabilidades e foram aprovados. Isso significa que este website está protegido contra tentativas de exploração e obtenção de informações confidenciais não autorizados através das técnicas de invasão mais conhecidas. É de conhecimento comum que o ambiente computacional capaz de captar e processar informações de usuários ou dados de pagamentos É extremamente complexo e mutável frequentemente. Este, ou quaisquer outro teste de vulnerabilidades avaliam apenas o perímetro do ambiente, não levando em consideração fatores externos, somente identificáveis através de uma análise completa e abrangente de risco operacional. O Site Blindado cumpre todas as exigências do padrão de segurança da indústria de cartões de crédito PCI-DSS relativas a scans remotos de vulnerabilidades em servidores de Internet. Apesar de todo o esforço para garantir a*

---

terceiro, absolutamente, independente – antes do deferimento do pedido. Realiza-se, em suma, um controle a priori dos serviços a fim de se verificar se a empresa já privilegiava a observância das regras de segurança, qualidade, respeito à privacidade ou presteza no serviço que a autorizem a portar o símbolo distintivo.

Por sua vez, a labelização interna está em um patamar inferior, isto é, ocorre a concessão do selo, independente de uma verificação prévia quanto ao cumprimento das normas particulares. Ainda que ela também possa estar sujeita a controles posteriores por parte de auditores imparciais, essa característica não lhe é fundamental.". Idem. Ibid, p. 110.

379 Especificamente sobre a segurança da loja Submarino, as informações podem ser verificadas em https://selo.siteblindado.com.br/verificar?url=http://www.submarino.com.br.

> *proteção dos servidores auditados pelo Site Blindado, não podemos dizer que tais servidores e aplicações web estão à prova de hackers. Dados enviados e recebidos de servidores em ambiente externo, e não auditados pelo Site Blindado são passíveis de falhas de segurança, bem como dados que podem ser acessados por funcionários da empresa ou terceiros autorizados. Portanto a Site Blindado S.A. não fornece nenhuma garantia de nenhuma forma em relação à total proteção dos serviços disponibilizados pela Internet, ainda que certificados pelo Site Blindado. O uso das informações deste website é de total responsabilidade do usuário que concorda com seus termos e risco e isenta a responsabilidade do Site Blindado S.A. em qualquer eventualidade."*[380]

As ressalvas do serviço Site Blindado são bastante interessantes. Deve ser destacado que há clara menção à proteção contra "*tentativas de exploração e obtenção de informações confidenciais não autorizados através das técnicas de invasão mais conhecidas*". Essa frase destaca muito bem o fato de que se deve ter conhecimento dos riscos e das vulnerabilidades. Aqui, o processo não protege contra toda e qualquer vulnerabilidade ou ataque técnico, mas sim aos mais conhecidos: é uma expressão do avanço e do estado da técnica. Há uma clara limitação ao conhecimento de técnicas de ataque atuais para a extensão da proteção e, em tese, o aparecimento de uma novíssima vulnerabilidade de segurança completamente desconhecida, não estaria, *a priori*, abrangida nos testes dos serviços.

Além do mais, o processo de segurança prometido contém a menção explícita de que "*apesar de todo o esforço para garantir a proteção dos servidores auditados pelo Site Blindado, não podemos dizer que tais servidores e aplicações web estão à prova de hackers*". Nesse sentido, entende-se que há a declaração de que todos os meios estão (teoricamente) sendo tomados, sem garantir completamente a

380 Tais informações também dispostas no endereço https://selo.siteblindado.com.br/verificar?url=http://www.submarino.com.br.

segurança do site. Mais adiante há a ressalva de que o Site Blindado "*não oferece nenhuma garantia de nenhuma forma em relação à total proteção dos serviços disponibilizados pela Internet, ainda que certificados pelo Site Blindado*". Também, em seguida, é mencionada a circunstância de que há elementos não auditados pelo Site Blindado, e isso, pelo fato de tais elementos não estarem sendo auditados, podem carregar neles uma vulnerabilidade que pode, em tese, ser explorada em um ataque virtual.

Mesmo assim, não se desconhece a responsabilidade do fornecedor de serviços de comércio eletrônico pela violação de confidencialidade de dados, mesmo no caso do site estar certificado por uma entidade semelhante ao Site Blindado. É, portanto, ineficaz qualquer alegação do fornecedor no sentido de afastar sua responsabilidade por uma certificação dessa natureza por dois motivos: o primeiro, e mais evidente, pela responsabilidade objetiva do fornecedor reconhecida nas relações de consumo; o segundo motivo é que é impossível que uma dessas certificações consiga cobrir todas as variáveis que possam ser envolvidas em um incidente de segurança, como diz a ressalva feita pelo próprio Site Blindado, à medida que *"dados que podem ser acessados por funcionários da empresa ou terceiros autorizados".*[381]

Como o recolhimento de informações pessoais na Internet é realizado, em muitos casos, sem que o usuário perceba, os termos de serviço podem constituir também o veículo de informação sobre as características de recolhimento de dados. Também chamadas de políticas de privacidade, esses termos informam como as informações são recolhidas, armazenadas, processadas e utilizadas.[382]

---

381 Sobre a questão da labelização e certificação aplicada especificamente à proteção da privacidade, nos EUA, a empresa TRUSTe criou um certificado chamado TRUSTemark, que tem o propósito de constatar se as empresas de comércio eletrônico respeitam as políticas de privacidade que adotam. Cf. RIBEIRO, Luciana Antonini. Ibid, p. 163.

382 Cf. RIBEIRO, Luciana Antonini. Ibid, p. 161. "*Transpondo-se a situação em questão à realidade virtual, verificamos que quando do preenchimento de um formulário virtual, deverá o consumidor ser expressamente cientificado de que aquelas informações constarão de um banco de dados, se for o caso. Cabe, ainda, ao fornecedor informar qual a utilização que será conferida às informações lá constantes,*".

No entanto, para o cumprimento adequado[383] do dever de informar, entende-se que, na geralidade dos casos, há falhas dos fornecedores. Quem navega na Internet certamente já viu links para políticas de privacidade e de uso, em geral posicionadas no rodapé dos sites e publicadas com letras pequenas. Ora, se a proteção de informações pessoais é um direito fundamental e sua divulgação não autorizada pode trazer graves danos para os consumidores, os fornecedores certamente devem empregar um empenho maior para informar acerca das políticas de privacidade. Um link no rodapé das páginas, certamente não atende ao requisito da informação eficiente.[384] É evidente que há uma questão comercial nessa situação: se os riscos forem expostos de maneira muito extensa e insistente, podem afastar o consumidor. Deve haver um balanceamento entre a transparência e o dever de informar que o fornecedor possui, sem afastar, no entanto, a divulgação das vantagens comerciais do serviço. Nenhum serviço é vendido apenas com a demonstração de seus riscos, e não é isso que é defendido aqui.

A.3 - Os bancos de dados de informações de consumidores

O Código de Defesa do Consumidor trata especificamente da questão de armazenamento de dados pessoais dos consumidores em seu art. 43. Como o título da seção é "*Dos bancos de dados e cadastros dos consumidores*", é possível encontrar com maior frequência a doutrina comentando acerca do armazenamento de informações em cadastros negativos de crédito dos consumidores. Mais recentemente, tem-se a lei 12.414 de 9 de Junho de 2011 que "*Disciplina a*

383 FABIAN, Christoph. Ibid, p. 81-82. A adequação deve estar relacionada com a possibilidade de prestar a informação. Assim diz o autor: *"A informação deve ser adequada. Ela não precisa ser profunda ou muito detalhada. Devem ser informações de quantidade e qualidade, para que o consumidor possa formar livremente a sua vontade de consumidor. Este conceito é uma delimitação para que o dever de informar torne-se praticável."* No mesmo sentido, por óbvio, a informação deve ser verdadeira, sendo este "*talvez o elemento mais importante, pois a informação falsa prejudica o consumidor...*" cf. HARTMANN, Ivar Alberto Martins. Ibid. p. 170.

384 Conforme LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados. 2003, p. 169: "*La información deve ir dirigida al consumidor particular y estar sometida a las relaciones del caso, y correponderse con el nivel educativo del profano; debe ser "pertinente".*"

formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito", ou seja, os chamados cadastros positivos.[385]

Ocorre, no entanto, que a sociedade atual, baseada no armazenamento e processamento desenfreado de informações, não limita os fornecedores de serviços a armazenarem apenas informações relacionadas ao crédito. Ao contrário, os bancos de dados atuais armazenam informações e dados pessoais dos mais variados possíveis. Dessa forma, as disposições sobre o armazenamento de informações em bancos de dados do art. 43 do CDC, aplicam-se a qualquer armazenamento de informações pessoais dos consumidores.[386]

A relação que os usuários possuem com os provedores de serviços na Internet é classificada como de consumo. Mesmo que existam muitos serviços que são utilizados sem a contraprestação de uma remuneração (como e-mails gratuitos, redes sociais, etc), a interpretação dominante é que os fornecedores de tais serviços retiram um lucro indireto por meio, por exemplo, das propagandas veiculadas. De qualquer forma, existem decisões contrárias, no sentido de não entender a utilização de serviços gratuitos na Internet (como as redes sociais) como uma relação de consumo.[387]

---

385 Segundo MENDES, Laura Schertel. Ibid, p. 64. "*A sua principal característica [da lei] reside no fato de ter ampliado a possibilidade do fluxo de dados no mercado, ao possibilitar a formação de bancos de dados com informações de adimplemento, ao mesmo tempo em que buscou estabelecer regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade.*"

386 De acordo com a lição de RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na Internet - Uma primeira reflexão. Revista de direito do consumidor, São Paulo, n. 41, jan.-mar./2002, p. 161. "*o art. 43 do Código abrange a criação e manutenção de todas as espécies do gênero banco e consumo, (grifo nosso) regulando, pois todos os "cadastros, fichas, registros e dados pessoais e de consumo" que venham a ser formados acerca de um determinado consumidor*"

387 TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70027619519. Google Brasil x Cassilda Salete Prigol. Relator: Des. Romeu Marques Ribeiro Filho. Porto Alegre, 11 de Março de 2008. Ementa: APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO INDENIZATÓRIA POR DANOS MORAIS. CRIAÇÃO DE PÁGINA E COMUNIDADE NO ORKUT COM CARÁTER DIFAMATÓRIO. CONTEÚDO PEJORATIVO. OFENSA À IMAGEM E À HONRA DA AUTORA. RELAÇÃO EXTRACONTRATUAL. "SERVIÇO" PRESTADO DE FORMA GRATUITA. NÃO APLICAÇÃO DO CDC. DANO MORAL CONFIGURADO. QUANTUM INDENIZATÓRIO REDUZIDO, DE ACORDO COM OS PARÂMETROS DESTA CÂMARA PARA CASOS ANÁLOGOS. JUROS DE MORA A PARTIR DO EVENTO DANOSO. SÚMULA 54 DO

Adota-se como conceito de banco de dados, para fins de seu entendimento no sistema de consumo, aquele trazido por Ana Paula Gambogi Carvalho:

> "*Considera-se banco de dados, em um sentido amplo, toda compilação de informações, obras e outros materiais organizados de forma sistemática e ordenada, segundo determinados critérios e finalidades específicas, feitas por pessoa física ou jurídica, privada ou pública, sob a forma de fichas, registros ou cadastros, por processo manual, mecânico ou eletrônico, para uso próprio ou fornecimento a terceiros, de forma a facilitar o seu acesso e manuseio.*"[388]

Por sua vez, Michele Keiko Mori sustenta, ao comentar sobre os sistemas de armazenamento de dados pessoais, que, entre eles, há "*serviços de proteção ao crédito, bancos, Receita Federal, bem como empresas que contêm cadastro de dados pessoais de seus clientes.*"[389] É possível afirmar que, na sociedade da informação, "*o processamento de dados é generalizado, pois ocorre nas múltiplas situações de vida e, por isso, também os riscos ao cidadão são generalizados.*"[390]

Sabe-se que não apenas o acesso, mas também a utilização de informações pessoais dos usuários em bancos de dados só podem ocorrer com a comunicação e

---

STJ. SUCUMBÊNCIA MANTIDA. Ausência de remuneração como forma de contraprestação do "serviço" prestado. Relação de consumo não configurada, pois não preenchidos os requisitos do art. 3, § 2º do CDC. A relação em tela é extracontratual, regida pelo Código Civil. A autora comprovou inequivocamente a criação de página, por terceiro, em seu nome, com conteúdo pejorativo, configurando a ofensa à imagem e à honra da demandante. Redução do quantum para o patamar de R$ 9.300,00, que equivale a 20 salários mínimos, com base nos parâmetros desta Câmara para casos análogos. Por se tratar de relação extracontratual, os juros devem incidir a partir do evento danoso, com base na Súmula nº 54 do STJ. Ausência de pedido, na apelação, de redução da verba honorária. Sucumbência mantida. APELAÇÃO PARCIALMENTE PROVIDA. Nesse sentido, ver também MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009, p. 53.

388 CARVALHO, Ana Paula Gambogi, p. 88.

389 MORI, Michele Keiko. *Direito à indimidade versus informática*. Curitiba: Juruá, 2001.p. 47.

390 MENDES, Laura Schertel. Ibid, p. 58-59.

a autorização prévia dos consumidores, sendo vedado o uso de tais dados para fins diversos daqueles autorizados.[391] A autorização é, portanto, um requisito prévio a ser obtido pelo fornecedor se quiser acessar e utilizar as informações pessoais dos consumidores.

Um dos exemplos da utilização de dados para fins diversos do recolhido ocorre nas empresas que trabalham com serviços de mala direta virtuais. Tais empresas precisam retirar os endereços de e-mail para o envio das malas diretas de algum lugar. Caso o consumidor não forneça seu e-mail para aquela empresa, em tese, não poderia ele receber mensagens sem que a empresa tivesse adquirido uma listagem de endereços.[392]

Neste aspecto, Danilo Doneda destaca quatro princípios gerais acerca da proteção de informações em bancos de dados[393]:

> *a) Princípio da publicidade (ou transparência) que prega a necessidade de dar conhecimento e autorização prévios para que o banco de dados possa funcionar;*

391 RIBEIRO, Luciana Antonini. Ibid, p. 164. No mesmo sentido CARVALHO, Ana Paula Gambogi. Ibid, p. 98. "*O uso dos dados para fins diversos, como a comercialização ou cessão a terceiros, ofende a boa-fé objetiva e o direito constitucional do consumidor à intimidade e à vida privada, podendo lhe causar sérios e irreparáveis danos.*"
Na realidade americana, Daniel Solove, no artigo "I've Got Nothing to Hide" and Other Misunderstandings of Privacy" relata que, em 2002 "*the media revealed that the Department of Defense was constructing a data mining project, called "Total Information Awareness" (TIA), under the leadership of Admiral John Poindexter. The vision for TIA was to gather a variety of information about people, including financial, educational, health, and other data. [...] When the program came to light, a public outcry erupted, and the U.S. Senate subsequently voted to deny the program funding, ultimately leading to its demise. Nevertheless, many components of TIA continue on in various government agencies, though in a less systematic and more clandestine fashion.*" SOLOVE, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, 2007. Disponível em: <http://ssrn.com/abstract=998565>. Acesso em: 10 Jan. 2012, p. 746.

392 Sobre isso ver a reportagem disponível em TELES, Giovana. Venda de listas de e-mails causa transtorno com mensagens de spam. G1. 24 de Janeiro de 2012. Disponível em: <http://g1.globo.com/jornal-hoje/noticia/2012/01/venda-de-listas-de-emails-causa-transtorno-com-mensagens-de-spam.html>. Acesso em: 24 Jan. 2012. Observar também a recente proposta de atualização do Código de Defesa do Consumidor que trata também do envio de mensagens não solicitadas no artigo 45-E.

393 DONEDA, Danilo. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em: 12 Fev. 2012, p. 16 e 17.

> *b) Princípio da boa-fé (ou finalidade) que prega a necessidade de uso dos dados apenas no cumprimento dos objetivos informados quando da coleta de dados, bem como a coleta de dados apenas de forma lícita e relacionada com os objetivos e ainda a limitação no tempo de armazenamento dos dados;*[394]
>
> *c) Princípio do livre acesso que permite que a pessoa que tenha seus dados armazenados consiga acessá-los a qualquer tempo, bem como corrigí-los.*
>
> *d) Princípio da segurança física e lógica que prevê a proteção contra riscos de "extravio, destruição, modificação, transmissão ou acesso não autorizado."*

Em outro estudo, Danilo Doneda atualizou a denominação desses princípios, assim os chamando de: princípio da publicidade (ou da transparência); princípio da exatidão; princípio da finalidade; princípio do livre acesso (onde o indivíduo deve possuir acesso aos seus dados armazenados) e, por fim, princípio da segurança física e lógica.[395]

Igualmente, o anteprojeto de lei brasileiro de proteção de dados pessoais[396] enumera em seu art. 8º os seguintes princípios: princípio da finalidade; princípio da necessidade; princípio do livre acesso; princípio da proporcionalidade; princípio da qualidade dos dados; princípio da transparência; princípio da segurança física e lógica; princípio da boa-fé objetiva; princípio da responsabilidade e o princípio da prevenção.

---

394 Esse princípio é complementado pela lição de MENDES, Laura Schertel. Ibid, p. 53, quando comenta o princípio da qualidade de dados: "*Ele se refere à exigência de que os dados constantes em um banco sejam objeto de um tratamento leal e lícito, sejam adequados pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados.*"

395 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 216-217

396 Que pode ser encontrado no endereço culturadigital.br/dadospessoais

Do ponto de vista histórico, não se perca de vista que a principiologia sobre proteção de dados pessoais já existe desde 1981, conforme a Convenção de Proteção dos Indivíduos acerca do Processamento Automático de Dados Pessoais – 108/81[397]. Nela, no capítulo 2, são estabelecidos os princípios básicos de proteção de dados, entre os quais se destacam: princípio da qualidade (envolvendo a obtenção justa, legal, acurada e atualizada dos dados; o armazenamento e uso para fins legítimos; o não armazenamento excessivo de dados, fora dos propósitos para os quais foram recolhidos); o princípio das categorias especiais (que impede o armazenamento e tratamento de dados sensíveis); o princípio da segurança, além de outras questões atualmente já conhecidas pela doutrina.

Os princípios recém citados estão de acordo com a disciplina relacionada aos bancos de dados de consumidores estipulada no art. 43 do CDC. A doutrina entende que a análise direta do referido artigo possibilita extrair, portanto, seis preceitos: o direito de acesso, o princípio da qualidade dos dados, o princípio da transparência, o direito de retificação e cancelamento e o princípio do esquecimento (baseado no "limite temporal para armazenamento de dados pessoais").[398]

Acerca de práticas envolvendo os bancos de dados de consumo, o Decreto 2.181, de 20 de Março de 1997, ao dispor sobre a organização do Sistema Nacional de Defesa do Consumidor e ainda estabelecer normas gerais de aplicação das sanções administrativas do CDC, estabelece em seu art. 13, como práticas infrativas:

> *X - impedir ou dificultar o acesso gratuito do consumidor às informações existentes em cadastros, fichas, registros de dados pessoais e de consumo, arquivados sobre ele, bem como sobre as respectivas fontes;*

397 Do título em inglês "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ".
398 Idem. Ibid, p. 63

> *XI - elaborar cadastros de consumo com dados irreais ou imprecisos;*
> *XII - manter cadastros e dados de consumidores com informações negativas, divergentes da proteção legal;*
> *XIIII - deixar de comunicar, por escrito, ao consumidor a abertura de cadastro, ficha, registro de dados pessoais e de consumo, quando não solicitada por ele;*
> *XIV - deixar de corrigir, imediata e gratuitamente, a inexatidão de dados e cadastros, quando solicitado pelo consumidor;*
> *XV - deixar de comunicar ao consumidor, no prazo de cinco dias úteis, as correções cadastrais por ele solicitadas;*

A prática destas infrações sujeita o fornecedor a cumprir as penalidades administrativas assim dispostas no art. 18 do mesmo decreto, que repete o estabelecido no art. 56 do CDC.[399] De qualquer forma, a proteção de informações contidas nos bancos de dados, no âmbito do direito do consumidor, "*vai se concentrar sobretudo na tutela da sua integridade moral [do consumidor], em especial a proteção do direito à privacidade e do direito à honra*".[400]

B) Dever de confidencialidade de dados

399 Marcel Leonardi reconhece que há uma dificuldade prática na utilização do habeas data. A principal delas seria o custo. O autor, mesmo que a ação seja gratuita, necessita da contratação de uma advogado para a propositura da ação. Sugere ele a possibilidade de admissão da propositura nos juizados especiais cíveis, através de uma alteração na lei 9.099/95. LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 206

400 Cf. o alerta de MIRAGEM, Bruno. Os direitos da personalidade e os direitos do consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 451-452. "*O principal direito subjetivo ofendido pela conduta ilícita é o direito à honra do consumidor, violado pela projeção externa de informações desabonatórias não-verdadeiras, o que enseja a indenização por danos morais advindos da ofensa.*"

Uma noção geral de segurança aplicada ao ambiente virtual de consumo, que tem na proteção da confidencialidade de dados um de seus desdobramentos, pode ser definida pelo fato de que:

> "*não devem ser afetados os bens que são depositados nas mãos do provedor, e que os bens que integram a prestação não devem causar prejuízos a outros bens do usuário. Em um segundo aspecto, o dever de segurança faz o provedor responsável por todos os danos que sofra o consumidor, em sua pessoa, conforme o regime de responsabilidade aplicável.*"[401]

A Constituição, em seu art. 5º, inc. XII, como já se mencionou, protege a inviolabilidade do sigilo (ou confidencialidade) dos dados. Nesse contexto, dados "*em matéria constitucional, corresponde a informações sobre as pessoas, merecendo a inviolabilidade dos dados individuais proteção constitucional, em decorrência expressa do dispositivo legal na Constituição.*"[402]

Manter a confidencialidade dos dados[403] também significa cumprir outros dois deveres: o de informar sobre os possíveis riscos de violação da confidencialidade daquele ambiente e também o de informar caso haja alguma violação de confidencialidade que exponha os dados dos consumidores. Além do mais, o direito à proteção de dados, que se desdobra na proteção da confidencialidade, possui um duplo aspecto: o aspecto negativo (através da abstenção da violação da confidencialidade – direito de defesa) e o aspecto positivo (direito à prestação em caso de violação).[404]

É possível chegar a essa conclusão mediante a interpretação do art. 10, §1º do CDC, que diz:

---

401 LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 130.
402 MORI, Michele Keiko. Ibid, p. 47.
403 Cf. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 84, um dos deveres dos provedores de internet é justamente o de manter em sigilo os dados dos usuários.
404 MENDES, Laura Schertel. Ibid, p. 74.

> "*O fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários*".

Essa mesma conclusão pode ser alcançada, em relações que não sejam de consumo, por meio da aplicação do princípio da boa-fé objetiva. Um dever de geral de informar a ocorrência de incidentes de segurança abrangeria, portanto, qualquer tipo de contato informático.[405]

Esta constatação é apoiada, no Direito Comunitário, pela Diretiva 2002/58/CE[406] que estabelece claramente, no seu art. 4º, 2., sob o caput "Segurança", o dever de informar quanto aos riscos especiais:

> *2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações electrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.*

405 Eberlin ensina que não pratica ato ilícito o fornecedor "*que não deveria saber da nocividade ou periculosidade do produto e que, ao tomar conhecimento do defeito, comunica as autoridades e consumidores*". EBERLIN, Fernando Büscher von Teschenhausen. Ibid, p. 34.
O anteprojeto brasileiro de lei de proteção de dados pessoais estabelece, no seu art. 27, obrigação semelhante: "*O responsável pelo tratamento deverá comunicar à Autoridade de Garantia e aos titulares dos dados, imediatamente, sobre o acesso indevido, perda ou difusão acidental, seja total ou parcial, de dados pessoais, sempre que este acesso, perda ou difusão acarretem riscos à privacidade dos seus titulare s*"

406 UNIÃO EUROPEA. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa.

Isso nada mais é do que um alerta[407] para os usuários de um sistema. Importante destacar que esse dever de alerta a respeito dos riscos informáticos existe tanto nas relações entre fornecedores-consumidores quanto nas relações entre empresas.[408]

Mesmo que haja uma diferenciação na extensão dos deveres nas duas situações, não se pode negar que o ambiente tecnológico é bastante complexo, e sua segurança depende de uma série de variáveis. Até o mais diligente homem de negócios, em algumas situações, pode não conseguir ter a exata noção dos riscos e das vulnerabilidades de um sistema informático.

