2017 - 01 - 30

Revista de Direito do Consumidor
2016
RDC VOL. 106 (JULHO - AGOSTO 2016)
XIII CONGRESSO DE DIREITO DO CONSUMIDOR, FOZ SO IGUAÇU, 1 A 4 DE MAIO
2. O DIÁLOGO ENTRE O MARCO CIVIL DA INTERNET E O CÓDIGO DE DEFESA DO CONSUMIDOR

2. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor

Dialogue between the Framework Internet Act and the Consumer Protection Code

(Autor)

LAURA SCHERTEL MENDES

Doutora em Direito Privado pela Humboldt Universität zu Berlin. Mestre em Direito, Estado e Constituição pela Universidade de Brasília – UnB. Graduada em Direito pela UnB. Professora do Instituto Brasiliense de Direito Público – IDP e Gestora Governamental. lauraschertel@hotmail.com Recebido em: 22.03.2016 Convite 2

Sumário:

Área do Direito: Consumidor

Resumo:

O texto trata do diálogo das fontes como modelo de aplicação simultânea de fontes normativas, em especial do diálogo entre o Marco Civil da Internet (Lei 12.965/2014) e o Código de Defesa do Consumidor, Lei

8.078/1990. O foco especial é o direito básico do consumidor à proteção de dados pessoais na internet, a exigência do consentimento e suas exceções e a necessária boa-fé objetiva, para a realização das expectativas legítimas do consumidor e o combate aos riscos do tratamento de dados pessoais. O texto analisa os procedimentos para a garantia do direito básico do consumidor à proteção de dados pessoais na internet, a sua fiscalização prevista e a possibilidade de aplicação de sanções e reparação, assim como casos, em especial o dos cookies e da publicidade comportamental.

Abstract:

The text deals with the sources as simultaneous application model of normative sources dialogue, especially the dialogue between the Civil Marco Internet (Law 12.965/2014) and the Código de Defesa do Consumidor, Law 8.078/1990. The special focus is the basic consumer rights the protection of personal data on the internet, the requirement of consent and its exceptions and the necessary objective good faith, for the realization of consumer legitimate expectations and the fight against the processing of personal data risks. The text analyzes the procedures to guarantee the basic consumer's right to protection of personal data on the Internet, its planned inspection and the possibility of sanctions and repair, as well as cases, especially cookies and behavioral advertising.

Palavra Chave: Internet - Proteção de Dados Pessoais - Diálogo das Fontes - Marco Civil da Internet - Código de Defesa do Consumidor
Keywords: Internet - Data Protection - Dialogue Des Sources - Framework Internet Act - Consumer Protection Code

1. Introdução

Este artigo[1] propõe-se a estabelecer um diálogo entre o Marco Civil da internet (Lei 12.965/2014) e o Código de Defesa do Consumidor (Lei 8.078/1990), de modo a garantir a privacidade e a proteção dos dados pessoais dos consumidores no ambiente virtual. Como se verá a seguir, uma interpretação sistemática à luz do diálogo das fontes permite extrair um direito básico do consumidor à proteção de dados pessoais na internet. Analisaremos os principais dispositivos legais tanto do Código de Defesa do Consumidor quanto do Marco Civil da Internet relativos à privacidade, com vistas a demonstrar como se conforma esse direito básico do consumidor, quais são os seus limites e quais os procedimentos existentes para a sua proteção.

Com a entrada em vigor da Lei 12.965/2014, no dia 23.06.2014, o Brasil passou a contar um marco jurídico atual e avançado sobre os princípios, direitos e obrigações para o uso da internet.[2] O texto aprovado pelo Congresso apresenta diferenças significativas em relação à proposta inicial do Executivo. Uma das diferenças mais evidentes é a quantidade e especificidade de normas relacionadas à privacidade e à proteção de dados presentes no texto final, que não constavam da proposta inicial. Enquanto a primeira versão trazia o direito à privacidade como princípio e regra geral da disciplina do uso da internet no país, a Lei 12.965/2014 acabou por disciplinar de forma bastante específica a proteção de dados na internet, estabelecendo normas sobre danos morais e materiais em caso de violação da intimidade e vida privada (art. 7.°, I), a inviolabilidade e sigilo do fluxo de comunicações e das comunicações privadas armazenadas (art. 7.°, II e III), o direito ao não fornecimento a terceiros de dados pessoais salvo mediante consentimento do usuário (art. 7.°, VII), a exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet (art. 7.°, X), a publicidade e clareza de eventuais políticas de uso dos provedores de conexão e de aplicações (art. 7.°, XI), entre outras.

Com essas normas, o Marco Civil da Internet tornou-se a Lei com o conjunto mais moderno e completo de normas de proteção de dados no país, ajudando a suprir, em alguma medida, a lacuna da ausência de uma lei geral de proteção de dados no Brasil.[3] Embora não seja fácil precisar os motivos que ensejaram a inserção desses dispositivos no texto final da Lei, é possível supor que os escândalos relativos à espionagem da internet e dos meios de comunicação, que atingiram a Agência Nacional de Segurança dos EUA em 2013, expuseram de forma inédita os riscos a que os cidadãos estão submetidos na era da informação, o que acabou contribuindo também para a repercussão no Brasil acerca dos perigos da violação à privacidade e dos dados pessoais em um mundo conectado em rede.[4]

Acertou o Legislador ao estabelecer um regime jurídico de proteção de dados pessoais no âmbito da regulamentação do uso da internet no país. Tendo em vista que a internet constitui um ambiente de exercício de diversos direitos fundamentais[5] – como, por exemplo, o direito à liberdade de expressão, associação, informação, comunicação e profissão – a proteção da privacidade e dos dados pessoais apresenta-se como um pressuposto para o exercício desses direitos. Afinal, para que o usuário possa se comunicar e se expressar livremente, é preciso que ele confie na funcionalidade e na segurança da estrutura da rede, ou seja, que ele confie que o seu ambiente de navegação está livre de vigilância e interceptações.[6] Ao contrário, se o usuário acreditar que seus dados e informações de navegação poderão ser utilizados para fins alheios às suas expectativas ou de forma a prejudicá-lo no futuro, ele não agirá livremente no ambiente virtual nem compartilhará as suas ideias com liberdade.

A importância da confiança do usuário na infraestrutura de comunicação e informação foi destacada na inovadora decisão da Corte Constitucional alemã a respeito de monitoramento *online* de sistemas informáticos pelos órgãos de segurança (BVerfGE 120, 274, *Online Durchsuchung* – Monitoramento eletrônico). Em vez de aplicar o direito à autodeterminação informativa,[7] a Corte extraiu do direito geral à personalidade (Art. 2, I, c/c Art. 1, I, da Lei Fundamental alemã) um direito à garantia da confidencialidade e da integridade dos sistemas informáticos (*Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).[8] Esse direito, que ficou conhecido na opinião pública alemã como "direito fundamental informático" (*Computergrundrecht*)[9], exige que qualquer monitoramento policial dos sistemas informáticos pessoais (como computador pessoal, smartphones ou agendas eletrônicas) somente possa ser realizado se houver uma base legal específica, uma autorização judicial e a identificação de um perigo concreto a um bem jurídico fundamental, como a vida e a liberdade individuais ou a segurança da coletividade. A inovação da decisão reside no fato de que o objeto da proteção constitucional passa a ser o próprio sistema informático pessoal e, por consequência, o indivíduo que o utiliza.[10] Como principal fundamento do acórdão, consta a proteção da confiança do usuário no funcionamento adequado dos sistemas informáticos: dado que o ambiente virtual é caracterizado pela impossibilidade de controle do fluxo de dados pessoais pelo usuário, este precisa confiar na funcionalidade do sistema e no fato de que as suas informações serão tratadas de forma confidencial e segura para que possa utilizar livremente o sistema e exercer os seus direitos fundamentais por meio dele.

