UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS
DEPARTAMENTO DE DIREITO PRIVADO

A NECESSIDADE DE LEI DE PROTEÇÃO DE DADOS NO BRASIL

Daniel Bender Gehrke

Prof. Dr. Fabiano Menke

Porto Alegre, 15 de dezembro de 2016.

DANIEL BENDER GEHRKE

A NECESSIDADE DE LEI DE PROTEÇÃO DE DADOS NO BRASIL

Monografia apresentada como exigência parcial para a obtenção do título de Bacharel em Direito na Universidade Federal do Rio Grande do Sul - UFRGS - Faculdade de Direito.

Aprovada em ___ de _____ de 2016.

BANCA EXAMINADORA:

_____
Prof. Dr. Fabiano Menke

_____
Prof. Dr. Luís Renato Ferreira da Silva

_____
Prof. Dr. Gerson Luiz Carlos Branco

AGRADECIMENTOS

Ao Prof. Fabiano Menke, por ter despertado a minha atenção sobre o tema dos direitos da personalidade e do direito aplicado às novas tecnologias, ainda no início do curso, em suas aulas sobre a Parte Geral do Direito Civil, e também pela orientação tranquila e segura para a realização desta monografia;

Ao Prof. Luís Renato e Prof. Gerson, por ter a honra da sua participação nesta banca e por terem sido pessoas que contribuíram muito na minha formação;

Aos professores Sérgio Mattos, Vivian Caminha, Juarez Freitas, Adão Cassiano, Jamil Bannura, Mauro Andrade, Carlos Reverbel, Leandro Dorneles, Sami El Jundi, Francisco Rossal, Klaus Koplin, Augusto Jaeger Jr., Alejandro Alvarez e Simone Cardoso por fazerem diferença dentro do curso de Direito.

.

DEDICATÓRIA

Dedico este trabalho às mulheres da minha vida:
Minha esposa Mirian, amada companheira há mais de 3 décadas, que me faz uma pessoa melhor a cada dia, e cujos conhecimentos de ABNT foram imprescindíveis para esta monografia;
Minha filha Julia, amadinha que é a luz de nossa vida, guria incrível, criativa, inteligente, à qual não pude dar a atenção devida nestes 5 anos de faculdade;
Minha mãe Suzana, mulher que sempre esteve à frente do seu tempo, à qual amo com intensidade somente comparável com a que sinto a sua falta, e que se estivesse entre nós não perderia por nada a minha formatura.

RESUMO

Esta monografia, cujo objeto é a necessidade de lei relativa à proteção de dados em nosso país, com vista a garantir a privacidade digital dos usuários de internet e a sua autodeterminação informativa, busca, através da abordagem dogmática do ordenamento jurídico brasileiro, identificar se este, em seu bojo, já contém os elementos aptos a garantir estes direitos fundamentais de forma efetiva, ou se é imperiosa a edição de um novo diploma legislativo específico para preencher a lacuna. O método de abordagem escolhido é o dedutivo, embasado em pesquisa bibliográfica, dogmática e jurisprudencial, pelo entendimento deste ser o mais adequado ao alcance da finalidade a que se propõe a monografia. A fundamentação teórica aborda a temática do desenvolvimento do cenário digital (CASTELLS, 2003; LESSIG, 2006), privacidade (MARTINS, 2014; VANCIM e MATIOLI, 2014; PINHEIRO, 2013) proteção de dados e autodeterminação informativa (DONEDA, 2006, 2014; MENKE, 2015), contratos de adesão eletrônicos e políticas de privacidade (GONÇALVES, 2012; TEIXEIRA, 2014), legislação em vigor (DUARTE, 2010; NUNES, 2012; VANCIM e MATIOLI, 2014; TEIXEIRA, 2014) e projetos de lei. Apresenta considerações sobre o atual modelo de negócios utilizado na internet, o fornecimento forçado de dados pessoais para a utilização de recursos virtuais e do quanto atualmente encontram-se os usuários em uma situação de hipossuficiência técnica e jurídica para fazer frente ao problema apresentado. Aborda também a inexistência de fiscalização adequada, o conhecimento técnico deficiente de operadores do direito e magistrados sobre o assunto, a jurisprudência não-consolidada e a falta de tutela prévia e coletiva do direito fundamental à proteção de dados pelo Estado. Aventa a possibilidade de utilização de soluções tecnológicas e de segurança em conjunto com soluções jurídicas para o enfrentamento da situação, e demonstra a necessidade de legislação específica para a proteção de dados pessoais como indispensável para a resolução do problema.

Palavras-Chave: Proteção de Dados. Privacidade. Autodeterminação Informativa. Internet. Contratos de Adesão eletrônicos. Políticas de Privacidade.

ABSTRACT

This monograph, whose object is the need for a law on data protection in our country, with a view to guarantee the digital privacy of Internet users and their self-determination, seeks, through the dogmatic approach of the Brazilian legal system, to identify if this, in its bulge, already contains the elements capable of guaranteeing these fundamental rights effectively, or whether it is imperative to issue a new specific legislative act to fill the gap. The method of approach chosen is the deductive one, based on bibliographical, dogmatic and jurisprudential research, for the understanding that this is the most adequate for the purpose of the monograph. The theoretical basis of this paper is the theme of the development of the digital scenario (CASTELLS, 2003; LESSIG, 2006), privacy (MARTINS, 2014; VANCIM and MATIOLI, 2014; PINHEIRO, 2013), data protection and informative self-determination (DONEDA, 2006, 2014; MENKE, 2015), and the use of electronic adhesion contracts and privacy policies (GONÇALVES, 2012, TEIXEIRA, 2014), legislation in force (DUARTE, 2010, NUNES, 2012, VANCIM and MATIOLI, 2014, TEIXEIRA, 2014) and legislative bills. It presents considerations about the current business model used on the internet, the forced supply of personal data for the use of virtual resources and how currently the users are in a situation of technical and legal hyposufficiency to face the presented problem. It also addresses the lack of adequate oversight, poor technical knowledge of legal practitioners and magistrates on the subject, unconsolidated jurisprudence and lack of prior and collective protection of the fundamental right to data protection by the State. It highlights the possibility of using technological and security solutions together with legal solutions to face the situation, and demonstrates the need for specific legislation for the protection of personal data as indispensable for solving the problem.

Keywords: Data Protection. Privacy. Informational Self-Determination. Internet.

Electronic Adhesion Contracts. Privacy Policy.

SUMÁRIO

1 INTRODUÇÃO

A utilização da internet é ainda um fenômeno recente em termos históricos, tendo há pouco completado 25 anos de existência no Brasil. Mesmo assim, neste curto período, seu explosivo desenvolvimento fez com que sua utilização, por grande parcela da população, a tornasse praticamente indispensável para a realização das mais diversas atividades que cotidianamente fazemos, como as de comunicação, lazer, pesquisa, ensino, e comercialização de produtos e serviços, entre outros exemplos que poderiam ser citados.

Dentre os direitos da personalidade, encontra-se o direito à privacidade das pessoas naturais, disposto no Art. 5º, X, da *Constituição Federal*, com a seguinte redação: "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" (BRASIL, 1988).

Para a garantia deste direito, é indispensável que existam recursos que efetivamente assegurem aos indivíduos a proteção de seus dados pessoais, especialmente na Internet, onde a possibilidade de sua replicação, coleta, processamento e uso indevido é potencializada pela arquitetura e características intrínsecas à rede.

Consequência disto é que a proliferação de dados de todos os tipos pela rede mundial, associada à capacidade praticamente sem limites de processamento de informações pelo setor público e privado, fez com que as pessoas naturais tivessem sua privacidade ameaçada como em nenhum momento anterior da história.

Consciente ou não desta realidade, geralmente o usuário da internet aceita esta situação, pela imperiosa necessidade atual dos recursos da rede e dificuldade de defender-se, o que propicia a ocorrência da violação da sua privacidade *on-line.* As consequências ainda não estão ainda devidamente tipificadas, nem existem conceitos amplamente aceitos e normas específicas para regularem essas situações no Brasil.

A União Europeia (EUROPEAN COMISSION, 24 nov. 2016), que já possuía legislação considerada paradigma sobre o assunto, avançou recentemente nesta questão reformando-a, através de dois instrumentos. O primeiro é a Regulamentação Geral de Proteção de Dados - *Regulation (EU) 2016/679*, de forma a capacitar às pessoas um melhor controle sobre seus dados pessoais e constituir o Mercado Único Digital Europeu, acabando com a fragmentação legal ainda existente e possibilitando simplificação

de regras para as empresas. Esta Regulamentação revogou a *Directive 95/46/EC (General Data Protection Regulation).*

O outro instrumento (idem) é a Diretiva de Proteção de Dados – *Directive (EU) 2016/680*, que possibilitará uma melhor proteção para as pessoas naturais quanto ao processamento de seus dados pessoais pelas autoridades competentes para os propósitos de prevenção, investigação, detecção ou persecução criminal, ou a execução de penas criminais, e sobre a livre movimentação destes dados. Esta Diretiva revogou a *Council Framework Decision 2008/977/JHA*.

A Regulamentação entrou em vigor em 24 de maio de 2016, mas será aplicada somente a partir de 25 de maio de 2018. Já a Diretiva entrou em vigor em 5 de maio de 2016, mas será aplicada após a sua transposição para as leis nacionais dos membros da União Europeia, que deverá ocorrer até 6 de maio de 2018.

O Direito é uma ciência social que tem por característica a sua reatividade, ou seja, desenvolve-se *a posteriori* das mudanças que ocorrem na sociedade e na tecnologia, na tentativa de resolver os novos problemas que se apresentam, a partir da regulação das relações jurídicas decorrentes e estabelecer as sanções necessárias.

Enquanto a proteção de dados pessoais não é devidamente regulada, apresentam-se hiatos jurídicos, pois não havia no passado condição de prever o rumo que tomariam as importantes mudanças em curso no ambiente virtual.

Assim, são, de forma potencial ou efetiva, violados direitos da personalidade por governos e empresas, com a utilização da tecnologia, geralmente sem que os usuários tenham sequer conhecimento disso, não conseguindo, assim, defender-se, devido à sua hipossuficiência técnica, financeira e jurídica.

Entidades governamentais e não-governamentais recolhem dados pessoais e os processam para utilização em segurança pública e estatal, definição de políticas diversas, desenvolvimento de projetos, etc.

Mas, atualmente, o caráter comercial da Internet sobrepõe-se em relação ao caráter público e educacional de seus primeiros tempos, e desenvolvem-se a todo momento novos modelos de negócio na rede mundial, nos quais o principal insumo são dados pessoais. Estes são cobiçados para o desenvolvimento de produtos, marketing e publicidade e, em muitos casos, vendidos como mercadoria para que terceiros os utilizem em suas finalidades, que podem ser as mais diversas.

Além disso, a questão da segurança dos dados pessoais não é menos importante, pois os grandes bancos de dados empresariais formados são igualmente cobiçados, e

eventual negligência em seu cuidado que acarrete vazamento ou apropriação ilícita pode gerar danos aos usuários envolvidos.

Com a expansão comercial na internet, globalmente passaram a ser utilizadas políticas de privacidade, com a finalidade declarada de “aumentar a transparência para o usuário quanto à coleta, armazenamento, processamento e utilização dos dados”, “melhorar a experiência do usuário com o produto ou serviço”, entre outros argumentos.

Na realidade, políticas de privacidade servem como anteparo, para proteção jurídica quanto à forma de obtenção de consentimento do usuário, em geral obrigatório, quanto às suas cláusulas, que incluem o uso de seus dados para a descoberta de preferências, hábitos e opiniões compartilhadas através da Internet, conscientemente ou não, para a formação de perfis.

Disto que vivem, por exemplo, empresas como Google e Facebook, as quais, disponibilizando serviços aparentemente gratuitos aos seus usuários, comercializam informações obtidas acerca deles, direcionando-as para outro tipo de clientes, que os desejam para publicidade e outros fins, talvez menos nobres.

Atualmente, um dos principais problemas refere-se justamente à obrigatoriedade da concordância para a cessão de dados pessoais para que o usuário possa utilizar programas, acessar conteúdo, participar de redes sociais, etc.; não capitulando a esta exigência, ele nada pode utilizar.

A proteção de dados pessoais visa à manutenção do direito à privacidade dos usuários e possui relevância prática, imediata e cotidiana em nossa vida, pois estamos cada vez mais conectados em rede, em escala mundial, com navegação na internet e dados pessoais sendo rastreados.

O objeto do presente trabalho é relativo à suficiência da proteção atualmente existente quanto à proteção de dados pessoais e privacidade dos usuários no ambiente virtual no contexto brasileiro e se existe necessidade de uma lei de proteção de dados para o nosso país.

A hipótese apresentada nesta monografia é a da real necessidade da edição de uma lei específica para esta finalidade, cuja validação será realizada por meio do estudo do ordenamento jurídico brasileiro, e o que diz a doutrina e a jurisprudência sobre o assunto.

A importância do trabalho teórico referente a este tema decorre do fato de que a violação ou a má utilização de dados pessoais projetam reflexos negativos na autodeterminação informativa da pessoa. Caso a violação seja realizada em relação a dados sensíveis, pode ainda atingir a esfera mais íntima da personalidade do ser humano, a qual deve contar com a máxima proteção.

O controle sobre os dados do usuário para monopolização da experiência na Internet, almejada por diversas empresas, atinge o comportamento daquele, e, potencialmente, também a própria democracia, pois manipula artificialmente o fluxo de informações necessárias à formação de seu livre convencimento sobre o que é importante para ele e a sociedade em que vive.

1.1 ESTRUTURA DO TRABALHO

Para possibilitar o estudo da questão apresentada, e posteriormente a validação da hipótese – a necessidade de edição de lei específica quanto à privacidade e proteção de dados pessoais para usuários no ambiente virtual – apresentaremos inicialmente um breve histórico do cenário digital e o contexto brasileiro com relação à privacidade no ambiente virtual.

Realizaremos uma revisão teórica a respeito do que se trata, em geral, a privacidade, proteção de dados, autodeterminação informativa, dispondo sobre a expressão dessas no meio digital.

Também serão vistos o conceitos e características do gênero *contrato de adesão* e de sua espécie denominada *política de privacidade*, que dispõe unilateralmente acerca de tópicos importantes quanto à proteção de dados e direito à privacidade, de maneira a sedimentarmos conhecimentos basilares sobre o assunto.