De qualquer forma, a diretiva 95/46/CE estabelece, em seu art. 17, as definições acerca da segurança no tratamento de informações, e, entre os casos aplicáveis, há a proteção contra "*a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.*" Tal disposição enquadra-se em um dever geral de confidencialidade dos responsáveis. Na Argentina, por exemplo, a lei 25.326/2000, no seu art. 9º até proíbe o armazenamento de registro de dados pessoais em bancos de dados que não possuam a segurança adequada.[409]

---

407 Conforme Christine Noiville, "*a ideia de convidar todos aqueles que têm conhecimento de uma ameaça de perigo a assinalar, a alertar, se impôs naturalmente. Assim, o alerta tornou-se um elemento das políticas de prevenção de todos os tipos de riscos reunidos.*" NOIVILLE, Christine. Para uma proteção do lançador de alerta. In: VARELLA, Marcelo Dias. *Direito, Sociedade e Riscos: A sociedade contemporânea vista a partir da ideia de risco*. Brasília: UNICEUB, 2006, p. 124.

408 É evidente que o padrão do dever de alerta em um e outro caso é diferenciado, conforme destaca Paula Forgioni: "*Eis outra diferença entre o sistema consumerista e o comercialista. O padrão imposto aos homens de negócio supõe que buscarão diligentemente as informações necessárias à tomada da sua decisão; ao revés, não se espera do consumidor grande empenho na coleta de dados a partir do momento em que o fornecedor está vinculado à 'transparência obrigatória nas relações de consumo'*". FORGIONI, Paula A. *Teoria Geral dos Contratos Empresariais*. 2ª Ed. São Paulo: RT, 2010, p. 141-142.

409 Cf. Lei Argentina n. 25.326/2000 (Ley de Protección de los Datos Personales), art. 9º: "*1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.*

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad."

De forma geral, o dever de confidencialidade é constituído pela própria manutenção do sigilo e proteção das informações pessoais e sensíveis tanto no seu armazenamento quanto na sua transmissão. A disciplina tecnológica entende que há duas formas de garantir a confidencialidade de dados, por meio do controle de acesso ou por intermédio da criptografia.[410]

No mesmo sentido, o art. 26 do anteprojeto brasileiro de lei de proteção de dados pessoais estabelece que aquele que fizer parte da tarefa de tratamento de proteção de dados pessoais "*obriga-se ao dever de segredo em relação aos mesmos, dever este que permanece após o término do respectivo tratamento ou do vínculo empregatício existente.* "

Manter a confidencialidade do acesso à informação também desdobra-se em outras ações, como a própria identificabilidade de acessos e o armazenamento de informações sobre os acessos, que serão tratados em seguida.

B.1 - A identificabilidade de acessos e o armazenamento de logs

A importância do destaque das questões de controle de acesso tecnológico nesse trabalho, remete ao fato de estabelecer que o dever de segurança da informação e de confidencialidade desdobra-se também no dever de identificabilidade digital. O responsável pelos sistemas informáticos deve manter mecanismos específicos que permitam a identificação dos usuários daquela estrutura, bem como reconhecer as ações realizadas em seu ambiente. Só é

Inclusive o decreto 1.558/2001, que regulamenta referida lei, ao tratar da regulamentação específica do art. 9º, assim dispõe: "p*romoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que suscitenla confianza en los sistemas de información, así como en susmodalidades de provisión y utilización.*"

410 HÉLIE-GHERNAOUTI, Solange. *Internet et sécurité*. 2ª Ed. Paris: Puf, 2002, p. 43.

possível permitir o acesso autorizado a uma informação se houver a identificação da pessoa que tenta realizá-lo.

A não identificação dos usuários em uma estrutura computacional pode permitir que o instrumento seja utilizado para fins ilícitos, frente à possibilidade de não identificação[411]. Ademais, deve ser observada a vedação do anonimato assim prevista pela Constituição Federal.[412]

Além do mais, o fornecedor que não cumpre com o dever adequado de identificabilidade no ambiente virtual, arca com a obrigação de indenizar o consumidor em função da impossibilidade da identificação do autor de fato.[413]

411 Cf. DE VILLIERS, Meiring. Ibid, p. 142: "*The Internet provides the technological platform and opportunity to a skilled operator to assume different identities, erase his digital footprints, and transfer incriminating evidence electronically to innocent computers, often without leaving a trace. Courts have recognized the perverse incentives and law enforcement problems created by anonymous defendants in cyberspace.* "

412 Cf. o Art. 5o, inc. IV da Constituição Federal. No mesmo sentido de estabelecer um dever de identificabilidade nas estruturas ou sistemas computacionais, temos a lei do estado de São Paulo n. 12.228/2006 que "Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências." Nela, o requisito da identificabilidade também é encontrado.

413 TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 6ª Câmara Cível. Apelação n. 70013361043. Jocelei Perdomo das Neves X Terra Networks Brasil S/A. Relator: Des. Artur Arnildo Ludwig. Porto Alegre, 21 de Dezembro de 2006. Ementa: APELAÇÃO CÍVEL. INDENIZAÇÃO POR DANO MORAL. ANÚNCIO INVERÍDICO OFENSIVO À HONRA DA AUTORA VEICULADO NO SITE DA REQUERIDA. RESPONSABILIDADE DO PROVEDOR E DO FORNECEDOR DE SERVIÇOS. APLICAÇÃO DA TEORIA DA CARGA DINÂMICA DO ÔNUS DA PROVA. VALOR DA INDENIZAÇÃO. ATENÇÃO AO CRITÉRIO PUNITIVO-PEDAGÓGICO AO OFENSOR E COMPENSATÓRIO À VÍTIMA. INAPLICABILIDADE AO CASO PELO JUÍZO A QUO DO INSTITUTO NORTE-AMERICANO DO PUNITIVE-DAMAGES. 1 – Incontroverso o fato de que o anúncio registrado no site "Almas Gêmeas" pertencente à requerida, foi efetuado por terceiro alheio ao processo. 2- Atuando a ré como provedora de acesso à Internet e não sendo possível a identificação do real responsável pelo conteúdo ofensivo do anúncio, é seu o dever de indenizar pelos danos à personalidade da autora. Aplicação da Teoria da Carga Dinâmica da Prova, ou seja, incumbe a quem tem mais condições a prova de fato pertinente ao caso. 3 - Não só como provedora de acesso em sentido amplo atuou a ré na relação em análise, como atuou também como prestadora de serviços, mesmo que gratuitamente. Evidencia-se a desmaterialização e despersonalização das relações havidas pelo uso da Internet, não sendo mais possível identificar o objeto e muito menos os sujeitos de tais relações. Assim, sendo a ré empresa que possui site na Internet de relacionamentos deve, a fim de evitar a incomensurável dimensão dos danos oriundos do mau uso de seus serviços, adotar medidas de segurança que diminuam tais riscos. 4 – Valor da Indenização que atendeu o caráter punitivo-pedagógico ao ofensor e compensatório à vítima pelo dano sofrido. Ademais, para o arbitramento do dano moral deve-se levar em conta as condições econômicas da vítima e do ofensor. Inaplicabilidade do instituto norte-americano do punitive damages. Aplicação ao caso dos critérios para aferição do quantum a indenizar em consonância com o instituto da responsabilidade civil do direito brasileiro. NEGADO PROVIMENTO AOS APELOS, COM EXPLICITAÇÃO.

O dever de identificabilidade deve ser visto, portanto, dentro dos limites do ambiente digital em questão. Ele é limitado tecnicamente às características do serviço e aos dados que são recolhidos naquela atividade. O fornecedor de serviços, por óbvio, não pode ser compelido a fornecer dados que não possui. Nos casos das redes sociais, por exemplo, são armazenados os dados da conta criada pelo usuário, além de endereço IP bem como a hora de utilização de serviços. Como, via de regra, os provedores não solicitam CPF, RG e endereço pessoal dos usuários, não podem, portanto, fornecê-los.[414]

Marcel Leonardi explica que o dever de possibilitar a identificação dos usuários de provedores de serviços, ocorre: "*para que tais informações sejam disponibilizadas a quem de direito em caso de ato ilícito, pois nem sempre os dados cadastrais contendo os nomes, endereços e demais dados pessoais dos usuários estarão corretos ou atualizados.* "[415]

A lição de Leonardi é esclarecedora, porém entende-se que o dever é mais amplo e não se aplicaria apenas aos provedores de serviços, mas sim a todo aquele que dispõe de uma estrutura computacional acessada por diversas pessoas. Uma empresa que apenas mantém seu site institucional na Internet, mediante seus próprios esforços, pode não ser considerada um provedor de serviços. No entanto, caso a referida empresa mantenha um fórum de discussão em seu site, e alguém

414 Cf. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 10ª Câmara Cível. Agravo de Instrumento n. 70028102291. Google Brasil Internet Ltda. X Sabemi Seguradora S.A e Luiz Carlos Franca Martinez. Relator: Des. Paulo Antônio Kretzmann. Porto Alegre, 19 de Março de 2009. Ementa: AGRAVO DE INSTRUMENTO. Internet. COMUNIDADE ORKUT. GOOGLE BRASIL. IDENTIFICAÇÃO DO CRIADOR DA PÁGINA. IMPOSSIBILIDADE. Considerado o fato de que o Google, como provedor de hospedagem da página na Internet, não possui os dados relativos aos nomes, endereço e outros identificadores dos hospedantes, a não ser o número do IP (Internet Protocol), e também pelo fato de que não é obrigado a armazenar dados pessoais de seus usuários, então não pode ser compelido a fornecer informações que não possui em seu banco de dados, tais como o nome, o CPF, o RG e o endereço pessoal de seu usuário. AGRAVO PROVIDO.

415 LEONARDI, Marcel. Determinação da Responsabilidade Civil pelos Ilícitos na Rede: Os Deveres dos Provedores de Serviços de Internet. In: SANTOS, Manoel J. Pereira dos; SILVA, Regina Beatriz Tavares da Silva. (coord). *Responsabilidade Civil na Internet e nos Demais Meios de Comunicação*. São Paulo: Saraiva, 2007, p. 74-75.

manifeste-se anonimamente nele causando dano a um terceiro, teria a empresa o dever de identificar os referidos autores.

Da mesma forma, as próprias “lan houses” (cibercafés), apesar de não figurarem como um provedor de serviços, ou provedor de acesso, por disponibilizarem uma infraestrutura de acesso, teriam o dever de identificabilidade do ambiente, “*mantendo um cadastro atualizado dos usuários a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos*”[416]

No âmbito de acesso a dados de consumidores, a lei 12.414/2011 estabelece um dever geral de identificabilidade no ambiente de sistemas que envolvem os cadastros positivos, por meio do inc. IV do art. 6º[417]. Note-se que, além do pressuposto de identificabilidade, há também o dever de armazenar os registros de consultas pelo período de seis meses. Mais adiante, no art. 9º, parágrafo 4º, da mesma lei, é estipulado o dever de manter a identificação “*do equipamento ou terminal a partir do qual foi processada tal ocorrência*”, referente à inscrição e atualização de dados cadastrados.

Portanto, em qualquer situação de acesso a dados pessoais de consumidores sempre deve ser mantido o registro dos acessos, visando identificar quem os efetuou.

---

416 Conforme julgado neste sentido que ressalta a aplicabilidade da lei 12.228/2006 naquele estado. TRIBUNAL DE JUSTIÇA DE SÃO PAULO. 8ª Câmara de Direito Privado. Apelação n. 604.346.4/7-00. Gisele Colombo de Andrade Rodrigues x Maifa Café Ltda. - EPP. Relator: Salles Rosso. São Paulo, 11 de Dezembro de 2008. Ementa: AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM PERDAS E DANOS - Mensagem eletrônica recebida pela autora de teor ofensivo à sua honra - Obrigação do estabelecimento de onde partiu o envio de manter cadastro atualizado dos usuários, a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos - Aplicação da Lei Estadual n 12.228/06 que obriga os estabelecimentos que fornecem serviços de acesso à Internet de manter referido cadastro - Atividade destes estabelecimentos que pode ser considerada de risco, caso não tomem as medidas necessárias que possibilitem a identificação dos usuários (art. 927, parágrafo único, do Código Civil) - Responsabilidade civil pelos danos causados caracterizada - Cabimento do pedido alternativo para conversão em perdas e danos - Procedência mantida - Recurso desprovido.

417 *Art. 6º - Ficam os gestores de bancos de dados obrigados, quando solicitados, a fornecer ao cadastrado: IV - indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos 6 (seis) meses anteriores à solicitação;*

Quanto ao armazenamento de logs, cabe primeiro sua conceituação. Um log ou um “log de dados” é nada mais do que registro que permite identificar quem realizou determinada ação em um ambiente virtual. Basicamente eles são “provas” automaticamente produzidas pelos sistemas que registram detalhes sobre um acesso.[418]

A norma NBR ISO/IEC 27002, trata sobre a questão dos logs no título 10.10.1 - Registros de auditoria. Ela estabelece, nesse controle, o seguinte:

> *Convém que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.*
> *Diretrizes para implementação:*
> *Convém que os registros (log) de auditoria incluam, quando relevante:*
> *a) identificação dos usuários;*
> *b) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;*
> *c) identidade do terminal ou, quando possível, a sua localização;*
> *d) registros das tentativas de acesso ao sistema aceitas e rejeitadas;*
> *e) registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;*
> *f) alterações na configuração do sistema;*
> *g) uso de privilégios;*
> *h) uso de aplicações e utilitários do sistema;*

418 Um dos deveres dos provedores de serviços, de acordo com Marcel Leonardi, é o de manter informações por tempo determinado, cf. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 84.

> *i) arquivos acessados e tipo de acesso;*
> *j) endereços e protocolos de rede;*
> *k) alarmes provocados pelo sistema de controle de acesso;*
> *l) ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus e sistemas de detecção de intrusos.* [419]

Embora a referida norma contenha detalhes técnicos relacionados aos processos informáticos de segurança da informação, ela estabelece importantes requisitos que podem ser transpostos para o direito. Por exemplo, ao definir a importância da identificação dos usuários, o terminal usado, as datas e horários, os arquivos acessados, os endereços e protocolos de rede ela orienta o próprio dever de identificabilidade em um ambiente computacional. Ora, os responsáveis por bancos de dados contendo informações pessoais dos consumidores precisam, necessariamente, cumprir esses requisitos para, em um incidente, poderem identificar adequadamente quem realizou os acessos aos dados. A própria lei 12.414/2011, como já se viu, estabelece a necessidade de identificabilidade do ambiente e o apontamento de quem realizou as consultas.[420]

B.2 - Uso e acesso controlado no tratamento de informações pessoais

419 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2005, p. 61.

420 Importante ressaltar que o REsp. n.1193764/SP, já citado anteriormente neste trabalho, reconhece que em situações envolvendo provedor de conteúdo e a publicação de conteúdos por terceiros, o dever de identificabilidade é atendido apenas com o registro do endereço IP, em função até dos limites da própria atividade.

Via de regra, dados pessoais de consumidores não podem ser recolhidos e tratados sem o seu devido consentimento[421]. Sempre que houver o recolhimento de dados é necessário que o fornecedor:

> "*expressamente informe ao consumidor qual a utilização que será conferida aos seus dados pessoais, concedendo-lhe a oportunidade para que o mesmo manifeste sua contrariedade na utilização destes dados*".[422]

Não é permitido, portanto, o uso secundário das informações. A confidencialidade abrange, assim, o próprio controle do uso e acesso das informações.

O fornecedor responsável pelo armazenamento de dados do usuário deve informar detalhadamente a finalidade pela qual os dados estão sendo recolhidos e não utilizá-los para outros fins: é o uso "*segundo a finalidade específica para o qual foram coletados.*"[423] Esse uso é decorrente:

> "*da sistemática do Código de Defesa do Consumidor, que considera a transparência e a confiança princípios orientadores das relações de consumo, assegurando ao consumidor o direito básico à informação e protegendo a sua legítima expectativa*". [424]

Cumpre destacar que essa questão da finalidade do uso também é chamada, pela doutrina americana, como o princípio da especificação de propósito. Esse princípio foi utilizado em diversas legislações americanas como no "*Privacy Act*" de

---

421 No direito comunitário, os considerandos 30 e 33, bem como o art. 7º alínea a) da Diretiva 95/46/CE estabelecem a necessidade do "consentimento explícito da pessoa em causa" para o tratamento de dados pessoais. UNIÃO EUROPÉIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa. Já no anteprojeto de lei brasileiro de proteção de dados pessoais o consentimento é estabelecido como requisito para tratamento de dados, conforme o art. 9º.

422 RIBEIRO, Luciana Antonini. Ibid, p. 160.

423 CARVALHO, Ana Paula Gambogi. Ibid, p. 109.

424 Idem. Ibid, p. 109.

1974; "*Fair Credit Reporting Act*" de 1970 (em que havia uma limitação do própósito para o qual os relatórios de crédito poderiam ser usados); "*Driver Privacy Protection Act*" de 1994; "*Cable Communications Policy Act*" de 1984 (em que há a disposição de destruir os dados pessoais que não sejam mais necessários para o propósito que foram recolhidos); "*Video Privacy Protection Act*" de 1988; "*Health Insurance Portability and Accountability Act*" (em que há a disposição para o uso restrito de dados médicos).[425]

Mais recentemente, com a lei 12.414/2011, em seu art. 7º, é estabelecido expressamente o princípio de que as informações só podem ser utilizadas para os fins que foram recolhidas. Além do mais, o art. 9º não permite o compartilhamento de informações de adimplemento sem uma autorização expressa do cadastrado "*por meio de assinatura em instrumento específico ou em cláusula apartada",* em uma ampliação do entendimento do que pode ser o consentimento do consumidor para esses fins. Nesse aspecto, a confidencialidade é relacionada com o uso: para outros usos e acessos, além dos previstos, a informação deve permanecer confidencial, sigilosa, sendo assim, não utilizável.[426]

Dessa maneira, é justo considerar que as eventuais políticas de privacidade de sites que considerarem de forma genérica a viabilidade de uso dos dados pessoais para outros fins, afrontam o art. 43 do CDC. O fim para o qual as informações serão usadas deve ser expressamente especificado. De qualquer forma, a própria disposição genérica de uso para "outros fins" não possui sentido, uma vez que se os fins não forem informados, não há como saber quais os danos de uma potencial utilização e, com isso, opor-se a essa determinação.[427]

425 Conforme a lição de SOLOVE, Daniel J.. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Vol. 154, N. 3, p. 477-560, jan./2006. Disponível em: <http://ssrn.com/abstract=667622>. Acesso em: 12 Fev. 2012, p. 518-519.

426 Lembre-se que os próprios sistemas podem ser construídos a fim de regular o uso que se fará das informações. Um exemplo pode ser o sistema perguntar ao solicitante para quais fins a informação será utilizada o que pode, dependendo da resposta, gerar avisos ou, até mesmo, não revelar a informação.

427 Segundo Danilo Doneda, em função do princípio da finalidade de recolhimento de dados, é impossível estabelecer uma interpretação extensiva ao consentimento genérico. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 383. O autor explica que "*Nesta perspectiva, não seria possível o consentimento genérico para o*

Com a popularização de *smartphones* equipados com Global Positioning System (GPS), uma série de aplicativos contam com a utilização de dados de localização. Algumas redes sociais[428], inclusive, são fundadas no compartilhamento de dados de localização[429] do usuário. Claro que, em tais redes sociais, o usuário voluntariamente compartilha seus dados de localização para poder participar dela. No entanto, há a possibilidade de alguns serviços recolherem informações de localização do usuário sem sua ciência.[430]

Não é por que o *smpartphone* possui um dispositivo de GPS que o fornecedor dos serviços pode utilizá-lo de forma descontrolada. Dessa maneira, há um dever implícito de o fornecedor de serviços informáticos não utilizar arbitrariamente e sem autorização do usuário os dados de seus dispositivos de localização. Trata-se de um dever negativo na fase de recolhimento de informações para uso dos serviços.

No entanto, na comunidade europeia, esse dever não é implícito. O art. 4º da Diretiva 2002/58/CE, por exemplo, delineia o dever de segurança nos casos de

---

tratamento de dados pessoais, porém somente quando é especificada sua finalidade, bem como não seria cabível sua interpretação extensiva para hipóteses fora das expressamente previstas."

428 Talvez a mais famosa seja o FourSquare - *https://foursquare.com/*. Já o Google Latitude ao recolher os dados do usuário, gera estatísticas de uso, indicando quanto tempo o usuário passa em casa, quanto tempo passa no trabalho e quanto tempo usa nos deslocamentos. Ademais, indica também lugares mais frequentados. Todos os dados são apresentados ao próprio usuário que pode acompanhar seus trajetos em cada dia da semana.

429 Conforme a diretiva 2002/58/CE, em seu art 2º, alínea c, os dados de localização são caracterizados como "*quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível;*"

430 O art. 9º da Diretiva 2002/58/CE estabelece o cuidado que deve ser tomado acerca de processamento de dados de localização, aplicáveis, neste caso, aos serviços de comunicação:
Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações electrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. Os utilizadores ou assinantes devem dispor da possibilidade de retirar em qualquer momento o seu consentimento para o tratamento dos dados de localização, para além dos dados de tráfego.

serviços de comunicações eletrônicas. A diretiva adota parâmetros limitativos para o dever de segurança estipulando expressamente, acerca da segurança, que "*tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes*". É possível perceber que há a consideração do *estado da arte* das medidas de proteção existentes. Segundo a diretiva, não é possível exigir do fornecedor de serviços que ele implante medidas que sejam tecnicamente impossíveis de serem realizadas.

O mesmo artigo estipula um dever de o fornecedor também informar sobre os riscos extraordinários que estejam fora de seu âmbito de controle ou das soluções possíveis existentes. Isso significa que, mesmo que o fornecedor não consiga controlar o risco (por ser impossível tecnicamente, por exemplo), permanece um dever ampliado de informar o usuário de tal circunstância.

Têmis Limberger entende, acerca da proteção dos dados pessoais, que é necessário prevenir ou eliminar as discriminações sobre eles. Ainda, que isso seria "*uma nova leitura do princípio da igualdade, e sua intenção é a de que os dados armazenados não sirvam para prejudicar as pessoas.*"[431] Esse seja, talvez, o objetivo maior em relação ao uso de dados pessoais ou sensíveis.

A manutenção da confidencialidade de dados pessoais dos consumidores deve ocorrer tanto na sua transferência quanto no seu armazenamento. Já se falou aqui nesse trabalho sobre a questão da perda de fitas de backup, que engloba o cuidado na manutenção de confidencialidade de dados no armazenamento de informações. Nessa linha, o Tribunal de Justiça gaúcho já enfrentou situação em que uma seguradora, ao vender computador usado e sinistrado para terceiros, não efetuou a deleção dos arquivos pessoais do usuário anterior, expondo a privacidade

431 LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). Direitos Fundamentais, Informática e Comunicação: algumas aproximações. Porto Alegre: Livraria do Advogado, 2007, p. 218.

deste, numa clara demonstração de não ter cumprido com o dever de confidencialidade.[432]

Nesse âmbito, a diretiva 2002/58/CE estabelece também um dever geral de confidencialidade nas comunicações – ou seja, na transferência -, em seu art. 5º, assim dispondo:

> "*Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.1 do artigo 15. O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.*"

---

432 TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 1ª Turma Recursal Cível. Recurso Inominado n. 71001199744. Vilmar Luiz Sartori X Indiana Seguros S/A. Relator: Des. João Pedro Cavalli Júnior. Porto Alegre, 26 de Abril de 2007. Ementa: SEGURADORA. ENTREGA DE HD DO COMPUTADOR. DANO MORAL CONFIGURADO. FALTA DE DEVER DE CUIDADO AO VENDER O BEM SEM APAGAR AS INFORMAÇÕES PESSOAIS do segurado. Tendo a seguradora não diligenciado de forma correta ao efetuar a venda do HD sinistrado entregue pelo autor para o recebimento da indenização, sem apagar seus dados pessoais, expondo sua privacidade perante terceiros, faz jus à indenização extrapatrimonial. Recurso do autor parcialmente provido para majorar o valor da indenização. Recurso do réu desprovido e provido em parte o recurso do autor. Unânime.
No mesmo sentido:
TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 6ª Câmara Cível. Apelação n. 70032084923. Marcelo Saute X Madeireira Herval Ltda. Relator: Des. Léo Romi Pilau Júnior. Porto Alegre, 24 de Novembro de 2011. Ementa: APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. VENDA DE COMPUTADOR USADO PELOS AUTORES A TERCEIRO PELA LOJA RÉ CONTENDO ARQUIVOS PESSOAIS DOS APELADOS. DEVER DE INDENIZAR CONFIGURADO. QUANTUM READEQUADO. DERAM PARCIAL PROVIMENTO AO APELO. UNÂNIME.

Essa diretiva estabelece, portanto, um dever geral de confidencialidade, abrangendo, inclusive os "dados de tráfego"[433]. Esses dados de tráfego têm, entre outras funções, a de permitir a cobrança dos usuários, além de também permitem que se identifiquem quais as ligações que foram efetuadas pela pessoa, ou seja, podem ser considerados dados pessoais.