2. Diálogo das fontes como modelo de aplicação simultânea de fontes normativas

A análise do regime jurídico do tratamento de dados pessoais dos usuários da internet exige, além da interpretação da Lei 12.965/2014, a interpretação do Código de Defesa do Consumidor – CDC, também aplicável ao espaço virtual.[11] O âmbito de aplicação do CDC é definido em seu art. 3.°, § 2.°, segundo o qual o Código é aplicável aos serviços fornecidos no mercado de consumo mediante remuneração. Esse conceito abrange as transações realizadas pela internet, incluindo aquelas que não acarretam diretamente ônus aos usuários. Conforme interpretação dominante da jurisprudência, um serviço pode ser oferecido gratuitamente ao consumidor e, ainda assim, ser considerado remunerado, tendo em vista que obtém ganhos indiretos.[12] É o que ocorre com diversos serviços e aplicações na internet, que, embora aparentemente gratuitos, se remuneram por meio de publicidade e da comercialização dos dados de navegação do usuário.

O Código de Defesa do Consumidor foi um dos precursores na previsão de normas sobre proteção de dados pessoais no ordenamento jurídico brasileiro, como se percebe a partir de seu art. 43. Este inovou na forma de regulamentação dos cadastros e bancos de dados de consumo no Brasil, permitindo o funcionamento desses bancos de dados dentro de parâmetros legais claros. Para além dessa norma, o Código estabelece princípios que devem nortear as ações de todos os atores das relações de consumo, tais como o reconhecimento da vulnerabilidade do consumidor (art. 4.º, I), a garantia de serviços e produtos com padrões com qualidade, segurança, durabilidade e desempenho (art. 4.º, II, *d*), o respeito à boa-fé objetiva (art. 4.°, III) e o incentivo à criação pelos fornecedores de meios eficientes de solução de conflitos (art. 4.º, V). Podem-se citar também os direitos básicos previstos no Código, como a proteção da vida, saúde e segurança (art. 6.º, I), a informação adequada e clara sobre os diferentes produtos e serviços (art. 6.°, III), a proteção contra práticas abusivas (art. 6.º, IV), a efetiva prevenção e reparação de danos morais (art. 6.º, VI), bem como o acesso aos órgãos

judiciários e administrativos (art. 6.º, VII).

Nota-se, assim, que o Código de Defesa do Consumidor estabelece uma proteção integral da pessoa nas relações de consumo, seja dos seus interesses econômicos, seja da sua integridade e personalidade. Ademais, o caráter principiológico das suas normas tem se mostrado aberto o suficiente para oferecer soluções para os novos conflitos relacionados à tecnologia da informação. O papel central que o Código de Defesa do Consumidor exerce para a proteção da pessoa no ordenamento jurídico brasileiro, para além do mero funcionamento adequado do mercado, pode ser explicado em razão da sua origem e de sua vinculação constitucional (art. 5.°, XXXII e 170, V, da Constituição Federal e art. 48 de suas Disposições Transitórias). De especial importância se reveste, no contexto da sociedade da informação, o art. 5.°, XXXII, que determina que "o Estado promoverá, na forma da lei, a defesa do consumidor". Essa norma expressa um dever de proteção (*Schutzpflicht*),[13] que é direcionada ao Estado como um todo – aos poderes Executivo, Legislativo e Judiciário.[14] O dever de proteção pode envolver, nesse contexto, várias dimensões: dever de interpretação conforme a Constituição, de modo a se levar em conta a vulnerabilidade do consumidor e a sua necessidade de proteção; dever de atuação administrativa para a proteção do consumidor; dever de desenvolvimento de uma arquitetura regulatória para a efetividade dessa proteção.

Ao tratarmos do processamento de dados pessoais do consumidor na internet, são aplicáveis, portanto, tanto o Marco Civil como o Código de Defesa do Consumidor. Destaca-se que não se trata de um conflito entre legislações, a ser resolvido pelas regras de conflitos de leis no tempo, mas da aplicação simultânea de ambas as leis. Por isso, estamos a falar de um caso de diálogo das fontes, que constitui um modelo de aplicação simultânea de fontes normativas diversas, adequado aos atuais fenômenos jurídicos complexos, não mais passíveis de serem resolvidos à luz dos conceitos de ab-rogação, derrogação e revogação. Conforme explicado por Claudia Lima Marques, o diálogo das fontes é "a atual aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o Código de Defesa do Consumidor, a lei de seguro-saúde) e gerais (como o CC/2002), com campos de aplicação convergentes, mas não mais iguais."[15]

3. O direito básico do consumidor à proteção de dados pessoais na internet

Por meio da aplicação simultânea do Código de Defesa do Consumidor e do Marco Civil da Internet ao tratamento de dados pessoais dos consumidores no ambiente virtual, é possível se extrair um direito básico do consumidor à proteção de dados pessoais, como se verá a seguir. Este nada mais é que o reflexo, no âmbito infraconstitucional, do direito fundamental à inviolabilidade da intimidade e da vida privada (art. 5.°, X), na sua dimensão da proteção de dados pessoais.[16] Afinal, como previsto pelo próprio art. 7.° do CDC, o catálogo de direitos básicos do consumidor não é *numerus clausus*, possibilitando o reconhecimento de outros direitos "decorrentes de tratados ou convenções internacionais 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 equidade."

Ademais, o Marco Civil também traz um catálogo de direitos do usuário relacionados à privacidade e à proteção de dados (art. 7.°, I, II, III, VI, VII, IX, X e XI), que, interpretados em conjunto com os direitos do consumidor, acabam por formar um imponente arsenal de proteção da privacidade e dos dados pessoais do consumidor na internet. Por meio de uma interpretação sistemática dessas normas, buscar-se-á delinear os contornos iniciais de um direito básico do consumidor à proteção de dados pessoais.

Como ponto de partida, tem-se que o direito básico do consumidor à proteção de dados pessoais envolve uma dupla dimensão: (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade.

Como se percebe, o conceito elaborado envolve tanto um aspecto subjetivo (controle dos dados pessoais pelo próprio consumidor) quanto um aspecto objetivo (proteção contra os riscos causados pelo tratamento de dados pessoais). A importância das duas dimensões é fundamental para possibilitar a autodeterminação informativa do consumidor, ao mesmo tempo que propicia um controle objetivo de legitimidade do

tratamento de dados pessoais. Esse controle objetivo torna-se ainda mais relevante no mercado de consumo, em que a discrepância de poderes e de informação entre consumidores e fornecedores é tão grande que dificulta ao consumidor a tomada de decisão livre e informada a respeito do fluxo de seus dados.[17] Não obstante, tal conceito não reduz a autonomia do consumidor no controle de seus dados; ao contrário, trata-se de garantir a sua liberdade material e não meramente formal, a partir da verificação do respeito à boa-fé objetiva e às suas legítimas expectativas.

3.1. A exigência do consentimento e suas exceções

A autorização pelo consumidor, como regra geral, é um pressuposto essencial para ao tratamento de dados pessoais nas relações de consumo, inclusive aquelas desenvolvidas no ambiente virtual. Afinal, se os dados pessoais referem-se ao seu titular e o representam, afetando a sua personalidade, somente ele pode decidir a respeito do fluxo desses dados, salvo em casos excepcionais ou expressa previsão legal. Tal conceito, que já podia ser extraído do Código de Defesa do Consumidor, tornou-se requisito expresso a partir da promulgação do Marco Civil.