Referentemente à coleta e utilização de dados pessoais, identificaremos as maneiras de como ela ocorre e sua repercussão na vida e personalidade do indivíduo.

Seguiremos com uma abordagem dogmática do tema, apresentando a privacidade como direito da personalidade, de acordo com o disposto na *Constituição Federal* e no *Código Civil*.

Demonstraremos como a proteção de dados pessoais e da privacidade estão ali caracterizadas, bem como em que limites a jurisprudência julga, de forma geral, que é lícito exercer e defender estes direitos.

Será observado, também, de que maneira o *Código de Defesa do Consumidor* e o *Marco Civil da Internet* tratam o mesmo assunto, apresentando a jurisprudência sobre defesa daqueles direitos, com base nesta legislação.

Descoberta a existência de questões relativas à privacidade e proteção de dados pessoais em aberto, analisaremos sua relevância e necessidade de sua garantia, bem como se existem projetos de lei em elaboração para esse fim.

Desta forma, será possível então chegarmos à conclusão sobre o problema levantado nesta monografia, acerca da necessidade de legislação específica sobre proteção de dados pessoais e da privacidade.

1.2 BREVE HISTÓRICO DO CENÁRIO DIGITAL

A Internet é uma plataforma multimídia, multilateral e multipropósito surgida de um projeto do Departamento de Defesa dos Estados Unidos da América (ARPANET) em plena Guerra Fria, nascendo deslocada de uma arquitetura de controle, pelo fato de ser baseada em uma arquitetura de múltiplas camadas, descentralizada e de protocolos abertos (TCP/IP) (CASTELLS, 2003).

Utilizando processamento distribuído através de nós de rede e de redundância de funções entre esses, seria reduzido o risco de desconexão, de forma a suprir a necessidade militar de capacidade de sobrevivência do sistema em caso de ataque nuclear, possuindo características de flexibilidade, ausência de um centro de comando e autonomia máxima dos nós (idem).

A Internet também foi influenciada em sua configuração pela tradição de formação de base de rede de computadores pessoais, iniciada no final da década de 70 pelos *Bulletin Board Systems* (BBS), destinados à transferência de arquivos, armazenagem, e transmissão de mensagens.

Além desses fatos, Castells (2003) também diz que, a par de outros avanços tecnológicos, o que permitiu que a Internet abarcasse o mundo todo foi o desenvolvimento da *World Wide Web* por Tim Berners-Lee, que desenvolveu a linguagem de hipertexto e construiu o primeiro navegador/editor para esse ambiente.

Em meados da década de 90, após a desvinculação do ambiente militar, devido à montagem de uma rede específica para este uso (MILNET), o ciberespaço continuou sem regulação, e de difícil controle por quem quer que seja, sendo defendido pelos seus primeiros teóricos justamente por estas características. Nas palavras de Lessig (2006, p. 17), “Primeiro nas universidades e centros de pesquisa, e então por toda a sociedade em geral, ciberespaço tornou-se o novo alvo do utopismo libertarianista. Aqui liberdade em relação ao Estado poderia reinar”.

Na abertura de seu livro, Castells (2003) utiliza como título “A rede é a mensagem”, em uma paródia a McLuhan, teórico da comunicação de massa que disse que “o meio é a mensagem”, pois, na Era da Informação, a Internet passou a ser a base tecnológica para a sua forma organizacional.

Como Lessig (2006) assevera, as possíveis ameaças, já então imaginadas no início de seu desenvolvimento, como a do ciberespaço ser dominado para servir aos interesses de corporações ou do Estado, ainda eram contos de ficção científica. Certamente, já existia o interesse negocial na rede, mas havia desconhecimento de como rentabilizá-la e um grande receio das companhias de cartão de crédito em relação à realização de negócios nesse ambiente.

Então, conforme Castells (idem), mesmo que o desenvolvimento da Internet tenha sido informado pelos valores da liberdade e excelência tecnológica, provindos do meio acadêmico, comunidades virtuais e *hackers*, foi a partir da participação de empresários, com seu conjunto próprio de valores, voltados à percepção de lucro através da inovação em serviços e produtos, que ocorreu sua rápida expansão.

Lessig (idem) opina que as forças econômicas e as novas tecnologias desempenharam, do início do segundo milênio aos dias atuais, papéis importantes na transformação da rede no espaço mais perfeitamente regulado. Aqui, o autor refere-se a uma regulação não somente por leis, mas principalmente por mudanças de arquitetura de rede.

Castells (2003, p. 8) refere que, a partir dos últimos anos do segundo milênio, "atividades econômicas, sociais, políticas e culturais essenciais por todo o planeta estão sendo estruturadas pela Internet e em torno dela, como por outras redes de computadores".

A luta pela defesa de direitos autorais foi uma das forças que impulsionou comércio e governo a mudarem a infraestrutura, de forma a possibilitar o maior controle possível, tornando, para muitos, o perigo Orwelliano uma hipótese bastante plausível, informa Lessig (2006).

De acordo com este autor, atualmente o comércio alimenta uma grande parte da rede e, para muitos, isso não apresenta problema nenhum; se o inimigo antigamente apresentado pelos primeiros teóricos, como Vinge e Madson, era bastante óbvio, hoje não é mais.

Uma imagem do futuro do controle que pode ser antevista é que ele será exercido em grande parte pelas tecnologias do comércio, amparadas pelas leis – ou pelo que delas restarem.

A questão atual é como proteger a liberdade com arquiteturas de controle gerenciadas tanto pelo governo quanto pelo setor privado, as quais, dependendo do seu uso, podem proteger ou atingir direta e cotidianamente a privacidade de todos nós, pois são fundadas em informação e comunicação.

Conforme Castells (idem), não somente esses atores, mas as pessoas, instituições e sociedade em geral transformam a tecnologia, apropriando-a, experimentando-a e modificando-a, afetando nossas vidas profundamente, mas que um novo padrão sociotécnico emerge desta interação.

Segundo o autor, expurgar um agente da rede pode ser considerada uma das formas mais danosas de exclusão[1] em nossa atual configuração econômica e cultural, podendo-se acrescentar que, para o uso praticamente essencial[2] de seus recursos, os usuários sucumbem, sacrificando a sua privacidade.

Quanto a esse tema, o cenário é incerto; sabe-se que o governo é necessário à proteção da liberdade, mas também pode destruí-la. O comércio e os novos serviços pela rede são extremamente úteis e necessários na nova economia, mas podem invadir fortemente a privacidade dos cidadãos.

Conforme Lessig (idem), esta é uma discussão em andamento, na qual acadêmicos e ativistas possuem um papel determinante na defesa de importantes valores de nossa sociedade. Podemos acrescentar a essa ideia a importância do capital privado para o constante desenvolvimento da Internet e da igualmente necessária e adequada regulação pelo Estado de interesses diversos, para o equilíbrio de poder na rede.

1.3 PRIVACIDADE DIGITAL E CONTEXTO BRASILEIRO

A inserção do Brasil no ciberespaço foi tardia, chegando em setembro de 1988 (MÜLLER, 2008) no Laboratório Nacional de Computação Científica (LNCC), no Rio de Janeiro.

Quando foram reunidas condições para o acesso à Internet pela massa da população, a revolução comercial neste ambiente já se encontrava em andamento no mundo e celeremente apropriou-se, ao menos em nosso país, de um espaço de poder maior do que o do Estado, devido à falta de controle e regulamentação desse tema em nosso país.

---

[1] Vide o caso de bloqueio do aplicativo WhatsApp pela justiça brasileira, para tentar fazer cumprir decisão judicial, e que causou imensa repercussão junto aos seus usuários, que consistem em 93% dos brasileiros, segundo pesquisa do Ibope (SORDI; ROSO, 18 dez. 2015, p. 40).

[2] O mesmo caso foi tema de Editorial de Zero Hora dois dias após, com o título *Bloqueio Desarrazoado* (20 dez. 2015, p. 26). Matéria de página inteira refere que a proibição gerou um fenômeno social que mesclou cultura hacker, desobediência civil e ataques políticos ao Marco Civil da Internet (BITTENCOURT, 20 dez. 2015, p. 3).

A exploração comercial iniciou baseada em assinatura paga de serviços e da incipiente venda de *softwares* e produtos. A publicidade na internet era realizada pelas empresas basicamente através de anúncios, *banners* e *pop-ups* em *sites* e aplicações, o que se mostrou inconveniente pela poluição visual ocasionada e pelo retorno incerto do investimento, devido ao fato de não se direcionar a um público-alvo específico.

Posteriormente, com o desenvolvimento da tecnologia, foi propiciado o surgimento de novos modelos de negócio, já relatados anteriormente, através dos quais abandonou-se, em grande parte, a cobrança pela navegação em sites, uso de aplicações e *downloads* de software na internet, tornando sua utilização aparentemente livre, sem custos, mas que utiliza dados pessoais como pagamento.

Importante salientar que a coleta de dados também ocorre da mesma forma quando serviço ou produto é comprado pela internet (não somente quando o uso de facilidade é "gratuito"), como pode atestar empiricamente qualquer pessoa que já sofreu uma sobrecarga de publicidade após realizar uma transação por meio digital.

O desconhecimento da maioria dos usuários sobre a realização dessa atividade é uma situação que persiste até os dias de hoje, causada pela falta de conhecimentos técnicos dos usuários, de divulgação sobre a importância do assunto e da condição socioeconômica da maioria da população.

As empresas brasileiras também utilizam costumeiramente políticas de privacidade, a fim de conferirem imagem de confiabilidade, transparência e legalidade relativas à atividade de utilização de dados pessoais dos seus usuários.

No Brasil, é recente, pouco extensa e fragmentada a legislação existente relativa à internet, e a dificuldade quanto à proteção de dados pessoais sofridas pelo usuário é bastante intensa no contexto atual.

Entretanto, para Pinheiro (2013), que acredita não haver lacuna jurídica no tocante à privacidade, o que deve ocorrer é as leis em vigor serem interpretadas de maneira apropriada em novas situações que exigem adequação para o caso concreto.

O uso da Internet também no Brasil tornou-se praticamente indispensável na vida diária, principalmente a urbana, pois as pessoas foram condicionadas ao seu uso, e dele dependentes.

Pinheiro (2013) acredita que os usuários não estariam dispostos a deixar de utilizar serviços gratuitos em troca dos seus dados e que ganhará o mercado quem liderar a proteção da privacidade sustentável, mas que, até lá, eles devem cuidar o que contém as políticas de privacidade.

Hoje, os usuários consideram inimaginável deixar de usar a Internet e voltar ao *status quo ante* (aliás, a geração atual nem conhece o mundo sem a internet), visto que já se encontram totalmente imersos no ambiente digital.

O uso das facilidades oferecidas pela Internet, por assim dizer, tornou-se artigo de primeira necessidade; assim, mesmo que não concordem ou desconheçam a existência de violação, *conformam-se aceitando políticas de privacidade abusivas, em troca desse admirável mundo novo.*

É importante lembrar fato divulgado recentemente pela imprensa internacional (junho/julho 2016), de que a ONU propõe entender o acesso à internet como um direito do ser humano, devido à importância atual deste recurso de alcance planetário.

Assim, compreende-se que tanto a liberdade de acesso, a informação e a comunicação pela Internet são fundamentais, quanto a sua utilização comercial é muito relevante para o desenvolvimento da economia nacional.

Mas, para a utilização dos recursos possibilitados pela Internet sem que sejam sacrificados direitos fundamentais, torna-se imperativo o desenvolvimento de garantias efetivas quanto à proteção de dados pessoais e da privacidade em nosso país.

2 PRIVACIDADE, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA

2.1 PRIVACIDADE

O tema da garantia da privacidade individual é antigo, mas também cada vez mais emergente e importante em nossa (ainda) jovem sociedade da informação.

Segundo Vancim e Matioli (2014, p. 233), "temos, hoje, uma sociedade virtual parcialmente constituída, onde os personagens, ou melhor, os sujeitos, não só atuam, como também dependem diretamente ou indiretamente da rede. "

Esta dependência, que ocorre de forma acelerada e intensa, transforma o espaço virtual cada vez mais em um produto ou serviço essencial aos seus usuários, no qual devem ser garantidos direitos fundamentais, como a privacidade, através da adequada proteção de seus dados pessoais.

A concepção clássica de privacidade, definida como o "o direito de estar só" ou o "direito de ser deixado em paz", é indicada por Martins (2014) como originária do artigo *The Right of Privacy*, de Samuel Warren e Louis Brandeis (1890), considerado marco do direito da privacidade e que profetizou, em determinada medida, o efeito que a matéria assumiria com o desenvolvimento das tecnologias da informação.

Para Silva (1994, p. 204), "a privacidade também pode ser entendida como o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso ser legalmente sujeito".

Martins (2014, p. 9-10) faz contraponto citando Doneda, que critica essa concepção inicial, pois entende a privacidade dentro de um paradigma de relação:

> ...a proteção da privacidade na sociedade da informação, tomada na sua forma de proteção dos dados pessoais, avança sobre terrenos outrora não proponíveis e induz a pensá-la como um elemento que, antes de garantir o isolamento ou tranquilidade, proporcione ao indivíduo os meios necessários para a construção e consolidação da esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, tenha um papel positivo na sua própria comunicação e relacionamento com os demais.

Em relação à sociedade da informação, Castells (2003, p. 108-109) afirma que "a primeira característica do novo paradigma é que a informação é sua matéria-prima: são tecnologias para agir sobre a informação...".

Sua segunda característica é a penetrabilidade dos efeitos das novas tecnologias, pois "todos os processos de nossa existência individual e coletiva são diretamente moldados (embora, com certeza, não determinados) pelo novo meio tecnológico" (idem, ibidem).

A lógica das redes é sua terceira característica, pois ela está presente "em qualquer sistema ou conjunto de relações, usando estas novas tecnologias da informação. A morfologia da rede parece estar bem adaptada à crescente complexidade da interação e aos modelos imprevisíveis do desenvolvimento derivados do poder criativo desta interação..." (idem, ibidem).

A quarta característica é a sua extrema flexibilidade, potencializada pela quinta característica, "a crescente convergência de tecnologias específicas para um sistema altamente integrado" (idem, ibidem).