Após essa exposição, analisar-se-á, agora, os danos pela violação dos dados.

B.3 - O dano pela violação de dados

O dano pela violação de dados pessoais e sensíveis não se dá, por certo, apenas no caso de violação de bancos de dados de consumo. Sabe-se que dados pessoais e sensíveis não se encontram apenas em bancos de dados. Uma caixa de e-mail pode conter uma série de informações que revelem situações merecedoras de sigilo e confidencialidade. A doutrina entende que o e-mail deve ser tratado como correspondência, merecendo a mesma natureza jurídica correspondente, inclusive, envolvendo a inviolabilidade de sigilo estabelecida na constituição. [434]

Ao contrário do que ocorre na relação entre responsabilidade criminal e o problema de, na falta de uma legislação específica, existirem problemas de tipificação, o mesmo não ocorre com a responsabilidade civil.[435]

---

433 No art. 2º alínea b) da referida diretiva a definição de "dados de tráfego":
"*são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma;* "

434 Cf. TEIXEIRA, Tarcísio. Ibid, p. 67. "*Considerando-se que o e-mail é uma espécie de correspondência, apesar da forma eletrônica, ele teria, antes de tudo, a mesma natureza jurídica de correspondência convencional ou epistolar, cuja inviolabilidade e sigilo estão assegurados no inc. XII, no art. 5º da Constituição Federal."*

435 De acordo com Idem. Ibid, p. 149. "*À margem da discussão sobre a necessidade de se criar normas específicas para a internet ou a aplicação ou não de certos preceitos normativos, na questão da responsabilidade civil, parece não haver nenhum óbice à sua aplicação nas relações dadas na internet.*"

O maior problema, talvez seja, diante das especifidades da Internet, a dificuldade de encontrar e identificar os agentes causadores dos danos.[436] Nos casos de guarda de informações pessoais e sigilosas, é comum que ela seja realizada por provedores de serviços, seja em atividades de comércio eletrônico, redes sociais, etc.[437]

As novas tecnologias e seu uso massificado, além das próprias características da Internet, fazem com que seja ampliada[438] a violação da privacidade dos usuários. É possível afirmar que a violação da privacidade é facilitada

> "*pelas mesmas características e peculiaridades que tornam a Internet tão atraente, a tremenda facilidade de disseminação, de busca e de reprodução de informações, em tempo real, sem limitações geográficas aparentes.*"[439]

É comum que, nas relações de comércio, sejam recolhidas informações dos clientes. A situação agrava-se, no entanto, no comércio eletrônico. As razões são várias. A própria atividade de acessar o site e realizar uma compra faz com que o fornecedor necessite manter um cadastro atualizado do comprador, inclusive para

---

436 Idem. Ibid, p. 149. No mesmo sentido: MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009, p. 59: "*A aplicação destes pressupostos da responsabilidade civil à Internet oferecem sensíveis desafios, sobretudo, no que se refere à sua adequada demonstração. Ou seja, a prova de que uma conduta deu causa a determinados danos é providência que demanda a utilização de instrumental tecnológico da própria Internet, o que muitas vezes revela-se custoso, assim como dificuldade pela inexistência de registros precisos, ou cujo acesso é restringido em vista da proteção do sigilo de comunicações ou da privacidade dos envolvidos.*"

437 Evidentemente que há a possibilidade de pessoas físicas possuírem informações pessoais e sensíveis de outras pessoas, havendo a responsabilidade delas pela divulgação indevida. No entanto, este trabalho não trata destas relações.

438 Fala-se também em efeito multiplicador dos danos quando ocorridos no âmbito da Internet. Sobre isso ver LUÑO, Antonio-Henrique Pérez. *Ciberciudadani@ o ciudadani@.com*. Barcelona: Gedisa, 2004, p. 96: "*Su potencialidad em la difusión ilimitada de imágenes e informaciones la hace [a Internet] un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos como la intimidad, la imagen, la dignidad y el honor de las personas, la libertad sexual, la propiedad intelectual y industrial, el mercado y los consumidores...*"

439 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 42.

poder realizar a entrega, caso tratem-se de bens materiais. Alguns fornecedores, com base no histórico de compras, aprimoram a experiência do usuário realizando indicações mais precisas de produtos.

A ocorrência de incidentes digitais que violem as informações pessoais dos usuários[440] pode ter, via de regra, duas fontes: as causas externas (um ataque de um cracker) ou causas internas (ações culposas do próprio afetado, como por exemplo, não utilização de antivírus[441], escolha de senhas fracas[442], ou ações consideradas ilegais ou negligentes por parte do responsável pelo banco de dados).

Ao contrário do que se pode pensar, causas internas de violações de segurança são tão comuns quanto causas externas[443]. As empresas prestadoras de serviços informáticos[444] precisam manter uma série de ações de rotina em seu

---

440 Cláudia Lima Marques ressalta que "*a segurança dos dados coletados dos consumidores nas práticas – lícitas e ilícitas – do comércio eletrônico é uma das preocupações maiores de todos os autores e da OECD. Aqui há o jurista de ponderar entre os vários direitos fundamentais e liberdades constitucionais envolvidas.*" MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico)*. São Paulo: RT, 2004, p. 281.

441 Ver TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70011140902. Paulino Provin Miola x Empresa Brasileira de Telecomunicações S/A. Relator: Des. Luiz Augusto Coelho Braga. Porto Alegre, 26 de Outubro de 2005. APELAÇÃO. DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO. TELEFONIA. SERVIÇO NÃO PRESTADO. COBRANÇA. INSCRIÇÃO NO SERASA. Internet. conexão a provedor internacional. vírus. A ligação telefônica internacional para a Ilha Salomão, que ocasionou o alto valor cobrado na fatura emitida pela ré, decorreu de discagem internacional provocada por vírus instalado na máquina do autor. Quem navega na rede internacional (WEB) deve, necessariamente, utilizar um programa 'anti-vírus' para evitar tais acontecimentos. Negligência do autor. Inexistência de ato ilícito atribuível à Embratel. AÇÃO IMPROCEDENTE. APELAÇÃO IMPROVIDA.

442 Sobre isso ver LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 197. "*Além disso, a utilização de técnicas avançadas de criptografia pouco importa se o usuário comete erros, utiliza senhas fracas e compromete sua própria segurança. É por isso que as fraudes online não se limitam a explorar falhas em sistemas informáticos, mas aproveitam-se principalmente do elo mais fraco de toda a corrente de segurança: o indivíduo, sujeito a golpes de engenharia social, e mais interessado em sua conveniência cotidiana do que na segurança de suas informações.*"

443 Um recente exemplo de vazamento de dados ocorreu na Universidade do Vale do Rio dos Sinos - Unisinos, em que um funcionário da instituição enviou, por engano, um email para 800 pessoas com um arquivo contendo dados pessoais de 23.000 alunos. Esta situação qualifica-se como uma causa interna. Ver ROHR, Altieres. Universidade do RS se desculpa por vazar dados de 23 mil alunos. 26 de Janeiro de 2012. Disponível em: <http://g1.globo.com/rs/rio-grande-do-sul/noticia/2012/01/universidade-do-rs-se-desculpa-por-vazar-dados-de-23-mil-alunos.html>. Acesso em: 26 Jan. 2012.

444 Por empresa prestadora de serviço informático pode-se entender qualquer instituição que preste um serviço informático. Essa lista pode ser indefinida, passando por um banco (e seu serviço de

ambiente digital. Paul Ohm faz a referência a uma pesquisa acerca da fonte dos incidentes de segurança. Em tal pesquisa, realizada pela Universidade de Washington[445], foram analisados dados de um período de 26 anos e chegou-se a uma conclusão bastante interessante: no período de 2000 a 2006, 31% dos incidentes foram causados por hackers; 8% por causas não esclarecidas e 61% envolvendo o que o autor chama de "d*iferentes tipos de culpabilidade organizacional*". Dentre esses 61% dos casos, havia casos como divulgação acidental de registros[446], má conduta de funcionários; perda de fitas de backup, e notebooks perdidos[447].

No que se refere à situação de perda de fitas de backup, as empresas comumente realizam backups (cópias de segurança) de seus arquivos importantes. Na maior parte dos casos, esses dados são armazenados em fitas magnéticas, que são levadas para fora do espaço físico da empresa[448]. Isso é feito, pois, no caso de haver algum incidente físico na área onde ficam armazenados os servidores, é possível realizar a recuperação dos dados com a utilização das fitas magnéticas. O problema é que, se os dados não estiverem criptografados (ou cifrados) nas fitas, e

---

homebanking) até uma universidade (e seu serviço de renovação de livros pela Internet).

445 O nome da pesquisa citada pelo autor é "A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records" de Kris Erickson e Philip N. Howard. OHM, Paul, Ibid, p. 1343.

446 Ver no Brasil o caso da acidental divulgação de dados dos alunos do ENEM. Vazamento de dados de estudantes do Enem será apurado, diz Inep. G1, Brasília, 04 de Agosto de 2010. Disponível em: <http://g1.globo.com/vestibular-e-educacao/noticia/2010/08/vazamento-de-dados-de-estudantes-do-enem-sera-apurado-diz-inep.html>. Acessado em 04 de Agosto de 2010.

447 Esse é um fato bastante corriqueiro. Funcionários de empresas que realizam viagens, com frequência, perdem notebooks ou até mesmo os têm furtados em aeroportos ou hotéis. Em 2009, foi realizado um estudo pela empresa Intel, onde foi apontado o custo médio para as empresas, pela perda de notebooks . É fato notório que os dados contidos nos computadores, na maior parte dos casos, têm maior valor do que o próprio equipamento em si. Perda de notebook dá prejuízo médio de R$ 110 mil a empresas. G1, São Paulo, 27 de Abril de 2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1099646-6174,00 -PERDA+DE+NOTEBOOK+DA+PREJUIZO+MEDIO+DE+R+MIL+A+EMPRESAS.html>. Acessado em 27 de Abril de 2009.

448 Algumas empresas já realizam backups em serviços hospedados na nuvem. Nesta modalidade, contrata-se um serviço que permite à empresa enviar seus dados de backup para um local remoto. Em tais serviços, também devem ser aplicados fortes controles de criptografia para evitar que terceiros ou até a própria empresa que fornece o serviço consigam ter acesso aos dados de backup.

esta for perdida, quem a encontrar pode ter acesso aos dados ali gravados. Um exemplo aconteceu na Universidade de Harvard, em 2008, quando foi perdida uma fita de backup contendo informações pessoais de 21000 pessoas.[449]

Baseado nessa estatística, a análise das causas internas [das empresas] que permitem a ocorrência de incidentes de segurança da informação é importante. Paul Ohm faz a constatação de que:

> "*Nunca houve uma morte reportada proveniente de um ataque a uma rede ou sistema de computadores. Na verdade, apesar de afirmações ao contrário, há muitas dúvidas se um ataque irá desativar, com sucesso, uma parte significativa da internet.*"[450]

Na verdade, à época em que o artigo acima foi escrito, ainda não ocorrera o incidente envolvendo o vírus Stuxnet. Esse vírus foi projetado para atingir sistemas industriais. Especialistas constataram que foi tal vírus o responsável pelos danos físicos causados a uma usina nuclear no Irã. A empresa de segurança Symantec alertou, à época, que esse foi o primeiro vírus a causar danos físicos a equipamentos. [451]

449 PARISEAU, Beth. Harvard Law School offers clarifications on lost backup tape. IT Knowledge Exchange. 6 de Novembro de 2008. Disponível em: <http://itknowledgeexchange.techtarget.com/storage-soup/harvard-law-school-offers-clarifications-on-lost-backup-tape>. Acesso em: 21 Nov. 2011.

450 OHM, Paul. Ibid, p. 1344 e 1345.

451 O comportamento do vírus consistia na alteração do funcionamento dos programas que controlam centrífugas utilizadas para enriquecimento de urânio, fazendo com que estas funcionassem de forma anormal, inutilizando o urânio, além de causar danos físicos às centrífugasl. Este vírus, inofensivo para computadores comuns, foi concebido para ter efeito apenas em computadores que controlam sistemas industriais, como os que controlam as centrífugas nucleares. Nota-se que se há uma evolução no mercado de segurança da informação, ao mesmo tempo, há também um acompanhamento surpreendente de novas técnicas de invasão e de quebra de dispositivos digitais. Ressalta-se aqui, que mesmo que os computadores que comandavam as centrífugas nucleares não estivessem ligados à internet, foi possível introduzir o vírus no ambiente, através de um pendrive contaminado com o vírus. Um conhecido dispositivo de segurança da informação chamado Firewall, que tem a função de realizar o controle e bloqueio do tráfego de rede que entra e sai através da internet, não teve qualquer utilidade neste caso, já que o vírus chegou através de um pendrive. Para tudo ver WORM STUXNET. Symantec. Disponível em: <http://www.symantec.com/pt/br/theme.jsp?themeid=stuxnet>. Acessado em 10 de Novembro de 2011 e BROAD, J. William. MARKOFF, John. SANGER, David E.. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. The New York Times. 15 de Janeiro de 2011. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>. Acesso

Mesmo assim, tendo em vista essa constatação, é inegável que os chamados superusuários, também possuem um papel ativo na violação de dados. Essa figura[452] possui amplos poderes de administração sobre um sistema. Com esse usuário, é possível ler e apagar quaisquer arquivos do sistema, além de executar qualquer tipo de programa. Em outras palavras, esse poder pode ser definido como a capacidade de controlar ou modificar computadores ou redes[453]. Há duas formas de entender o termo superusuário: a primeira delas é pela visão do sistema. Nessa visão, o superusuário é o usuário criado dentro de um sistema que possui as permissões técnicas para a realização das ações. Outra acepção do termo está ligada a um usuário que possui conhecimentos excepcionais, acima da média, na área de tecnologia da informações. Esse usuário, também é comumente chamado de hacker.

Esse superusuário, em oposição aos usuários comuns que possuem conhecimento e poderes limitados dentro dos ambientes computacionais, tem uma série de poderes que não os limita dentro das restrições normais para os usuários comuns.[454] Na lição do autor, haveria uma certa mística sobre esse superusuário. Segundo ele, dá-se um grande foco a esse tipo de usuário, sendo que, ao contrário do que se pensa, ele desempenharia um pequeno papel nos incidentes. Não haveria evidências empíricas de que seja o superusuário utilizado em todos os incidentes de

em: 15 Jan. 2011. Sobre a questão do Firewall já alerta FILHO, Adalberto Simão. Dano ao consumidor por invasão do site ou da rede: Inaplicabilidade das Excludentes de Caso Fortuito ou Força Maior. In: FILHO, Adalberto Simão; DE LUCCA, Newton. (coord.). Direito & Internet – Aspectos Jurídicos Relevantes. Bauru: Edipro, 2000 , p. 108. "*Aqueles que se envolvem com questões de segurança na Internet desenvolvem seus esforços para evitar acessos não autorizados entre Internet e a rede interna através da criação de barreiras de proteção firewall ou assemelhados.*"

452 Chamada comumente nos sistemas de "usuário admin", "usuário administrator" ou, nos sistemas Linux/Unix, o usuário root. Cf. DE VILLIERS, Meiring. Reasonable Foreseeability in Information Security Law: A Forensic Analysis. University of New South Wales Faculty of Law Research Series, Sydney, p. 102-160, Abr. 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1158165>. Acesso em: 12 Fev. 2012, p. 152. "*"Root" is the conventional name of the super-user who has all rights in all modes on a computer system. This is usually the system administrator's account. The super-user has privileges that an ordinary user does not have, such as authority to change the ownership of files; install and run programs; change Web Server databases; add, change, or delete system files or data; and change or replace web pages."*

453 OHM, Paul. Ibid, p. 1333

454 Idem. Ibid, p. 1330

segurança da informação.[455] O chamado "*mito do superusuário*", na visão de Ohm, também é entendido como a crença de que "*os conflitos on-line não podem ser resolvidos sem encontrar uma forma de neutralizar o superusuário*".[456]

Acerca da violação de dados contidos em bancos de dados, a doutrina entende que:

> "*violada qualquer uma das regras que regem a criação, manutenção e divulgação dos bancos de dados e cadastros de dados de consumo, desconfigura-se a pretensão de exercício regular do direito e adentra-se no campo do abuso do direito e de ilicitude, dando ensejo à responsabilidade penal, administrativa e civil do organizador do banco de dados e do fornecedor responsável pela inclusão no arquivo de dados sobre o consumidor. Trata-se de responsabilidade civil objetiva e solidária que, por ser objeto de norma de ordem pública, é indisponível, não sendo possível a sua exclusão ou atenuação por instrumento contratual.*"[457]

A ideia de violação de dados também está relacionada com o direito ao esquecimento[458], especificamente quanto ao armazenamento de informações negativas. A previsão do armazenamento de informações negativas pelo prazo máximo de cinco anos, assim estabelecida no art. 43, §1º do CDC, se desrespeitada, constitui uma violação. Há a possibilidade, também, de que as empresas vendam para outras empresas, informações pessoais[459] ou sensíveis de

455 Idem. Ibid, p. 1331

456 Idem. Ibid, p. 1335

457 CARVALHO, Ana Paula Gambogi. Ibid, p. 101.

458 LIMBERGER, Têmis. O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 199. O direito ao esquecimento é um assunto bastante complexo e envolve a própria circunstância de eternização das informações nos meios digitais. Ao mesmo tempo, envolve o controle que as pessoas podem ter sobre seus dados em um ambiente que incentiva, justamente, o armazenamento descontrolado.

459 Ver a lição de CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito*

consumidores, constituindo uma verdadeira violação de privacidade. Fernanda Nunes Barbosa menciona que essa atividade:

> "*além de consistir numa efetiva violação do direito à privacidade, constituiria até mesmo enriquecimento sem causa do fornecedor, uma vez que logra este, à custa de outrem, a saber, o consumidor – que forneceu seus dados com uma finalidade específica (normalmente a compra ou contratação de algum serviço), a qual viu, posteriormente, desvirtuada -, ganhos para o qual consideramos, não concorreu de forma relevante*".[460]

De forma geral, as pessoas não desejam que suas informações pessoais ou sensíveis sejam acessadas, utilizadas ou publicadas de forma indevida, uma vez que tais informações, se mal utilizadas, podem deixar as pessoas em situações de vulnerabilidade emocional, financeira ou até mesmo afetar sua reputação.[461] Tem-se aqui, a ocorrência do dano pela violação dos direitos da personalidade. Nas situações envolvendo a violação de dados pessoais, em alguns casos, a publicação desses dados na Internet pode eternizá-los de uma forma que a tutela jurisdicional tenha pouco ou nenhum efeito na cessão da publicação e, consequentemente, do dano.[462]

- *UFPR*, Curitiba, n. 47, 2008, p. 149. "*A mercantilização dos dados pessoais acarreta a perda da importância de sua dimensão política como instância de proteção da liberdade no espaço público. Relativiza-se, com isso, também a inviolabilidade da intimidade e da vida privada também em face da intervenção do Estado, cuja ingerência se amplia à medida que cresce a exigência de medidas protetivas e preventivas nas áreas de segurança e saúde públicas.*"

460 BARBOSA, Fernanda Nunes. Ibid, p. 49

461 SOLOVE, Daniel J.. A Taxonomy of Privacy. Ibid, p. 530. Continua o autor, afirmando que "*People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life's direction. Moreover, when information is released publicly, it can be used in a host of unforeseeable ways, creating problems related to those caused by secondary use*." p. 531.

462 Cf. LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 222: "*Note-se que não há uma maneira simples de remediar os casos em que o ato ilícito se espalha de modo viral na Internet, ou seja, é veiculado em centenas de milhares de Web sites distintos e constantemente republicado por usuários quando removido, restando à vítima apenas tentar eliminar este conteúdo dos Websites mais populares e, caso possível, mover ação de responsabilidade civil contra o responsável original pela veiculação, ante a complexidade e a dificuldade de punição da pluralidade de agentes envolvidos.*"

Daniel Solove, no artigo "*A Taxonomy of Privacy*", realiza uma série de constatações sobre da ideia de privacidade que merecem análise. Segundo o autor há basicamente quatro grupos de atividades danosas em relação à privacidade: a coleta de informações; o processamento de informações; a disseminação de informações e por fim a invasão.[463]

Em relação ao processamento das informações, há subatividades que, geralmente, são coletivamente referidas simplesmente como processamento. A primeira delas é a agregação, que indica a combinação de várias partes de informações sobre uma pessoa. A segunda é a identificação que se consubstancia na ligação de informações aos indivíduos. A insegurança no processamento, portanto, envolve a falta de cuidado em proteger informações armazenadas contra vazamentos ou acessos não autorizados. Há, também, o que Solove chama de "*uso secundário*", isso é, o uso das informações coletadas para propósitos diferentes daqueles que foram consentidos pelos usuários. Tais atividades, como se vê, envolvem a forma com que os dados são usados e mantidos.[464]

Em relação à disseminação de informações, também é possível apontar subatividades. A quebra de confidencialidade é a violação da promessa de manter as informações de alguém confidenciais. A "divulgação"[465] envolve a revelação de informações sobre alguém, que tenha impacto na forma como os outros avaliam seu caráter. A "exposição" envolve a atividade de revelar informações relativas à nudez, às funções corporais, à dor, etc. O "aumento de acessibilidade" é a amplificação do acesso a uma informação. A "apropriação" envolve o uso dos dados de alguém para servir às intenções e aos interesses de terceiros. A "distorção" envolve a disseminação de informações falsas ou incorretas sobre um indivíduo.[466]

---

463 SOLOVE, Daniel J.. Ibid, p. 488.
464 Idem. Ibid, p. 490.
465 Ou revelação, do inglês "disclosure"
466 Idem. Ibid, p. 491.

Nesse contexto, Solove propõe que a atividade de coleta de informações pode ser realizada pela vigilância ou pelo interrogatório.[467] Como efeitos destacados da vigilância existem os sentimentos gerais de ansiedades e desconforto de quem sabe que está sendo vigiado. Além do mais, ela pode criar sentimentos de inibição e de auto-censura. Isso se refere aos efeitos inibitórios da vigilância. Ademais, ela serve como um controle social, aumentando o poder de normas sociais que são melhores cumpridas quando as pessoas sabem que estão sendo observadas. Na verdade, a própria vigilância pode ter um efeito dissuasório em relação ao cometimento de ilícitos.[468]

O procedimento chamado pelo autor de "interrogatório", além da figura clássica de alguém sendo interrogado em uma delegacia, aplica-se também em situações de questionamento de empregados, visando à informação no que diz respeito a doenças, como o HIV, a convicções políticas, ou até mesmo à realização de testes genéticos, por exemplo.[469] Os questionários apresentados aos usuários de sistemas ou sites são abrangidos por essa categoria.

A ideia, portanto, de um conceito plural de privacidade engloba o fato de que a violação e a consequente produção de danos, também podem ocorrer por várias formas. Daniel Solove diz que o que é chamado de violação de privacidade consiste em um grupo de possíveis danos, sendo que o entendimento do que é privacidade é fragmentado e inconsistente, inclusive pelo fato de algumas formas de violação não serem socialmente indesejáveis ou vistas como algo proibido.[470]

Marcel Leonardi realiza uma crítica acerca da taxonomia proposta por Solove. Embora ele a considere útil por apontar e identificar as situações mais comuns de violação à privacidade, a teoria de Solove não aborda um tema central da proteção da privacidade em nosso sistema jurídico, que é a proteção da dignidade da pessoa

467 Idem. Ibid, p. 491.
468 Idem. Ibid, p. 493.
469 Idem. Ibid, p. 502.
470 Idem. Ibid, p. 559.

humana.[471] Nesse sentido a privacidade pode ser valorada através de alguns elementos: a) promoção do bem-estar; b) criação de espaços para relações de intimidade; c) livre desenvolvimento da personalidade e d) manutenção do Estado democrático de direito.[472]

Por óbvio, o responsável por manter dados pessoais confidenciais ou sigilosos, assim recebidos, coletados, armazenados ou transferidos em uma relação de consumo, deve preservar esse atributo das informações. Se não as mantiver confidenciais ou permitir, por meio da violação do dever de confidencialidade, que um terceiro tenha acesso a tais informações, o responsável por esses dados causará um dano e deverá indenizar os atingidos.[473] Esse dano pode ser puramente moral, pela violação da privacidade e atingimento dos aspectos relativos à personalidade, como pode ser patrimonial, em situações que envolvem a descoberta de números de cartão de crédito, ou o uso indevido de uma conta bancária via home-banking, por exemplo.[474]

Entre as possibilidades de danos baseados na violação da confidencialidade, analisar-se-ão aqueles baseados no cruzamento de dados.