Trata-se da concretização do princípio da liberdade de escolha do consumidor (art. 6.°, II, CDC). A regra do consentimento está prevista no art. 7.°, VII e IX, do Marco Civil da Internet. Enquanto o inc. VII condiciona o fornecimento a terceiros dos dados pessoais ao consentimento livre, expresso e informado do usuário, salvo em caso de previsão legal, o inc. IX estabelece norma geral acerca do consentimento em caso de coleta, uso, armazenamento e tratamento de dados pessoais, prevendo ainda que o consentimento deve constar de cláusula destacada.

Essa regra básica para a legitimidade do tratamento de dados pessoais também está presente na Lei federal de proteção de dados alemã, que determina que a coleta, o processamento e a utilização de dados pessoais somente são *permitidos se autorizados por lei ou consentidos pelo titular (§ 4, 1, BDSG).*

Para que o consentimento constitua a real manifestação de vontade do consumidor de submeter os seus dados pessoais a tratamento, ele tem que atender a determinados requisitos. Assim, entende-se que o consentimento somente é válido se for *expresso, livre, específico e informado.*

Nesse sentido, cabe aqui o questionamento sobre qual a forma que o consentimento deve assumir: se o modelo *opt out*, que pressupõe o consentimento do titular se este não se manifestar de forma contrária ou o modelo *opt in,* que exige uma postura ativa da pessoa, declarando a sua vontade de realizar o tratamento de dados. Como visto acima, um dos requisitos para a validade do consentimento é que ele seja expresso. Isso implica a necessidade de que a declaração de vontade seja manifesta e clara, não podendo ser oculta, subentendida ou implícita. Dessa forma, compreendemos que, em regra, somente o modelo de consentimento *opt in* confere validade ao consentimento e torna legítimo o tratamento de dados.[18]

Como exemplo, entende-se que caixas previamente assinaladas em uma página na internet, configurações de browser que são instaladas por *default*, ou cláusula de autorização em contrato de adesão sem o devido destaque não constituem um consentimento válido. Já uma assinatura adicional em um contrato acerca da autorização do processamento de dados pode ser considerada uma manifestação de vontade clara. Como destacado no parecer do "Grupo de Trabalho do art. 29",[19] o consentimento válido pressupõe uma manifestação de vontade, isto é, uma indicação, uma ação no sentido de consentir, o que dificilmente poderia ser pressuposto de uma inação ou da ausência de comportamento.[20]

O modelo *opt out* não se coaduna, a princípio, com o requisito do *consentimento expresso* e pode ser considerado legítimo apenas em casos excepcionais, quando o tratamento de dados não acarretar riscos à personalidade do consumidor e se o sistema de *opt out* disponibilizado for realmente efetivo para a proteção da personalidade consumidor. Além disso, para que o sistema *opt out* seja considerado legítimo, ele precisa se fundar numa relação entre empresa e cliente já existente, a partir da qual o consumidor tenha fornecido voluntariamente os seus dados e, portanto, pode ter a expectativa de receber, eventualmente, ofertas publicitárias dessa empresa.[21] Assim, por exemplo, poder-se-ia considerar legítimo o envio de e-mails para

fins de marketing direto por uma empresa aos seus próprios clientes, se a empresa disponibilizasse um meio eficiente, único e sem ônus de recusar o recebimento desses e-mails.

Ademais, o consentimento somente é valido se o consumidor tiver sido informado de todas as condições do tratamento de dados: quem é o responsável, qual a finalidade do tratamento, como os dados serão usados etc. O Marco Civil estabelece normas relevantes sobre o dever de informação, que acabam por condicionar a validade do consentimento: o art. 7.°, VI trata das informações que devem ser prestadas acerca do regime de proteção aos registros de conexão e aos registros de acesso, enquanto o art. 7.°, VIII prevê um direito geral do usuário de obter informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos seus dados pessoais.

Por fim, o consentimento também precisa ser específico, isto é, precisa indicar exatamente o propósito do processamento de dados. Assim, um *cheque em branco* não atende aos requisitos de validade do consentimento.[22] Tampouco é válido o consentimento dado pelo consumidor, com base em informações enganosas veiculadas pelo fornecedor, nos termo do art. 37, § 1.° do Código de Defesa do Consumidor.

Não sendo consentido pelo consumidor, o tratamento de dados somente pode ser considerado legítimo em casos excepcionais, isto é: a) se o tratamento de dados for indispensável para o cumprimento da finalidade contrato; ou b) for necessário para a execução de obrigação legal do fornecedor.

A execução de um contrato fundamenta a coleta ou o processamento de informações pessoais, sem as quais não seria possível executar o negócio jurídico acordado pelas partes. Um caso bastante evidente consiste, por exemplo, na necessidade de uma empresa do ramo de comércio eletrônico de obter os dados do cartão de crédito para a efetuação do pagamento e do endereço do consumidor para a entrega do produto; sem esses dados, não seria possível cumprir com o contrato de compra e venda acordado, hipótese na qual resta a clara a necessidade de seu processamento.

A execução de obrigação legal do fornecedor também constitui fundamento legítimo para o tratamento de dados pessoais sem o consentimento do consumidor. É o caso, por exemplo, do requerimento de dados pessoais dos consumidores por autoridades policiais para a investigação de crimes. Nesse caso, entende-se que o fornecedor deve providenciar o acesso aos dados, na extensão do fundamento legal. Ressalta-se que em alguns casos pode ser necessário, além do fundamento legal, também a ordem judicial circunstanciada, conforme determina o art. 5.°, XII da Constituição Federal e a Lei 9.296/1996.

3.2. A boa-fé objetiva, as expectativas legítimas do consumidor e os riscos do tratamento de dados pessoais

Além do consentimento ou outro fundamento legítimo para o tratamento de dados, a análise da legitimidade do tratamento de dados deve levar em conta a boa-fé objetiva, as expectativas legítimas do consumidor, bem como os impactos e os riscos do tratamento de dados pessoais para o consumidor.

A boa-fé pode ser entendida, nas palavras de Claudia Lima Marques, como "uma atuação refletida, uma atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando os seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, cooperando para atingir o bom fim das obrigações (...)".[23] A boa-fé objetiva foi positivada no Código de Defesa do Consumidor em seu art. 4.°, III, como guia hermenêutico e em seu art. 51, IV, como cláusula geral.[24] Tem especial relevância no processamento de dados pessoais do consumidor a boa-fé, na sua função limitadora[25], que restringe a liberdade de conduta das partes, ao considerar certas práticas e cláusulas como abusivas. A abusividade, nesse sentido, independe do consentimento do consumidor, pois a boa-fé impõe uma regra de conduta[26] e um *standard* objetivo, de cunho imperativo e não dispositivo.

Como afirma Stefan Grundmann, uma das principais tendências do direito contratual moderno é a "otimização da liberdade por meio do fortalecimento de *standards* protetivos", o que denota a tendência atual de se buscar mais liberdade material para ambas as partes contratuais, em detrimento de um conceito exclusivamente formal de liberdade contratual.[27] Esse fenômeno, também conhecido como a materialização

do direito privado[28], tem sido realizado por meio de importantes instrumentos normativos, dentre eles, a concretização do princípio da boa-fé.