Sobre a convergência tecnológica, pode-se dizer que, já fortemente impulsionada pelo atual uso de *smatphones,* se intensificará com o desenvolvimento da internet das coisas, que consiste na conexão à rede de aparelhos do cotidiano, como geladeiras, televisões, automação residencial, etc.

Martins (2014, p. 10) entende que, nesta sociedade, "tendem a prevalecer definições funcionais da privacidade, que se referem à possibilidade de um indivíduo conhecer, controlar, endereçar ou interromper o fluxo das informações que lhe dizem respeito", complementando que o direito à autodeterminação informativa é a base na qual deve apoiar-se a sua tutela.

Embora a violação da privacidade seja proibida pela *Constituição Federal*, salvo as exceções indicadas, na verdade ela pode ocorrer faticamente de inúmeras maneiras quando se utiliza a rede. As ameaças mais comuns encontradas neste estágio de desenvolvimento começam pela própria autoexposição de informações pessoais, ou de sua exposição por terceiros, propiciando a outros conhecimento e potencial utilização indesejada, antiética ou mesmo criminosa.

A violação da privacidade por *hackers* ocorre através de diversos meios, como o uso de engenharia social, vírus, *bots, worms e spywares*, e é muito praticada para finalidades ilícitas, embora em alguns casos seja utilizada na resistência política e delação de práticas antiéticas e criminosas de estados e corporações.

A vigilância eletrônica dissimulada, ou mesmo invisível, é realizada de forma muito contundente por determinados estados (Estados Unidos da América, Grã-Bretanha e China, entre outros), que possuem capacidade de rastrear praticamente qualquer informação que circule pelos *backbones*. Tal atividade acarreta violação de soberania, espionagem ilegal de pessoas e empresas e ameaça à democracia.

A violação de privacidade realizada por empresas ou outras entidades pode ser agravada pela falta de segurança física ou tecnológica na guarda de dados, sua utilização indevida por empresas terceirizadas, a obrigatoriedade de sua cessão ao estado, entre outros motivos.

Talvez a violação de privacidade efetuada comercialmente seja a que mais impacte o usuário comum, pois "a tentativa de saber o máximo possível sobre seus usuários tornou-se a batalha fundamental da nossa era entre gigantes da Internet, como Google, Facebook, Apple e Microsoft..." (PARISIER[5] apud MARTINS, 2014, p. 6), e porque, "Por trás das páginas que visitamos, está crescendo um enorme mercado de informações sobre o que fazemos na rede, movido por empresas de dados pouco conhecidas, mas altamente lucrativas, como BlueKai e a Acxiom" (idem, ibidem).

O aumento da agressividade desta atividade, em relação à privacidade do usuário, pode ter sido causado pelo súbito desenvolvimento da comercialização pela internet, pois da mesma forma que ela teve surtos de crescimento, também teve forte impacto negativo pelo estouro da "bolha acionária" de empresas .com., segundo Castells (2003).

No início do segundo milênio, muitas empresas experimentaram dificuldades, devido a custos mal dimensionados, pela complexidade da entrega de produtos vendidos pela rede, e pelo fato da publicidade realizada na época ter sido um grande fracasso, devido à falta de percepção da especificidade da internet em relação à televisão (idem). A publicidade dirigida, que afeta a privacidade do consumidor, também foi parcialmente rejeitada, pela negativa das pessoas à realização de cadastro.

Ainda de acordo com Castells (2003), a cobrança de taxas por serviços afastou muitos potenciais clientes, que procuravam passar ao lago dos *sites* que realizavam esta prática, com exceção dos que atendiam diretamente às suas necessidades, pois sentiram-se traídos na ideia de acesso gratuito.

Assim, ainda conforme esse autor, foi fundamental para as empresas o desenvolvimento de tecnologias de coleta de dados a serem utilizadas conjuntamente ao comércio eletrônico (2003, p. 143):

> Em muitos casos, a principal fonte de rendimentos das companhias de comércio eletrônico são a publicidade e o marketing. [...] Por um lado, elas recebem os lucros das faixas de publicidade que podem exibir para seus usuários. Por outro, vendem os dados de seus usuários para seus clientes para fins de marketing, ou os utilizam elas próprias para melhor mirar seus clientes. Em todos os casos, informação preciosa deve ser colhida a cada clique no website. [...] As companhias juram

[5] PARISIER, Eli. *O filtro invisível*: o que a Internet está escondendo de você. Rio de Janeiro: Jorge Zahar, 2012.

> que só usam os dados de forma agregada para perfis de marketing. E, afinal de contas, a maioria dos compradores não exerce o direito de exclusão que lhes é facultado, e não clica para que seus dados pessoais não sejam usados. Advogados de consumidores mostraram como é inconveniente, na prática, o exercício desta cláusula de exclusão, propondo em lugar dela uma decisão afirmativa de inclusão.

Martins (2014, p. 7) afirma que, hoje, qualquer empresa (não apenas as grandes), pode participar dessa prática com uso da tecnologia, pois, "para os comerciantes do mercado do comportamento, cada indicador de clique que enviamos é uma mercadoria, e cada movimento que fazemos com o *mouse* pode ser leiloado em microssegundos a quem fizer a melhor oferta".

Os dados coletados são sobre todo tipo: análise de crédito, utilização de sites de encontros, compra de medicamentos, posicionamento político, consumo de bebida ou drogas, atividades profissionais, geolocalização, etc.

As pessoas são hipossuficientes nessa relação assimétrica com as organizações e, geralmente, desconhecem as possíveis consequências do seu comportamento *on-line*.

Aos fatos apresentados soma-se o de que o desenvolvimento tecnológico fez com que seja praticamente impossível eliminar uma informação da rede após sua inserção, devido à sua replicação para outros servidores, não havendo, assim, um poder efetivo de controle temporal e territorial de dados. Isso significa uma perda de capacidade de controlar a própria identidade, o que afeta a autodeterminação informativa (MARTINS, 2014).

> Produzem-se incessantemente, informações pessoais na rede, seja diretamente, por meio do fornecimento do próprio usuário, seja indiretamente, por meio de terceiros, através de postagens de fotos, indicação de amizades, de aposição de *tags* em fotos que identificam o outro usuário e de fornecimento de dados geográficos de onde se está. Sem mencionar as informações produzidas sem que se saiba, o que torna ainda mais grave e acentua a dificuldade muitas vezes enfrentada de apagar dados produzidos na rede (COSTA[6] apud MARTINS, 2014, p. 6).

O controle temporal dos dados, pela importância da qual reveste-se, é item obrigatório a ser considerado em uma lei de proteção de dados. Mesmo no caso de admitir-se o uso de dados pessoais como moeda de troca pelo uso de alguma facilidade, sua coleta e uso ilimitados no tempo certamente configura-se como uma cobrança desproporcional.

---

[6] COSTA, André Brandão Nery. Direito ao esquecimento na internet: a scarlet letter digital. In: SCHREIBER, Anderson (coord.). *Direito e mídia*. São Paulo: Atlas, 2013.

2.2 CONCEITOS SOBRE DADOS, TECNOLOGIAS DE COLETA E ALGORITMOS

Alguns conceitos utilizados sobre o tema e outras informações devem ser apresentados para um entendimento mais específico do que representam.

O termo *dado* é "usado para indicar números, letras, símbolos ou fatos que se referenciam à descrição de um determinado objeto, ideia, condição, situação ou outros fatores. Refere-se, quando se trata de computador, aos elementos básicos que são fornecidos, processados ou produzidos pela máquina. " (SAWAYA, 1999, p. 111)

Os dados podem ser de vários tipos.

Dados anônimos são os "dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular". [8]

Doneda (2014, p. 61) afirma que "os dados pessoais acabam por identificar ou mesmo representar a pessoa em uma série de circunstâncias nas quais sua presença não é possível ou conveniente. São elementos centrais, portanto, da construção da identidade em nossa sociedade".

A expressão dados pessoais refere-se aos relacionados "à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". [9]

São considerados dados cadastrais[10] a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

Os dados sensíveis são os "dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos".[11]

Já informações pessoais "são aquelas relacionadas à pessoa natural identificada ou identificável, cujo tratamento deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. As informações pessoais terão seu acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos a contar da sua data de produção" (SEDESTMIDH, 19 nov. 2016).

---

[8] PL 5276/2016, art. 5º, Inciso IV.

[9] Dec. nº 8771, de 11 de maio de 2016, art. 14, inciso I.

[10] Dec. nº 8771, de 11 de maio de 2016, art. 11, § 2º, incisos I, II e III.

[11] PL 5276/2016, art. 5º, Inciso III.

Doneda (2014) explica que a informação chega ao limiar da cognição, ultrapassando a representação contida no dado, incluindo também um sentido instrumental, que reduz o estado de incerteza, e, dessa forma, fica a privacidade em uma proporção inversa à divulgação de informações pessoais.

Greenwald (2014) esclarece que dois tipos de informação devem ser distinguidos: o conteúdo, p. ex., textos de *e-mails* ou *chats*, históricos de navegação e buscas, gravação de conversas telefônicas, e os metadados, que consistem em informações sobre essas informações. Segundo o autor, metadados sobre uma informação são: quem mandou para quem, hora de envio, localização do envio e do destino, números de IP ou telefone, tipo de aparelho, entre diversos outros identificadores técnicos.

Existe quem ache que a coleta de metadados não seja tão intrusiva, já que não acessa o conteúdo transmitido, mas na realidade este tipo de rastreamento pode ser tanto ou mais intrusivo que a interceptação de conteúdo.

O autor afirma que, com este tipo de informação, é possível que se realize um completo levantamento do perfil da vida de uma pessoa, dos seus contatos e atividades e de certas informações mais reservadas e pessoais, podendo ser mais informativos do que o conteúdo da comunicação.

Cruzando essas informações com as dos contatos da pessoa, históricos, etc., é possível evidenciar um panorama completo do perfil pois, devido à natureza matemática, limpa e precisa dos metadados, estes são muito mais fáceis de analisar do que o conteúdo das comunicações, que possuem uma natureza desestruturada.

Um resumo dessa problemática pode ser expresso por fragmento de decisão, de 1995, do Ministro Ruy Rosado de Aguiar, no REsp n. 22.337-8-RS (STJ, 20 mar. 1995).

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma preocupação do Estado moderno, onde o uso da informática e a possibilidade do controle unificado das diversas atividades da pessoa, nas múltiplas situações da vida, permitem o conhecimento da sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto desta indiscriminada colheita de informações, muitas vezes, sequer sabe da existência desta atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser utilizado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.

O tratamento sistematizado da informação é realizado milenarmente para algum tipo de censo populacional, de forma a embasar a administração governamental. A grande diferença dos dias atuais é a incrível facilidade de acumular e processar estes dados pelo desenvolvimento da tecnologia, multiplicando a forma como serão utilizadas as informações decorrentes.

Bancos de dados são fundamentalmente um conjunto de informações estruturado de acordo com uma determinada lógica, possui aspecto utilitarista, segundo Doneda (2014), e procura proporcionar a extração do máximo proveito possível a partir de um conjunto de informações. O autor também assevera (idem, p. 66):

> Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico destes dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.

Cookies, *beacons* e outras tecnologias semelhantes[13] são utilizadas para a coleta de dados do usuário que navega ou utiliza as facilidades disponibilizadas pela internet.

Cookies são pequenos arquivos de texto que armazenam informações no computador, TV, celular ou em outros dispositivos. Eles permitem que a entidade que insere o *cookie* no dispositivo reconheça o usuário em vários sites, serviços, dispositivos e/ou sessões de navegação. Podem gravar credenciais de *login*, páginas e recursos que os usuários estão acessando, tempo gasto nas páginas, anúncios visualizados, partes dos serviços mais utilizadas, informações sobre o uso dos serviços e de outros sites e aplicativos, etc.

Navegadores da Web e sistemas operacionais de dispositivos podem ser configurados para aceitar, rejeitar ou notificar quando um *cookie* for recebido, podendo conter controles adicionais. No entanto, diversos serviços são projetados para funcionar usando *cookies* e sua desativação pode impossibilitar a capacidade de usar esses serviços ou algumas das suas partes.

Outros tipos de tecnologias de armazenamento local são chamados de "*Cookies Flash*" e o armazenamento local HTML5, semelhantes aos *cookies* anteriormente descritos, mas essas tecnologias podem fazer uso de partes diferentes do dispositivo em comparação com os *cookies* padrão, e assim pode não ser possível controlá-los por meio de ferramentas e configurações padrão do navegador.

---

[13] Como exemplo, pode ser vista a *Política de Privacidade Local da Samsung*, disponível em: <http://www.samsung.com/br/info/privacy.html>. Acesso em: 14 set. 2016, 18:31.

Beacons (ou "*pixels*") transmitem informações do dispositivo para um servidor e podem ser incorporados em conteúdo *on-line*, vídeos e *e-mails*, permitindo ao servidor a leitura de determinados tipos de informações do aparelho, como data e hora de visualização de conteúdo ou do e-mail, o endereço IP, entre outras finalidades, em conjunto com *cookies*.

Algoritmos são códigos de programação utilizados para processar informação recebida por diversos meios, como os vistos anteriormente, mas não se limitando a esses – podem incluir curtidas, postagens, informações inseridas pelo usuário, marcações em fotos, etc. –, de forma a traçar um perfil acurado do usuário para uso em publicidade e direcionamento de informação, entre outros (FONSECA; MINOZZO, 17 maio 2015).

Esses recursos são interessantes às empresas na tentativa de monopolização da experiência da internet, pois apresentam apenas o que o usuário demonstra desejar, fazendo com que ele permaneça em determinado serviço, sem sair para outros. Entretanto, exemplos de reflexos negativos causados pelos algoritmos são o enclausuramento informativo e ideológico, que influencia o comportamento do usuário.

Por exemplo, o Facebook usa o algoritmo chamado EdgeRank, que foi alterado com o passar do tempo (SANTI, jun. 2015, p. 32-34):

> ...foi criado pelo próprio Face e originalmente seguia três critérios: afinidade (o quanto você interage com o autor daquele post), engajamento (número de *likes*, comentários e compartilhamentos que o *post* teve) e tempo (notícia velha não tem vez). Hoje, o algoritmo é muito mais complexo – segundo o Facebook, calcula mais de 100 mil variáveis, ajustadas de acordo com cada usuário. A empresa não diz quais são, inclusive por um segredo comercial – do contrário, o algoritmo poderia ser copiado por outras redes sociais.