---

471 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 88-89. O autor aponta o consenso doutrinário e jurisprudencial "*a respeito da necessidade de sua tutela do modo mais amplo possível, ante a caracterização da privacidade como direito de personalidade e como direito fundamental, cuja base é o princípio da dignidade da pessoa humana, consagrado pela Constituição Federal de 1988 como um dos fundamentos da República...*"

472 LEONARDI, Marcel. Ibid, p. 114-115.

473 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr-jun/2009. p. 83. O autor ainda afirma que: "*E da mesma forma, [responde] aquele que não tendo violado por ato próprio o dever de sigilo, permite que o façam terceiros, conduta em razão da qual resulta lesado o direito do titular das informações, assim como de todos aqueles que tinham interesses legítimos na manutenção da legislação nestas condições.*"

474 Cf. PODESTÁ, Fábio Henrique. Direito à intimidade em ambiente da Internet. In: FILHO, Adalberto Simão; DE LUCCA, Newton. (coord.). Direito & Internet – Aspectos Jurídicos Relevantes. Bauru: Edipro, 2000, p. 163. "*Destas observações, denota-se que em tema de violação da intimidade, o campo fértil para sua ocorrência verifica-se normalmente na obtenção por hackers das senhas pessoais, o que possibilita o acesso a uma gama considerável de informações íntimas do usuário, e notadamente na descoberta dos números de cartões de crédito quando é realizado o comércio eletrônico...*"

B.3.1) A violação da confidencialidade pelo cruzamento de dados

É possível afirmar que a massificação do uso da informática, no que se refere ao tratamento de dados pessoais, possui dois efeitos: o primeiro, que permite o processamento de muitos dados em um curto espaço de tempo, e o segundo, que envolve a aplicação de novas técnicas para a obtenção de "*resultados mais valiosos*".

Conforme já exposto, na sociedade da informação, nota-se um implemento do recolhimento de dados pessoais de consumidores seja por meio de formulários, seja mediante a formação de perfis pelo uso de emails, pela realização de pesquisas em *search engines* ou até mesmo pela simples navegação em um site[475]. As ferramentas tecnológicas, por intermédio do cruzamento de dados[476], permitem facilmente a formação de grandes perfis – em alguns casos até perfis psicológicos -, apenas pela análise de dados básicos (dados de cartões de crédito, dados de compras em supermercado[477], etc).[478] Tais perfis podem ser vistos como produtos de

475 Como se sabe "*Os meios de comunicação interativos modificam a capacidade de coleta de dados, instituindo uma comunicação eletrônica contínua e direta entre os gestores dos novos serviços e os usuários. Portanto, é possível não só um controle do comportamento dos usuários, mas também um conhecimento mais estreito de seus costumes, inclinações, interesses e gostos. Disso deriva a possibilidade de toda uma série de empregos secundário dos dados recolhidos*". LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações.* Porto Alegre: Livraria do Advogado, 2007, p. 215.

476 Segundo CARVALHO, Ana Paula Gambogi. Ibid, p. 89, entre os fins de composição que os bancos de dados têm sido utilizados "*vão desde o mero arquivamento de informações simples, como o nome e o endereço do usuário, para facilitar a sua identificação nas relações com fornecedores de bens e serviços, até a combinação de dados mais complexos para se traçar um perfil detalhado do usuário, de seus hábitos, gostos e preferências.*"

477 Ver a lição de PAREDES, Marcos. Violação da privacidade na Internet. *Revista de Direito Privado*, São Paulo, n. 9, jan.-mar./2002, p. 187. "*É comum verificar-se no comércio brasileiro, supermercados que oferecem cartões personalizados aos clientes habituais, prometendo-lhes descontos e brindes surpresa pela utilização dos mesmos. Para adquiri-los, basta que o consumidor preencha um cadastro com seus dados pessoais, e em seguida receberá um cartão magnético para ser utilizado em todas as suas compras. Por meio de práticas como essas, as empresas têm registrado em seus bancos de dados, informações de caráter pessoal dos consumidores, seus hábitos e preferências de consumo, cuja análise traduzem características da personalidade capazes de traçar inclusive o perfil psicológico de seus clientes.*"

478 Ver RIBEIRO, Luciana Antonini. Ibid, p. 154: "*De forma sintética, poder-se-ia afirmar que a proteção da privacidade na Internet vê-se questionada em razão de duas problemáticas fundamentais. De um lado, verifica-se um incremento na coleta dos dados pessoais, em especial*

uma decomposição ou transferência das características pessoais para a criação de perfis digitais ou artificiais (em oposição ao natural)[479].

Cesar Santolim ensina que, em face do cruzamento, as informações podem ser submetidas a um tratamento estático ou dinâmico.[480] Acerca disso, o autor ressalta o seguinte:

> "*sempre que as informações obtidas forem objeto de cruzamento, cotejo ou integração com outras informações, sobre o mesmo consumidor, através de um processo dinâmico de manipulação de dados que é característico dos sistemas informatizados, pode-se estar diante de violações de privacidade, tuteláveis na forma da proteção dos direitos da personalidade. Isso pode acontecer tanto diante do tratamento de informações prestadas conscientemente pelo usuário/consumidor quanto (o que é mais provável) na combinação destes dados e de outros, obtidos sem o seu conhecimento, como quando da utilização de cookies, por exemplo.*"[481]

---

dos consumidores, colhidos através de inúmeros formulários apresentados na rede como condicionantes ao exercício de certos benefícios concedidos por intermédio de rede. […] De outro lado, verifica-se a criação de mecanismos capazes de vigiar os passos do consumidor enquanto navegador da rede de computadores, possibilitando-se seja traçado seu exato perfil, registrando-se cada um de seus movimentos. São os chamados cookies." Ainda sobre as técnicas gerais de recolhimento e processamento de informações ver a obra jornalística de BAKER, Stephen. *Numerati*. São Paulo: Saraiva, 2009.

479 Neste sentido, já em 1978, quando nem existia a ideia de *data mining* ou da formação de perfis digitais, ver a valiosa lição de FROSINI, Vittorio. Ibid, p. 169, que assim já previa: "*Si consideramos la imagen colective del hombre contemporáneo, situado entre las máquinas que constituyen ahora su condición de vida, o por lo menos de supervivencia, se nos aparece, em realidad, como una intrincada envoltura, como una simbiosis entre elementos naturales y elementos tecnológicos em los que la fisionomía, la voz, los miembros del hombre llegan a ser reproducidos, registrados, sustituidos, duplicados, multiplicados, separados de la persona humana, a la cual antes pertenecían de manera inalienable. Este proceso de descomposición y de transferencia se perfila ahora para las formas de su actividad intelectual: la máquina podrá calcular, razonar, proyectar por el hombre y también em el puesto del hombre.*"

480 SANTOLIM, Cesar Viterbo Matos. Ibid, p 72.

481 Idem. Ibid, p 72.

Uma das modalidades mais interessantes de cruzamento de dados é a chamada "*data mining*". Segundo Danilo Doneda:

> *"Ela consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informações em estado bruto e não classificada, podem ser identificadas informações de potencial interesse.*"[482]

Observa-se que o CDC considera como consumidor aquele que tem seus dados armazenados em banco de dados. Naturalmente, a regra dos consumidores equiparados (conforme o parágrafo único do art. 2 º do CDC) também se aplica à questão dos bancos de dados, abrangendo "*a coletividade que haja intervindo nas relações de consumo [...], qualquer vítima de um acidente de consumo (art. 17 do CDC), bem como quaisquer pessoas, determináveis ou não, expostas às práticas previstas nos Capítulos V e VI do CDC, dentre as quais estão abrangidas a coleta, manutenção e divulgação de dados sobre o consumidor (art. 29 do CDC)*."[483]

A falha no dever de cuidado, tanto na abertura e manutenção de cadastros e bancos de dados, assim definida no Código de Defesa do Consumidor, além de violar a própria confidencialidade desses dados é considerada fato do serviço de consumo.[484]

Se há a necessidade de autorização para o recolhimento de informações pessoais dos usuários, o problema aparece quando elas são "descobertas" pelo

482 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 176. Se se concebe a ideia de que informação é poder, quem conseguir organizar e, consequentemente, produzir mais informação com base em informações parciais ou dispersas, deterá mais poder. Sobre a questão da informação e poder, ver LUÑO, Antonio-Henrique Pérez. Ibid, p. 95.

483 CARVALHO, Ana Paula Gambogi. Ibid, p. 89.

484 BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno. Ibid. 2ª ed. São Paulo: RT, 2006, p. 612.

cruzamento de informações não consideradas pessoais ou sensíveis. Pode-se dizer que tais informações primárias[485] fornecidas pelos usuários, não caracterizadas como sensíveis ou pessoais, encontram-se isentas de autorização para serem recolhidas. No entanto quando o fornecedor de serviços cruza e processa tais informações e descobre, por meio desse processo, novas informações acerca do uso - essas sim sensíveis ou pessoais -, surgem informações novas, secundárias.[486] Com isso, afirma-se que "*nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para os quais é utilizada...*"[487].

Em tais situações, defende-se que é necessária uma autorização prévia para a combinação e processamento de dados não sensíveis. Nesses casos, o fornecedor de serviços deve informar quais os tipos de informações podem ser extraídas após a combinação e o processamento das informações primárias. Por exemplo: se mediante o processamento de informações de uso de cartão de crédito é possível identificar preferências sobre produtos, marcas, estilos, etc, a possibilidade de descoberta deve ser amplamente informada aos usuários. Caso esse consentimento não seja fornecido, o mero tratamento e cruzamento com a obtenção de novos dados, viola a privacidade do usuário. Se não houver consentimento, não deve haver o cruzamento.

---

485 Não confundir aqui o termo "primário", utilizado aqui como informação não pessoal, com o conceito de "primariedade" assim disposto no art. 4º, inc. IX da lei 12.527/2001.

486 Danilo Doneda chama estas informações de "informação de base" e "informação de resultado". Cf. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar. 2006, p. 181. *"Podemos identificar a existência de "uma informação de base", proveniente diretamente de uma pessoa, e uma "informação-resultado", obtida pela aplicação de um certo método de tratamento à informação de base, de forma a gerar alguma utilidade para aquele que realiza o tratamento. Este "método" pode ser uma operação de análise estatística da informação, como pode também abranger sofisticados meios de obtenção de informações a partir de dados brutos como o data mining. Porém o elemento essencial é a diferença entre uma informação e outra – também chamada de secundarização da informação. Os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade, prepostos nem sempre autorizados e capazes, e é justamente isto que produz como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade."*

487 RODOTÀ, Stefano. Ibid, p. 77.

A análise de dados comportamentais[488], provenientes de redes sociais, por exemplo, frequentemente sugerem comunidades ou perfis a serem seguidos, bem como possíveis amigos, baseados nos mesmos perfis de uso. A mesma situação ocorre em sites de comércio eletrônico – como a Amazon – em que são feitas recomendações baseadas no "*browser history*", ou seja, nos itens verificados pelo usuário na loja. Ora, não é difícil imaginar que seja possível descobrir, diante de uma grande massa de dados, a orientação sexual ou religiosa de uma pessoa, com base nos dados de comunidades, amigos e comentários.[489]

Mesmo que a lei brasileira não mencione a questão específica do cruzamento de dados, há o risco evidente à privacidade quando são centralizadas muitas informações dos usuários em um único banco de dados. Ana Paula Gambogi Carvalho afirma que

> "*o cruzamento de várias informações, gerando condições para manipulação automatizada de grandes quantidades de dados sobre o indivíduo, torna possível o conhecimento de detalhes mínimos da vida do indivíduo, ameaçando não só a sua privacidade, como também o seu direito à liberdade.*"[490]

488 Um outro exemplo sobre a análise de dados comportamentais ocorre nos sites que prometem encontrar o "par ideal" de alguém. Um destes sites é o eHarmony. Ian Ayres fala sobre esse site bem como o seu modo de funcionamento: "*Neil Clark Warren, eHarmony's founder and driving force, studied more than 5,000 married people in the late 1990s. Warren patented a predictive statistical model of compatibility based on twenty-nine different variables related to a person's emotional temperament, social style, cognitive mode, and relationship skills.*" AYRES, Ian. Ibid, p. 23.

489 Embora seja negado pelas administradoras de cartão de crédito, a imprensa já noticiou o fato de que, por meio da análise de histórico, padrões e tendências de gastos, é possível saber com uma antecedência considerável se alguém irá se divorciar. As administradoras de cartão de crédito não têm interesse em saber quem irá se divorciar, porém quem se divorcia tem suas finanças geralmente prejudicadas e isso pode afetar o perfil de crédito do consumidor. Sobre isso ver CIARELLI, Nicholas. How Visa Predicts Divorce. The Daily Beast. 6 de Abril de 2010. Disponível em: <http://www.thedailybeast.com/articles/2010/04/06/how-mastercard-predicts-divorce.html>. Acesso em: 12 Fev. 2012.

490 CARVALHO, Ana Paula Gambogi. Ibid, p. 110.

A agregação de dados não é tarefa nova. Porém, há uma ampliação de sua eficiência com as novas tecnologias em função do baixo custo de implementação e do alto poder de processamento atual.

A questão da agregação de dados e sua descoberta pelo cruzamento são muito bem explicadas pela chamada Teoria do Mosaico. Conforme Luciano Soares Maia, a referida teoria foi "*proposta por Fulgêncio Madrid Conesa, justamente em virtude da insuficiência da teoria das esferas*[491] *para fazer frente a formas novas e sofisticadas de ataque à privacidade, como a criação ilegítima de bancos de dados...*"[492] A teoria citada prega que, mesmo os dados aparentemente irrelevantes, se combinados com outras informações, podem revelar detalhes sobre a personalidade de uma pessoa. A alegoria do mosaico é utilizada pois esses dados são vistos como pedras de um mosaico: se olhadas unitariamente não significam nada; porém, se juntadas, formam a imagem de um mosaico.[493] De uma forma geral, a agregação de dados diminui a expectativa de privacidade que os consumidores possuem sobre seus dados.

Não se defende aqui que não é possível o tratamento e processamento de dados pessoais. Ele pode ocorrer, sim, para a composição de históricos e formação de dados estatísticos, no entanto, devem ser aplicadas medidas que impeçam "*a utilização de dados em apoio de medidas ou decisões tomadas em desfavor de uma pessoa.*"[494] Presume-se, nesse caso, que a utilização dos dados seja empregada

491 Sobre a teoria alemã das três esferas, Marcel Leonardi explica que há a esfera mais interior, íntima, inviolável, protegida de forma absoluta; a espera privada ampliada, que é privada mas não pertence à esfera anterior e a esfera social, que inclui aquilo que não pertença às outras. No entanto, o autor destaca também estar tal teoria ultrapassada, principalmente pela forma rudimentar com que "*os diferentes graus de intensidade aos quais, sob diferentes condições, a proteção de direitos fundamentais está submetida.*" LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 58.

492 MAIA, Luciano Soares. *A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais*. Disponível em: <http://www.conpedi.org.br/manaus/arquivos/anais/bh/luciano_soares_maia.pdf>. Acesso em: 12 Fev. 2012, p.5. No mesmo sentido LEONARDI, Marcel. Ibid, p. 73 e também MIGUEL, Carlos Ruiz. En torno a la protección de los datos personales automatizados. *Revista de Estudios Políticos Nueva Epoca*, Madrid, n. 84, Abr.-Jun./1994, p. 241.

493 MAIA, Luciano Soares. Ibid, p. 6.

494 Cf. O disposto no art. 29 da Diretiva 95/46/CE. UNIÃO EUROPÉIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho da Europa. Para este fim, podem ser usadas medidas de

para a implementação de medidas que promovam apenas a melhoria dos serviços pelos fornecedores. É nesse contexto que se entende ser possível o processamento e cruzamento de dados pessoais.

Ao mesmo tempo, os critérios utilizados para o tratamento cruzado de tais informações devem ser expostos aos usuários como cumprimento do dever de informar e também em respeito à própria transparência e harmonia (art. 4º do CDC) das relações de consumo.[495]

---

desidentificação ou anonimização dos dados.

495 A lei 12.414/2011 no seu art. 5º, traz como direitos do cadastrado, em seu inc. IV "*conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;*" Ver também um julgado do Tribunal de Justiça tratando sobre este assunto:
TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70038911400. Carla de Deus Vieira Silveira X Câmara de Dirigentes Lojistas de Porto Alegre e Companhia Zaffari Comércio e Indústria. Relator: Des. Jorge Luiz Lopes do Canto . Porto Alegre, 26 de Janeiro de 2011. Ementa: PELAÇÕES CÍVEIS. AÇÃO DE NULIDADE DE REGISTRO CUMULADA COM PEDIDO DE INDENIZAÇÃO POR DANOS MORAIS. SPC CREDISTORE. PRINCÍPIO DA TRANSPARÊNCIA. DEVER DE BOA-FÉ. FALHA NO DEVER DE INFORMAR. ABUSO DE DIREITO. DANOS MORAIS. PRELIMINAR AFASTADA. [...] 4.O SPC Credistore se trata de um verdadeiro cadastro para obtenção de crédito, utilizado para negar este aos consumidores por vias transversas, aplicável ao caso em tela o disposto na Súmula n. 359 do STJ. Mérito dos recursos em exame 5.A demandada CDL criou um verdadeiro cadastro de consumidores, denominado "SPC Creditore" em que são armazenadas informações relativas a estes, lastreadas em critérios obscuros e não divulgados nem mesmo à própria empresa contratante, mas utilizado como instrumento na avaliação para concessão do crédito. Portanto, se sujeita as regras dispostas no Capítulo V, Seção VI, do CDC, relativo aos bancos de dados e cadastros. 6.Trata-se de verdadeira ofensa ao princípio da transparência, o qual regula todas as práticas abrigadas pelo Código de Defesa do Consumidor, pois o fornecedor é obrigado a esclarecer e divulgar todos os parâmetros que regem a análise de risco feita, o que inocorreu no caso em exame. 6.Em se tratando de relações jurídicas de consumo afetas ao campo do direito empresarial, por óbvio que não se cria um cadastro para benemerência dos associados ou dos consumidores, mas sim para aferir as condições e viabilidade dos negócios entabulados entre estes, de sorte a minimizar os riscos e aumentar os ganhos. Assim, a inscrição de consumidor no referido cadastros destina-se a indicar a probabilidade de inadimplemento e como tal restrição ao crédito, sem que haja na hipótese do novo cadastro criado direito de o consumidor aferir e contraditar a avaliação feita. 7.O consumidor não pode ficar sujeito ao alvedrio do órgão de restrição de crédito na escolha das informações que prestará a respeito deste, a míngua de critérios preestabelecidos e transparentes ao público em geral, em verdadeiro abuso de direito. Isso porque tal prerrogativa foi exercitada de maneira desconforme com a legislação civil e o microssistema o Código de Defesa do Consumidor 8. No que tange à prova do dano moral, por se tratar de lesão imaterial, desnecessária a demonstração do prejuízo, na medida em que possui natureza compensatória, minimizando de forma indireta as conseqüências da conduta da ré, decorrendo aquele do próprio fato. Conduta ilícita da demandada que faz presumir os prejuízos alegados pela parte autora, é o denominado dano moral puro. 9. A demandada Zaffari recusou crédito ao consumidor sem esclarecer o motivo concreto da negativa, apenas divagando sobre os critérios de análise do crédito, o que impossibilita o consumidor de se contestar os critérios e contra-argumentar para liberar a concessão do crédito. 10. Destarte, os critérios utilizados são obscuros, sendo que o único dado objetivo utilizado, o credit score, o qual também é desconhecido do consumidor a forma e dados levados em conta para tanto, o que contraria o

Em relação ao cruzamento de dados, ainda há a possibilidade de ser realizado mediante a utilização de bancos de dados de mais de um fornecedor. Em geral, essa situação possui uma difícil apuração de responsabilidade, uma vez que pode não ser possível afirmar se a referida informação é advinda de um ou de outro fornecedor. Bruno Miragem pondera que, pelas próprias características da Internet, há realmente a possibilidade de dificuldade na apuração. Ao falar sobre a responsabilidade solidária nas relações de consumo (assim baseada no art. 18 do CDC), afirma a possibilidade de utilização da teoria da causalidade alternativa, nas situações de difícil apuração da conduta determinante. Em suas palavras "*Estendem-se, pois, as causas possíveis aos vários membros do grupo, que a partir disso, só poderão se desonerar da responsabilidade se afastarem expressamente o nexo causal.*"[496]

De qualquer forma, acerca da prova de nexo causal, Cavalieri Filho ressalta que "*não se exige da vítima uma prova robusta e definitiva*". Segundo ele, basta a chamada "*prova de primeira aparência*", que é uma alegação baseada na verossimilhança assim "*decorrente das regras da experiência comum, que permita um juízo de probabilidade...*".[497] Cabe sim, ao fornecedor, a prova de que não existe o nexo.

C) Excludentes de responsabilidade na proteção de dados

---

direito de informação consagrado na lei consumerista, ou seja, o direito de contratar depende da livre manifestação das partes. Contudo, a recusa se deu por razão que não corresponde à realidade e nem encontra qualquer parâmetro conhecido para importar em justificativa jurídica, o que importa em abusividade por parte da demandada, conduta lesiva que leva ao dever de reparar o dano imaterial ocasionado. Afastada a preliminar suscitada, à unanimidade e, no mérito, negado provimento aos recursos, por maioria, vencido o Revisor.

496 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor,* São Paulo, n. 70, abr.-jun./2009, p. 87-88.

497 Por tudo ver FILHO, Sérgio Cavalieri. O direito do consumidor no limiar do século XXI. Revista de direito do consumidor, São Paulo, n. 35, jul.-set./2000, p. 106.

Embora a regra, nas relações de consumo, seja a responsabilidade objetiva dos fornecedores, Adalberto Simão Filho destaca que *"nem sempre será efetiva a responsabilidade do fornecedor".*[498] O autor sustenta tal informação, pois os próprios consumidores podem agir de má-fé, fazendo com que seja afastada a responsabilidade dos fornecedores. Ademais, mesmo que não estipulado de forma expressa no CDC, é reconhecida pela doutrina a possibilidade da aplicação das excludentes de caso fortuito e força maior nas relações de consumo.[499]

Sobre a questão da exclusão de responsabilidade, é possível considerar que ela deve ser encarada sob dois aspectos dependendo da relação entabulada entre as partes. A isenção genérica de responsabilidade não foi incluída no Novo Código Civil, pois:

> "*interpretação teleológica e mesmo sistemática, não mais se admite a inclusão de qualquer cláusula genérica de isenção de responsabilidade, tornando o vício um instituto de interesse social, inclusive se o não-cumprimento se der por ato de preposto o funcionário (art. 932, III, do CC*)"[500].

No entanto, o mesmo autor adverte acerca da possibilidade de cláusula de isenção de responsabilidade em casos de problemas específicos "*devidamente informado ao adquirente*". Trata-se, portanto, da informação sobre um vício conhecido.

---

498 FILHO, Adalberto Simão. Ibid, p. 111.

499 BINICHESKI, Paulo Roberto. *Responsabilidade civil dos provedores de Internet: direito comparado e perspectivas de regulamentação no direito brasileiro*. Curitiba: Juruá, 2011, p. 202. "*Também impõe desde logo afirmar que o CDC, a par de não prever o caso fortuito e a força maior como excludentes da responsabilidade civil, mas também não as excluiu, com apoio de significativa parcela da doutrina nacional, sob o enfoque de que a excludente em causa é ínsita ao sistema jurídico.*"
As razões assim expostas nos arts. 12, §3º e 14, §3º têm como fundamento a inexistência do nexo causal, cf. CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8ª Ed. São Paulo: Atlas, 2009, p. 486.

500 GUIMARÃES, Paulo Jorge Scartezzini. Vícios do produto e do serviço por qualidade, quantidade e e insegurança: cumprimento imperfeito do contrato. São Paulo: RT, 2004, p. 354.

Há que se observar, por sua vez, que nas relações consumeristas, o próprio art. 24 do CDC alerta sobre a vedação da exoneração contratual do fornecedor em caso de ignorância sobre os vícios de qualidade por inadequação. Mas, o mesmo código, em seu artigo 51, inc. I, permite a limitação de indenização em casos de consumidores pessoas jurídicas, em situações justificáveis. Nesse contexto, em razão de o consumidor ser uma pessoa jurídica, haveria maior equilíbrio entre a relação, justificando-se a regra citada, observando-se ainda o caso concreto e a real condição da empresa consumidora em questão.[501]

Embora as excludentes de responsabilidade apresentadas influam diretamente no nexo causal, não se pode perder de vista a consideração do art. 47 do CDC que:

> "*instituiu como princípio geral a interpretação pró-consumidor das cláusulas contratuais. Relembre-se, porém, que o art. 47 é iluminado pelo princípio da boa-fé, positivado no art. 4º, III do CDC, e a interpretação de todo o contrato de consumo deve (e será sempre) conforme as imposições da boa-fé objetiva e do mandamento constitucional de promoção dos interesses dos consumidores.*"[502]

C.1 - Culpa exclusiva do usuário e acesso não autorizado

501 Idem. Ibid. Observar também a ressalva feita por Paula Forgioni no que diz respeito às diferenças de ambos os sistemas.