Nesse contexto, vale mencionar o caso *Sears*, investigado pela *Federal Trade Comission*[29], que suscitou o debate sobre os limites do consentimento no tratamento de dados pessoais. No caso, a empresa foi investigada por suspeita de violação à privacidade, em razão da prática de oferecer US$ 10,00 aos consumidores que visitassem o site da empresa e permitissem a instalação de um "*software* de pesquisa", que iria analisar a navegação *online* do consumidor.[30] A publicidade da prática envolvia termos como "participe de interações emocionantes – sempre nos seus termos e de acordo com a sua escolha".[31] Ocorre que o *software*, na realidade, possibilitava um vasto grau de monitoramento dos hábitos dos consumidor relacionados à navegação na internet, inclusive de *sites* criptografados, abrangendo desde extratos bancários *online*, registros de remédios, registros de aluguel de vídeo, históricos de empréstimo de biblioteca até dados relativos ao e-mail do consumidor. A *Federal Trade Comission* entendeu serem insuficientes as informações fornecidas ao consumidor a respeito da extensão do monitoramento, pois elas eram veiculadas apenas no meio de um longo termo de licença, ao qual os consumidores só conseguiam acesso depois de um complicado processo de registro.[32] Um acordo foi fechado em 2009 com a empresa, que previu a destruição de todos os registros armazenados e a comunicação aos consumidores sobre como desinstalar o referido *software*.[33]

Entendemos que o enfoque com base na boa-fé objetiva poderia contribuir para análise desse caso. Afinal, a forma em que a empresa optou para coletar os hábitos do consumidor foi extremamente invasiva e não parece ter cumprido, em absoluto, com os requisitos de uma conduta leal, sem abuso e sem a busca de vantagens indevidas. Ademais, em nenhum momento parece ter sido levado em conta os riscos de um monitoramento tão completo da vida do consumidor, nem tampouco o seus interesses legítimos. Por fim, o conteúdo enganoso da publicidade indica uma tentativa ardilosa de obter o consentimento do consumidor, contrariando claramente o princípio da boa-fé objetiva.

Também o princípio da proteção das legítimas expectativas do consumidor tem um importante papel no processamento de dados pessoais no âmbito de uma relação de consumo. Esse princípio, considerado como parte da teoria da confiança, busca proteger as "expectativas legítimas que nasceram no outro contratante, que confiou na postura, nas obrigações assumidas e no vínculo criado através da declaração do parceiro."[34] A sua positivação deu-se, por exemplo, na normas relativas à responsabilidade pelo fato do produto e do serviço, especificamente na qualificação do defeito (art. 12, § 1.°, e art. 14, § 1.°). Assim, percebe-se que o Código relaciona a reparação dos danos causados ao consumidor por produto ou serviço com a "segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I – o modo de seu fornecimento; II – o resultado e os riscos que razoavelmente dele se esperam; III – a época em que foi fornecido" (art. 14, § 1.°, CDC).

Dessa forma, importante critério de análise da violação de privacidade é a expectativa de privacidade do indivíduo em uma situação concreta.[35] Afinal, é de se levar em conta, na análise de uma eventual violação desse direito, se se trata, por exemplo, de monitoramento de e-mails, em que há grande expectativa de confidencialidade de seu conteúdo, ou da coleta de dados postados em uma rede social. No caso das redes sociais, não há uma expectativa do consumidor de confidencialidade em relação àqueles dados; há, contudo, uma expectativa de que os dados não sejam utilizados em contexto completamente diverso daquele em que ele foi gerado.[36]

Por fim, outro critério essencial para o avalição da legitimidade do tratamento de dados pessoais é o exame do impacto e dos riscos para o consumidor decorrentes do tratamento de dados. Afinal, se um dos objetivos principais do direito básico à proteção de dados é exatamente a proteção contra os riscos advindos do processamento de informações, é preciso verificar quais são os efeitos de um determinado tratamento de dados para que se avalie a sua legitimidade ou não. Assim, é possível afirmar que se o processamento de dados ocasionar um efeito tido como ilícito pelo ordenamento jurídico, ele será claramente ilegítimo.

Esse é o caso do processamento de dados pessoais cujo efeito é a discriminação do consumidor do mercado; esse processamento será considerado ilegítimo, independentemente do consentimento do consumidor, por

ferir não apenas o direito à proteção de dados, mas, especialmente, o princípio da igualdade, protegido constitucionalmente[37]. Um exemplo é a discriminação racial realizada com base em dados pessoais, também denominada de *racial profiling*, em que um fornecedor realiza cadastros de seus consumidores com base em perfis étnicos ou raciais e oferece vantagens para um determinado grupo em detrimento de outro.[38]

Novas formas de discriminação passam a ser possíveis a partir da associação entre tecnologias da informação e o armazenamento de enormes quantidades de dados pessoais, fenômeno também conhecido como *Big Data*[39]. É o caso, por exemplo, da discriminação estatística[40], segundo a qual grupos de consumidores recebem tratamentos diferenciados (preços ou condições de contratação diferentes), em razão de atributos aparentemente inofensivos, como idade, gênero, nacionalidade ou endereço. Essa prática se baseia em informações estatísticas, que associam esses atributos a outras características, cuja identificação pelo fornecedor é mais difícil, como nível de renda, risco de inadimplência etc.O principal problema da discriminação estatística é a atribuição de uma suposta característica do grupo ao indivíduo, sem levar em conta as suas caraterísticas e condições individuais.[41]Isto é, muitas vezes a justiça do caso individual fica prejudicada a partir de um resultado meramente probabilístico, segundo o qual um percentual de determinado grupo de pessoas agiria de determinada maneira.

Dessa forma, constata-se que o tratamento de dados pessoais pode ser considerado ilegítimo em razão dos efeitos negativos causados ao consumidor, tais como os riscos de discriminação e estigmatização. Como a conduta discriminatória é ilícita *a priori*, a constatação de sua ilegitimidade independe de eventual consentimento do consumidor, pois este não tem o condão de transformar a conduta ilícita em lícita.

3.3. Procedimentos para a garantia do direito básico do consumidor à proteção de dados pessoais na internet

Os procedimentos para a garantia do direito básico de proteção de dados, que podem ser encontrados nas mais diversas legislações nacionais, tratados internacionais e instrumentos regionais, são conhecidos também como *Fair Information Principles*. No Brasil, esses procedimentos estão positivados em normas esparsas, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Cadastro Positivo (Lei 12.414/2011) e a Lei de Acesso à Informação (Lei 12.527/2011). Os principais procedimentos que devem ser garantidos são os seguintes:

i)Transparência:

Todo o tratamento de dados pessoais tem como pressuposto a sua completa transparência em relação a quem são os responsáveis e os gestores do tratamento, qual a sua finalidade, qual é a utilização dos dados e que tipos de dados são processados etc. Sem a devida transparência, torna-se impossível qualquer tipo de controle pelo titular do fluxo de seus dados, assim como qualquer fiscalização pelos órgãos de controle.

Isso envolve, com base no art. 6.°, III, do CDC, o direito do consumidor de ser informado sobre: i) quais os dados pessoais são tratados e para quais finalidades; ii) se os dados pessoais são transmitidos para terceiros; iii) para quais países os dados pessoais são transmitidos, se for o caso; iv) qual é o período de conservação de dados; e v) quais os mecanismos de segurança utilizados para garantir a segurança dos dados pessoais. Afinal, como determina o art. 46 do CDC, "os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo (...)". Ademais, na hipótese de oferta de serviços e produtos, é possível se extrair o dever de que a informação seja fornecida de forma correta, clara, precisa, ostensiva e em língua portuguesa (art. 31, CDC).

Há importantes normas no Marco Civil da Internet que visam garantir a transparência do processamento de dados. Destaca-se o inc. VIII do art. 7.°, que instituiu um direito do usuário – bastante abrangente e geral – a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais. O inc. VI do mesmo dispositivo trata das informações que devem constar dos contratos de prestação de serviços, explicitando que deve haver nesses contratos o "detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de

gerenciamento da rede que possam afetar sua qualidade". Já o art. 7.°, XI, aborda a questão das políticas de uso dos provedores de conexão e de aplicações de internet e estabelece a obrigação de clareza e publicidade das eventuais políticas de uso existentes.