No universo Google, algoritmos de grande poder servem não apenas à própria empresa como *search machine* e a seus diversos produtos disponibilizados para consumo direto pelos usuários, mas também são oferecidos comercialmente a terceiros em soluções completas para marketing digital, que realizam gerenciamento de métricas e análise de dados, como o Google Analytics e o DoubleClick.

O chamado *big data* é o resultado da possibilidade dessa coleta, processamento e utilização de dados, através das redes, realizado não em um banco de dados, mas em múltiplos, e envolve o cruzamento e correlação daqueles blocos de dados e informações dispersos para a geração de nova informação útil.

A empresa Acxiom, por exemplo, possui perfis que chegam a ter 1,5 mil atributos diferentes, incluindo raça, sexo, número de telefone, endereço, tipo de carro,

tipo de residência, locais de férias, compras recentes, problemas de saúde, parentes, cônjuges, amantes, etc. A empresa possui informações de 96% dos lares americanos e 700 milhões de perfis de pessoas do mundo todo (MATTOS[14], 19 abr. 2015).

Pesquisas em redes sociais com base em *likes* e outras informações não explícitas podem revelar a orientação sexual, QI alto ou baixo, estabilidade emocional, problemas familiares e outras características das pessoas, conforme pesquisas do Massachusetts Institute of Technology – MIT e da Academia de Ciências dos EUA, citadas pelo mesmo autor.

Para Alex Pentland[15], o *big data* faz com que seja possível medir diretamente o comportamento humano real, pois sua análise, em vez de mostrar o que as pessoas pensam ou declaram pensar, revela o que elas escolheram fazer, tornando a predição daquele muito precisa, pelo cruzamento de dados pessoais e metadados.

O cientista é otimista em relação ao seu uso, que pode servir aos mais diversos propósitos, como saúde, planejamento urbano, transporte público, economia de energia, entre outros, mas rejeita que dados pessoais fiquem sob o domínio de superempresas privadas (pois visam ao lucro, e não ao bem comum) e governos. Argumenta que é preciso evoluir muito na questão da privacidade de dados pessoais, pois a liberdade individual ficará seriamente afetada se não houver definição, através de uma reforma legal de grandes proporções, sobre a guarda e armazenagem dos dados digitais, defendendo, ainda, o direito de propriedade da pessoa sobre eles, como um ativo individual, o que permitiria inclusive vendê-los. Pentland alega que é algoritmicamente impossível analisar dados pessoais sem identificá-los, ou seja, de maneira anônima, mas que há como garantir o sigilo deles, dando como melhor exemplo o sistema bancário. Pensa ser possível criar um sistema de controle semelhante para os dados pessoais.

Ronaldo Lemos[16] (28 set. 2016) alerta que os algoritmos são alimentados por grande quantidade de dados e, atualmente, estão sendo desenvolvidos de forma que aprendam através destes. Entretanto, este tipo de aprendizado não possui um controle real pelo programador, o que pode gerar erros e, mesmo, preconceitos, devido à massa de dados analisados.

---

[14] Nelson Mattos é doutor em Ciências da Computação e assina coluna mensal sobre tecnologia em *Zero Hora*.

[15] Cofundador e Diretor do Media Lab do Instituto de Tecnologia de Massachusetts, autor de *Social Physics: How Good Ideas Spread – The Lessons of a New Science*, em entrevista às *Páginas Amarelas* de *Veja* (ZALIS, 11 mar. 2015).

[16] "Advogado, professor e pesquisador brasileiro respeitado internacionalmente, especialista em temas como tecnologia, mídia e propriedade intelectual" (Disponível em: <.https://www.google.com.br/?gws_rd=ssl#q=ronaldo+lemos>. Acesso em 01 dez. 2016.).

Esse fato faz com que esteja ocorrendo na União Europeia uma discussão sobre o direito ao esclarecimento pelo usuário da causa de determinada avaliação quanto à sua pessoa, em certa transação. O direito discutido daria inclusive ao usuário a possibilidade de ter o seu caso reavaliado por um ser humano.

2.3 PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA

Em 1977 foi editada, na Alemanha, a lei federal de proteção de dados – a primeira no mundo sobre o assunto (na verdade a primeira lei federal foi a sueca, em 1973, mas a primeira lei mesmo do mundo foi a do Estado de Hessen, Alemanha, em 1970).

O conceito de autodeterminação informativa também surgiu naquele país, na década de 1980, através de julgado do Tribunal Constitucional Alemão sobre as informações coletadas pelo censo, que incluiriam diversos dados pessoais, devido ao seu processamento e transferência a outros órgãos do governo.

O Tribunal Constitucional Federal, atendendo às reclamações constitucionais, acabou por julgá-las, em 15 de dezembro de 1983, parcialmente procedentes no que se referia ao necessário resguardo da segurança dos dados dos cidadãos a serem entrevistados.

As circunstâncias históricas deste fato ajudam a entender o porquê dos grandes protestos contra a maneira de realizar o censo naquela época: o receio quanto ao estado espião foi aumentado pela proximidade temporal com o que ocorre no livro *1984*, de George Orwell; a percepção de um grande risco referente à informação centralizada no governo, em uma época em que não havia a disseminação e descentralização propiciada pela internet e computadores pessoais; e também a presença próxima da espionagem estatal na Alemanha Oriental, em um tempo no qual ainda vigorava a guerra fria e não havia ocorrido a reunificação.

Sobre esta decisão, Menke (2015) refere que ela foi um marco na proteção de dados, influenciando diversos países, e consagra definitivamente a autodeterminação informativa.

Menke (idem) informa que a autodeterminação informativa integra o direito geral da personalidade, derivado dos princípios da dignidade da pessoa e da liberdade, e garante que seja possível a cada indivíduo desenvolver a sua personalidade.

Além da autodeterminação, o direito da personalidade engloba também o direito à autopreservação, que garante ao indivíduo o direito de recolher-se para si e ficar só, sem intromissões indevidas de terceiros, tanto na dimensão espacial como na social.

Engloba ainda o direito à autoapresentação, que possibilita a ele tanto insurgir-se quanto às representações falsas, deturpadas, degradantes ou não-autorizadas da sua pessoa, como também proteger-se de observações secretas e indesejadas da sua personalidade.

Assim, o indivíduo, através da autodeterminação informativa, obtém o poder de decidir acerca da divulgação e utilização de seus dados pessoais.

Segundo o autor, o direito à autodeterminação informativa insere-se no denominado direito geral da personalidade, que protege elementos da personalidade que não estejam cobertos pelas garantias especiais de liberdade da Lei Fundamental Alemã.

A autodeterminação informativa possui uma ligação direta com o princípio da dignidade humana e concede poder às pessoas sobre a tomada de decisão relativa à divulgação e utilização de seus dados pessoais, de forma que não tenham sua liberdade tolhida, o que influenciaria no exercício de outros direitos fundamentais de forma negativa.

A manipulação do indivíduo, por entes estatais ou privados que detenham informações pessoais suas, sem que ele tenha consciência disso, é uma das preocupações fundamentais do instituto da proteção de dados. Nessa situação, o direcionamento exercido pelo detentor dessas informações faz com que a relação não se desenvolva naturalmente devido à sua assimetria, dificultando, ou mesmo impedindo, o indivíduo de desdobrar/desenvolver a sua personalidade.

Esse raciocínio também é válido na relação entre duas empresas em que uma possua dados privilegiados que façam com que a relação ou negociação se torne um "jogo de cartas marcadas".

Nesse sentido, cabe alertar quanto ao comportamento adotado hoje por muitos, expondo-se excessivamente na Internet pela divulgação de seus dados pessoais sem nenhum controle, notadamente em sites e/ou aplicativos de relacionamento, como redes sociais e outros.

Menke (2015, p. 212), citando Alexander Roßnagel, quando "afirma que a proteção de dados é pré-requisito de um engajamento do indivíduo em questões públicas e, portanto, pressuposto funcional da comunicação democrática", sustenta que ela também "é pressuposto de uma 'autodeterminada decisão contratual' e, por conseguinte, pressuposto funcional da economia de mercado".

Roßnagel adverte, entretanto, que os dados pessoais não podem ser considerados propriedade do indivíduo, mas sim o resultado de uma observação social ou de um processo de comunicação multirrelacional.

Portanto, o direito da proteção de dados não regula o direito de propriedade, pois é um conjunto de normas sobre a informação e a comunicação a eles relacionada (idem p. 213).

Partilhando desta visão de que os dados pessoais não seriam de propriedade do indivíduo, Leonardi (2011) indica que devido à sua natureza intangível, dados e informações, depois de transmitidos não podem ser removidas do conhecimento alheio, e que parte das informações pessoais de um indivíduo é gerada em função de suas relações sociais e comerciais com outras pessoas, que também possuem algum direito sobre estas informações.

Devido a este fato, a autodeterminação informativa não pressupõe o domínio absoluto do indivíduo sobre os dados, excluindo os demais membros da sociedade, mas colabora para que ele tome as melhores decisões acerca da defesa dos seus interesses, que é o objetivo da sua proteção.

Entretanto, a utilização por terceiros dos dados pessoais de outrem sempre deverá se pautar pelo princípio da necessidade, tanto na coleta como no seu uso, preferindo-se a utilização de dados anônimos ou por meios que exponham só excepcionalmente a identificação do indivíduo, sempre que a finalidade possa, dessa maneira, ser atingida.

Alguns anos após ter sido a autodeterminação informativa reconhecida como direito fundamental, em 27 de fevereiro de 2008 o Tribunal Constitucional Federal proferiu decisão reconhecendo novo direito fundamental, em certa medida um desdobramento da *Informationelle Selbstbestimmung*: o denominado direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais (MENKE, 2015).

Essa decisão importantíssima insurgiu-se contra uma lei estadual que "permitia que aquela unidade da federação realizasse busca ou investigação secreta e remota de computadores de pessoas suspeitas de cometerem ilícitos criminais, autorizando ainda o monitoramento de todas as atividades do suspeito na internet" (idem, p. 216).

O contexto desta decisão insere-se em uma realidade onde não só o Estado, mas também a iniciativa privada, são atores que representam perigo ao indivíduo quanto aos seus dados pessoais, pelo fato deste estar cada vez mais exposto a modelos de negócio, equipamentos e programas que coletam dados referentes à sua personalidade.

A impugnação desta lei estadual foi uma reação à reação. A primeira reação parte do Estado editando leis tentando evitar que o terrorismo continuasse em solo alemão após a derrubada das Torres Gêmeas em 11 de setembro 2001 (World Trade Center, Nova York, EUA).

A segunda reação foi a do Tribunal Constitucional Federal, reafirmando os direitos da personalidade dos cidadãos, através do controle dos excessos legislativos praticados tendo em vista o controle do terrorismo.

Por tudo isso, "o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais atualiza a proteção da personalidade à realidade tecnológica do séc. XXI" (RAINER ERD apud MENKE, 2015).

Menke (2015, p. 218) informa que:

> Segundo o Tribunal Constitucional Federal, a autodeterminação informativa vai além da proteção da privacidade. Ela confere ao indivíduo o poder de basicamente determinar por si próprio sobre a divulgação e a utilização de seus dados pessoais. A autodeterminação informativa complementa a proteção constitucional da liberdade comportamental e da privacidade.

A proteção deve ir além das informações, que já são constitucionalmente protegidas, englobando também dados pessoais, pois, de acordo com tipo de coleta, tratamento, associação e propósitos de quem os utiliza, podem impactar fortemente a privacidade do indivíduo, alterando, assim, a liberdade do seu comportamento.

Conforme decisão do Tribunal Constitucional Federal, é necessário suprir lacuna existente na proteção ao indivíduo, pois a autodeterminação informativa protege o dado individualmente considerado ou um conjunto de dados, enquanto o direito geral da garantia da confidencialidade e da integridade dos sistemas técnicos-informacionais resguarda o próprio sistema e os dados vistos no seu sentido mais amplo, suprindo lacuna de proteção da autodeterminação informativa quanto ao direito geral da personalidade.

A proteção da Lei Fundamental é referente a dados pessoais do indivíduo em extensão e variedade que possam possibilitar conhecer as suas diversas dimensões, identificando, assim, a condução de sua vida pessoal, podendo chegar a um perfil extremamente acurado de sua personalidade, não importando tipo de aparelho utilizado, se fixo ou móvel.

A restrição dos direitos continua possível através de reserva legal, com edição de lei especial clara e específica, para prevenção e persecução criminal em caso concreto. Deve obedecer, ainda, a princípios da proporcionalidade e necessidade, sendo esse tipo de controle considerado *ultima ratio*, somente utilizado quando bens jurídicos como o corpo, a vida ou a liberdade da pessoa sejam atingidos ou quando a coletividade e o próprio Estado estejam ameaçados.

Não são meras suposições ou dados de experiência que autorizam a intervenção no novo direito fundamental da confidencialidade e integralidade dos sistemas técnico-informacionais, nem no direito da autodeterminação informativa.

É preciso verificar: a) o caso concreto, b) a proximidade temporal da transformação do perigo em dano e c) a ligação de determinadas pessoas individuais como causadoras do dano iminente.

A identificação de pessoas individualmente consideradas é indispensável para o monitoramento ser direcionado precisamente a elas, sem ofender direito de inocentes.

A autorização judicial também é indispensável, visto ser necessário uma instância independente e neutra para sopesar decisão tão invasiva, ainda mais pelo fato de o indivíduo desconhecer essa ação, não podendo se defender.

É aceita pelo Tribunal a autorização para monitoramento por comissões parlamentares de nível estadual ou federal, com expressa previsão legal para decidir sobre as restrições aos direitos de correspondência e comunicações à distância.

Menke (2015) considera essencial a criação de proteção com *status* de direito fundamental, para que essa garantia seja apenas excepcionalmente relativizada, devido à importância que as comunicações digitais atingiram no cotidiano das pessoas, sendo um avanço considerável na proteção aos direitos da personalidade.

Apesar de no Brasil existir proteção constitucional, com status de direito fundamental, com relação aos direitos anteriormente discutidos (Art. 5º, *caput* e Inciso X), a privacidade não é levada em consideração como deveria nos debates públicos, mesmo que a doutrina venha chamando a atenção sobre o assunto.