502 MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 903. Continua a autora dizendo que "*a interpretação pró consumidor é uma regra geral do sistema de direito brasileiro (direito privado e público), que no microssistema do CDC consubstancia-se através da norma do art. 47, mas nela não se exaure.*" p. 907. Mais adiante, ainda aponta que "*O direito opta por proteger o consumidor como parte contratual mais débil, a proteger suas expectativas legítimas, nascidas da confiança no vínculo contratual e na proteção do direito.*"

Em situações envolvendo a culpa exclusiva do usuário, é necessário que sua culpa seja determinante para a produção do resultado. Conforme José de Aguiar Dias "*se embora culposo, o fato de determinado agente era inócuo para a produção do dano, não pode ele, decerto, arcar com prejuízo nenhum.*"[503] A doutrina menciona também que, em tais casos, há a necessidade de que o comportamento do consumidor seja a "*única causa do acidente de consumo.*"[504]

Ao destacar o fato de que a insegurança é um problema bastante sério, Lorenzetti expõe a ponderação na consideração do dever de segurança e até estabelece uma visão econômica da questão:

> "*Este dever de segurança, expressado de forma genérica, poderia levar a uma impossibilidade de prestar os serviços, porque o ofertante não pode garantir um ambiente confiável e seguro, por exemplo quando atua em redes abertas. Por isso, este dever, como todos os demais, deve ser interpretado como uma conduta de cooperação (grifo nosso) exigida sobre a esfera de controle, ou seja, sobre as variáveis sobre as quais o ofertante possa agir, e não sobre as que escapam de sua possibilidade de garantir. Ainda assim, seria possível exigir que informe sobre os aspectos que poderá controlar e sobre os quais não se responsabiliza".*[505]

É essa conduta de cooperação que deve ser estabelecida entre o usuário e o fornecedor de serviços no que diz respeito à proteção de segurança[506]. Segundo Cavalieri Filho, a culpa exclusiva do consumidor ou de terceiro é "*causa de exclusão do nexo causal equiparável à força maior.*"[507]

---

503 DIAS, José de Aguiar. *Da responsabilidade Civil*. 8ª Ed. Rio de Janeiro: Forense, 1987, p. 811.

504 CAVALIERI FILHO, Sérgio. Ibid. 487. O exemplo trazido pelo autor é o consumidor que toma remédios em doses inadequadas ou fora da prescrição médica.

505 LORENZETTI, Ricardo L.. Comércio Eletrônico. São Paulo: RT, 2004, p. 313

506 A ideia de cooperação também pode ser alcançada pelas consideração das expressões "harmonia" e "equilíbrio" no art. 4º do CDC.

507 CAVALIERI FILHO, Sérgio. Programa de Responsabilidade Civil. 8ª Ed. São Paulo: Atlas, 2009,

Por mais protetivo que seja o sistema consumerista, não se afasta o fato de que o consumidor também possui deveres. Mesmo em sede de responsabilidade objetiva, o fornecedor, muitas vezes, não possui controle total sobre os aspectos de segurança do próprio usuário.[508] Da mesma forma, em função do princípio protetivo do consumidor, é necessário "*definir com precisão seu alcance conceitual, sobretudo em vista de sua interpretação restritiva*".[509] Com isso, não se pode considerar como excludente, a circunstância na qual um dano é concretizado, justamente pelo "*não atendimento de condições de segurança pelo fornecedor*".[510]

A jurisprudência já reconheceu o dever dos consumidores manterem o sigilo e o zelo no que se refere à preservação da confidencialidade de seu nome de usuário e de sua senha.[511] Nessa situação o dano só aconteceu à medida que não houve o

---

p. 486 e 487. O autor afirma ainda que "*Lamenta-se que o Código, que tão técnico foi ao falar em fato do produto e fato do serviço, tenha, aqui, falado em culpa exclusiva do consumidor ou de terceiro, em lugar de fato exclusivo dos mesmos. Em sede de responsabilidade objetiva, como a estabelecida no Código do Consumidor, tudo é resolvido no plano do nexo de causalidade, não se chegando a cuidar da culpa.*"

508 Em tais situações, permanece o dever do fornecedor de informar adequadamente sobre as variáveis que não possui controle e quais devem ser as ações a serem tomadas pelo consumidor no uso de seus serviços.

509 MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de direito do consumidor*, São Paulo, n. 70, abr.-jun./2009. p 85.

510 Idem. Ibid, p. 85.

511 TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 2ª Turma Recursal. Recurso Inominado n. 71001598341. Cátia Nascente da Cunha X Google Brasil Internet Ltda. Relator: Hilbert Maximiliano Akihito Obara. Porto Alegre, 26 de novembro de 2008. Ementa: REPARAÇÃO POR DANOS MORAIS. CRIAÇÃO DE PERFIL FALSO NO ORKUT. CONTEÚDO DEPRECIATIVO. LESÃO À HONRA E À IMAGEM DA AUTORA. NÃO EXCLUSÃO DA PÁGINA FRAUDULENTA, APESAR DAS SUCESSIVAS SOLICITAÇÕES. CONDUTA OMISSA DO RÉU. DEVER DE INDENIZAR. CULPA CONCORRENTE DA DEMANDANTE. Caso em que terceiro criou perfil falso da autora, remetendo-o aos amigos e colegas de trabalho desta. Conduta omissa do réu, que, apesar de ter sido acionado por diversas vezes, não procedeu à exclusão da conta fraudulenta. Dessa forma, permitiu que a honra e a imagem da requerente continuassem a ser atingidas dia após dia, durante meses. Uma vez constatada a sua negligência e a prática de ato ilícito, nasce o dever de indenizar. Da análise da documentação carreada aos autos depreende-se que o ex-companheiro da autora é o responsável pela criação do perfil falso. Assim, configurada a culpa concorrente da requerente, que não cumpriu com o dever de zelar pelo seu nome de usuário e senha, informando-os ao seu ex-companheiro [*grifo nosso*] ou simplesmente permitindo, através de algum descuido, que este tivesse acesso aos dados. Quantum fixado tendo em vista precedentes jurisprudenciais. DERAM PARCIAL PROVIMENTO AO RECURSO. UNÂNIME.
No mesmo sentido:
TRIBUNAL DE JUSTIÇA DE SÃO PAULO. 35ª Câmara do oitavo grupo - Seção de Direito Privado. Apelação cível n. 9059673-92.2005.8.26.0000. Naildes de Jesus dos Santos X Terra

zelo na confidencialidade das credenciais de acesso. Cláudia Lima Marques entende, sobre este assunto, que a jurisprudência brasileira deveria evoluir:

> "*no sentido de considerar estas inovações tecnológicas como práticas comerciais de risco opcional do fornecedor para vender mais, assumindo o risco típico desse tipo de negócio com cartões e a distância (daí valer a máxima cujus commodum, eijus periculum), podendo a presunção de boa-fé do consumidor ser elidida por prova do fornecedor bancário e de cartão de que este foi negligente ou agiu com culpa, não o contrário.*"[512]

Todas as medidas de segurança propostas e empregadas pelo fornecedor de serviços podem ser anuladas em função da falta de cuidado do usuário no acesso, bem como pela não manutenção da confidencialidade de suas credenciais. É dever do usuário cumprir as determinações de segurança estipuladas pelo mantenedor de serviço[513].

Ao mesmo tempo, a extensão do dever de informar sobre os riscos dos serviços encontra-se limitada pelo reconhecimento de fatos amplamente conhecidos, como os fatos notórios.[514] Se há um dever de manutenção de confidencialidade de dados por parte do fornecedor, há o dever de confidencialidade de credenciais por

---

Networks Brasil S/A Relator: Des. Artur Marques. São Paulo, 12 de Fevereiro de 2007. Ementa: PRESTAÇÃO DE SERVIÇOS - SÍTIO DE RELACIONAMENTO - ALTERAÇÃO DOS DADOS CADASTRAIS COM ACRÉSCIMO DE QUALIFICAÇÃO DESABONADORA DO USUÁRIO - PROVAS COLHIDAS NOS AUTOS SUFICIENTES PARA DESLOCAR A CULPA DO ILÍCITO PARA A PRÓPRIA USUÁRIA - RECURSO PROVIDO PARA JULGAR IMPROCEDENTE A AÇÃO. "A verdade é que, embora a responsabilidade da prestadora de serviços seja objetiva, não há como se aceitar a idéia de impor-lhe a reparação de danos causados pelo descuido da própria consumidora, principalmente porque há nos autos indícios de que sua senha já foi utilizada por terceira pessoa"

512 MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011, p. 1261.

513 Cf. BRANCO, Gerson Luiz Carlos. Ibid, p. 198. "*Havendo uma operação econômica por meio magnético, eletrônico ou pela Internet que não tenha sido efetuada pelo consumidor, mas por algum fraudador, o fornecedor responderá objetivamente pelos danos provocados ao consumidor, salvo se o fornecedor provar a culpa exclusiva do consumidor.*"

514 Cf. LORENZETTI, Ricardo Luis. Consumidores. Buenos Aires: Rubinzal y Asociados, 2003, p. 180.

parte do usuário-consumidor. Em um caso interessante[515], uma usuária - descumprindo as determinações do banco de não utilizar computadores públicos para o acesso à sua conta bancária - acessou sua conta através de um computador público. A usuária informou que após esse acesso, inclusive, outras transações indevidas também ocorreram em uma conta de outro banco (que não o banco réu e que também foi acessado através do computador público). Isso significa que, após utilizar o computador público para acessar suas contas bancárias, houve transações indevidas em duas instituições diferentes. Essa circunstância foi fundamental para a apuração da culpa exclusiva do consumidor, uma vez que as recomendações de segurança do banco eram justamente de não acessar o homebanking através de equipamentos públicos.

É sabido que os computadores públicos, utilizados por diversas pessoas em ambientes públicos, não oferecem a segurança que se espera de um computador doméstico, por exemplo. Nesse sentido, não se admitiu a responsabilização do banco. Mesmo assim a questão é controvertida. Nesse mesmo caso, houve um voto divergente, apontando que não foram tão evidentes as ressalvas de segurança dos serviços prestados pelo banco, pois elas não estariam amplamente informadas no site. As informações de segurança estavam no link “Ajuda”, não despertando a atenção e interesse dos usuários. Destaca-se que a inconformidade no voto

515 TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Sexta Turma Cível. Apelação n. 2004.01.1.014499-5. Célia Bretas Netto X BRB - Banco de Brasília S/A. Relator: Sandra de Sentis. Brasília, 09 de Maio de 2005. REPARAÇÃO DE DANOS - SAQUE INDEVIDO EM CONTA CORRENTE - FRAUDE ELETRÔNICA - Internet - NÃO OBSERVÂNCIA DAS RECOMENDAÇÕES PARA UTILIZAÇÃO DOS SERVIÇOS - CULPA EXCLUSIVA DO CONSUMIDOR - AFASTAMENTO DE DEVER DE INDENIZAR. 1. O dever de indenizar será afastado quando ocorre a culpa exclusiva da parte contrária. Impõe-se, evidentemente, a existência de liame causal entre a atuação ou omissão do banco e o resultado danoso, impondo-se também que se identifique a má prestação dos serviços. 2.Portanto, o fornecedor dos serviços não tem o dever de indenizar os danos causados se houve culpa exclusiva por parte do consumidor.
É possível ver a mesma questão do descumprimento do afastamento da responsabilidade do fornecedor, em caso de culpa exclusiva do consumidor, justamente pelo não cumprimento de recomendações de segurança em TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. 3ª Turma Recursal. Recurso Cível n. 024.06.990.953-9. Patrícia da Conceição Freitas X Mercado Livre.com Atividade de Internet Ltda. Relator: Juiz Anacleto Rodrigues. Belo Horizonte, 08 de Março de 2006. Negócio pela Internet. Fraude. Inobservância das recomendações de segurança do “site”. Risco do negócio. Culpa exclusiva da consumidora. Intermediação não caracterizada. Pedido improcedente.

divergente ocorreu pela falha no dever de informar acerca do risco e não sobre a utilização do computador público.

Em outra situação, foi reconhecido que o fornecedor de serviços na Internet não possui responsabilidade pelo fato do computador do usuário estar contaminado com um vírus, sendo dever deste último tomar as medidas acautelatórias e de segurança.[516]

De outra forma, a má-fé do consumidor no ambiente virtual é suficiente para afastar qualquer responsabilidade do fornecedor.[517] Isso pode ser visto nos casos de autofraude, em que o usuário fornece voluntariamente seus dados para crackers realizarem operações de transferência de valores, para depois alegar a insegurança do sistema. A real dificuldade, em tais situações, é o ônus da prova que, via de regra, é do fornecedor do serviço.

Por fim, há a possibilidade ainda da culpa concorrente do consumidor, conforme o entendimento de Cavalieri Filho. Mesmo se tratando de responsabilidade

---

516 TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70030254841. Telão Ltda X Mercado Livre S/A. Relator: Des. Romeu Marques Ribeiro Filho. Porto Alegre, 17 de Março de 2010. Ementa: APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO INDENIZATÓRIA POR DANOS MORAIS E MATERIAIS. NEGLIGÊNCIA DOS AUTORES CONFIGURADA. PRESSUPOSTOS DA RESPONSABILIDADE CIVIL. ATO ILÍCITO NÃO DEMONSTRADO. DANO MORAL E MATERIAL NÃO CONFIGURADOS. SENTENÇA DE IMPROCEDÊNCIA MANTIDA. É incontroversa a invasão de um vírus no computador dos requerentes, tendo um "hacker" modificado a senha de acesso dos recorrentes nos cadastros do réu. Compulsando os autos, verifica-se que o requerido não teve participação na invasão de vírus no computador dos autores, que deixaram de tomar as medidas acautelatórias e de segurança, permitindo a entrada de vírus em sua máquina. Negligência demonstrada. Não se podia esperar outra atitude da ré que não fosse o bloqueio da conta dos autores, com o intuito de evitar fraudes. A medida tomada pela requerida foi correta, não havendo como responsabilizá-la. Ausente um dos pressupostos da responsabilidade, não há falar em dever de indenizar por parte da ré. APELO DESPROVIDO. (Apelação Cível Nº 70030254841, Quinta Câmara Cível, Tribunal de Justiça do RS, Relator: Romeu Marques Ribeiro Filho, Julgado em 17/03/2010)

517 FILHO, Adalberto Simão. Ibid, p. 111-112. "*Assim, situações de má-fé exercitadas pelo consumidor em ambiente de Internet podem afastar o fornecedor da responsabilidade indenizatória. Como exemplo temos o fato do consumidor que por qualquer motivo previamente sabia de uma ação de invasão sobre determinado site, com objetivos espúrios. Mesmo assim, o consumidor se submete às operações naquele site com fins de sofrer efetivamente o dano para, após, buscar a indenização sob alegação de que um ataque hacker ou uma invasão não deve ser visto como excludente de responsabilidade.*"

objetiva[518], a culpa concorrente do consumidor teria o condão de "*atuar como minorante da responsabilidade do fornecedor*"[519]. Em tais situações, ainda é necessário o fornecedor provar que o acidente de consumo não ocorreu em função de defeito do produto ou serviço.[520] Nesses casos, a eventual situação de culpa do usuário que tenha contribuído para o acidente pode também ser vista como culpa concorrente e não exclusiva. Daí a importância do fornecedor de serviços informar sempre acerca dos riscos atinentes ao ambiente virtual.

C.2 - Risco do desenvolvimento

A teoria do risco do desenvolvimento pode ser conceituada como "*a descoberta, graças à evolução científica após a introdução de um bem de consumo no mercado, de que ele é intrinsecamente lesivo à saúde e à segurança dos consumidores*"[521]. Essa teoria abrange duas correntes: a de que o risco do

---

518 Atentar também para o Enunciado 459 da V Jornada de Direito Civil do Centro de Estudos Judiciários da Justiça Federal: "*Art. 945: A conduta da vítima pode ser fator atenuante do nexo de causalidade na responsabilidade civil objetiva.*"

519 CAVALIERI FILHO, Sérgio. Programa de Responsabilidade Civil. 8ª Ed. São Paulo: Atlas, 2009, p. 488. O autor cita o seguinte julgado do STJ:
SUPERIOR TRIBUNAL DE JUSTIÇA. 4ª Turma. REsp 287849/SP. Renato Esteves Versolatto X Big Valley Hotel Fazenda Ltda e Agência de Viagens CVC Tur Ltda. Relator:Ministro Ruy Rosado de Aguiar. Brasília, 17 de Abril de 2001. CÓDIGO DE DEFESA DO CONSUMIDOR. Responsabilidade do fornecedor. Culpa concorrente da vítima. Hotel. Piscina. Agência de viagens. Responsabilidade do hotel, que não sinaliza convenientemente a profundidade da piscina, de acesso livre aos hóspedes. Art. 14 do CDC. A culpa concorrente da vítima permite a redução da condenação imposta ao fornecedor. Art. 12, § 2º, III, do CDC. A agência de viagens responde pelo dano pessoal que decorreu do mau serviço do hotel contratado por ela para a hospedagem durante o pacote de turismo. Recursos conhecidos e providos em parte. Neste caso, o autor da ação ao usar o escorregador deu um salto em direção à piscina e veio a bater com a cabeça no piso, sofrendo danos físicos. O mau uso do equipamento, segundo a decisão, concorreu para o resultado danoso. De igual forma, a empresa concorreu também para o resultado uma vez que não informou a profundidade da lâmina de água, advertindo assim um banhista afoito do perigo.

520 Idem. Ibid, p. 488.

521 Cf. EBERLIN, Fernando Büscher von Teschenhausen. Responsabilidade dos fornecedores pelos danos decorrentes dos riscos do desenvolvimento: análise sob a ótica dos princípios da atividade econômica. *Revista de Direito do Consumidor*, São Paulo, n. 64, out.-dez./2007, p. 26.
CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8ª Ed. São Paulo: Atlas, 2009, p. 492. Este autor ressalta que "*o risco do desenvolvimento diz respeito a um defeito de concepção, que, por sua vez, dá causa a um acidente de consumo por falta de segurança.*"

desenvolvimento deve ser suportado pelo fornecedor de serviços e a de que ele não deve ser suportado.

Não se desconsidera o fato de que quando um fornecedor de serviços informáticos mantem um banco de dados em meio eletrônico, isso o obriga a manter também sistemas de segurança modernos como:

> "*firewalls, tecnologias de critpografia e assinatura digital, para proteger as informações pessoais, sensíveis ou não, armazenadas no banco de dados. Entretanto, sabe-se, que no atual estágio de desenvolvimento tecnológico, embora seja possível minimizar em muito o risco de invasão de rede, não é possível eliminá-lo por completo.*" [522]

A análise que deve ser feita, no estudo da responsabilidade pelo risco de desenvolvimento, abrange a investigação do chamado *estado da arte*[523] *da tecnologia*. Seria necessário comprovar, para o fornecedor se eximir da responsabilidade pela eventual violação de confidencialidade e do sigilo de dados, que de acordo com o *estado da arte*, ou seja, de acordo com os conhecimentos científicos existentes na época do lançamento do produto ou serviço, não seria possível prever a nocividade ou o risco.[524] Essa análise deve ser objetiva, para todo

522 CARVALHO, Ana Paula Gambogi. Ibid, p. 110.

523 CODERCH, Pablo Salvador; PUIG, Antoni Rubí. Riesgos de desarrollo y evaluación judicial del carácter científico de dictámenes periciales. *Revista para el análisis del derecho - InDret*, n. 1, 2008. Disponível em: <http://www.raco.cat/index.php/InDret/article/view/77867>. Acesso em: 10 Jan. 2012. Estes autores fazem uma interessante análise do conceito de "state of art" no common law: "*En el Common Law norteamericano, en cambio, la expresión "State of Art" es más ambigua que la anterior, pues refiere, bien al hecho de que un producto incluye todas aquellas características de seguridad que en el momento de su puesta en circulación resultan usuales en la industria o que deberían serlo (conformidad con las prácticas o buenas prácticas, customary Practice in Industry); bien al de que reúne todas aquellas que sean disponibles y más beneficiosas que costosas (viabilidad económica; Cost & Benefit Analysis) o razonablemente viables (ALARA: As Low As Reasonably Achievable); o bien, que incluye, además, todas aquellas disponibles de acuerdo con la tecnología más avanzada y con independencia de su coste (adecuación a la tecnología puntera; BAT: Best Available Technology)*." p. 5.

524 Cf. FABIAN, Christoph. Ibid, p. 151, ao falar sobre o dever de informar nestas situações: "*O dever de instrução depende também do conhecimento científico no momento da introdução do produto. O fabricante não pode informar sobre circunstâncias ainda não descobertas. Importante é o nível*

o universo científico, de acordo com a evolução técnica[525], e não pela impossibilidade subjetiva de um fornecedor em específico.[526]

Embora essa teoria tenha aplicação controvertida no direito brasileiro[527], ela deve ser considerada no caso do ambiente digital. Eberlin[528], ao comentar a obra de Lorenzetti, afirma que esse autor, ao mesmo tempo que entende que a corrente majoritária[529] é a que defende a responsabilidade do fornecedor pelos casos de risco de desenvolvimento, afirma também que não se poderia aceitar a "*responsabilidade pelos riscos do desenvolvimento, pois estes revelam consequências mediatas não previsíveis*".[530]

De acordo com Rui Stocco o risco do desenvolvimento:

> "*não pressupõe e não se identifica com o defeito de origem, ou seja, defeitos do projeto. O defeito de concepção ou do produto, como resultado desse desenvolvimento, só se revela quando há, na origem, imperfeição ou deficiência que poderia ser identificada, tendo em vista o estágio e desenvolvimento técnico e científico naquele momento de criação e fabricação*".[531]

---

de conhecimento da comunidade científica no momento da introdução do produto."

525 Conforme FONSECA, Arnoldo Medeiros da. *Caso fortuito e teoria da imprevisão*. 3ª Ed. Rio de Janeiro: Forense, 1958, p. 151 "*O que hoje é caso fortuito, amanhã deixará de sê-lo, em virtude do progresso da ciência ou da maior previdência humana*". Embora falando sobre caso fortuito, esta lição aplica-se também ao questão da responsabilidade pelo risco do desenvolvimento.

526 EBERLIN, Fernando Büscher von Teschenhausen. Ibid, p. 26-27.

527 CAVALIERI FILHO, Sérgio. Ibid, p. 178, defendendo o risco de desenvolvimento como sendo um "fortuito interno" sendo "*risco integrante da atividade do fornecedor, pelo que não exonerativo da sua responsabilidade*".

528 EBERLIN, Fernando Büscher von Teschenhausen. Ibid, p. 31.

529 Inclusive no Brasil, pelo argumento principal de que "*as hipóteses de exclusão de responsabilidade são taxativas no CDC*" além da questão da "*responsabilidade social*" do fornecedor. Idem. Ibid, p. 32.

530 LORENZETTI, Ricardo Luis. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003, p. 450. O comentário completo do autor é: "*La principal objeción que existe respecto de esta tesis es lá limitación causal: em el Derecho argentino sólo se responde por las consecuencias mediatas previsibles. En nuestro Derecho no sería admisible la responsabilidad por el riesgo de desarollo, simplesmente por es, claramente, una consecuencia mediata no previsible".*

531 STOCCO, Rui. Defesa do consumidor e responsabilidade pelo risco do desenvolvimento. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). *Doutrinas Essenciais Direito do Consumidor*.

Da mesma forma, a evolução da técnica informática pode fazer que um risco que atualmente não possa ser evitado, em um futuro próximo, possa vir a ser. Por outro lado, uma técnica de segurança da informação que hoje é eficaz, em um futuro, pode tornar-se ineficaz[532]. Esse aspecto transitório deve sempre ser observado sob pena de exigir a prática de ações impossíveis de serem implementadas. Dessa maneira, o art. 17 da Diretiva 95/46/CE, ao estabelecer o dever de segurança, ressalta que:

> "*medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.*"

Na sociedade da informação, em que o uso da tecnologia é crucial para o acesso aos mais variados serviços informáticos[533], há que se equacionar o risco com o benefício do uso de um produto ou serviço para toda a sociedade. Evidentemente, com isso, não se defende a transferência do risco para o consumidor.

Poderia ser considerada a possibilidade de eximir o fornecedor de um risco tecnológico[534], no caso de incidentes de segurança, quando a sua causa consistir em uma vulnerabilidade completamente desconhecida pela comunidade científica. Reconhece-se que o tema é delicado, uma vez que a sua consideração exacerbada pode trazer um incentivo pernicioso, que é o não estudo das vulnerabilidades de

---

São Paulo: RT, 2011. Vol. V, p. 282.