Assim, a partir do art. 7.°, VI, VIII e XI, do Marco Civil, e do art. 6.°, III, do CDC, resta claro que os fornecedores que realizam o tratamento de dados pessoais por meio da internet devem divulgar nas suas respectivas páginas – de forma clara e completa – informações a respeito da coleta, uso, armazenamento e tratamento de dados pessoais dos seus usuários. A forma de divulgação dessas informações pode variar conforme o caso: seja por meio das políticas de privacidade, seja pelos contratos de prestação de serviço publicados nos *sites* dos provedores ou mesmo por meio de informações específicas fornecidas ao consumidor antes da obtenção do consentimento do consumidor, o importante é que o processamento de dados pessoais seja realizado de forma transparente e que o consumidor seja informado de forma clara e precisa, especialmente, sobre os tipos de dados coletados, quais as finalidades da coleta e do uso de dados pessoais, se há acesso de terceiros a esses dados e quais as medidas de segurança adotadas.

ii) Tratamento de dados compatível com a finalidade da coleta:

Todo tratamento de dados pessoais deve respeitar o contexto no qual os dados foram coletados. Assim, as informações pessoais não podem ser utilizadas para finalidade incompatível com aquela para a qual foram coletadas. Esse princípio, como visto, é um dos conceitos fundamentais da proteção de dados, que visa assegurar que os dados pessoais não sejam descontextualizados, provocando riscos e danos ao consumidor. O princípio da finalidade foi positivado pela Lei do Cadastro Positivo (art. 5.°, VII), mas já estava implícito no Código de Defesa do Consumidor, conforme afirma Ana Paula Gambogi Carvalho.[42]

Com o advento do Marco Civil da Internet, o ordenamento jurídico brasileiro passou a contar com norma ainda mais específica e completa acerca do princípio da finalidade, estabelecida em seu art. 7.°, VIII. Este determina que os dados pessoais somente poderão ser usados para as finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e que estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. O art. 16, II, do Marco Civil remete novamente ao princípio da finalidade e prevê que "na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular."

iii) Garantia dos direitos de acesso, retificação e cancelamento:

O titular deve ter livre acesso aos seus dados (direito de acesso), deve poder corrigir dados equivocados e desatualizados (direito de retificação) e deve poder cancelar dados que foram indevidamente armazenados ou cujo consentimento tenha sido revogado por ele (direito de cancelamento). Esses direitos, que podem ser extraídos do art. 43 do CDC, são essenciais para fazer valer o direito básico do consumidor à proteção de dados pessoais.

Pressuposto do sistema de proteção de dados pessoais, baseado no controle dos dados pessoais por seu titular, é que ele possa revogar o seu consentimento a qualquer momento. Afinal, se o início do tratamento de dados depende de sua autorização, é natural que ele possa determinar o fim do tratamento de dados, fazendo valer a sua autodeterminação informacional. Exemplo de revogação do consentimento é o caso do usuário da internet que deseja encerrar o seu perfil na rede social, com o cancelamento de todos os seus dados pessoais armazenados durante o período de utilização desse serviço. É fundamental que essa opção lhe seja assegurada de forma simples e sem ônus, sob pena de violar o seu direito básico à proteção de dados pessoais. É o que determina o art. 7.°, X, do Marco Civil da Internet, que prevê o direito à "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

iv) Proteção dos dados sensíveis:

Os dados sensíveis, entendidos como aqueles capazes de gerar a discriminação do consumidor, exigem, além

do consentimento específico do consumidor, a adoção pelo fornecedor de mecanismos adicionais de segurança. São exemplos de dados sensíveis os referentes à origem racial ou étnica, às convicções religiosas, filosóficas ou políticas, à saúde e à vida sexual, bem como os dados genéticos e biométricos. Como visto acima, o tratamento de dados sensíveis para fins discriminatórios é vedado pelo ordenamento jurídico, independentemente do consentimento do consumidor.

v) Segurança dos dados pessoais:

A segurança dos dados pessoais é aspecto essencial no âmbito da garantia do direito básico à proteção de dados e impõe ao responsável a adoção de medidas técnicas e organizatórias adequadas para atender a esse fim. Especialmente no mundo digital, ampliam-se enormemente os riscos de destruição, alteração, divulgação e acesso indevido dos dados pessoais, em razão da estrutura aberta da internet.

Da responsabilidade objetiva do fornecedor, estabelecida no art. 14 do CDC, extrai-se a obrigação do fornecedor de propiciar a segurança adequada e suficiente aos bancos de dados e cadastros sob a sua responsabilidade, sob pena de responder pelos danos materiais e morais oriundos da falha de segurança (art. 6.°, VI, CDC). Assim, decorre do risco da atividade de processamento de dados pessoais o dever do fornecedor de manter sistemas seguros, que protejam os dados pessoais em relação a sua confidencialidade, integridade e disponibilidade. Esses são os objetivos clássicos da segurança da informação, conforme definido por normas técnicas internacionais.[43] Enquanto a confidencialidade refere-se à segurança dos dados contra o acesso não autorizado, a integridade diz respeito à proteção contra a manipulação dos dados e dos respectivos sistemas de informação.[44] Já a disponibilidade denota a necessidade de que os dados estejam acessíveis e visa à proteção contra a perda dos dados.

As medidas a serem adotadas pelo fornecedor para atender a essas finalidades são extremamente diversas, mas podem incluir desde medidas técnicas, como a utilização da criptografia e antivírus, até medidas organizatórias e procedimentais, destinadas a impedir o acesso e a manipulação dos dados por terceiros não autorizados.

Como o Código de Defesa do Consumidor prevê a responsabilidade objetiva do fornecedor, não cabe a avaliação a respeito da ocorrência de culpa. Excludentes de responsabilidade previstos pelo Código de Defesa do Consumidor e pelo Código Civil são a culpa exclusiva da vítima ou de terceiro, bem como o caso fortuito ou força maior. Ocorre que, em geral, as ameaças de segurança aos sistemas de informação raramente se enquadram nessas categorias, na medida em que normalmente os eventos não são imprevisíveis, nem tampouco inevitáveis, pois decorrem, em geral, da utilização de sistemas antiquados de segurança ou fora dos padrões recomendados.[45] Assim, havendo uma relação do evento causador do dano com a atividade do fornecedor, fica mantido o nexo entre o dano e o defeito, persistindo, portanto, o dever de indenizar.[46]

Dessa forma, conclui-se que o fornecedor deve adotar todas as medidas técnicas e procedimentais necessárias para garantir a segurança dos dados pessoais processados, levando em conta, especialmente, a rápida evolução tecnológica e o surgimento de novos riscos e ameaças.

Caso ocorra um incidente de segurança, que possa acarretar riscos ao consumidor, como, por exemplo, o vazamento de dados pessoais de um sistema, faz-se necessária a aplicação das normas do art. 10, § 1.° e § 2.°, do CDC, que determinam a comunicação imediata do fato aos consumidores e aos órgãos competentes, por meio de anúncios publicitários. Esses dispositivos, que tratam do chamado *Recall*, também devem ser aplicados ao problema do vazamento de dados pessoais, na medida em que a comunicação de risco constitui aspecto essencial para que os consumidores afetados possam tomar as medidas de proteção adequadas em relação aos seus dados. Nesse sentido, é fundamental que a comunicação seja dirigida não apenas aos consumidores, mas também aos órgãos responsáveis, que, conforme o caso, podem ser os órgãos de defesa do consumidor nacional, estaduais ou municipais, bem como os órgãos reguladores setoriais. Essa comunicação de risco, também conhecida como *data breach notification*, demonstrou ser um mecanismo importante em caso de vazamento de dados pessoais, especialmente nos EUA, em que quase todos os Estados regulamentam

a matéria.[47]

Com o advento da Lei 12.965/2014, o tema da segurança da informação foi alçado a um dos princípios da regulamentação da internet no Brasil. É o que dispõe o art. 3.°, III, segundo o qual a "preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas" constitui um princípio da disciplina do uso da Internet no país. A referida lei também trata da segurança da rede em seu art. 9.°, § 2.°, ao abordar a questão da neutralidade de rede e da necessidade do responsável pela transmissão de informar os usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede, nas hipóteses de degradação do tráfico previstas legalmente. Por fim, o Marco Civil dispõe sobre o tema em caso de guarda e disponibilização de acesso dos registros de conexão e de acesso a aplicações de internet, nos seguintes termos: "§ 4.º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais".