Verifica-se que nosso país não possui lei específica sobre o assunto (embora existam projetos de lei em andamento). Este fato, aliado à falta de informação das pessoas referente à proteção de seus dados pessoais, e da transformação de aplicações e *sites* em objeto de obtenção de informação, o torna especialmente preocupante.

2.4 CONTRATOS DE ADESÃO E POLÍTICAS DE PRIVACIDADE

O contrato de adesão é aquele onde um dos contratantes redige e determina todas as cláusulas, não havendo liberdade contratual devido à prevalência da vontade daquele, cabendo ao outro apenas aderir ao contrato previamente confeccionado, sem poder fazer nenhuma modificação; é aceitar ou rejeitar o contrato, de forma simples e em bloco, devido à inexistência da hipótese de qualquer discussão (GONÇALVES, 2012, p. 102).

O *CDC* deu a seguinte redação, quanto ao seu conceito (Vade Mecum Saraiva, 2016, p. 799):

> Art. 54. Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo.

Segundo Gonçalves (2012), esse tipo de contrato é normalmente disponibilizado por grandes empresas, em estado de oferta permanente e na forma de contrato-padrão, normalmente de consumo, e utilizado na maioria dos serviços essenciais, dos quais o consumidor não possui também a escolha de privar-se (idem, p. 102).

Já foi questionada sua natureza contratual, pela total falta de vontade de uma das partes, evidenciando um caráter institucional, mas prepondera a opinião daquela natureza, pela aceitação das suas cláusulas.

Hoje já existe alguns mecanismos que procuram consolidar uma concepção social, no sentido de procurar afastar estas desigualdades presentes nos contratos de adesão, como, por exemplo, a inversão do ônus da prova e a fixação do foro brasileiro nas questões consumeristas, em virtude da supremacia socioeconômica de um dos contratantes sobre o outro, reduzindo em algum termo a fixação das cláusulas contratuais e da aplicação plena do *pacta sunt servanda*, proveniente do liberalismo econômico (VANCIM; MATIOLI, 2014).

Os contratos de adesão eletrônicos são utilizados pela necessidade de padronização, pela celeridade na sua celebração (através de apenas um clique) e pela facilidade na sua administração pós-contratual. Na maioria das vezes, estaremos diante de contratos conhecidos, como compra e venda, cessão de uso, prestação de serviço, etc. (TEIXEIRA, 2014).

Estes contratos obedecem a lógica da contratação "convencional", segundo o autor citado, sendo exigível capacidade do agente, objeto lícito e forma válida, com a diferença de efetuarem-se através da internet, com auxílio de computador (ou outro dispositivo) e *software*.

Na sua celebração, devido à rapidez com que é realizada, e de forma a reduzir alegações dos usuários de não terem tido oportunidade de ler o contrato, em diversas oportunidades é utilizada a estratégia de somente poder aceitar o contrato se a barra de rolagem tiver chegado ao fim do documento ou, ainda, que o mesmo seja impresso (TEIXEIRA, idem).

Uma diferença nesse tipo de contratação é que o seu objeto pode ter entrega física, eletrônica (*download*) ou, ainda, pelo uso de serviço virtual, como acesso a sites ou outros, segundo Teixeira (idem). Ou seja, a execução do contrato pode se dar pelo meio físico, muito embora a sua formação tenha ocorrido pelo meio eletrônico.

A contratação pela internet disponibiliza um alcance territorial muito grande a um custo muito baixo, o que favoreceu o rápido crescimento do *e-commerce*, mas esses contratos de adesão eletrônicos podem causar dificuldades aos usuários na garantia de seus direitos, pois sua celebração, muitas vezes, é feita com empresas internacionais que não possuem representação no Brasil ou que possuem sites localizados em locais distintos da sua sede, o que pode levar a controvérsias jurídicas dada a insegurança do usuário quanto ao conteúdo de eventual lei estrangeira a ser aplicável.

Um problema seriamente considerado nesse ambiente é a segurança da transação, que hoje praticamente foi resolvido com a utilização da criptografia e certificação digital em inúmeros sites. Nesse sentido, o contrato de adesão eletrônico é um documento eletrônico que deve ter garantida a sua autenticidade, integralidade e validade jurídica (TEIXEIRA, 2014).

A política de privacidade de um provedor de conteúdo, de um produto ou serviço prestado virtualmente pode ser conceituada como um contrato de adesão eletrônico. Neste contrato, é exigida aceitação das práticas da empresa/entidade (ou mesmo pessoa) em relação à privacidade e proteção de dados referentes às informações do usuário.

Hoje existem requisitos importantes a serem observados na contratação eletrônica estabelecidos no Dec. nº 7962/2013, especialmente em seu art. 4º [17], mas inexiste um formato padrão exigido para sua formulação. Seu conteúdo é livremente

---

[17] **Art. 4º** Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:

I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos;

II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação;

III - confirmar imediatamente o recebimento da aceitação da oferta;

IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;

V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato;

VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor; e

VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

Parágrafo único. A manifestação do fornecedor às demandas previstas no inciso V do caput será encaminhada em até cinco dias ao consumidor.

determinado por quem o propõe, embora, em tese, devesse tratar da garantia de direitos dos usuários, informando quais informações são coletadas, de que maneira, com qual fim, por quanto tempo e qual o poder de retificação e cancelamento das informações após sua coleta, etc. Estes pontos quase sempre são abordados, com maior ou menor especificação, mas normalmente de forma a privilegiar a proteção jurídica de quem os propõe quanto às possíveis demandas movidas pelos usuários.

Dessa forma, uma política de privacidade não possui o condão de colocar o usuário no pleno domínio de sua autodeterminação informativa, muito antes o contrário. É questionável o *quantum* de autonomia da vontade deveria ser aceitável tanto na proposição de um contrato de adesão dessa natureza como na sua aceitação pelo usuário, por tratar-se de direito da personalidade constitucionalmente protegido de uma parte hipossuficiente, frente a outra assimetricamente poderosa técnica e economicamente.

Na maioria das vezes, esses contratos obtêm o aceite (“assinatura”) do usuário através de apenas um clique, condição para uso da facilidade, embora possam existir ou ser inventadas outras variantes. Podem revestir-se, eventualmente, da forma de simples declaração, escondida atrás de um *link* ao pé da página, ou apenas como aviso de que serão utilizados *cookies*, com aceite tácito do usuário pelo uso.

Em tese, deveriam ser documentos redigidos obedecendo ao disposto em nosso ordenamento jurídico, o que, muitas vezes, não ocorre, pois, certamente, a maioria dos domínios registrados são estrangeiros, como já foi referido, o que influi na legislação escolhida como base para sua formulação e na escolha do foro competente para proposição de ações pelos contratantes.

Entretanto, essa breve exposição sobre o que é uma política de privacidade e suas principais características serve apenas para demonstrar a “ponta do iceberg”, a parte mais visível da problemática relativa à proteção de dados.

Nosso foco será visto a seguir, analisando com mais profundidade, mas certamente não esgotando o assunto, o que atualmente o ordenamento jurídico brasileiro dispõe sobre a privacidade e a proteção de dados pessoais no meio virtual, verificando seus pontos mais relevantes, para concluir sobre a necessidade de criação de lei específica para o tema em questão, como já implementado em outros países.

3 PRIVACIDADE E PROTEÇÃO DE DADOS NA CONSTITUIÇÃO FEDERAL E NO CÓDIGO CIVIL

3.1 PRIVACIDADE COMO DIREITO FUNDAMENTAL DA PERSONALIDADE

O direito à privacidade do indivíduo é um direito fundamental de primeira dimensão, na classificação de Bobbio (2004) (liberdade negativa), que explicita o dever estatal de abstenção quanto à sua intromissão na esfera da intimidade da pessoa[18].

Como será visto na sequência, o direito fundamental à privacidade está positivado na *Constituição Federal*, representado pelos termos "intimidade" e "vida privada" (SUPREMO..., 26 jul. 2011), e melhor detalhado ainda pelo nosso *Código Civil*.

Privacidade é direito que aparece positivado também em outros diplomas jurídicos do nosso ordenamento, que abordam de maneira mais específica a privacidade na internet, os quais serão vistos na seção seguinte.

Embora a proteção devesse ser integrada em um eixo constitucional, o que se observa é uma atuação fracionada, através de *habeas data*, *CDC* ou outras garantias e recursos, mais orientada por uma lógica específica de determinados campos do que uma estratégia baseada na tutela integral da personalidade através da proteção de dados pessoais (DONEDA, 2006).

O que é possível depreender da exposição do assunto até agora é que a proteção de dados é parte integrante do conceito de privacidade, assim como a autodeterminação informativa.

Proteção de dados e autodeterminação informativa representam o aspecto mais específico da privacidade no ambiente virtual e, portanto, apesar de não expressamente citados no Art. 5º da *Constituição Federal*, assumem também o caráter de direitos fundamentais que devem ser respeitados e garantidos de forma enérgica.

Segundo Doneda (2006), a privacidade metamorfoseou-se, especializando-se em proteção de dados pessoais na Internet. A proteção dos dados é a proteção da privacidade por outros meios, confirmando o dito anteriormente e, destas observações do autor, pode-se deduzir de que a autodeterminação informativa é o direito que exsurge da proteção de dados a ser garantida no ciberespaço.

---

[18] Hoje, além da intromissão do estado na vida privada, se faz sentir de forma intensa a intromissão pelo setor privado, especialmente pelo desenvolvimento da tecnologia e das novas mídias. É lícito questionar, neste cenário, se os direitos do homem no ciberespaço, devido às suas características únicas, não deveriam ser considerados uma nova dimensão.

Segundo o autor, a força expansiva da função da proteção de dados pessoais verifica-se na própria mudança do ambiente no qual circulam os dados e se manifestam os interesses ligados à privacidade.

Como refere Doneda (2006), uma atividade que utiliza os dados pessoais não é um problema, mas deve ser harmonizada com os direitos fundamentais através de instrumentos que possibilitem um efetivo controle sobre eles.

A utilização do princípio da proporcionalidade é importante porque a tecnologia frequentemente se sobrepõe à regulação e foge da possibilidade de controle pessoal devido à velocidade do fluxo de dados e ao desconhecimento sobre quem os usa e como eles são usados.

Por último, não é possível perder de vista a visceral correlação dos aspectos da privacidade com o princípio que é base para o nosso ordenamento jurídico, que é a dignidade humana.

3.2 PRIVACIDADE NA CONSTITUIÇÃO FEDERAL

Este direito está positivado em nossa *Constituição*, no Art. 5º, em aspectos diferentes, em seus incisos X, XI e XII.

O inciso X afirma que "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" (SUPREMO..., 26 jul. 2011).

Para esta monografia, a condição de ser humano pressupõe sua titularidade de direitos da personalidade como os elencados anteriormente na *CF*, principalmente o da privacidade, pois é ordinariamente a pessoa natural que sofre a violação desses direitos e não a pessoa jurídica – no mais das vezes, a violadora.

Nesse inciso, o aspecto concernente à privacidade é tomado em um sentido amplo, abrangendo aspectos gerais da subjetividade do ser humano, ressaltando o caráter de inviolabilidade que deve ser respeitado tanto pelo Estado como por quaisquer terceiros, evidenciando-se, assim, que se trata de um direito oponível *erga omnes* e que justifica a sanção de indenização material ou moral de quem o violar (SUPREMO..., 26 jul. 2011).

Já o inciso XI apresenta, em sua redação, a primeira concepção histórica de privacidade, a de ser deixado só, sem ser incomodado, em um local de extrema importância para o indivíduo, o seu lar, da seguinte maneira: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em

caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" (idem).

Aqui a inviolabilidade é ressaltada no seu aspecto material, que hoje se traduz não somente na morada, mas também em um sentido mais abrangente, como outros locais que sejam importantes para a manifestação da individualidade e que assim mereçam a proteção da sua privacidade, como a garagem, o escritório/local de trabalho e imóvel de lazer, entre outros[19], e assim protegendo reflexamente dispositivos eletrônicos no seu interior que contenham dados e informações pessoais.

No inciso XII é que está expresso diretamente o aspecto do direito à privacidade de maior interesse para este estudo, o das comunicações de dados, com a seguinte redação: "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" (SUPREMO..., 26 jul. 2011).

A diferença é que, quanto aos dados armazenados, fica claro, pelo inciso XI, que seu sigilo pode ser quebrado por ordem judicial, enquanto o inciso XII dá a entender (por exclusão) que a interceptação de dados somente pode ser determinada na ocorrência de estado de defesa ou de sítio, salvo melhor juízo (LENZA, 2012).[20]

---

[19] Abaixo, fragmentos de decisões referentes à inviolabilidade material da privacidade, exemplificando a aplicação sobre o disposto no Art. 5º, XI.

"De que vale declarar a Constituição que 'a casa é asilo inviolável do indivíduo' (art. 5º, XI) se moradias são invadidas por policiais munidos de mandados que consubstanciem verdadeiras cartas brancas, mandados com poderes de a tudo devassar, só porque o habitante é suspeito de um crime? Mandados expedidos sem justa causa, isto é, sem especificar o que se deve buscar e sem que a decisão que determina sua expedição seja precedida de perquirição quanto à possibilidade de adoção de meio menos gravoso para chegar-se ao mesmo fim. A polícia é autorizada, largamente, a apreender tudo quanto possa vir a consubstanciar prova de qualquer crime, objeto ou não da investigação. Eis aí o que se pode chamar de autêntica 'devassa'. Esses mandados ordinariamente autorizam a apreensão de computadores, nos quais fica indelevelmente gravado tudo quanto respeite à intimidade das pessoas e possa vir a ser, quando e se oportuno, no futuro, usado contra quem se pretenda atingir" (HC 95.009, Rel. Min. Eros Grau, julgamento em 6-11-2008, Plenário, *DJE* de 19-12-2008.)

"Domicílio – Inviolabilidade noturna – Crime de resistência – Ausência de configuração. A garantia constitucional do inciso XI do art. 5º da Carta da República, a preservar a inviolabilidade do domicílio durante o período noturno, alcança também ordem judicial, não cabendo cogitar de crime de resistência. " (RE 460.880, Rel. Min. Marco Aurélio, julgamento em 25-9- 2007, Primeira Turma, *DJE* 29-2-2008.)