532 Um exemplo prático diz respeito à situação do tamanho das senhas. Com o avanço do poder de processamento dos computadores, senhas pequenas demais podem ser "adivinhadas", por meio de mecanismos de tentativa e erro com uma velocidade cada dia maior. Se no passado uma senha de 8 dígitos era considerada segura, atualmente, não se pode dizer o mesmo.

533 Não se perca de vista o fato de que, cada vez mais, o serviços antes prestados fisicamente, passem a ser disponibilizados de forma digital.

534 Entendendo o dever de segurança da informação como um dever geral, aplicável a qualquer relação havida no meio informático, há que considerar a extensão deste dever, em cada uma das relações (relação normal entre civis, entre comerciantes e as consumeristas).

segurança pelos fornecedores de serviços informáticos[535]. Nessa situação, o ônus pela inércia dos fornecedores seria transferido para os usuários dos serviços. Mesmo assim, Rui Stocco, ao comentar a questão do risco de desenvolvimento especificamente no CDC afirma:

> "*Portanto, o Código do Consumidor não é infenso à exclusão da responsabilidade quando há o rompimento do nexo causal, de modo a impedir a ligação entre o produtor, comerciante, prestador de serviço e outros com o resultado danoso, embora tenha consagrado o princípio da responsabilidade objetiva. O código cuidou de adotar a teoria do risco criado, mas não da teoria do risco integral […] Admitem-se, portanto, como causas excludentes, o caso fortuito, a força maior, a culpa exclusiva da vítima, o risco de desenvolvimento e, ainda, as causas especiais estabelecidas no próprio CDC, como acima apontadas. Pode-se afirmar que qualquer causa ou condição que tenha o poder de excluir o nexo de causa e efeito assume a qualidade de excludente de responsabilidade*".[536]

Por meio do mandamento do art. 10 do CDC é possível destacar o dever de manter o processo contínuo de estudo[537], acerca dos riscos, uma vez que sua redação estabelece que "o *fornecedor não poderá colocar no mercado de consumo produto ou serviço que sabe ou deveria saber apresentar alto grau de nocividade ou periculosidade à saúde ou segurança*". A expressão "deveria saber" pode ser

535 Nesse sentido, e de forma analógica, ver a aplicação do princípio da precaução à questão em HARTMANN, Ivar Alberto Martins. Ibid, p. 161: "*Assim, o mandado de precaução implica igualmente uma obrigação de pesquisa, de desenvolvimento do aparelhamento científico e certa pressa em obter informações sobre os riscos de determinadas atividades mais importantes ou estratégicas (obrigação esta não apenas do Estado mas também dos particulares...)*"

536 STOCCO, Rui. Ibid, p. 287.

537 Sobre o dever contínuo de estudo, FABIAN, Christoph. Ibid, p. 152, ensina que "*O fabricante deve prestar atenção, também, após a venda do produto, para que o produto não produza algum risco para o consumidor. Do dever de vigilância pode resultar um dever de o fabricante a) avisar ou advertir o consumidor, b) fornecer mais instruções ou c) como advertência qualificada, pedir o recolhimento do produto.*"

interpretada como o dever "*de constante estudo sobre o bem que está inserindo no mercado de consumo*".[538]

Eberlin, ao explicar a questão do princípio da precaução e o aparecimento de deveres e obrigações aplicada à indústria farmacêutica, afirma que "*o fabricante de remédios tem o dever de estudar, de forma constante, a evolução dos riscos no uso das substâncias que produz, adotando providências tão logo descubra uma determinada nocividade*"[539]. Essa orientação, embora feita no contexto da indústria farmacêutica, aplicar-se-ia perfeitamente ao ambiente digital, em face da questão do risco inerente dessa atividade. O autor também ressalva a diferença entre o risco de desenvolvimento e o fortuito interno, na medida em que este seria imprevisível[540]

Já Ivar Hartmann, ao dissertar sobre o mesmo assunto, estabelece uma diferenciação muito importante acerca da ideia de prevenção[541] e de precaução[542]. Afirma este autor que a prevenção "*visa evitar um dano ou coibir um risco que afigura-se certo ou confirmado*" sendo que ela "*impõe-se a curto prazo diante de alto grau de segurança por parte da ciência ao afirmar a possibilidade de um dano ao meio ambiente ou à saúde dos indivíduos*"[543]. Já a precaução é mais ampla e ocorre "*em termos de longo em longuíssimo prazo*" em função de uma "*possibilidade incerta de dano*". No último caso, tratam-se de riscos que a ciência não consegue compreender e nem, consequentemente, confirmar sua existência[544].

538 EBERLIN, Fernando Büscher von Teschenhausen. Ibid p. 34.

539 Idem. Ibid, p. 26.

540 Idem. Ibid, p. 29.

541 É possível ver a previsão explícita do princípio da prevenção no anteprojeto de proteção de dados pessoais, em seu art. 8º, inc. X: "*Princípio da prevenção: o dever do responsável de, para além das disposições específicas desta Lei, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais* "

542 Outro entendimento do princípio da precaução pode ser visto em COSTA, Luiz. Ibid, p. 16: "*From a legal perspective, the precautionary principle implies that in the face of situations in which there is uncertainty with regards to the existence or extent of risks, protective measures shall be taken without waiting that these risks become fully apparent.*"

543 HARTMANN, Ivar Alberto Martins. Ibid, p. 157-158.

544 Por tudo Idem. Ibid. p. 158. Nesse aspecto, em relação ao direito de proteção de dados, pode ser defendida a aplicação não apenas do princípio da prevenção mas também do princípio da precaução. Tal doutrina é importante pois propõe o afastamento de uma possível incerteza científica para postergar medidas de proteção. Ou seja, parece racional, também, a aplicação do princípio da precaução, por exemplo, no que diz respeito ao não recolhimento e tratamento indiscriminado de dados sensíveis.

Luiz Costa, em artigo na Computer Law & Security Review, também propõe uma diferenciação entre prevenção e precaução. Ele afirma que embora muito similares os dois conceitos não são equivalentes. Enquanto a prevenção consiste em ações contra uma ameaça conhecida, a precaução atua no sentido de evitar a possibilidade de ocorrência de ameaças ou perdas[545]. Este mesmo autor defende a aplicação do princípio da precaução no âmbito da proteção de dados e privacidade por meio do chamado *Privacy Impact Assessment* (PIA) que seria um tipo de análise de risco específica para a proteção da privacidade e dos dados pessoais.[546] É possível fazer um paralelo entre o PIA e os estudos de impacto ambientais.[547]

Seria necessário, através do estudo das normas técnicas pertinentes à atividade[548], realizar uma comprovação científica de que foram cumpridos os estudos referentes aos riscos, de forma a eximir o fornecedor da responsabilidade. Nesse sentido, Cláudio Luiz Bueno de Godoy cita o Decreto-lei Português n. 383/89 (art. 5º, e), que prevê a possibilidade de liberação da responsabilidade do fornecedor mediante uma prova que ateste de modo "objetivo e absoluto" que o defeito era incognoscível à época.[549]

Puig e Coderch destacam que, nas situações de risco de desenvolvimento, há uma impossibilidade científica de reconhecimento do defeito. Segundo os autores:

> "*não se leva em conta a violação deste ou daquele dever de cuidado, muito menos na impossibilidade de formular*

545 COSTA, Luiz. Ibid, p. 16.

546 Idem. Ibid, p. 18. Mais adiante, o autor afirma: *"As a risk assessment, PIAs are an instrument of anticipating threats to privacy*". p. 20.

547 Idem. Ibid, p. 24: "*As within the protection of health or environment, some goods of privacy may be considered inalienable; paying for the damage shall not be the sole response of law regarding liability.*" No mesmo sentido de reconhecer a necessidade de procedimentos de avaliação de impacto sobre a privacidade ver a lição de RODOTÀ, Stefano. Ibid, p. 20.

548 Quando diz-se normas técnicas, invoca-se principalmente, no caso da segurança da informação, a norma técnica ISO/IEC NBR 27002.

549 GODOY, Cláudio Luiz Bueno de. Responsabilidade pelo Fato do Produto e do Serviço. In: SILVA, Regina Beatriz Tavares da Silva. (coord). *Responsabilidade Civil nas Relações de Consumo*. São Paulo: Saraiva, 2009.

> *um juízo de reprovação e é também irrelevante a circunstância de que um ou, inclusive, muitos fabricantes não reconheceram o defeito se este, dado o estado da ciência e da tecnologia era de fato reconhecível (critério da cognoscibilidade do defeito)*"[550]

Embora exista o entendimento de que o risco do desenvolvimento rompe o próprio nexo causal, por sua vez, não é possível desprezar o fato de que quando um fornecedor de serviços informáticos escolhe uma determinada tecnologia, ele deve arcar com os riscos e a insegurança de suas escolhas[551]. Não é possível afastar, ao mesmo tempo, a própria questão da responsabilidade objetiva e toda a sistemática de proteção ao consumidor[552], além de sua própria vulnerabilidade técnica, sob pena de afetar a própria ideia do sistema de proteção de consumo. Nesse sentido, Cavalieri Filho defende que os riscos do desenvolvimento são caracterizados como fortuitos internos, vistos como defeito de concepção, integrando a órbita de responsabilidade do fornecedor de serviços.[553]

Mesmo assim, no difícil caso de absoluta impossibilidade científica de reconhecimento de uma vulnerabilidade técnica que comprometa a confidencialidade de dados, defende-se aqui impossibilidade de responsabilização do fornecedor de serviços em tais situações, pelo próprio afastamento do nexo causal, de acordo com Rui Stocco.

---

550 CODERCH, Pablo Salvador; PUIG, Antoni Rubí. Ibid, p. 21.

551 De acordo com LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 106, ao comentar a responsabilidade dos provedores de acesso, afirma: "*Nesse contexto, os provedores de acesso à Internet devem arcar com os riscos de falhas nos equipamentos e sistemas por eles utilizados, jamais podendo transferii-los a seus usuários.*"

552 Nesse sentido GODOY, Cláudio Luiz Bueno de. Ibid, p. 154. Inclusive, o autor cita o Enunciado 43 da I Jornada de Direito Civil , realizada pelo Centro de Estudos Judiciários do Conselho da Justiça Federal: "*a responsabilidade civil pelo fato do produto, prevista no art. 931 do novo Código Civil, também inclui os riscos do desenvolvimento.*"

553 CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8ª Ed. São Paulo: Atlas, 2009, p. 492. No Mesmo sentido VENOSA, Sílvio de Salvo. *Direito Civil: Responsabilidade Civil*. Vol. 4. São Paulo: Atlas, 2010, p. 274.

No entanto, também é possível citar a posição intermediária – e menos restritiva – proposta por Ivar Hartmann acerca da responsabilidade pelos riscos do desenvolvimento. Ele ressalta, de forma menos rigorosa, que o princípio da precaução prevê a possibilidade da responsabilidade subjetiva em situações de verificação defeitos posteriores ao lançamento do produto. A questão seria de verificar, junto ao fornecedor, que não havia uma "*dúvida razoável no meio científico e comunitário acerca das substâncias ou métodos que empregou*"[554]. A precaução, segundo esse autor, não é vista como obrigação de resultado mas sim de meio, visto que há "*diversas maneiras de gerenciar o risco*"[555]. Além do mais, na visão de Luiz Costa, a precaução deve ser vista como um valor normativo na proteção de dados e também como uma expressão do princípio do *neminem laedere*[556].

C.3 - Caso fortuito e força maior

É fato que a noção do caso fortuito está sempre ligada com a regra da impossibilidade. Essa impossibilidade pode estar relacionada com "*a impossibilidade de evitar o próprio acontecimento ou seus efeitos que tanto podem acarretar a impossibilidade da prestação, como uma dificuldade ou onerosidade maior."*[557] Igualmente, há dois elementos caracterizadores do caso fortuito: o primeiro é

554 HARTMANN, Ivar Alberto Martins. Ibid, p. 169.

555 Idem. Ibid. Este autor não defende uma aplicação desmedida do princípio da precaução. Ao contrário, ele prega que "*a proporcionalidade na aplicação da precaução requer seja sopesado inclusive outro objetivo da política nacional de defesa do consumidor, que explicita a função social da empresa: a necessidade e os benefícios que trazem para a sociedade o desenvolvimento econômico e tecnológico empreendido pelas empresas.*", p. 171.

556 COSTA, Luiz. Ibid, p. 22: "*precaution as a normative value in privacy and data protection legislation. Precaution is "an action taken to avoid a dangerous or undesirable event" or a "caution practised beforehand; circumspection" […] Precaution found its legal basis on the neminem laedere principle in a wider sense and on the prior checking rules of the Directive 95/ 46/EC63 in a strict one.*"

557 FONSECA, Arnoldo Medeiros da. *Caso fortuito e teoria da imprevisão*. 3ª Ed. Rio de Janeiro: Forense, 1958, p. 145-146.

interno, ou objetivo: que é a própria inevitabilidade;[558] já o segundo é externo, ou subjetivo: a ausência de culpa.

A ausência de culpa é primordial para a ocorrência do caso fortuito. Nenhuma das partes poderá ter contribuído, mesmo que culposamente, na situação que provocou o dano.[559] Claro que em situações de responsabilidade objetiva, como nas relações de consumo, não se investiga a culpa do fornecedor de serviços.

Já a inevitabilidade é vista em face da:

> "*realidade concreta de cada caso, encarado objetivamente em toda sua generalidade, atendidas as possibilidades humanas, mas com abstração completa da pessoa do devedor considerado e grau de diligência a que estivesse obrigado.*"[560]

O critério é, por óbvio, objetivo porém não absolutamente abstrato.[561] Sobre a questão das excludentes de caso fortuito e força maior[562], em casos de invasão, Adalberto Simão Filho relata que:

> "*teria campo nos casos em que a empresa tenha adotado a seu favor toda a melhor tecnologia mundial desenvolvida para possibilitar a necessária segurança do consumidor quando este se encontra em operações e inter-relacionamento do interior do site. Para que a invocação fosse realmente de impacto, teria a empresa que comprovadamente demonstrar toda a extensão dos aspectos de*

558 Idem. Ibid, p. 147. Nas palavras de Medeiros da Fonseca "*a impossibilidade de impedir ou resistir ao acontecimento considerado, tendo em vista as possibilidades humanas, atendidas em toda sua generalidade, sem nenhuma consideração pelas condições pessoais do indivíduo cuja responsabilidade está em causa.*"

559 Idem. Ibid, p. 147. Caso o consumidor tenha concorrido culposamente, não se falará em fortuito e, se aquela foi a causa exclusiva do dano, incida a culpa exclusiva da vítima.

560 Idem. Ibid, p. 149.

561 Idem. Ibid, p. 149.

562 Não se entra na questão de diferenciação entre o caso fortuito e a força maior uma vez que tal discussão já está superada pela doutrina. Cf. CAVALIERI FILHO, Sérgio. Programa de Responsabilidade Civil. 8ª Ed. São Paulo: Atlas, 2009, p. 65. Principalmente pois o art. 393 do Código Civil os considera como sinônimos.

> *segurança adotados para a proteção do site no que tange a eventuais invasores*."[563]

De outra forma, Ana Paula Gambogi Carvalho defende, nessas situações, que essa excludente não pode ser utilizada pelo simples fato de não preencher o requisito da imprevisibilidade.[564] Sobre isso, é importante notar a lição de Arnoldo Medeiros da Fonseca que considera apenas a inevitabilidade como requisito do caso fortuito. A imprevisibilidade ficaria afastada pela necessidade de ausência de culpa. Segundo o autor "*a inevitabilidade é o único requisito objetivo que subsiste, quer decorra da própria imprevisibilidade do evento, quer de modo irresistível pelo qual este se manifeste.*"[565]

A alegação de força maior ou caso fortuito como caso de excludente de responsabilidade, na sistemática consumerista, só pode ser feita no caso de força maior externa.[566] Em função disso:

> "*invasão do banco de dados por um terceiro não autorizado é um risco inerente à gestão de bancos de dados eletrônico, não se prestando a descaracterizar a existência de um defeito juridicamente relevante e a elidir a responsabilidade do fornecedor. Destaque-se que a doutrina dos riscos, adotada pelo Código de Defesa do Consumidor, tem como fundamento a necessidade de justiça social e a socialização dos riscos do mercado, com fins a assegurar a vítima a reparação do dano mesmo nos casos em que se torna impossível para ela comprovar a culpa do ofensor.*"[567]

---

563 FILHO, Adalberto Simão. Ibid, p. 102.
564 CARVALHO, Ana Paula Gambogi. Ibid, p. 112.
565 FONSECA, Arnoldo Medeiros da. Ibid, p. 150.
566 Embora a doutrina majoritária entenda a aplicabilidade das excludentes de caso fortuito e força maior nas relações de consumo, há vozes dissonantes. Por exemplo CASADO, Márcio Melo. Responsabilidade objetiva no Código de Defesa do Consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: Doutrinas Essenciais Direito do Consumidor. São Paulo: RT, 2011. Vol. V, p. 763-765. O mesmo autor entende também não ser aplicável no Brasil a teoria do risco do desenvolvimento.
567 CARVALHO, Ana Paula Gambogi. Ibid. 112.

Sabe-se que a atividade de fornecimento de produtos e serviços informáticos exige uma constante atualização técnica dos responsáveis, seja pela rapidez da técnica informática, seja pela própria evolução dos dispositivos e hardwares. É natural e bastante comum, em tais situações, que os defeitos (*bugs*) dos softwares só sejam descobertos após o uso maciço pelos usuários. Isso tanto é verdade que corriqueiramente há atualizações nos sistemas operacionais visando a constante correção dos referidos bugs.[568]

A questão da inevitabilidade de um risco pode ser vista também sob o ponto de vista econômico. Até que ponto é possível exigir que sejam evitados todos os riscos, de forma absoluta, de um produto ou serviço?[569] Cavalieri Filho, leciona que "*os bens de consumo sempre têm um resíduo de insegurança, que não pode merecer a atenção do legislador. O Direito só atua quando a insegurança ultrapassar o patamar da normalidade e da previsibilidade*".[570] No entanto, Adalberto Simão Filho faz a ressalva de que a força maior ou o caso fortuito não possuem a relação com a onerosidade de implantar uma determinada solução técnica.[571]

---

568 As conhecidas "atualizações automáticas" do sistema operacional Windows. DE VILLIERS, Meiring. Ibid. indica, acerca 4 tipos de correções para vulnerabilidades: (1) correção oficial – representada pela disponibilização de uma correção final e oficial pelo fabricante do software que elimina a vulnerabilidade; (2) Correção temporária – representada pelo lançamento de uma correção temporária pelo fabricante do software; (3) Workaround – representado por uma solução temporária e não oficial, ou seja, não lançada pelo fabricante, mas sim pelo grupo de usuários da comunidade técnica e ainda (4) – Indisponível – A inexistência de correção para a vulnerabilidade.

569 Conforme Eberlin ao tratar sobre a questão do risco do desenvolvimento: "*A responsabilização dos empresários pelos riscos do desenvolvimento, de forma radical e desmedida, pode elevar os custos de produção a ponto de tornar a atividade inviável, o que andaria na contramão dos princípios constitucionais da atividade econômica. A necessidade de estabelecer a interpretação jurídica adequada sobre os riscos do desenvolvimento, através da definição de regras de conduta e deveres objetivos dos empresários, se impõe em face do igualmente necessário desenvolvimento da economia.*" EBERLIN, Fernando Büscher von Teschenhausen. Ibid, p. 12. Mais adiante é destacado que não é possível atingir o risco zero, p. 26.

570 CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8ª Ed. São Paulo: Atlas, 2009, p. 174.

571 Cf. FILHO, Adalberto Simão. Ibid, p. 106. "*A verificação da força maior ou do caso fortuito não está ligada à dificuldade da prestação ou onerosidade desta, mas sim, à impossibilidade de cumprimento desta por fato de terceiro. Portanto, em questões de Internet, torna-se provável que não teria qualquer respaldo uma tese que venha objetivar a excludência de responsabilidade alicerçada nas dificuldades de obtenção de equipamentos certeiros de segurança para a proteção do consumidor em ambiente de Internet ou, ainda no fato de que eventualmente esta tecnologia seja por demais onerosa.*"

Cf. FONSECA, Arnoldo Medeiros da. Ibid, p. 155-156. "*somente quando acarreta a impossibilidade objetiva ou absoluta de executar, seja natural ou jurídica, é que o caso fortuito extingue a obrigação. A onerosidade mesmo excessiva, ou dificuldade imprevista, não bastam*

É possível perceber, com base na lição de Villiers, uma questão interessante sobre a previsibilidade de vulnerabilidades em um sistema informático. Dependendo da vulnerabilidade técnica, é possível que ela seja explorada apenas por pessoas com um alto conhecimento técnico. Já no caso de uma vulnerabilidade simples, ela pode ser explorada por pessoas com menor potencial técnico. Em outras situações, ainda, há inclusive a criação de vírus que exploram vulnerabilidades técnicas conhecidas para a sua propagação e infecção. O ponto defendido pelo autor é o de que há um grau de dificuldade na exploração de vulnerabilidades que deve ser levado em consideração. Há uma diferença, portanto, entre vulnerabilidades desconhecidas, e ainda não exploradas pela comunidade técnica, e as vulnerabilidade já conhecidas, que são exploradas, de forma automática, por um vírus. Esta seria muito mais "vulnerável" do que a primeira e, consequentemente, mais previsível para o responsável técnico da infraestrutura.[572] Além do mais, essa facilidade de explorar uma vulnerabilidade conhecida[573] permite que um número maior de pessoas maior possa explorá-la. Porém, em casos de responsabilidade objetiva, como nas relações de consumo, esta circunstância não pode ser alegada.

Imagine-se a situação em que toda a comunidade técnica utiliza um software, com padrões de construção abertos, por exemplo, para a prestação de uma atividade. Pode-se utilizar neste exemplo o caso da tecnologia utilizada na Infraestrutura de Chaves Públicas Brasileira - ICP Brasil. Nessa situação, foi escolhido o mecanismo técnico que envolve um par de chaves (pública e privada) com o emprego da criptografia assimétrica[574], devido a sua segurança e pretensa impossibilidade de violação deste mecanismo, com base nos conhecimentos técnicos até hoje existentes. Note-se que há, inclusive, a previsão legal da utilização

para isentar o devedor de responsabilidade." Mais adiante diz "*só a impossibilidade, nunca a dificuldade ou onerosidade excessiva, exonera, em regra, o devedor não se atentendo também senão à impossibilidade absoluta ou objetiva, seja permanente ou temporária, total ou parcial, natural ou jurídica*", p. 161.

572 Por toda esta explicação, ver DE VILLIERS, Meiring. Ibid, p. 144.

573 Algumas das vulnerabilidades mais conhecidas possuem inclusive softwares específicos que permitem que uma pessoa sem nenhum conhecimento técnico possa explorá-las, apenas com o uso do referido software.

574 Cf. MENKE, Fabiano. Ibid, p. 44.

de mecanismos de pares de chaves criptográficas[575]. Por meio dessa previsão, os órgãos governamentais e as empresas usam esse modelo tecnológico para a garantia de autenticidade, integridade e validade jurídica de documentos no meio digital. Uma série de atos são praticados com a utilização desta tecnologia, justamente, pela sua segurança até então garantida pela técnica,

Considere-se, apenas a título de argumentação, que se descubra uma vulnerabilidade técnica no algoritmo de geração do par de chaves criptográficas, que implique na possibilidade de que alguém consiga passar-se por outra pessoa, com a simulação ou emissão fraudulenta de um par de chaves. Isso acabaria com a segurança prevista para essa tecnologia, inviabilizando a garantia de autenticidade e integridade dos atos praticados através de seu uso.

A hipótese, mesmo que aparentemente absurda, não pode ser afastada pois a evolução da informática pode permitir isso. Em tais casos, defende-se a existência de um fortuito digital, em função da total inevitabilidade e irresistibilidade de evitar os possíveis danos daí advindos.