Dessa forma, constata-se que o tema da segurança da informação não passou desapercebido pelo Legislador, ao estabelecer princípios e garantias para o uso da internet no país. Não obstante tal disciplina conta apenas com algumas normas bastante gerais, que carecem de regulamentação mais detalhada acerca da segurança da rede, especialmente, no que se refere a i) que padrões técnicos deverão ser seguidos pelos responsáveis pelo gerenciamento da rede; ii) quais órgãos ou entidades poderão fomentar a criação desses padrões e controlar a sua utilização; iii) que políticas devem ser adotadas para fomentar a educação e orientação do usuário em relação a práticas seguras de navegação. Essas são questões que poderiam ser abordadas na regulamentação do Marco Civil.

vi) Limitação temporal:

Fundamental para a efetivação do direito à proteção de dados pessoais é a determinação de um lapso temporal para o armazenamento, utilização e transferência de dados pessoais. Tal limitação é essencial para garantir que a pessoa não seja julgada eternamente com base em fatos e informações do passado ou desatualizadas. Nesse sentido, o Código de Defesa do Consumidor estabeleceu, em seu art. 43, § 1.°, o período máximo de cinco anos para o armazenamento de informações negativas. Já a Lei do Cadastro Positivo estabeleceu o prazo de 15 anos para o armazenamento de informações positivas, período que pode ser considerado preocupante, por ser demasiado longo.

Como regra geral – a ser aplicada também ao tratamento de dados pessoais na Internet – entende-se que os dados não devem ser armazenados por um período superior ao tempo necessário para atender a finalidade pela qual eles foram coletados. Ademais, uma avaliação de risco também é relevante para determinar o prazo limite de armazenamento e processamento. Isto é, quanto maior os riscos e a probabilidade de efeitos negativos para o consumidor, menor deve ser o tempo de armazenamento. Nesse sentido, é razoável que as informações sobre inadimplência possuam um prazo inferior de armazenamento que as informações positivas: afinal, os efeitos para o consumidor "com nome sujo" podem ser muito prejudiciais, não sendo razoável puni-lo por um tempo extremamente longo. Em relação às outras áreas das relações de consumo, para as quais não há norma específica, é fundamental destacar que nenhum tratamento de dados pessoais deve ser realizado por período indeterminado ou extremamente longo. É a avaliação do caso concreto que deverá indicar o período adequado de tratamento de dados, conforme os riscos, benefícios e a sensibilidade do tratamento.

3.4. Fiscalização, aplicação de sanções e reparação

Como se sabe, o Código de Defesa do Consumidor estabelece um amplo aparato administrativo para fiscalizar a aplicação de suas normas, com a previsão do Sistema Nacional de Defesa do Consumidor e de mecanismos para a realização da Política Nacional de Relações de Consumo. Ademais, ele estabelece, em seu cap. VII, uma série de sanções administrativas a serem aplicadas pelos órgãos municipais e estaduais de defesa do Consumidor (Procons) e pela Secretaria Nacional de Defesa do Consumidor.

O descumprimento do direito básico do consumidor à proteção de dados viola o Código de Defesa do Consumidor e pode ser qualificado como prática abusiva, ensejando a atuação dos órgãos estatais de defesa do consumidor, em todos os níveis da Federação, de modo a fiscalizar e aplicar as sanções administrativas adequadas, nos termos dos arts. 56 e 57 do CDC.

Também o Marco Civil estabeleceu sanções administrativas em caso de violação da privacidade, da intimidade e do sigilo das comunicações privadas. É o que prevê o seu art. 12[48]:

"Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III – suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no País."

Além do controle administrativo, o Código de Defesa do Consumidor estabelece medidas penais, em seus art. 72 e 73, em relação às condutas, respectivamente, de "impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros" e de "deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata".

Por fim, é de se ressaltar que existe um importante sistema de reparação de danos previsto no Código de Defesa do Consumidor. Conforme determina o seu art. 6.°, VI, é direito do consumidor a "efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos". Aliado à interpretação do art. 12 do CDC, vê-se que o Código traz um verdadeiro sistema objetivo de reparação integral de danos. A violação do direito à proteção de dados pode gerar tanto dano patrimonial quanto um dano moral. O dano patrimonial pode ocorrer, por exemplo, se o armazenamento de dados pessoais incorretos ensejar a contratação de um crédito mais caro pelo consumidor. Já o dano moral configura-se com a simples violação do direito à personalidade, isto é, comprovada a violação dos dados pessoais do consumidor, sem o seu consentimento ou base legal, cabe a reparação dos danos morais. Não é o elemento subjetivo – dor, vexame ou humilhação – que configura o dano moral, mas o elemento objetivo – interesse lesado[49]. Ressalta-se que também o Marco Civil da Internet previu, em seu art. 7.°, I, a indenização por danos morais ou materiais decorrente da violação da intimidade e da vida privada.

Cabe ao Poder Judiciário o importante papel de aplicar o direito à reparação do consumidor, calculando os danos patrimoniais e morais. Além disso, o Judiciário deve cumprir outra importante função, prevista no art. 51 do CDC: a declaração da nulidade das cláusulas abusivas nos contratos de consumo, que violem a privacidade do consumidor. Tendo em vista que as cláusulas enumeradas nesse dispositivo são apenas exemplificativas[50], é possível realizar um controle das cláusulas contratuais referentes à privacidade com base, especialmente, no art. 51, inc. IV, XV e § 1.°, isto é, se as cláusulas estabelecerem "obrigações iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada", forem "incompatíveis com a boa-fé" ou "estiverem em desacordo com o sistema de proteção ao consumidor".

Esse controle adquire ainda mais relevância diante das evidências de que as políticas de privacidade de algumas empresas estabelecem, na realidade, o contrário do que aparentam: são uma carta branca para o

fornecedor processar de forma ilimitada os dados pessoais dos consumidores. Ademais, a declaração de nulidade das cláusulas pelo Poder Judiciário poderia incentivar a melhoria das políticas de privacidade das empresas, prevenindo futuros danos aos consumidores.

O controle da abusividade das cláusulas contratuais em razão de violação da privacidade não é uma novidade. Na Alemanha, por exemplo, foi declarada em 1985 pelo Tribunal Federal Superior (*Bundesgerichtshof – BGH*), responsável pelas questões infraconstitucionais, a nulidade de cláusula de contrato de serviço financeiro, que possibilitava a transferência dos dados pessoais dos consumidores de forma geral e ilimitada para um serviço de proteção ao crédito (*Schufa*).[51] O fundamento da decisão consistia no fato de que a cláusula representava uma desvantagem exagerada (*unangemessene Benachteiligung*), contrariando a Lei relativa às condições gerais do contrato (*Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen – AGBG*[52]) à época vigente.