"Para os fins da proteção jurídica a que se refere o art. 5º, XI, da CF, o conceito normativo de 'casa' revela-se abrangente e, por estender-se a qualquer aposento de habitação coletiva, desde que ocupado (CP, art. 150, § 4º, II), compreende, observada essa específica limitação espacial, os quartos de hotel. Doutrina. Precedentes. Sem que ocorra qualquer das situações excepcionais taxativamente previstas no texto constitucional (art. 5º, XI), nenhum agente público poderá, contra a vontade de quem de direito (*invito domino*), ingressar, durante o dia, sem mandado judicial, em aposento ocupado de habitação coletiva, sob pena de a prova resultante dessa diligência de busca e apreensão reputar-se inadmissível, porque impregnada de ilicitude originária. Doutrina. Precedentes (STF)." (RHC 90.376, Rel. Min. Celso de Mello, julgamento em 3-4-2007, Segunda Turma, *DJ* de 18-5-2007.)

[20] Nota: Até a edição da Lei 9.296/1996, o entendimento do Tribunal era no sentido da impossibilidade de interceptação telefônica, mesmo com autorização judicial, em investigação criminal ou instrução

Atualmente, as comunicações telegráficas estão praticamente extintas, devido à sua obsolescência técnica. A correspondência postal está cada vez mais em desuso, devido ao surgimento de novas formas de comunicação eletrônica, e quase somente empresas ou entidades ainda a utilizam como forma de comunicação, basicamente para a remessa de boletos bancários, notificações e, eventualmente, de mala-direta, forma de publicidade de baixa eficácia e decadente.

Entretanto, o serviço postal ainda é utilizado de forma intensa pelas empresas para o escoamento de produtos de pequeno volume, os quais são comprados, cada vez mais, em sites na Internet.

A telefonia digital, notadamente a móvel, e principalmente as novas mídias digitais é que são as formas de comunicação mais utilizadas pelas pessoas, fazendo com que seu crescimento seja vertiginoso, pois oferecem serviços cada vez mais diversificados, são praticamente instantâneas e, hoje, de utilização possível até mesmo pelas classes mais humildes.

São as mídias digitais que interessam à presente monografia, pelo enorme fluxo de dados e informações pessoais que canalizam através da internet, espaço onde, potencialmente, pode ocorrer o maior número de violações da privacidade.

---

processual penal, tendo em vista a não recepção do art. 57, II, e da Lei 4.117/1962 (Código Brasileiro de Telecomunicações).

Abaixo, fragmentos de decisões referentes à inviolabilidade da privacidade das comunicações, exemplificando a aplicação sobre o disposto no Art. 5º, XII.

"Conforme disposto no inciso XII do art. 5º da CF, a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, ficando a exceção – a quebra do sigilo – submetida ao crivo de órgão equidistante – o Judiciário – e, mesmo assim, para efeito de investigação criminal ou instrução processual penal. (...)

Conflita com a Carta da República norma legal atribuindo à Receita Federal – parte na relação jurídico-tributária – o afastamento do sigilo de dados relativos ao contribuinte. " (RE 389.808, Rel. Min. Marco Aurélio, julgamento em 15-12-2010, Plenário, *DJE* de 10-5-2011.)

"Colima o investigado o bloqueio do levantamento de dados, informações, enfim, todas as diligências típicas de um inquérito, procedimento este já autorizado judicialmente e que nada tem de inconstitucional ou ilegal." (Inq. 2.727-ED, Rel. Min. Ellen Gracie, julgamento em 25-3-2010, Plenário, *DJE* de 7-5-2010.)

"Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados', e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse. " (MS 21.729, voto do Rel. Min. Sepúlveda Pertence, julgamento em 5-10-1995, Plenário, *DJ* de 19-10-2001.)

Ação direta de inconstitucionalidade. Parágrafo único do art. 1º e art. 10 da Lei 9.296, de 24-7-1996. Alegação de ofensa aos incisos XII e LVI do art. 5º da CF, ao instituir a possibilidade de interceptação do fluxo de comunicações em sistemas de informática e telemática. Relevantes os fundamentos da ação proposta. Inocorrência de *periculum in mora* a justificar a suspensão da vigência do dispositivo impugnado. Ação direta de inconstitucionalidade conhecida. Medida cautelar indeferida." (ADI 1.488-MC, Rel. Min. Néri da Silveira, julgamento em 7-11-1996, Plenário, *DJ* de 26-11-1999.)

3.3 PRIVACIDADE NO CÓDIGO CIVIL DE 2002

Para Duarte (2010), a personalidade é um atributo do indivíduo que consiste na aptidão para o desempenho de um papel jurídico, ou seja, para adquirir direitos e contrair obrigações.

Diferentemente do código de 1916, o atual Código Civil de 2002 refere-se a deveres, em lugar de obrigações, evidentemente para abarcar não só as relações patrimoniais.

O Código Civil também nomina *pessoa* como sujeito de direito, "que indica o ser humano enquanto situado perante os demais componentes da coletividade" (REALE, 08 nov. 2003) em vez da expressão *homem*, palavra de sentido abstrato e genérico de indivíduo.

O objeto dos direitos da personalidade são faculdades jurídicas[21] que se situam no âmbito da própria pessoa, de acordo com Duarte (2010).[22].

Diga-se, de passagem, que os direitos fundamentais, como a privacidade, são concedidos à pessoa desde a condição de nascituro, que adquire a personalidade civil a partir do nascimento com vida (BRASIL, 10 jan. 2002, Art. 2º) Apesar de controvérsia doutrinária, Duarte (2010, p. 30) afirma que é:

> ...sustentável que a personalidade já se inicia com a concepção, pois, sem tal atributo, inviável supor a existência de direitos subjetivos; contudo, não se trata de um atributo definitivo para o nascituro, que se irá consolidar ou resolver conforme ocorra ou não o nascimento.

Certo é que a proteção de direitos fundamentais, notadamente a privacidade e seu corolário, acompanha a vida da pessoa, tanto a capaz como a incapaz (que pode ser representado ou assistido por responsável), pois ambas poderão ter seus dados pessoais violados ou serem rastreadas digitalmente, desde que possuam acesso e conhecimento básico para uso de dispositivo com conexão à internet.

---

[21] De acordo com Amaral (2008), as faculdades jurídicas são os poderes de agir que estão contidas no direito subjetivo, e consistem em possibilidade de atuação jurídica que o direito reconhece na pessoa que se encontra em uma determinada situação.

[22] "Os direitos da personalidade são *absolutos, extrapatrimoniais e perpétuos*. De seu caráter absoluto decorre a oponibilidade *erga omnes*, na medida em que geram o dever geral de abster-se de sua violação. Sua extrapatrimonialidade afasta a possibilidade de transmissão e, em consequência, são direitos impenhoráveis. Sendo perpétuos, não comportam renúncia, nascendo e extinguindo-se com a pessoa, embora sob alguns aspectos possam gozar de proteção para depois da morte.

A impossibilidade de renúncia não significa, entretanto, que a pessoa não possa em algumas circunstâncias, como ao revelar fatos de sua intimidade, deixar de exercê-los, mas tal não significa que deles abriu mão, podendo, por isso, a qualquer tempo recuperar-lhes o pleno exercício".

A personalidade, cuja existência termina com a morte (BRASIL, 10 jan. 2002, Art. 6º) – natural ou presumida – assim como os seus direitos irrenunciáveis e intransferíveis (idem, Art. 11), continuam a possuir tutela para fazer cessar ameaça ou lesão aos direitos da personalidade, cuja legitimidade processual continua através do cônjuge ou qualquer parente em linha reta ou colateral até o quarto grau, o que possibilita a reclamação de perdas e danos, sem prejuízo de outras sanções previstas em lei (idem, Art.12).

Essa legitimidade extraordinária revela a importância dada pelo diploma civil aos direitos da personalidade. Aliás, uma das grandes novidades do Código Civil de 2002 foi a criação de um capítulo específico para os direitos da personalidade.

A sanção privada compreende não só a indenização por perdas e danos, que não é instrumento específico de proteção dos direitos da personalidade, mas também a pretensão cominatória, pois o Art. 287 do Código de Processo Civil (BRASIL, 16 mar. 2015) prevê expressamente a indenização moral ou material como cumulável com a multa, para o caso de descumprimento da sentença ou da decisão antecipatória de tutela[23].

Um dado fundamental para qualquer ser humano é o nome, nele compreendido o prenome e o sobrenome (BRASIL, 10 jan. 2002, Art. 16).

Segundo Duarte (2010, p. 37), "Embora o legislador haja tomado o nome como objeto dessa proteção, mais amplo é o sentido, pois alberga a inviolabilidade dos direitos à honra, à intimidade, ao recato e ao segredo pessoal".

Existe a determinação que, sem autorização, não é possível a utilização do nome alheio em propaganda comercial (termo não técnico, que deve ser entendido como publicidade comercial), como consta no CC, Art. 18 (BRASIL, 10 jan. 2002). Aqui o que se dá é proteção ao que é considerado *res extra commercium*, o nome da pessoa, que, entretanto, poderá ser usado para fins comerciais desde que o seu uso seja expressamente concedido pelo interessado[24].

---

[23] Dano à imagem. Direito da personalidade. Veiculação da imagem do autor em carnês de pagamento (conta de energia elétrica). Ausência de autorização. Reprodução para fins comerciais. Sentença que reconheceu o dano moral. Apelação requerendo reforma total da sentença. Recurso adesivo para majoração. 1 – A imagem constitui um dos elementos inerentes à personalidade, sendo o respectivo direito intransmissível e irrenunciável, porém, disponível. 2 – 0 conjunto probatório é firme no sentido de que não houve autorização do titular do direito para o uso de sua imagem em propaganda da ré. 3 – A utilização da imagem ocorreu com nítidos fins publicitários e comerciais. 4 – 0 dever de indenizar decorre da constatação da utilização da imagem sem autorização e com fins comerciais, sendo desnecessária a comprovação de veiculação de cunho vexatório. 5 – Danos morais que devem ser majorados. Desprovimento do recurso da ré. Provimento parcial ao recurso adesivo (TJRJ, Ap. n. 2007.001.13848, rel. Des. Elton Leme, j. 26.06.2007).

[24] Jurisprudência: Associação civil. Estatuto. Inserção não autorizada de nome civil INADM. Direito personalíssimo protegido pelo ordenamento jurídico RNP. Sendo uma expressão da personalidade o nome de uma pessoa, viva ou morta, merece a proteção do direito. Assim, contra a sua vontade ou de cônjuge e herdeiros, se esta for falecida, não pode ser inserido em estatutos sociais (TJSP, Recurso n. 210.753, rel. Des. Gildo dos Santos, j. 19.08.1993).

Também a divulgação dos seus escritos, a transmissão da palavra ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas (salvo se autorizadas ou se necessárias à administração da justiça ou manutenção da ordem pública), a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade ou se destinarem a fins comerciais (idem, Art. 20). Nestes casos, tratando-se de morto ou ausente, possuem legitimidade para requerer sua proteção o cônjuge, os ascendentes e os descendentes, como já visto.

Decorrência lógica do exposto pelos artigos do CC, apresentados anteriormente, é o art. 21 (idem), que nos diz: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Conforme entende Duarte (2010, p. 40-41), o direito à integridade moral abarca, dentre outros, os aspectos referentes à intimidade, ao segredo e à imagem, sempre exigíveis e que acarretarão indenização caso violados, atinjam a honra ou tenham objetivos comerciais, neste caso com a devida autorização, e como os direitos da personalidade são irrevogáveis, esta sempre poderá ser revista pelo seu titular.

Atualizando a informação de Duarte (2010), a tormentosa questão referida pelo mesmo sobre a divulgação de cartas (transmissão escrita da palavra) hoje encontra paralelo na divulgação de e-mails transmitidos, mensagens instantâneas, *chats* e outros tipos de aplicativos, que podem conter ainda imagens ou áudio e que merecem redobrada proteção, devido à facilidade de replicação na rede. Ele diz que a legitimidade de autorizar a publicação pode ser tanto da pessoa referida, pelo subscritor, ou pelo destinatário.

Responsabilidade civil. Uso indevido do nome. Prejuízo extrapatrimonial. É vedada a utilização do nome alheio com propósito comercial sem a devida autorização - art. 18 do Código Civil/2002. Caso em que curso pré-vestibular incluiu o nome do autor dentre os seus ex-alunos que tiveram aprovação para ingresso em Universidades, a despeito de o demandante jamais haver frequentado a instituição-ré. Uso indevido do nome do indivíduo com fins comerciais. Dano moral expresso na natural contrariedade da pessoa em ter seu apelido vinculado a serviço do qual não se valeu. A indenização não deve ser em valor ínfimo, nem tão elevada que torne desinteressante a própria inexistência do fato. Atendimento às particularidades das circunstâncias do evento. Incidência do princípio da proporcionalidade. Indenização arbitrada em 1o grau mantida. Por maioria, acolheram os embargos, vencido o relator, que os acolhia em menor extensão (TJRS, Embargos infringentes n. 70025123647, 5o Grupo de Câmaras Cíveis, rel. Jorge Alberto Schreiner Pestana, j. 18.07.2008, *DJ* 12.09.2008).

"Pseudônimo" que etimologicamente significa falso nome, resultando do hibridismo *pseudos* (do grego, mentira, falsidade) e *nomen* (do latim, nome), não significa um nome destinado a ocultar ilicitamente por inteiro a identidade de quem o ostenta, mas encobrir a identidade somente em certos aspectos correspondentes à atividade profissional ou intelectual da pessoa.... Não se deve, porém, confundir pseudônimo com alcunha, que, na linguagem comum, também se designa por apelido e normalmente se refere a uma característica particular do indivíduo. Igualmente não se pode confundir com anonimato, pois o pseudônimo também tem função identificadora.... É, porém, necessário, para que o pseudônimo ganhe proteção, que haja adquirido a importância do nome, o que se configura pelo uso e pela notoriedade" (DUARTE, 2010, p. 39).

Tal afirmação é questionável, pois o subscritor pode estar transmitindo tanto informação sensível de outrem (e assim cometendo violação de direito) como segredo de si próprio (que também merece proteção) e, assim, não parece ser razoável a sua autorização pelo destinatário.

É certo que a lei contém ressalvas, admitindo a divulgação da imagem ou de fato quando necessária a fins judiciais ou quando interessem à ordem pública.