Na situação em que uma vulnerabilidade técnica não seja sanável pela utilização de melhores práticas de segurança, estando ela [a vulnerabilidade] dentro do próprio código fonte dos softwares utilizados para a prestação dos serviços, sendo alterável somente pelo fabricante do software, deve ser considerado, para o cumprimento do dever de segurança, o fornecimento de correções disponibilizadas pelo fabricante do software. Se não há uma solução técnica oficial, lançada pelo fabricante do software para a correção do problema, dependendo da situação, o fornecedor de serviços que utilize aquele software pode não ter ferramentas técnicas disponíveis para a solução da vulnerabilidade. É certo que por meio do regime de responsabilidade objetiva do fornecedor de serviços, ele responderá também pelo risco na escolha dos softwares usados em sua infraestrutura técnica. Mesmo

575 Cf. o art. 6º da MP 2.200-2 de 24 de Agosto de 2001.

porque, em tais situações, deve prevalecer a disciplina do art. 25, § 2º do CDC, que assim dispõe:

> *Art. 25. É vedada a estipulação contratual de cláusula que impossibilite, exonere ou atenue a obrigação de indenizar prevista nesta e nas seções anteriores.*
> *[...]*
> *§ 2° Sendo o dano causado por componente ou peça incorporada ao produto ou serviço, são responsáveis solidários seu fabricante, construtor ou importador e o que realizou a incorporação.*

Dependendo da situação técnica, o fornecedor pode tomar apenas medidas temporárias ou paliativas, que diminuam a probabilidade do risco tecnológico concretizar-se. Ainda, se não houver nenhuma correção técnica disponível, dependendo da amplitude da vulnerabilidade, o fornecedor pode não ter outra alternativa que descontinuar a prestação do serviço com o uso daquele software. Mesmo assim, ele responderá pela insegurança e eventual violação de confidencialidade que tenha origem na vulnerabilidade do software.[576] Ao mesmo tempo, dependendo da criticidade da vulnerabilidade e também das possibilidades de controle técnico pelo fornecedor do serviço, é inafastável o dever de comunicar a comunidade de usuários, através de avisos proporcionalmente visíveis à criticidade da vulnerabilidade.

Portanto, quanto à violação de dados pessoais por crackers ser considerada como caso fortuito ou de força maior, tanto a doutrina[577] quanto a jurisprudência[578] entendem de forma contrária.

---

576 Cf. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 106 e 109.

577 FILHO, Adalberto Simão. Ibid, p. 110-111. O autor chega à conclusão que a invasão de um cracker a um site, não se "*adapta à natureza jurídica específica do instituto do caso fortuito e força maior e nem tampouco à visão compartimentada desenvolvida pela doutrina sobre os elementos que compõem as excludentes."* No mesmo sentido BINICHESKI, Paulo Roberto. Ibid, p. 264.

578 Ver o julgado já citado na nota de rodapé 345.

Mesmo assim, há vozes dissonantes. Essas afirmam ser importante verificar se o fornecedor de serviços aplicou as normas de segurança técnicas atinentes ao serviço e também se cumpre o dever de informar sobre os riscos do serviço e sobre as normas de segurança a serem seguidas pelo usuário.[579] Paulo Roberto Binicheski afirma que:

> "*em acréscimo, também a ponderação de que, se por ocasião da prestação do serviço, o intermediário técnico esteja atento e utilize, dentro de suas forças, as proteções tecnológicas disponíveis, principalmente os chamados sistemas de firewall e um bem atualizado programa antivírus. Se mesmo assim o ataque ocorrer e tiver sucesso, a conclusão lógica será que o fato ocorreu por forças estranhas à sua vontade. Essa situação é muito semelhante à solução posta pela doutrina e pela jurisprudência brasileiras nos casos de assaltos ocorridos no transporte coletivo, cuja ação do agente direto do ilícito é considerada um caso fortuito externo, afastando a ocorrência do nexo causal, eis que estranha ao dever contratual da atividade.*"[580]

C.4) Fato exclusivo de terceiro

A exoneração de responsabilidade pelo fato de terceiro, só será possível "*quando realmente constitui uma causa estranha ao devedor, isto é, quando elimine totalmente a relação de causalidade entre o dano e o desempenho do contrato. A questão é essencialmente ligada ao problema do nexo causal...*"[581] Basicamente, o

579 BINICHESKI, Paulo Roberto. Ibid, p. 266.
580 Idem. Ibid, p. 266.
581 DIAS, José de Aguiar. *Da responsabilidade Civil*. 8ª Ed. Rio de Janeiro: Forense, 1987. Volume 2, p. 794.

fato de terceiro deve sustentar os pressupostos de causalidade, inimputabilidade (se não for imputado ao devedor), identidade (atribuído a alguém) e iliceidade. [582] O fato de terceiro deve ser a causa exclusiva do dano.

Em função da responsabilidade objetiva nas relações de consumo e da necessidade de inversão do ônus da prova em tais questões técnicas, o fornecedor de serviços afetado deve realizar a prova da causa exclusiva do fato de terceiro.

Essa questão é levantada pois o ataque de um cracker pode ser inicialmente entendido como fato de terceiro e, por isso, poder-se-ia presumir a irresponsabilidade do fornecedor do serviço. No entanto, há que se destacar que se o referido terceiro explore uma vulnerabilidade técnica que pudesse ser devidamente controlada pelo administrador de sistemas responsável, ou ainda, explore uma falha técnica conhecida na estrutura que não foi devidamente controlada, entende-se que fica afastado o reconhecimento do fato de terceiro. Isso pois, nessa situação, o ataque ocorreu em função de uma não correção de vulnerabilidade pelo responsável pelos sistemas.[583]

Neste sentido, Ana Paula Gambogi Carvalho entende também que não é possível afastar a responsabilidade do fornecedor de serviços, nesse caso o mantenedor do banco de dados de informações de consumo, uma vez que:

"*não se pode afirmar que o gestor do banco de dados em nada*

582 Idem. Ibid, p. 796.

583 Nestas situações, via de regra, a doutrina brasileira não entende a invasão de um cracker como sendo um fato exclusivo de terceiro e nem de força maior. Cf. CARVALHO, Ana Paula Gambogi. Ibid, p. 111. "*…lembre-se que a sistemática de responsabilidade civil do Código de Defesa do Consumidor admite como causas excludentes de responsabilidade tão-somente a culpa exclusiva da vítima ou de terceiro e a força maior ou caso fortuito, desde que alheios à atividade do agente. A invasão do servidor por um hacker não se enquadra, todavia, nem como fato de terceiro, nem como força maior, não podendo o organizador do banco de dados invocar essas excludentes de responsabilidade para se exonerar do dever de indenizar a vítima.*"
No mesmo sentido MIRAGEM, Bruno. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, São Paulo, n. 70, abr.-jun./2009. p 85. *"Não há de se tratar como excludente a hipótese em que a oportunidade para o cometimento do ilícito gerador do dano se dá em razão do não atendimento de condições de segurança pelo fornecedor."*

> *contribuiu para ocorrência do evento danoso, uma vez que foi exatamente a insegurança de seus serviços, isto é, a vulnerabilidade de seu site que criou condições para a invasão*".[584]

Em tal situação, houve a falha no dever de empregar as melhores práticas de segurança e, em função disso, a violação de dados cometida por um terceiro. A pergunta que deve ser feita é se a comunidade científica conhecia aquela vulnerabilidade técnica e, se caso ela fosse controlada, estaria eliminada a possibilidade de uma invasão por um cracker. Se a resposta for positiva, o responsável pela estrutura técnica não pode alegar o fato de terceiro.

Como é possível ver, há uma conexão entre a excludente do fato exclusivo de terceiro com a circunstância do fornecedor conseguir evitar, em face do avanço científico, a ação daquele. Nesse sentido é importante a lição de Paulo Roberto Binicheski. O autor, ao comentar sobre a responsabilidade dos fornecedores de serviços informáticos em casos de ataques de segurança baseada em técnicas de invasão até então desconhecidas pela comunidade informática, destaca:

> "*Indubitavelmente, cumpridas as obrigações do provedor, não se pode falar que seu produto ou serviço seja considerado defeituoso, se um hacker desenvolver uma técnica não prevista nas normas de segurança e conseguir burlar os sistemas de proteção, dado que as regras de experiência comum 'evidenciam que os bens de consumo sempre têm um resíduo de insegurança'. Ademais, a culpa exclusiva de terceiros - in casu a conduta do pirata virtual - afasta o nexo causal, lembrando que o CDC também contempla como excludente a ocorrência de um fato por culpa exclusiva de terceiro (art. 12, § 3º, inciso III e 14, § 3º, inciso II), cujas questões probatórias em um caso concreto poderão resolver a questão. Concluindo, temos que em caso de*

584 CARVALHO, Ana Paula Gambogi. Ibid, p. 112.

> *ataque perpetrado por um pirata cibernético, não tendo o provedor prometido contratualmente ou por informe publicitário segurança absoluta e cumpridos os deveres informativos e as diligências inerentes à atividade do serviço, o provedor de internet não será tido como responsável.* "[585]

Por sua vez se a conduta do terceiro estiver "*dentro do risco normal da atividade do fornecedor, sua responsabilidade persiste*."[586] Além do magistério de Binicheski e Godoy, é possível ver também no enunciado 448 da V Jornada de Direito Civil do Centro de Estudos Judiciários da Justiça Federal a regra específica acerca do risco normal da atividade, na interpretação do art. 927 do CC:

> *Art. 927: A regra do art. 927, parágrafo único, segunda parte, do CC aplica-se sempre que a atividade normalmente desenvolvida, mesmo sem defeito e não essencialmente perigosa, induza, por sua natureza, risco especial e diferenciado aos direitos de outrem. São critérios de avaliação desse risco, entre outros, a estatística, a prova técnica e as máximas de experiência.*

585 BINICHESKI, Paulo Roberto. Ibid, p. 267-268.
586 GODOY, Cláudio Luiz Bueno de. p. 164.

CONCLUSÕES

A falta de segurança nas relações de consumo na internet é um dos fatores que comprometem a confiança que o consumidor deposita no comércio eletrônico. A Internet, como foi visto, é repleta de riscos e, especialmente em relação à segurança da informação e à proteção da confidencialidade, os desafios são vários. A falta de informações acerca destes e, ainda, a complexidade do ambiente deixa o consumidor tecnicamente vulnerável. O dever de informar, nessas condições, deve ser ampliado.

A privacidade – assim como a determinação informativa -, vista como um direito da personalidade, possui o status de direito fundamental em nosso ordenamento. Consequentemente, a proteção de dados pessoais e sensíveis também possuem esse status. Ocorre que o conceito clássico de privacidade vem sendo alterado. A evolução da sociedade, o uso massificado das novas tecnologias, o recolhimento desenfreado de dados[587] são alguns dos fatores que contribuem para essa evolução. A vida privada foi "computadorizada",[588] e com isso surge a ideia de controle das próprias informações: a autodeterminação informativa que abrange o eixo pessoa-informação-circulação-controle. Como se viu, aquele que confia seus dados a terceiros possui a expectativa da proteção da confidencialidade.

Nesse panorama, há a importância da ciência e autorização dos atingidos para o tratamento de seus dados pessoais. O usuário pode realizar um controle sobre seus dados, seja por meio da exposição voluntária ou, até mesmo, pelo consentimento. Mesmo assim, esse consentimento deve ser claro, específico e adequado, considerando-se a proteção dos direitos fundamentais e da

587 Formando o que FROSINI, Vittorio, Ibid, p. 178 já chamava de "Juízo Universal".

588 Idem. Ibid, p. 179: "*Se puede, por conseguiente, comprobar una progresiva 'computarización' de la vida privada, no solo em cuanto se refiere a la cantidad numérica de los indivíduos fichados, sino también respecto a la particualridad, siempre más detallada y precisa, de las informaciones que les conciernen.*"

personalidade. De qualquer forma, o consumidor pode recorrer à ação de *habeas data* para a retificação de dados, ou mesmo apenas, para verificação de conteúdo.

A boa-fé objetiva possui um papel importante, pois orienta toda a sistemática do direito do consumidor. É a partir da observância da boa-fé que é possível descobrir o aspecto colaborativo do dever de confidencialidade de dados, bem como da importância do dever de informar. Da mesma forma, dentro de um ambiente complexo, é justo considerar a necessidade de os usuários também seguirem as instruções de segurança dispostas pelos fornecedores.

Além do mais, a expectativa de segurança de dados gerada pelos fornecedores nos usuários deve sempre ser atendida. O dever de confidencialidade, portanto, nasce quando há a necessidade dos fornecedores protegerem dados pessoais e sensíveis de seus usuários. São vários os danos pela violação de dados. Estes, muitas vezes, não são nem percebidos pelos usuários. Isso é verdade, principalmente, quando há o cruzamento de dados. O cruzamento de dados comuns pode revelar dados sensíveis sobre as pessoas. De outra forma, o uso de dados pelos fornecedores fora da finalidade pela qual foram coletados, também pode causar danos aos usuários. Por isso, há a necessidade do ambiente que armazena dados pessoais e sensíveis contar com a possibilidade de identificabilidade de acessos e armazenamento de *logs*. É a característica de auditabilidade do ambiente, que se torna mais importante, à medida que o ambiente informático dificulta a identificação dos agentes causadores de danos. Além disso, a taxonomia da privacidade, proposta por Solove, apoia a identificação de eventos danosos, mesmo diante da crítica de Leonardi acerca da não consideração da dignidade da pessoa humana na taxonomia em estudo.

As excludentes de responsabilidade, nos casos de falha na proteção de dados, também constituem um assunto relevante. Como foi visto, a culpa exclusiva dos usuários é uma causa importante nas violações envolvendo o acesso não autorizado. Por mais que, via de regra, a Internet seja um meio inseguro e repleto de

riscos, e vigore a responsabilidade objetiva dos fornecedores, o usuário deve manter um zelo e cuidado com seu computador e com suas credenciais de acesso.

A responsabilidade do fornecedor pelo risco do desenvolvimento também é um assunto importante na questão da insegurança na Internet. Como se viu, embora a maior parte da doutrina considere que o fornecedor responde pelos riscos do desenvolvimento, foi possível verificar que o desconhecimento dos riscos, em face do estado dos conhecimentos científicos, afasta o próprio nexo causal. Não se defende a pura transferência de riscos para o consumidor, em função da própria sistemática de proteção. Porém, no caso concreto, pode ser considerada a não responsabilização do fornecedor pelos riscos do desenvolvimento. Ao mesmo tempo, o caso fortuito e a força maior também representam, na sua ocorrência, o afastamento do nexo causal. Embora a análise do caso concreto revele a irresponsabilidade do fornecedor em casos de fortuito externo, a doutrina entende que o ataque de cracker, via de regra, não é compatível com a doutrina do caso fortuito e de força maior. Foi possível ver, por sua vez, a lição dissonante de Binicheski, que entende ser possível essa possibilidade.

A recente lei 12.414/2011 trouxe um grande avanço para as relações de consumo quando estabeleceu um "*controle da atividade de processamento de dados por autoridade administrativa, de modo a se ter um sistema administrativo de fiscalização e resolução de conflitos em conjunto com um sistema clássico judicial de solução de lides*", conforme estipulado em seu art. 17.[589] A proteção pelas vias administrativas pode constituir, de acordo com Têmis Limberger, "*uma alternativa importante para resolução de conflitos. Estes algumas vezes possuem pequeno valor pecuniário individualmente, porém no âmbito coletivo representam uma quantia patrimonial expressiva.*"[590]

Há quem defenda a criação de um órgão específico fiscalizador com o

589 MENDES, Laura Schertel. Ibid, p. 66.

590 LIMBERGER, Têmis. *O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais.* Porto Alegre: Livraria do Advogado, 2007, p. 159.

objetivo de:

> "*realizar um controle contínuo das atividades dos bancos de dados públicos e privados, poderia trazer maior eficácia na aplicação dos dispositivos legais e privados, poderia trazer maior eficácia na aplicação dos dispositivos legais pertinentes, na prevenção de dados aos titulares de informações arquivadas em bancos de dados e na imposição de sanções no caso de descumprimento pelos gestores de bancos de dados de seus deveres legais.*"[591]

Igualmente, a Diretiva 95/46/CE define a criação de autoridades de controle – em seu art. 28 – com o fim de realizar a "*fiscalização da aplicação no seu território das disposições adotadas pelos Estados-membros nos termos da presente diretiva.*"[592]

Defende-se aqui, que uma das formas de constituir a aplicação de efetiva proteção no tratamento de dados pessoais no Brasil deve passar pela criação de um órgão especial independente[593], nos moldes da autoridade de controle citada pela Diretiva 95/46/CE e também de acordo com o previsto no anteprojeto brasileiro de proteção de dados. Essa opinião é sustentada, inclusive, por Danilo Doneda[594] e

---

591 CARVALHO, Ana Paula Gambogi. Ibid, p. 118.

592 Basicamente os poderes destas autoridades encontram-se no n. 3 do art. 28: "*poderes de inquérito, tais como o poder de aceder aos dados objecto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controlo; de poderes efectivos de intervenção, tais como, por exemplo, o de emitir pareceres previamente à execução adequada desses pareceres, o de ordenar o bloqueio, o apagamento ou a destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentos nacionais ou para outras instituições políticas; do poder de intervir em processos judiciais no caso de violação das disposições nacionais adoptadas nos termos da presente directiva ou de levar essas infracções ao conhecimento das autoridades judiciais.*"

593 Esta independência é defendida por DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 393, como o "*atributo que reflete a sua própria razão de ser, lhes é atribuída por meio de mecanismos que afastem o máximo possível a sua atuação da influência dos poderes estatais constituídos*"

594 DONEDA, Danilo. Ibid, p. 385-386. Segundo o autor "*Não se trata, no entanto, de um fenômeno circunscrito ao espaço geográfico e político europeu, pois organismos do gênero estão presentes em países como Argentina, Austrália, Canadá, Japão, Israel, Hong Kong, Nova Zelândia e Taiwan, da maioria dos países em vias de aderir à União Europeia nos próximos anos. É também*

Marcel Leonardi[595]. A necessidade de tais órgãos "*surge como um resultado natural em um contexto no qual a atuação do estado se dilata e também se sofistica a demanda pelos direitos.*"[596] Igualmente, a falta de controle e de medidas organizadas neste assunto representam um empecilho para o desenvolvimento.

A regulação da privacidade através de uma lei que estabelece parâmetros mínimos em relação à privacidade, como o Marco Civil, o anteprojeto de proteção de dados bem como as medidas de atualização do CDC citadas nesse trabalho são muito bem-vindas. De qualquer forma, os dispositivos legais devem regular a proteção da privacidade tanto na sua coleta, armazenamento e processamento. Tais dispositivos devem prever, quando possível, a tutela da privacidade, inclusive, nos casos de violação desta por meio do cruzamento de dados. Igualmente, é útil o estabelecimento do regime de responsabilidade objetiva dos fornecedores para as situações envolvendo o tratamento de dados privados e pessoais.[597]

A proteção da confidencialidade dos dados pessoais só pode ser atingida com o atendimento de práticas de seguranças rígidas, principalmente no que diz respeito à autenticação adequada dos usuários. Urge que se adote um padrão regulatório de segurança para o comércio eletrônico que estabeleça minimamente padrões técnicos de segurança pertinentes à atividade. Um regulamento pode cumprir essa tarefa, estabelecendo claramente quais as medidas técnicas que devem ser observadas para a proteção da privacidade pelos fornecedores de serviços informáticos[598]. De forma limitada, no âmbito do Cadastro Positivo apenas, endente-

---

importante ressaltar que nos Estados Unidos a FTC (Federal Trade Comission), embora não seja um organismo propriamente comparável as authorities mencionadas, recebeu o encargo de fiscalizar a utilização de dados pessoais em relações de consumo, tarefa bastante relevante e que lhe rendeu a referência por alguns estudiosos sendo uma authority de fato para a proteção da privacidade." Entre o exemplo de organismos no Brasil que possuem funções semelhantes, porém em outras atividades, o autor ressalta o CADE, a CVM e o CMN. p. 389

595 LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, p. 209.

596 DONEDA, Danilo. Ibid, p. 396.

597 Sobre a questão da responsabilidade objetiva ver DONEDA, Danilo. Ibid, p. 365.

598 No âmbito do anteprojeto brasileiro de lei de proteção de dados pessoais, o art. 24, dispõe no mesmo sentido: "*Um conjunto de medidas mínimas de segurança preventiva será publicado pela Autoridade de Garantia dentro de, no máximo, um ano após a entrada em vigor da presente lei, e atualizado periodicamente, com base na evolução da tecnologia e na experiência adquirida .*"

se que a necessidade de um regulamento técnico de segurança da informação foi preenchida, como se viu, com o Dec. 7.829/2012.

No entanto, os dispositivos legais atuais também possuem mecanismos de tutela importantes. Assim ocorre com o *Habeas Data* e a própria Ação Civil Pública. A doutrina aponta a importância dos termos de ajustamento de conduta possibilitados por meio do art. 5º da Lei de Ação Civil Pública, estes caracterizados pela agilidade e eficiência na proteção de interesses.[599]

Como o comércio eletrônico é global e, assim, as questões de proteção à privacidade nos bancos de dados de consumidores também são, adota-se também como conclusão a lição de Lorenzetti. Ele defende a criação de organismos internacionais, de regulamentações e disposições de "*leis nacionais que atuem de forma homogênea*" bem como a ampliação de um sistema de arbitragem.[600]

No entanto, a adoção de um padrão global de proteção de privacidade esbarra na dificuldade natural de atingimento de um consenso entre os países[601], bem como nas diferenças culturais. Mesmo assim, é possível conceber a proposição de um padrão mínimo, especialmente no direito do consumidor, no que diz respeito a autorização e limitação do tratamento de dados pessoais e sensíveis.

599 LEONARDI, Marcel. Ibid, p. 234.
600 LORENZETTI, Ricardo L.. *Comércio Eletrônico*. São Paulo: RT, 2004, p. 371.
601 Embora pareça difícil, não é impossível. Lorenzetti dá como exemplo a consolidação de um padrão harmônico mundial relativo aos documentos eletrônicos, assinatura digital e contratos. Idem. Ibid, p. 371.

REFERÊNCIAS BIBLIOGRÁFICAS

ASCENSÃO, José de Oliveira. *Direito da Internet e da Sociedade da Informação: Estudos*. Rio de Janeiro: Forense, 2002. 329 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*. Tecnologia da informação. Técnicas de segurança. Sistemas de gerência da segurança da informação. Rio de Janeiro, 2005

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: Tecnologia da informação - Técnicas de Segurança - Código de prática para a gestão da segurança da informação. 2. ed. Rio de Janeiro, 2005.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. *Glossário da Sociedade da Informação.* APDSi: Lisboa, 2005. Disponível em: <http://www.apdsi.pt/>. Acesso em 17 de Dezembro de 2011.

AYRES, Ian. *Super Crunchers: Why thinking-by-numbers is the new way to be smart*. New York: Bantam Dell, 2007

BAKER, Stephen. *Numerati*. São Paulo: Saraiva, 2009.

BARBAGALO, Erica B.. Aspectos da responsabilidade civil dos provedores de serviços na Internet. In: LEMOS, Ronaldo; WAISBERG, Ivo. (org.) *Conflitos sobre nomes de domínio e outras questões jurídicas da Internet*. São Paulo: RT, 2003.

BARBOSA, Fernanda Nunes. *Informação: direito e dever nas relações de consumo*. São Paulo: RT, 2008.

BARRETO, Ricardo Menna; LIMBERGER, Têmis. Ciberespaço e obstáculos 3-D: Desafios à concretização dos direitos do consumidor. *Revista de direito do consumidor*, São Paulo, n 79, p. 101-120, jul.-set./2011.

BEAL, Adriana. *Segurança da Informação*. São Paulo: Atlas, 2005.

BECK, Ulrich. *La socied del riesgo: Hacia una nueva modernidad*. Barcelona: Editorial Paidós, 1998.

BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 2ª ed. São Paulo: RT, 2006.

BINICHESKI, Paulo Roberto. *Responsabilidade civil dos provedores de Internet: direito comparado e perspectivas de regulamentação no direito brasileiro*. Curitiba: Juruá, 2011.

BOBBIO, Norberto. *Teoria do Ordenamento Jurídico*. Brasília: UnB, 1996, 6ª Ed.

BRANCO, Gerson Luiz Carlos. A proteção das expectativas legítimas derivadas das situações de confiança: elementos formadores do princípio da confiança e seus efeitos. *Revista de Direito Privado*, São Paulo, n. 12, p. 169-225, out.-dez./2002.

BRANDEIS, Louis; WARREN, Samuel. The right to privacy. *Harvard Law Review*, Cambridge, v. IV, n. 5. Dec. 1890.

BROAD, J. William. MARKOFF, John. SANGER, David E.. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. The New York Times. 15 de Janeiro de 2011. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>. Acesso em: 15 Jan. 2011.

BRÜSEKE, Franz Josef. Risco e contingência. In: VARELLA, Marcelo Dias. *Direito, Sociedade e Riscos:A sociedade contemporânea vista a partir da ideia de risco*. Brasília: UNICEUB, 2006.

CADKIN, John; COURSON, J. Zachary; SOMA, John T. Corporate privacy trend: the "value" of personally identifiable information ("PII") equals the "value" of financial assets. *Richmond Journal of Law & Technology*. Volume XV, Issue 4. 2009. Disponível em <http://law.richmond.edu/jolt/v15i4/Article11.pdf>. Acesso em: 12 de jan. 2012.