O Marco Civil da Internet trouxe importante aporte nessa seara, ao prever que são nulas de pleno direito as cláusulas contratuais que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas pela internet (art. 8.°, parágrafo único, I). A partir dessa norma, pode-se inferir que o legislador alçou o sigilo das comunicações a um patamar especial de proteção – em consonância com a forte proteção conferida à inviolabilidade das comunicações pela CF (art. 5.°, XII) – não permitindo a quebra desse sigilo mediante simples cláusula contratual. Esse dispositivo abre portas para um controle judicial de cláusulas contratuais dos serviços virtuais, nos moldes já previstos pelo art. 51 do CDC.

Deve-se ressaltar que, embora a declaração da nulidade de cláusulas contratuais seja de responsabilidade exclusiva do Poder Judiciário, isso não exclui a possibilidade de aplicação de sanções administrativas pelos órgãos de defesa do consumidor, em razão da utilização de cláusulas contratuais abusivas pelo fornecedor.

4. Análise de casos

Para demonstrar a aplicação do modelo de um direito à proteção de dados, extraído da interpretação simultânea do Marco Civil da Internet e do Código de Defesa do Consumidor, vale realizar uma análise de casos específicos de tratamento de dados pessoais no mundo digital, como os *cookies* e a publicidade comportamental.

4.1. Cookies

Os *cookies* são marcadores digitais, inseridos nos discos rígidos do computador do usuário de Internet pelos *websites* visitados, que permitem a identificação e o armazenamento da navegação do internauta.[53] Ao mesmo tempo que são úteis, por possibilitar a memorização de senhas e a personalização de serviços, os *cookies* podem trazer riscos à privacidade, quando o computador passa a ser associado a um determinado usuário, a partir dos dados pessoais fornecidos a um *site* ou por meio dos dados pessoais armazenados pelo provedor de conexão que possui um contrato de prestação de serviços com o usuário. Além disso, se armazenados por um longo período de tempo, esses marcadores podem rastrear o comportamento do usuário *online* em diversos *sites*.[54]

À luz do direito básico do consumidor à proteção de dados pessoais, é importante analisar quais os pressupostos de legitimidade para a utilização de *cookies*.[55] Partindo da condição de legitimidade do tratamento de dados pessoais nas relações de consumo, segundo a qual o processamento de dados pessoais deve ser autorizado pelo consumidor (art. 7.°, VII e IX, Marco Civil), ao menos que seja imprescindível para o cumprimento do contrato, é preciso analisar em que situações será exigido o consentimento pelo consumidor e em que situações o consentimento será dispensado.

Adaptado ao mundo virtual e baseado nas funções que os *cookies* podem exercer para facilitar a comunicação e a navegação, o pressuposto da necessidade da execução do contrato pode ser reinterpretado. Isto é, se o *cookie* for utilizado exclusivamente para a transmissão de comunicações na Internet ou for estritamente necessário para a realização de um serviço *online* solicitado pelo consumidor, não lhe

acarretando riscos, não será necessário o seu consentimento.[56]

Por outro lado, sempre que o *cookie* visar outras funções, será necessário a obtenção do consentimento prévio do consumidor.[57] Esse é o caso, por exemplo, dos *cookies* das redes sociais (*social plug-in tracking cookies*), que são capazes de monitorar tanto os membros como os não membros dessas redes.[58] Além disso, os *cookies* utilizados para realizar a publicidade comportamental (*third party advertising*) também não são isentos do consentimento, pois, ao visarem a coleta de dados pessoais para terceiros, naturalmente não são essenciais para a relação entre o usuário e o *site*.[59] Por isso, todos os *cookies* de terceiros exigem o consentimento prévio do consumidor, antes de serem instalados. Por fim, os *cookies* dos *sites* chamados de *first part analytics* também necessitam do prévio consentimento do consumidor. Esses *cookies* geralmente são usados pelos responsáveis dos *websites* para estimar o número de visitas ou para monitorar a navegação do usuário.[60]

Para passar pelo pressuposto objetivo de legitimidade, os *cookies*, em nenhum dos casos, podem apresentar graves riscos para o usuários. Isto é, em nenhuma hipótese é legítimo submeter o usuário a uma vigilância ininterrupta, transformando-o em mero objeto de monitoramento, o que, naturalmente, violaria o seu direito à intimidade e à vida privada e o princípio da dignidade, protegidos constitucionalmente. Além disso, em qualquer dos casos é preciso que seja divulgada por meio da política de privacidade ou no contrato de prestação de serviços da empresa publicado no *site* a forma de utilização dos *cookies* e para quais finalidades eles são instalados (7.°, VI, VIII e XI, Marco Civil, e art. 6.°, III do CDC).

4.2. Publicidade comportamental

A publicidade comportamental, também conhecida como *behavioral advertising*,[61] constitui um dos temas mais polêmicos no debate atual da proteção de dados pessoais. Afinal, o meio de personalizar a publicidade é o monitoramento das atividades *online* do consumidor, o que pode acarretar inúmeros riscos à sua personalidade, suscitando questionamentos em relação inclusive à eventual violação das garantias de sigilo constitucionais.

Sem a pretensão de esgotar o debate, é importante analisar, à luz dos conceitos expostos, quais seriam os pressupostos de legitimidade dessa atividade e em que momento ela deixa de ser legítima e passa a se caracterizar como prática abusiva.

Primeiramente, não há dúvida de que o pressuposto inicial de legitimidade da publicidade comportamental é o consentimento do consumidor, que deve ser informado, expresso, específico e anterior, nos moldes do sistema *opt in* (art. 7.°, VII e IX, Marco Civil e 6.°, II, CDC). Tendo em vista os riscos dessa atividade, não restam dúvidas de que um modelo de consentimento *opt out* não supriria em absoluto os seus requisitos de legitimação. Não obstante, outros critérios relacionados ao consentimento precisam ser observados para que essa prática seja tida como legítima: a) é preciso que o consentimento seja específico em relação a essa prática e se refira à autorização do monitoramento da sua navegação; assim, não basta o consumidor concordar com termos genéricos de navegação da página ou funcionamento do serviço; b) se a decisão do consumidor se basear em informações enganosas ou omissivas, o consentimento não será válido e a prática será considerada abusiva; c) se o consentimento for obtido a partir da veiculação de informações enganosas ou por meio de práticas abusivas (como, por exemplo, por meio da prática de requerer incessantemente o consentimento do consumidor a cada acesso ou não permitir que ele acesse outro *site* enquanto não consentir), ele será claramente inválido; o consentimento deve ser limitado a um curto período de tempo, devendo ser constantemente renovado; d) mecanismos de revogação do consentimento devem estar facilmente disponíveis ao consumidor.

Além disso, em razão dos riscos envolvidos, a prática somente poderá ser tida como legítima se outros procedimentos adicionais de segurança forem adotados pelo fornecedor ou responsável pelo tratamento de dados pessoais, tais como procedimentos de anonimização e pseudonimização (art. 3.°, V, Marco Civil e arts. 6.°, I , 8.°, 9.° e 10.°, CDC). É preciso, além do mais, que os mecanismos tecnológicos utilizados para a coleta de dados sejam os menos invasivos possíveis, de modo que as informações coletadas se resumam a

determinadas informações aptas a identificar hábitos dos consumidores, sem acarretar a vigilância completa da sua vida e da sua navegação. Medidas técnicas precisam ser adotadas também para impedir qualquer coleta de dados sensíveis, tais como os referentes à origem racial ou étnica, às convicções religiosas ou políticas e à saúde e à vida sexual (arts. 2.°, II, 7.°, VIII e 16, II, Marco Civil; arts. 4.°, III, 6.°, II, 51, IV e § 1.°, I, CDC).[62] Por fim, informações de *sites* seguros ou criptografados não podem ser coletadas, em nenhuma hipótese, sob pena de violação das garantias de sigilo constitucionais da comunicação de dados, telegráficas ou telefônicas ou das garantias de sigilo legais (como o sigilo bancário e médico). É o que prevê o art. 8.°, parágrafo único, I, do Marco Civil, segundo o qual as cláusulas que violem o sigilo às comunicações privadas são nulas de pleno direito. Além das medidas técnicas de segurança acima mencionadas, é preciso adotar medidas procedimentais, tais como a impossibilidade de reidentificação do consumidor.