Não obstante a cessação da personalidade com a morte, mesmo assim são preservados certos aspectos do direito da sua personalidade, como a honra, a boa fama da pessoa falecida, o que, aliás, legitima a revisão criminal de condenado falecido (BRASIL, 10 jan. 2002, Art. 623), podendo a respectiva proteção ser reclamada pelo cônjuge, ascendente ou descendente, compreendendo-se nesse rol também o convivente.[25]

Com base no visto nos artigos anteriormente apresentados, podemos verificar que como Doneda (2005) nos mostra,

> A proteção da privacidade é um dos temas mais delicados na matéria dos direitos da personalidade, isto pelo potencial de ofensas à personalidade ter crescido abruptamente com o desenvolvimento tecnológico e também pela dificuldade dos instrumentos de tutela tradicionais do ordenamento realizarem adequadamente esta proteção. O novo Código dá mostras disto, ao prever que o juiz "adotará as providências necessárias" para impedir a violação da privacidade.
>
> Não deve entender-se que a proteção da privacidade não se possa fazer também por via da responsabilidade civil – ela é mais um instrumento que pode e deve ser utilizado.
>
> Apenas é patente a dificuldade em se utilizar este instituto quando o dano é tão dificilmente demonstrável, como em tantos casos de violação da privacidade, apesar de evidente a antijuridicidade pelo desrespeito à pessoa e à sua dignidade.
>
> Ao clamar pela criatividade do magistrado para que tome as providências adequadas, o Código dá mostras da necessidade de uma atuação específica de todo o ordenamento na proteção da privacidade da pessoa humana, que seja uma resposta eficaz aos riscos que hoje corre.

A proteção de dados, cada vez mais necessária, deriva diretamente do direito à privacidade, e desta busca tutelar aspecto importante. O referido pelo autor parece sinalizar a necessidade de novo instrumental jurídico, adequado e específico, como uma lei de proteção de dados pessoais, para que esta tutela possa ser efetiva.

---

[25] É importante ressaltar que o STF julgou procedente a ADIn n. 4.815, de 10/06/2015, que deu interpretação conforme à Constituição, sem redução de texto, aos Art. 20 e 21 para, em consonância com os direitos fundamentais à liberdade de pensamento e sua expressão, de criação artística e produção científica, declarar inexigível o consentimento de pessoa biografada e coadjuvantes relativamente a obras biográficas literárias ou audiovisuais, sendo por igual desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas) (VADE MECUM, 2016, p.157).

4 PRIVACIDADE E PROTEÇÃO DE DADOS NO CÓDIGO DE DEFESA DO CONSUMIDOR E NO *MARCO CIVIL* DA INTERNET

4.1 PRIVACIDADE E PROTEÇÃO DE DADOS NO *CÓDIGO DE DEFESA DO CONSUMIDOR*

Aspectos importantes sobre a proteção de dados de usuários na internet quanto aos provedores de conexão e de aplicações são garantidos pela Lei nº: 8.078/1990, o *Código de Defesa do Consumidor – CDC*.

O *CDC* é de grande aplicação prática nessa questão, apesar de, em uma visão inicial, não abarcar todas as situações passíveis de proteção para o usuário, como a simples navegação, ou outras situações que possam não se enquadrar como de consumo, como a utilização de sites governamentais, por exemplo.

De toda forma, como grande parcela das interações *on-line* do usuário (inclusive as aparentemente gratuitas) se dá em sites que contêm aplicações desenvolvidas por empresas, provedores de aplicação que obviamente possuem interesse econômico nessa relação, assim como através do comércio eletrônico propriamente dito, é extremamente ampla a abrangência de utilização do *CDC* para defesa dos consumidores virtuais (note-se que aqui não se fala de pessoas ou usuários, mas sim de consumidores).

No caso da Internet, na abordagem por parte do *CDC* quanto aos direitos do consumidor, parte hipossuficiente em relação às empresas, é importante fazer referência aos contratos de adesão, largamente utilizados e acerca dos quais serão abordadas as principais características.

No ambiente virtual, empresas são conceituadas como provedores de conexão ou de aplicação, e os contratos de adesão utilizados por elas diferem em alguns pontos dos aplicados no mundo físico – no ambiente virtual, estes contratos potencializam a possibilidade da violação de diversos direitos, um dos quais é a privacidade.

O *CDC* tem vida própria, tendo sido criado como subsistema autônomo e vigente dentro do sistema constitucional brasileiro (NUNES, 2012) que atinge toda e qualquer relação jurídica que possa ser caracterizada como de consumo, mesmo que ela esteja também regrada por outra norma jurídica infraconstitucional.

Assim, como lei especial, prevalece sobre as demais no que contrariar suas disposições, de tal modo que, naquilo que com elas colidirem, perdem eficácia no caso concreto, com exceção da *Constituição*, além de ser de aplicação supletiva e complementar quanto às outras normas.

De acordo com Vancim e Matioli (2014), seu campo de atuação é amplo, pois inclui em seu espectro protetivo, com o propósito de equilibrar as relações consumeristas, não somente os interesses individuais, mas também os individuais homogêneos, os difusos e os coletivos.

Segundo Nunes (2012), é por determinação constitucional, constante no art. 43 do ADCT/*CF*, que a Lei n. 8.078/90 é Código; além disso, o *CDC* é uma lei principiológica, modelo que até então não existia em nosso ordenamento jurídico.

Tem-se que a defesa do consumidor é cláusula pétrea, de dever absoluto para o Estado (BRASIL, 1988, art. 5º, XXXII); portanto, o *CDC* nada mais fez do que concretizar, em uma norma infraconstitucional, esses princípios e garantias constitucionais.

O *CDC* possui grande interesse social, pois pretende equiparar a parte hipossuficiente, o consumidor, na luta por seus direitos frente aos fornecedores.

Embora a privacidade relacione-se à pessoa natural, a proteção de dados é um direito a ser resguardado excepcionalmente, inclusive, em uma relação comercial entre empresas[26], já que, se uma delas possui uma informação privilegiada sobre a outra, ocorrerá uma assimetria de informações (podendo determinar o preço, por exemplo).

Entretanto, como *a priori* uma empresa não é considerada consumidora quando negocia com outra com o intuito de obter lucro, admite-se esta condição somente quando o produto ou serviço é utilizado na condição de destinatário final[27].

Como já visto, o *CDC* objetiva a garantia de direitos individuais e coletivos dos consumidores e, de acordo com o seu Art. 1º , é norma cogente, não disponível pelas partes, pois as regras são imperativas, obrigatórias e inderrogáveis.

Também já referido, o *CDC* é uma lei principiológica, conforme Teixeira (2014), que não versa sobre um contrato específico entre consumidor e fornecedor e,

---

[26] Art. 52, CC – Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade (BRASIL, 10 jan. 2002).

[27] A teoria finalista aprofundada ou mitigada amplia o conceito de consumidor incluindo todo aquele que possua vulnerabilidade em face do fornecedor. Decorre da mitigação dos rigores da teoria finalista para autorizar a incidência do CDC nas hipóteses em que a parte, pessoa física ou jurídica, embora não seja tecnicamente a destinatária final do produto ou serviço, se apresenta em situação de vulnerabilidade. Assim, o conceito-chave no finalismo aprofundado é a presunção de vulnerabilidade, ou seja, uma situação permanente ou provisória, individual ou coletiva, que fragiliza e enfraquece o sujeito de direitos, desequilibrando a relação de consumo (TRIBUNAL..., 21 nov. 2016).

"AGRAVO DE INSTRUMENTO. CONSUMIDOR. TEORIA FINALISTA APROFUNDADA. Ao aplicar o art. 29 do CDC, o STJ tem adotado a teoria do finalismo aprofundado, na qual se admite, conforme cada caso concreto, que a pessoa jurídica adquirente de um produto ou serviço possa ser equiparada a consumidor, quando demonstrada a sua vulnerabilidade frente ao fornecedor ou vendedor, ainda que não destinatária final do serviço. Agravo provido. (Acórdão n. 724712, 20130020163383AGI, Relatora: ANA MARIA DUARTE AMARANTE BRITO, 6ª Turma Cível, Data de Julgamento: 16/10/2013, Publicado no DJE: 22/10/2013. Pág.: 129)" (idem).

dessa forma, pode ser aplicado também às relações jurídicas estabelecidas através da internet, desde que configurada uma relação de consumo.

Este diploma legal possui alcance subjetivo abrangente, pois, de acordo com o Art. 2º, *caput*, *CDC* (BRASIL, 11 set. 1990), consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Além disso, no Art. 3º, *caput*, *CDC* (idem), descreve o fornecedor como toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, inclusive despersonalizada, que desenvolve atividade econômica, abrangendo os serviços.

Com a mesma abrangência, este artigo, em seu §1º, qualifica produto como qualquer bem, móvel ou imóvel, material ou imaterial, e no § 2º diz que "serviço é qualquer atividade fornecida no mercado de consumo mediante remuneração..." (idem).

Dessa forma, uma grande parte das atividades realizada pelos usuários da internet poderiam caracterizar-se como de consumo e, na condição de consumidores, poderiam ter assegurada a proteção de seus dados e da sua privacidade. Entretanto, a coleta de dados em troca de serviços parece não se enquadrar no conceito clássico de remuneração, por não ser pecuniário.

Segundo Teixeira (2014), de grande importância é a caracterização do consumidor por equiparação, estabelecida no Art. 29, *CDC* (BRASIL, 11 set. 1990), para o qual não é necessária configuração de uma relação de consumo "convencional", bastando a simples exposição a práticas comerciais e contratuais para restarem protegidos pelo *CDC*, pois ele também está em condição de hipossuficiência e vulnerabilidade, em um ambiente virtual que potencializa estas características.

Mais radical é a equiparação ao consumidor definida no Art. 17, *CDC* (idem), pois protege um terceiro prejudicado por uma relação entre um fornecedor e um consumidor, possibilitando, assim, reivindicar a reparação de eventual dano ocorrido.

O fornecedor é caracterizado de maneira ampla no *CDC*, de maneira que o organizador e comerciante dos dados pessoais pode ser incluído nesta categoria, por, além de outros fatos, exercer atividade econômica, conforme dispõe o Art. 3º, *caput*, do *CDC* (idem).

Dessa forma, acaba sendo possível a proteção de dados pessoais através do *CDC* não apenas em práticas comerciais em sua estrita acepção como também em atividades comuns aos usuários da internet, mesmo que não remuneradas – como a navegação em redes sociais e *downloads* gratuitos, por exemplo – pois essa importante lei protege contra cláusulas enganosas ou abusivas de contratos de adesão eletrônicos.

Em seu Art. 54 e seus parágrafos (idem), é exposta a conceituação do *CDC* para contrato de adesão, já vista, podendo-se destacar o §3º, referente à redação deste tipo de contrato, e ao igual destaque às cláusulas que implicarem limitação de direito, o que, infelizmente, muitas vezes não ocorre.

O Art. 6º, inciso III, *CDC*, refere-se à necessidade de informação ao consumidor sobre os produtos e serviços que seja adequada e clara, assim como quanto ao risco que representam.

O Art. 37, *CDC*, proíbe toda propaganda enganosa ou abusiva, que induza o consumidor a erro a respeito da natureza do serviço ou produto, inteira ou parcialmente, inclusive por omissão.

Teixeira (2014) entende que a relação de consumo se caracteriza a partir do momento que a pessoa tem inserido seus dados em cadastros ou banco de dados, transformando qualquer usuário em consumidor por equiparação.

Práticas como coleta de dados pessoais, formação de bancos de dados e sua comercialização, através de *cookies* ou outros meios, caso não suficientemente esclarecidas e aceitas pelo usuário, configuram-se como abusivas.

O Art. 4º, no inciso VI, *CDC* (BRASIL, 11 set. 1990), dispõe sobre "a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços" que atingem o usuário pelo uso comercial de seus dados, violação da privacidade e sua autodeterminação informativa.

Como esta publicidade direcionada (no caso de buscadores, uma oferta de opção direcionada) é realizada no mais das vezes sem solicitação prévia, viola também o Art. 39, inciso III, *CDC*, pois é prática abusiva, por não haver consentimento do usuário (TEIXEIRA, idem).

Deve-se dar destaque à proibição de práticas abusivas no Art. 39, inciso IV, *CDC* (BRASIL, 11 set. 1990), que trata do aproveitamento da hipossuficiência do consumidor para impingir-lhe produtos ou serviços e, principalmente, no inciso V, que proíbe exigir do consumidor vantagem manifestamente excessiva.

Este último fato é extremamente comum nas políticas de privacidade, pois exigem do consumidor que abra mão de seus dados pessoais e privacidade – em muitos casos, também de acesso à câmera e microfone –, ao local de armazenamento de dados no dispositivo utilizado (com poderes de leitura e gravação), à geolocalização, etc., tudo isso como condição *sine qua non* para uso do produto ou serviço.

O Art.43 do *CDC* (idem) garante ao consumidor que ele terá acesso aos bancos de dados e outras informações armazenadas sobre ele, bem como às suas fontes, os quais deverão ser fornecidos em formatos acessíveis e linguagem clara, dos quais poderá solicitar a imediata correção e que não podem conter informações *negativas* referente a um período maior do que cinco anos. Ressalta-se que a abertura de tais cadastros, caso não houver sido solicitada pelo consumidor, deverá ser comunicada a ele por escrito.

Embora esse dispositivo tenha sido formulado mais com vistas a arquivos e cadastros de crédito, pode-se incluir em sua abrangência os dados pessoais e outros obtidos pelo uso da internet e coletados por métodos eletrônicos, como já visto anteriormente.

A questão que permanece é se são apresentados integralmente, indicando qual foi o uso dos dados, por quem foram acessados e, ainda, por quanto tempo serão utilizados e armazenados, pois sabe-se da dificuldade de eliminar dados da internet, devido à sua replicação, bem como de fiscalização quanto ao processo como um todo.

O Art. 46, *CDC* (idem), é claro no sentido de que os contratos de consumo somente vincularão se for dada ao consumidor a oportunidade de tomar conhecimento prévio do seu conteúdo. Esse é, justamente, o objetivo das políticas de privacidade, mas que não servem à proteção de dados pessoais por serem contratos de adesão unilaterais e impositivos.[28]

Estes contratos, muitas vezes, não respeitam outro requisito necessário, pois a lei exige que não sejam redigidos "de modo a dificultar a compreensão de seu sentido e alcance" (BRASIL, 11 set. 1990), o que é exatamente o que ocorre, pois, além da linguagem técnica e jurídica e da sua extensão, é utilizado o expediente do hipertexto no contrato eletrônico, que remete a outras partes do documento em cascata, inclusive fazendo remissão a políticas de privacidade de outras empresas, o que dificulta muito a compreensão do sentido e alcance, em comparação a um documento redigido de forma linear.