CARTER, Helen. Internet Crime Eclipses Burglary in Survey of Perceived Risks. *The Guardian*, 9 de Outubro de 2006. Disponível em: <http://www.guardian.co.uk/technology/2006/oct/09/news.crime>. Acesso em: 8 jan. 2012.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *Revista de Direito do Consumidor*, São Paulo, n. 46, p. 77-119, abr.-jun./2003.

CASADO, Márcio Melo. Responsabilidade objetiva no Código de Defesa do Consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V. p. 729-768.

CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8ª Ed. São Paulo: Atlas, 2009.

CIARELLI, Nicholas. How Visa Predicts Divorce. *The Daily Beast*. 6 de Abril de 2010. Disponível em: <http://www.thedailybeast.com/articles/2010/04/06/how-mastercard-predicts-divorce.html>. Acesso em: 12 Fev. 2012.

CODERCH, Pablo Salvador; GONZALEZ, Sonia Ramos. El defecto en las instrucciones y advertencias en la responsabilidad de producto. Latin American and Caribbean Law and Economics Association (ALACDE). *Annual Papers, Berkeley Program in Law and Economics*, UC Berkeley. 2007. Disponível em: <http://escholarship.org/uc/item/8xg6n210>. Acesso em: 18 Jun. 2011.

_____; PUIG, Antoni Rubí. Riesgos de desarrollo y evaluación judicial del carácter científico de dictámenes periciales. *Revista para el análisis del derecho* - InDret, n. 1, 2008. Disponível em: <http://www.raco.cat/index.php/InDret/article/view/77867>. Acesso em: 10 Jan. 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. *TIC Domicílios e Empresas 2010. Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo, 2011. Disponível em: <http://www.cgi.br/publicacoes/pesquisas/index.htm>. Acesso em: 10 Jan. 2012.

CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito - UFPR*, Curitiba, n. 47, p. 141-153, 2008.

COSTA, Luiz. Privacy and the precautionary principle. *Computer Law & Security Review*, n. 28, 2012, p. 14-24.

DA SILVA, Eduardo Silva. *Segurança na sociedade da informação: uma visão desde a autonomia privada*. 2006. 178 p. Tese apresentada no Programa de Pós-Graduação em Direito da UFRGS, como requisito parcial para obtenção do grau de Doutor em Direito. Porto Alegre.

DALLARI JÚNIOR, Hélcio De Abreu; GARCEZ, Robson do Boa Morte. Desenvolvimento sustentável e o direito baseado em evidências. In: MESSA, Ana Flávia; THEOPHILO NETO, Núncio; THEOPHILO JÚNIOR, Roque (coord.).

Sustentabilidade ambiental e os novos desafios na era digital: Estudos em homenagem a Benedito Guimarães Aguiar Neto. São Paulo: Saraiva, 2011. p. 451-459.

DE VILLIERS, Meiring. Reasonable Foreseeability in Information Security Law: A Forensic Analysis. *University of New South Wales Faculty of Law Research Series*, Sydney, p. 102-160, Abr. 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1158165>. Acesso em: 12 Fev. 2012.

DIAS, José de Aguiar. *Da responsabilidade Civil*. 8ª Ed. Rio de Janeiro: Forense, 1987. Volume 1 e 2.

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

_____. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em: 12 Fev. 2012.

EBERLIN, Fernando Büscher von Teschenhausen. Responsabilidade dos fornecedores pelos danos decorrentes dos riscos do desenvolvimento: análise sob a ótica dos princípios da atividade econômica. *Revista de Direito do Consumidor*, São Paulo, n. 64, p. 9-42, out.-dez./2007.

FABIAN, Christoph. *O dever de informar no direito civil*. São Paulo: RT, 2002.

FABRI, Hélène Ruiz; HAMMAN, Andrea. Transnational networks and constitutionalism. *International Journal of Constitutional Law*, Volume 6, Número 3 & 4. p. 481-508. Disponível em:

<http://icon.oxfordjournals.org/cgi/content/abstract/mon024>. Acesso em: 12 Fev. 2012.

FAURE, Michael G. Calabresi and Behavioural Tort Law and Economics. *Erasmus Law Review*. Volume 01, Issue 04.

FILHO, Adalberto Simão. Dano ao consumidor por invasão do site ou da rede: Inaplicabilidade das Excludentes de Caso Fortuito ou Força Maior. In: FILHO, Adalberto Simão; DE LUCCA, Newton. (coord.). *Direito & Internet – Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2000. p. 101-115.

FILHO, Demócrito Reinaldo. A responsabilidade dos bancos pelos prejuízos resultantes do phishing. *Jus Navigandi*, Teresina, ano 12, n. 1836, 11 jul. 2008. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=11481>. Acesso em: 12 fev. 2012.

FILHO, Sérgio Cavalieri. O direito do consumidor no limiar do século XXI. *Revista de direito do consumidor*, São Paulo, n. 35, p. 97-107, jul.-set./2000.

FONSECA, Arnoldo Medeiros da. *Caso fortuito e teoria da imprevisão*. 3ª Ed. Rio de Janeiro: Forense, 1958.

FORGIONI, Paula A. *Teoria Geral dos Contratos Empresariais*. 2ª Ed. São Paulo: RT, 2010.

FROSINI, Vittorio. *Cibernética, Derecho y Sociedad*. Madrid: Tecnos, 1978.

GARFINKEL, Simson; SPAFFORD, Gene. *Practical Unix and Internet Security*. Sebastopol: O'Reilly, 2006.

GASSER, Urs; HAUSERMAN, Daniel. E-Compliance: Towards a Roadmap for Effective Risk Management. *Berkman Center for Internet & Society at Harvard University*. 2007. Disponível em: <http://cyber.law.harvard.edu/publications/2007/ECompliance>. Acesso em: 12 Fev. 2012.

GELBSTEIN, Eduardo; KAMAL, Ahmad. *Information Insecurity: A survivel guide to the uncharted territories of cyber-threats and cyber-security*. New York: United Nations ICT Task Force, 2002.

GODOY, Cláudio Luiz Bueno de. Responsabilidade pelo Fato do Produto e do Serviço. In: SILVA, Regina Beatriz Tavares da Silva. (coord). *Responsabilidade Civil nas Relações de Consumo*. São Paulo: Saraiva, 2009.

GRINBERG, Rosana. Fato do produto ou do serviço. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 783-815.

GUIMARÃES, Paulo Jorge Scartezzini. *Vícios do produto e do serviço por qualidade, quantidade e insegurança: cumprimento imperfeito do contrato*. São Paulo: RT, 2004.

HÄBERLE, Peter. A dignidade humana e a democracia pluralista – seu nexo interno. In SARLET, Ingo Wolfgang (org). *Direitos fundamentais, informática e comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007.

HARTMANN, Ivar Alberto Martins. O princípio da precaução e sua aplicação no direito do consumidor: dever de informação. *Direito & Justiça*. v. 38, n. 2, p. 156-182, jul.-dez./2012.

HÉLIE-GHERNAOUTI, Solange. *Internet et sécurité*. 2ª Ed. Paris: Puf, 2002.

JUCÁ, Francisco Pedro. Responsabilidade social e sustentabilidade. In: MESSA, Ana Flávia; THEOPHILO NETO, Núncio; THEOPHILO JÚNIOR, Roque (coord.). *Sustentabilidade ambiental e os novos desafios na era digital: Estudos em homenagem a Benedito Guimarães Aguiar Neto.* São Paulo: Saraiva, 2011. p. 27-43.

KURBALIJA, Jovan. *An Introduction to Internet Governance*. Genebra: DiploFoundation, 2008.

LEMOS, Ronaldo. *Direito, tecnologia e cultura*. Rio de Janeiro: FGV Editora, 2005.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.

_____. Determinação da Responsabilidade Civil pelos Ilícitos na Rede: Os Deveres dos Provedores de Serviços de Internet. In: SANTOS, Manoel J. Pereira dos; SILVA, Regina Beatriz Tavares da Silva. (coord). *Responsabilidade Civil na Internet e nos Demais Meios de Comunicação*. São Paulo: Saraiva, 2007.

_____. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. *Code: Version 2.0.* Basic Books: New York, 2006.

LEVY, PIERRE. *Cibercultura*. São Paulo: Editora 34, 1999.

LIMA, Alvino. *Culpa e Risco*. São Paulo: RT, 1960.

LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In SARLET, Ingo Wolfgang (org). *Direitos Fundamentais, Informática e Comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007. p. 196-226.

_____. *O Direito à intimidade na era da informática: A necessidade de proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007.

LISBOA, Roberto Senise. Direito na Sociedade da Informação. *Revista dos Tribunais*. São Paulo, v. 95, n. 847, p. 78 – 95, maio/2006.

_____. Tecnologia, confiança e sociedade. Por um novo solidarismo. In: PAESANI, Liliana Minardi (coord). *O Direito na Sociedade da Informação II*. São Paulo: Atlas, 2009. cap III.

LORENZETTI, Ricardo Luis. *Fundamentos do Direito Privado*. São Paulo: RT, 1998.

_____. *Tratado de los contratos*. Buenos Aires: Rubinzal y Asociados, 1999. Tomos I, II e III.

_____. *Consumidores*. Buenos Aires: Rubinzal y Asociados, 2003.

_____. *Comércio Eletrônico*. São Paulo: RT, 2004.

LUÑO, Antonio-Enrique Pérez. *Manual de informática y derecho*. Barcelona: Ariel, 1996.

_____. *Ciberciudadani@ o ciudadani@.com*. Barcelona: Gedisa, 2004.

MAIA, Luciano Soares. *A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais*. Disponível em: <http://www.conpedi.org.br/manaus/arquivos/anais/bh/luciano_soares_maia.pdf>. Acesso em: 12 Fev. 2012.

MANDARINO JR., Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Cuzbac, 2010.

MANDEL, Gregory N. History Lessons for a General Theory of Law and Technology. *Minnesota Journal of Law, Science & Technology*, Vol. 8, n. 20, Minneapolis, p. 551-570, 2007. Disponível em: <http://ssrn.com/abstract=1012612>. Acesso em: 12 Fev. 2012.

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico)*. São Paulo: RT, 2004.

_____. A chamada nova crise do contrato e o modelo de direito privado brasileiro: crise de confiança ou de crescimento do contrato. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual*. São Paulo: RT, 2007, p. 17-86.

_____. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 6ª Ed. São Paulo: RT, 2011.

MARTINS-COSTA, Judith. *A boa-fé no direito privado*. São Paulo: RT, 1999.

MARTINS, Guilherme Magalhães. Confiança e aparência nos contratos eletrônicos de consumo via internet. *Revista de Direito do Consumidor*, São Paulo, n. 64, p. 43-70, out.-dez./2007.

McINTYRE, Joshua J.. Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information. *DePaul Law Review*, Vol. 60, N. 3, 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621102>. Acesso em: 12 Fev. 2012.

MELO, Wilson Viera; KALIL, Lisiane Lindenmeyer; et al. O papel das heurísticas no julgamento e na tomada de decisão sob incerteza. *Estudos de Psicologia*, Campinas, n. 23(2), p. 181-189, abr – jun/2006. Disponível em: <http://www.iders.org/textos/o_papel_das_heuristicas_na_tomada_de_decisao.pdf>. Acesso em: 12 Fev. 2012.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, São Paulo, n. 79, p. 45-82, jul.-set./2011.

MENEZES CORDEIRO, António Manuel da Rocha E. *Da boa-fé no direito Civil*. Coimbra: Almedina, 1984. Volume 1 e 2.

MENKE, Fabiano. *Assinatura eletrônica no Direito Brasileiro*. São Paulo: RT, 2005.

_____. *A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. No prelo.

MERRIL, Charles R.. Terms and Definitions: ISOM, David K.; NELSON, Sharon D.; SIMEK. John W.(edit.). *Information Security for Lawyers and Law Firms*. Chicaco: American Bar Association Publishing, 2006.

MIGUEL, Carlos Ruiz. En torno a la protección de los datos personales automatizados. *Revista de Estudios Políticos Nueva Epoca*, Madrid, n. 84, p. 237-264, Abr.-Jun./1994.

MIRAGEM, Bruno. Função social do contrato, boa-fé e bons costumes: nova crise dos contratos e reconstrução da autonomia negocial pela concretização das cláusulas gerais. In: MARQUES, Cláudia Lima (coord). *A nova crise do contrato: Estudos sobre a Nova Teoria Contratual.* São Paulo: RT, 2007, p. 176-225.

_____. Responsabilidade por danos na sociedade da informação e proteção do consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, São Paulo, n. 70, p.41-92, abr.-jun./2009.

_____. Os direitos da personalidade e os direitos do consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 421-463.

MORAES, Paulo Valério Dal Pai. *Código de defesa do consumidor: o princípio da vulnerabilidade no contrato, na publicidade, nas demais práticas comerciais: interpretação sistemática do direito*. Porto Alegre: Livraria do Advogado, 2009.

MORI, Michele Keiko. *Direito à indimidade versus informática*. Curitiba: Juruá, 2001.

MOTA, Mauricio Jorge Pereira da. *A boa-fé objetiva nos contratos de licença de uso de software*. Disponível em: <www.estig.ipbeja.pt/~ac_direito/Software2.pdf>. Acesso em: 2 Dez. 2011.

NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: Wmf Martins Fontes, 2009.

NOIVILLE, Christine. Para uma proteção do lançador de alerta. In: VARELLA, Marcelo Dias. *Direito, Sociedade e Riscos: A sociedade contemporânea vista a partir da ideia de risco*. Brasília: UNICEUB, 2006, p. 124-157.

NOOR, Arshad; PELED, Ariel. Access Control. In: ISOM, David K.; NELSON, Sharon D.; SIMEK. John W.(edit.). *Information Security for Lawyers and Law Firms*. Chicaco: American Bar Association Publishing, 2006.

OHM, Paul. The Myth of the Superuser: Fear, Risk, and Harm Online. *University of Colorado Law Legal Studies Research Paper.* No. 07-14; UC Davis Law Review Vol.

41. No. 4. Apr., 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372>. Acesso em: 12 Fev. 2012, p. 1327-1402.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Guidelines for the Security of Information Systems and Networks - Towards a culture of security*. Paris: OECD. 2002. Disponível em: <http://www.oecd.org/>. Acesso em: 15 Dez. 2011.

PAREDES, Marcos. Violação da privacidade na Internet. *Revista de Direito Privado*, São Paulo, n. 9, p. 183-203, jan.-mar./2002.

PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2007.

PODESTÁ, Fábio Henrique. Direito à intimidade em ambiente da Internet. In: FILHO, Adalberto Simão; DE LUCCA, Newton. (coord.). *Direito & Internet – Aspectos Jurídicos Relevantes*. Bauru: Edipro, 2000. p. 155-176.

RANKING APONTA GOOGLE COMO MARCA MAIS VALIOSA DO MUNDO. *Idg Now*. 29 de Abril de 2010. Disponível em: <http://idgnow.uol.com.br/mercado/2010/04/29/ranking-aponta-google-como-marca-mais-valiosa-do-mundo/>. Acesso em: 29 Abr. 2010.

REIDENBERG, Joel. Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*. v. 76, n. 3, Feb. 1998. p. 553-584. Disponível em: <http://reidenberg.home.sprynet.com/lex_informatica.pdf>. Acesso em: 12 Fev. 2012.

RIBEIRO, Diógenes V. Hassan. *Proteção da Privacidade*. São Leopoldo: Unisinos, 2003.

RIBEIRO, Luciana Antonini. A privacidade e os arquivos de consumo na internet - Uma primeira reflexão. Revista de direito do consumidor, São Paulo, n. 41, p. 151-165, jan.-mar./2002.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: A privacidade hoje*. Rio de Janeiro: Renovar, 2008.

ROHR, Altieres. Universidade do RS se desculpa por vazar dados de 23 mil alunos. 26 de Janeiro de 2012. *G1*. Disponível em: <http://g1.globo.com/rs/rio-grande-do-sul/noticia/2012/01/universidade-do-rs-se-desculpa-por-vazar-dados-de-23-mil-alunos.html>. Acesso em: 26 Jan. 2012.

ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Belo Horizonte: Del Rey, 2005.

ROMANO, Santi. *Princípios de Direito Constitucional*. São Paulo: RT, 1977.

RUIZ, Carlos Barriuso. *Interacción del derecho y la informática*. Madrid: Dykinson, 1996.

SAAREMPÄÄ, Ahti. The importance of information security in safeguarding human and fundamental rights. *e-Stockholm 2008 Legal Conference*. p. 1-15. Disponível em: <http://www.juridicum.su.se/Iri/e08/documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf>. Acesso em: 20 Dez. 2012

SANTOLIM, Cesar Viterbo Matos. Os princípios de proteção do consumidor e o comércio eletrônico no direito brasileiro. *Revista de direito do consumidor*, São Paulo, n. 55, p. 53-84, jul.-set./2005.

_____. Anotações sobre o anteprojeto da comissão de juristas para a atualização do código de defesa do consumidor na parte referente ao comércio eletrônico. *Revista de Direito do Consumidor*, São Paulo, v. 83, p. 73-82, jul.-set./2012.

SCHNEIER, Bruce. *The Psychology of Security*. Disponível em: <http://www.schneier.com/essay-155.html>. Acesso em: 12 Fev. 2012.

SILVA, Clóvis V. do Couto. *A obrigação como processo*. Rio de Janeiro: FGV, 2006.

SILVA, De Plácido. *Vocabulário Jurídico*. Rio de Janeiro: Forense, 1987.

SMEDINGHOFF, Thomas J.. *Information Security Law: The Emerging Standard for Corporate Compliance*. Ely: IT Governance Publishing, 2008.

_____. *The State of Information Security Law: A Focus on the Key Legal Trends*. Disponível em: <http://ssrn.com/abstract=1114246>. Acesso em: 12 Fev. 2012.

SOLOVE, Daniel J.. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Vol. 154, N. 3, p. 477-560, jan./2006. Disponível em: <http://ssrn.com/abstract=667622>. Acesso em: 12 Fev. 2012.

_____. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, p. 745-772, 2007. Disponível em: <http://ssrn.com/abstract=998565>. Acesso em: 10 Jan. 2012.

STOCCO, Rui. Defesa do consumidor e responsabilidade pelo risco do desenvolvimento. In MARQUES, Cláudia Lima; MIRAGEM, Bruno. (org.). In: *Doutrinas Essenciais Direito do Consumidor*. São Paulo: RT, 2011. Vol. V, p. 277-288.

TADEU, Silney Alves. Algumas reflexões sobre a proteção da pessoa e o uso informatizado de seus dados pessoais. *Revista de Direito do Consumidor*, São Paulo, n. 79, p. 83-99, jul.-set./2011, p. 86.

TEIXEIRA, Tarcísio. *Direito Eletrônico*. São Paulo: Juarez de Oliveira, 2007.

TELES, Giovana. Venda de listas de e-mails causa transtorno com mensagens de spam. G1. 24 de Janeiro de 2012. Disponível em: <http://g1.globo.com/jornal-hoje/noticia/2012/01/venda-de-listas-de-emails-causa-transtorno-com-mensagens-de-spam.html>. Acesso em: 24 Jan. 2012.

UNIÃO EUROPEIA. *Diretiva 95/46/CE – Diretiva Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, de 24 de Outubro de 1995. Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu.

UNIÃO EUROPEIA. *Diretiva 2002/58/CE* - Diretiva relativa à privacidade e às comunicações eletrônicas, de 31 de Julho de 2002. Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu.

UNIÃO EUROPEA. *Diretiva 2000/31/CE – Diretiva relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno de 08 de Junho de 2000.* Jornal Oficial das Comunidades Europeias. Parlamento e Conselho Europeu.

VENOSA, Sílvio de Salvo. *Direito Civil: Responsabilidade Civil*. Vol. 4. São Paulo: Atlas, 2010.

VIANNA, Túlio Lima. *Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais*. Rio de Janeiro: Forense, 2003.

JURISPRUDÊNCIAS CONSULTADAS

SUPERIOR TRIBUNAL DE JUSTIÇA. 4ª Turma. REsp 287849/SP. Renato Esteves Versolatto X Big Valley Hotel Fazenda Ltda e Agência de Viagens CVC Tur Ltda. Relator:Ministro Ruy Rosado de Aguiar. Brasília, 17 de Abril de 2001.

SUPERIOR TRIBUNAL DE JUSTIÇA. 3ª Turma. REsp. n.1193764/SP. I.P da S.B X Google Internet Brasil Internet Ltda. Relator: Min. Nancy Andrighi. Brasília, 14 de Dezembro de 2010.

SUPERIOR TRIBUNAL DE JUSTIÇA. 3ª Turma. REsp. n.1.323.754/RJ. Google Internet Brasil Internet Ltda. X Grasiele Salme Leal. Relator: Min. Nancy Andrighi. Brasília, 19 de Junho de 2012.

TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. 11ª Câmara Cível. Apelação n. 2.0000.00.433758-0/000. ProInternet do Brasil Ltda X Websol - Soluções em Informática LTDA. Relator: Des. Teresa Cristina da Cunha Peixoto. Belo Horizonte, 2 de Fevereiro de 2000.

TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. 3ª Turma Recursal. Recurso Cível n. 024.06.990.953-9. Patrícia da Conceição Freitas X Mercado Livre.com Atividade de Internet Ltda. Relator: Juiz Anacleto Rodrigues. Belo Horizonte, 08 de Março de 2006.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. 35ª Câmara do oitavo grupo - Seção de Direito Privado. Apelação cível n. 9059673-92.2005.8.26.0000. Naildes de Jesus dos Santos X Terra Networks Brasil S/A Relator: Des. Artur Marques. São Paulo, 12 de Fevereiro de 2007.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. 8ª Câmara de Direito Privado. Apelação n. 604.346.4/7-00. Gisele Colombo de Andrade Rodrigues x Maifa Café Ltda. - EPP. Relator: Salles Rosso. São Paulo, 11 de Dezembro de 2008.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Sexta Turma Cível. Apelação n. 2004.01.1.014499-5. Célia Bretas Netto X BRB - Banco de Brasília S/A. Relator: Sandra de Sentis. Brasília, 09 de Maio de 2005.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70011140902. Paulino Provin Miola x Empresa Brasileira de Telecomunicações S/A. Relator: Des. Luiz Augusto Coelho Braga. Porto Alegre, 26 de Outubro de 2005.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 6ª Câmara Cível. Apelação n. 70013361043. Jocelei Perdomo das Neves X Terra Networks Brasil S/A. Relator: Des. Artur Arnildo Ludwig. Porto Alegre, 21 de Dezembro de 2006.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 1ª Turma Recursal Cível. Recurso Inominado n. 71001199744. Vilmar Luiz Sartori X Indiana Seguros S/A. Relator: Des. João Pedro Cavalli Júnior. Porto Alegre, 26 de Abril de 2007.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 9ª Câmara Cível. Apelação n. 70019549971. Rádio e TV PortoVisão Ltda X Kapitanski Representações Ltda. Relator: Des. Odone Sanguiné. Porto Alegre, 4 de Julho de 2007.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70027619519. Google Brasil x Cassilda Salete Prigol. Relator: Des. Romeu Marques Ribeiro Filho. Porto Alegre, 11 de Março de 2008.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 2ª Turma Recursal. Recurso Inominado n. 71001598341. Cátia Nascente da Cunha X Google Brasil Internet Ltda. Relator: Hilbert Maximiliano Akihito Obara. Porto Alegre, 26 de novembro de 2008.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 10ª Câmara Cível. Agravo de Instrumento n. 70028102291. Google Brasil Internet Ltda. X Sabemi Seguradora S.A e Luiz Carlos Franca Martinez. Relator: Des. Paulo Antônio Kretzmann. Porto Alegre, 19 de Março de 2009.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 3ª Turma Recursal Cível. Recurso Inominado n. 71002243293. Maria Elena Abdala Pinheiro X Banco do Estado do Rio Grande do Sul S/A. Relator: Eugênio Facchini Neto. Porto Alegre, 28 de Janeiro de 2010.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70030254841. Telão Ltda X Mercado Livre S/A. Relator: Des. Romeu Marques Ribeiro Filho. Porto Alegre, 17 de Março de 2010.

TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. 20ª Câmara de Direito Civil. Agravo de Instrumento n. 0013822-08.2010.8.19.0000. Wanderlei de Carvalho Rego X Net Serviços de Comunicação S/A. Relator: Des. Letícia Sardas. Rio de Janeiro, 30 de Junho de 2010.

TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. 5ª Câmara Cível. Apelação n. 70038911400. Carla de Deus Vieira Silveira X Câmara de Dirigentes Lojistas de Porto Alegre e Companhia Zaffari Comércio e Indústria. Relator: Des. Jorge Luiz Lopes do Canto . Porto Alegre, 26 de Janeiro de 2011.