Nesse sentido, considera-se muito preocupante algumas tendências de provedores de conexão à internet empregarem essas práticas para a realização da publicidade comportamental.[63] Afinal, como os provedores de conexão possuem um contrato de prestação de serviço com o consumidor, é impossível que o monitoramento seja realizado de forma anônima, pois o usuário poderá ser sempre identificado a partir de seu contrato ou assinatura. Outra preocupação que envolve a realização dessa prática pelos provedores de conexão diz respeito ao seu poder de mercado e à nítida posição de dependência do consumidor em relação a eles.[64] Ora, se os provedores de conexão são a porta de entrada do consumidor para a Internet, o monitoramento implicará a vigilância centralizada de toda a navegação do usuário, e não de apenas alguns *sites* ou serviços. Dessa forma, caso o provedor de conexão adote essas práticas, o consumidor não conseguirá ter certeza de que não está sendo monitorado, nem tampouco está em seu poder adotar alguma medida para reduzir esse risco, pois ele não tem outro meio de acesso à Internet. Assim, a posição de dependência do consumidor em relação ao seu provedor é enorme e a probabilidade de que ele mude de provedor são mínimas, tendo em vista a pouca competitividade do setor e as barreiras envolvidas (como os custos de cancelamento, por exemplo).[65]

Assim, conclui-se que, se a realização da prática de publicidade comportamental já suscita diversos questionamentos em relação à sua legitimidade, maiores ainda são as dúvidas quando essa prática é realizada pelos provedores de conexão. Afinal, ela parece contrariar os três critérios objetivos anteriormente mencionados: a boa-fé objetiva, as legítimas expectativas do consumidor e, especialmente, a proteção do consumidor contra os grandes impactos e riscos à sua personalidade, violando a equidade e a lealdade das relações de consumo.

5. Conclusão

Do exposto, viu-se que é possível por meio da aplicação simultânea do Código de Defesa do Consumidor e do Marco Civil da Internet extrair-se um direito básico do consumidor à proteção de dados pessoais na Internet. Objetivou-se, com isso, estabelecer uma dogmática de aplicação de ambas as leis para as hipóteses de tratamento de dados pessoais do consumidor no ambiente virtual. Para tanto, foram analisados os dispositivos de ambas as legislações relativas à privacidade, tais como normas sobre consentimento, direito à informação, segurança da informação, transparência e responsabilidade, entre outras. Ao final, foram analisados dois casos concretos – *cookies* e publicidade comportamental – evidenciando formas de garantir a privacidade e a proteção de dados nas relações de consumo à luz das novas perspectivas e desafios trazidos pela sociedade da informação.

6. Referências bibliográficas

BRITZ, Gabriele, Vertraulichkeit und Integrität Informationstechnischer Systeme – Einige Fragen Zu Einem 'Neuen Grundrecht', *Die Öffentliche Verwaltung* n. 10 (2008).

BRITZ, Gabriele. *Einzelfallgerechtigkeit versus Generalisierung*. Tübingen: Mohr Siebeck, 2008.

BUCHNER, Benedikt. Die Einwilligung im Datenschutzrecht, *Datenschutz und Datensicherheit – DUD*, 1, 2010.

BUCHNER, Benedikt. *Informationelle Selbstbestimmung im Privatrecht*, Tübingen 2006.

CANARIS, Claus-Wilhelm, Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner Materialisierung. *Archiv für die civilistische Praxis* – AcP 200 (2000), p. 273-364.

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

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

ELIXMANN, Robert. *Datenschutz und Suchmaschinen: neue Impulse für einen Datenschutz im Internet*, Berlin, 2012.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY – ENISA, *Privacy Considerations of Online Behavioral Tracking*, 19.10.2012. Disponível em: [www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking].

FEDERAL TRADE COMISSION. *Protecting Consumer Privacy in a Era of Rapid Change. A Proposed Framework for Businesses and Policy Makers. Preliminary Staff Report* de 2010. Disponível em: [www.ftc.gov/os/2010/12/101201privacyreport.pdf]

GRUNDMANN, Stefan. The Future of Contract Law.*European Review of Contract Law*, vol. 7, Issue 4, 490–527, nov. 2011.

GRUPO DE TRABALHO DO ART. 29. Parecer 04/2012 sobre *Cookie Consent Exemption*, de 07.06.2012. Disponível em: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf]

GRUPO DE TRABALHO DO ART. 29. Parecer 2/2010 sobre Online Behavioral Advertising. Disponível em: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf]

GRUPO DE TRABALHO DO ART. 29. Parecer 15/2011 sobre a definição de consentimento. Disponível em: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.]

GUSY, Cristoph. Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme: Neuer Grundrechtsname oder neues Grundrechtsschutz?. *Datenschutz und Datensicherheit* 1 (2009), 33.

HOFFMANN-RIEM, Wolfgang ,Informationelle Selbstbestimmung in der Informationsgesellschaft – auf dem Wege zu einem neuen Konzept des Datenschutzes. *Archiv des öffentlichen Rechts*, 123, 1998.

HOFFMANN-RIEM, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. *Juristen Zeitung* 21, 2008.

HOFFMANN-RIEM, Wolfgang, Grundrechts- Und Funktionsschutz Für Elektronisch Vernetzte Kommunikation. *Archiv Des Öffentlichen Rechts* 134 (2009).

HOFFMANN-RIEM, Wolfgang. Regelungsstrukturen für öffentliche Kommunikation im Internet. *Archiv Des Öffentlichen Rechts* 137 (2012).

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

LEONARDI, Marcel, *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012.

MARQUES, Claudia Lima. *Confiança no Comércio Eletrônico e a Proteção do Consumidor*. São Paulo: Ed. RT, 2004.

MARQUES, Claudia Lima, *Contratos no Código de Defesa do Consumidor: o novo regime das relações*

contratuais. 6. ed. São Paulo: Ed. RT, 2011.

MARQUES, Claudia Lima; et al., *Manual de Direito do Consumidor*. São Paulo: Ed. RT, 2008.

MAYER-SCHÖNBERGER, Viktor e CUKIER, Kenneth. *Big Data – A Revolution that will transform how we live, work and think*. London: John Murray, 2013.

MENDES, Laura Schertel. *Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental*, São Paulo: Saraiva, 2014.

LUCCA, Newton de. Aspectos atuais da proteção aos consumidores no âmbito dos contratos informáticos e telemáticos. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (org.). *Direito e Internet: aspectos jurídicos relevantes*. São Paulo: Quartier Latin, 2008.

NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford Law Books, 2010.

PIEROTH, Bodo; SCHLINK, Bernhard, *Grundrechte – Staatsrechte II*, Heidelberg: Müller, 2005.

SACHS, Ulrich, *Marketing, Datenschutz und das Internet*, Köln 2008.

SCHERMER, Bart, Risks of Profiling and the Limits of Data Protection. *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases*. Berlin: Springer, 2013.

SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2011.

SILVA, Clóvis do Couto e. *A obrigação como processo*, Rio de Janeiro: FGV, 2006.

TINNEFELD, Marie-Theres et al, *Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht*. München: Oldenbourg, 2012.