Por outro lado, o Art. 47 determina, praticamente reproduzindo o Art. 423 do *CC* (idem), que "as cláusulas contratuais serão interpretadas da forma mais favorável ao consumidor".

Alguns dos principais problemas dos contratos de adesão, e das políticas de privacidade em particular, estão incluídos no Art. 51, *CDC*, que dispõe sobre cláusulas

---

[28] O Regulamento (UE) 2016/679, de 27/04/2016 (EUROPEAN COMISSION, 24 nov. 2016), referente proteção de dados pessoais, prevê, em seu Art. 7º

4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

abusivas, considerando-as "nulas de pleno direito". Os incisos mais importantes ao nosso estudo são o I, III, IV, VI, VII, XIII e XV[29].

Os incisos VI e VIII do Art. 6º, *CDC*, são complementares na garantia ao consumidor de fazer valer os seus direitos de privacidade e proteção de seus dados pessoais, pois, além da "efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos", preveem "a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil...".

Já o Art. 25, *caput* e §1º, *CDC*, falam sobre a vedação de "estipulação contratual de cláusula que impossibilite, exonere ou atenue a obrigação de indenizar...", assim como a determinação de que "se houver mais de um responsável pela causação do dano, todos responderão solidariamente pela reparação prevista..." e, ainda, em seu §2º, o qual afirma que "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".

Essas disposições são muito importantes, porque em diversas políticas de privacidade existe tentativa de fuga a essa responsabilidade por diferentes maneiras,

---

[29] I – Impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos ou serviços ou impliquem em renúncia ou disposição de direitos. Nas relações entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis; ...

III – Transfiram responsabilidades a terceiros;

IV – Estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé e a equidade;

...

VI – Estabeleçam inversão do ônus da prova em prejuízo do consumidor;

VII – Determinem a utilização compulsória de arbitragem; ...

XIII – Autorizem o fornecedor a modificar unilateralmente o conteúdo ou a qualidade do contrato, após sua celebração;

...

XV – §1º Presume-se exagerada, entre outros casos, a vantagem que:

I – Ofende os princípios fundamentais do sistema jurídico a que pertence;

II – Restringe direitos e obrigações fundamentais inerentes à natureza do contrato, de tal modo a ameaçar seu objeto ou equilíbrio contratual;

III – Se mostra excessivamente onerosa para o consumidor, considerando-se a natureza e o conteúdo do contrato, o interesse das partes e outras circunstâncias peculiares ao caso.

§2º A nulidade de uma cláusula contratual abusiva não invalida o contrato, exceto quando de sua ausência, apesar dos esforços de integração, decorrer ônus excessivo a qualquer das partes.

§3º (Vetado.)

§4º É facultativo a qualquer consumidor ou entidade que o represente requerer ao Ministério Público que ajuíze a competente ação para ser declarada a nulidade de cláusula contratual que contrarie o disposto neste Código ou de qualquer forma não assegure o justo equilíbrio entre direitos e obrigações das partes.

inclusive a de querer isentar-se dela quando os dados privados coletados são manipulados por empresas terceirizadas, alegando que estas possuem políticas de privacidade próprias.

Neste §2º, interpretação possível a "componente ou peça incorporada ao produto ou serviço" seria o uso de *cookies*, *beacons*, HTML5, etc.

Complementando, o Art. 27 do *CDC* (BRASIL, 11 set. 1990) indica o prazo prescricional de cinco anos para a pretensão à reparação pelos danos sofridos, apresentados na Seção II deste código, por defeito na prestação de serviços ou informações. Especialmente importante para este estudo é o Art. 14, *CDC*[30], o qual dispõe que o fornecedor responde pela reparação de danos independentemente de culpa.

Não nos deteremos aqui em punições administrativas e penais resultantes da violação dos artigos do *CDC*, da defesa do consumidor em juízo ou conceituação do Sistema Nacional do Consumidor e Convenção Coletiva de Consumo, títulos que extrapolam o objetivo deste trabalho, mas que, se necessário, serão abordadas pontualmente.

4.2 PRIVACIDADE E PROTEÇÃO DE DADOS NO *MARCO CIVIL DA INTERNET*

A Lei nº12.965/2014, o chamado *Marco Civil da Internet*, é mais recente que o *CDC* e foi recentemente regulamentada pelo Decreto 8.771, de 11 de maio de 2016.

O *Marco Civil* estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. É fundamentado na liberdade de expressão e privacidade, finalidade social, livre inciativa e direitos do consumidor (BRASIL, 23 abr. 2014).

A liberdade de expressão é fundamento e princípio privilegiado nesta lei, mas ela também contempla expressamente, em seu Art. 3º, incisos II e III, a privacidade e a proteção de dados, respectivamente.

---

[30] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§ 1° O serviço é defeituoso quando não fornece 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.

§ 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.

§ 3° O fornecedor de serviços só não será responsabilizado quando provar:

I – que, tendo prestado o serviço, o defeito inexiste;

II – a culpa exclusiva do consumidor ou de terceiro.

§ 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa (BRASIL, 11 set. 1990).

Há potencial choque entre o princípio da liberdade de expressão, privilegiado no *Marco Civil*, com o princípio da privacidade e da proteção de dados, privilegiado no *CDC*. Entretanto, há de se considerar este choque como inerente à convivência entre direitos fundamentais, entre os quais incluem-se os direitos da personalidade.

Por outo lado, o *Marco Civil* refere-se a um usuário, embora não definido, o que lhe confere uma abrangência subjetiva maior do que o consumidor referido no *CDC*, implicando dizer que o usuário, como qualificado no *Marco Civil*, nem sempre será consumidor.

O *Marco Civil* apresenta disposições específicas quanto à neutralidade da rede, à proteção de registros de dados pessoais de conexão e de acesso às aplicações na internet, à atuação do poder público, à responsabilidade por danos, a respeito de requisição judicial, sobre mecanismos de governança, interoperabilidade e acessibilidade, entre outros.

Parte da doutrina[31] julga que o *Marco Civil* foi editado pensando mais nas garantias aos provedores, sejam de conexão ou de aplicações, deixando o usuário em segundo plano.

Conforme Teixeira (2014), além de ser uma lei principiológica, o *Marco Civil* estabelece regras específicas a serem cumpridas por provedores de acesso, provedores de conteúdo e outros agentes, mas não são tratados em seu texto temas importantes como comércio eletrônico, crimes de informática, propriedade intelectual, aspectos tributários ou *spam*, bem como não pode ser considerada uma lei de proteção de dados, por não abordar o assunto na extensão e especificidade necessárias.

Mesmo assim o *Marco Civil* garante o sigilo dos dados pessoais do usuário, bem como o que ele acessa na rede ou o conteúdo de suas comunicações, cujo monitoramento ou fiscalização dos pacotes transmitidos é possível apenas por ordem judicial (TEIXEIRA, idem). A proibição expressa a esse monitoramento está descrita no Art. 9º, §3º, *MCI* (BRASIL, 23 abr. 2014).

É interessante que já em seu Art. 3º, inciso VIII, *MCI* (idem), fique expresso que os novos modelos de negócio desenvolvidos no ambiente virtual gozam de liberdade em sua formulação desde que não se choquem com os outros princípios estabelecidos na lei. Este artigo, em seu inciso III, diz que a proteção de dados pessoais será exercida na "forma da lei", dando a entender a possível criação de norma específica para este fim.

---

[31] Guilherme Magalhães Martins, palestra na Faculdade de Direito da UFRGS, Salão de Atos, 28/11/2014.

Essa possibilidade, apesar de ainda não concretizada, é real, visto que já existiram diversos projetos de lei apresentados pelo Poder Legislativo que não tiveram seguimento[32], remanescem outros em tramitação e estão em construção, atualmente, propostas que parecem corresponder de forma mais completa e coerente às necessidades atuais referentes à proteção de dados para nosso país.

Os provedores de conexão são isentos de responsabilidade civil por danos decorrentes de conteúdo gerado por terceiros, conforme o Art. 18, *MCI* (idem), e como pelo Art. 14, *MCI,* é vedado a eles guardar os registros de acesso a aplicações de internet, Guardam entretanto os dados de conexão dos usuários, e como qualquer fornecedor, listas contendo nomes e outras informações associadas que devem ser igualmente protegidas contra uso indevido.

Pelo *Marco Civil* (idem, Art. 5º, II e V), aplicações "consistem no conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

Os provedores de aplicações são aqueles que, segundo Teixeira (2014, p. 92), "disponibilizam e armazenam informações criadas por terceiros ou meios próprios (sites, *blogs*, redes sociais) ".

Os provedores de aplicação são os principais alvos de interesse do presente estudo, pois, em geral, são os que se utilizam de coleta de dados e também de políticas de privacidade com a finalidade de resguardar os seus direitos.

O Art. 7º, *MCI*, é extenso e refere-se aos direitos e garantias que o usuário conta hoje no uso da rede mundial de computadores, sendo seus incisos I, II, II, VI, VII, VIII, IX, X, XI e XIII[33] de interesse específico neste trabalho, pois complementam o que é disposto no *CDC*.

---

[32] Ver item 5.3 desta monografia.

[33] Art. 7º - O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II – Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III – Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

...

VI – Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações da internet, bem como sobre práticas de gerenciamento da rede que possam afetar a sua qualidade;

VII – Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações da internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

A defesa desses direitos, conforme o Art. 30, *MCI* (idem), pode ser exercida em juízo individual ou coletivamente, na forma da lei. É salutar a possibilidade de ajuizamento coletivo, pois o hipossuficiente é empoderado por associações e outras entidades na luta por seus interesses, além do fundamental papel do Ministério Público.

Já o Art. 8º, em seus *caput* e parágrafo único, incisos I e II, *MCI* (idem), afirma que são nulas as cláusulas contratuais que atentem contra a garantia do direito à privacidade e à liberdade de expressão quando violem o sigilo das comunicações privadas pela internet e também quando não deem ao contratante de adesão a alternativa de adoção do foro brasileiro para resolução de demandas decorrentes de serviços prestados no Brasil.

O *caput* e seus parágrafos do Art. 10, *MCI* (idem), abordam a questão da guarda e disponibilização de registros de dados pessoais, de conexão e de acesso a aplicações da internet. Também garantem que o conteúdo das comunicações privadas deve respeitar a privacidade das partes direta e indiretamente envolvidas, com a exceção de serem requisitados por ordem judicial ou por autoridades administrativas que possuam competência para tanto, bem como reafirmam a necessidade de fornecimento de informações claras – aqui, a respeito das medidas e procedimentos de segurança que garantam o sigilo, que devem atender a padrões definidos em regulamento.

Reiteramos a informação de que esta regulamentação foi promulgada recentemente, em maio deste ano, através do Decreto nº 8.771 (BRASIL, 11 maio 2016), sobre o qual teceremos algumas considerações na próxima seção.

O Art. 11, *MCI* (BRASIL, 23 abr. 2014), afirma a prevalência da lei do foro brasileiro em qualquer operação que envolva dados e registros pessoais ou de

---

VIII – Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) Justifiquem a sua coleta;

b) Não sejam vedadas pela legislação; e

c) Estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX – Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X – Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação da internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei;

XI – Publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

...

XIII – Aplicação de normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 23 abr. 2014).

comunicações pela internet, desde que pelo menos um desses atos seja realizado no Brasil e que um dos terminais esteja localizado no país, mesmo que as atividades sejam realizadas por pessoa jurídica localizada no exterior, desde que oferte serviço ao público brasileiro ou, pelo menos, um integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Verifica-se que esta norma é cogente como o *CDC* na defesa do usuário, quanto ao foro e legislação aplicável nestas relações internacionais, o brasileiro, entendimento que é motivo de discussão por parte da doutrina.[34]

O §3º do Art. 11, *MCI* (idem), é de suma importância com relação ao tema da proteção de dados e da privacidade, pois diz que os provedores deverão prestar "informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações".

O modo como isso ocorrerá é definido no regulamento anteriormente mencionado, no seu Art. 13, III. O Art. 11, § 4º MCI (idem), informa que "decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo", o que consta no Art. 21 do Decreto 8.771/2016 (BRASIL, 11 maio 2016).

O Art. 15, *MCI* (BRASIL, 23 abr. 2014), informa que o provedor de aplicações[35] deve manter os registros de acesso "sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento".

Outros tipos de provedores de aplicações podem ser, por ordem judicial, obrigados a guardar registros, desde que sejam relativos a fatos específicos em período determinado.

Pode, ainda, ser requerido cautelarmente a qualquer tipo de provedor de aplicações, por autoridade policial, administrativa ou Ministério Público, que os registros em questão sejam guardados por prazo superior a seis meses, desde que com autorização judicial.

Já o Art. 16, *MCI* (idem), I, traz a determinação de que é proibida a guarda "dos registros de acesso a outras aplicações de internet" a qualquer tipo de provedor de aplicações sem prévio consentimento do titular dos dados, e o inciso II proíbe a guarda

---

[34] PINHEIRO (2013, p. 82 a 84); VANCIM e MATIOLI (2014, p. 65 a 71)

[35] O conceito de provedor de aplicações, para efeito deste artigo, é o "constituído na forma de pessoa jurídica e que exerça esta atividade de forma organizada, profissionalmente e com fins econômicos" (BRASIL, 23 abr. 2014).

“de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular”.

Entretanto, verifica-se, frequentemente, que ocorre exigência descabida de aceitação das situações proscritas nos incisos, como visto anteriormente na análise de artigos do *CDC*.

Finalmente, encerrando a abordagem do *Marco Civil*, o Art. 17 (idem) deixa clara a opção dos provedores de aplicação de não guardar dados (o que dificilmente irá ocorrer, pelo exposto neste trabalho), com exceção de hipóteses previstas em lei, e os isenta de responsabilidade civil por esta atitude em relação aos terceiros que usam seus serviços.

5 ANÁLISE DA LEGISLAÇÃO E OBSERVAÇÕES SOBRE A PROTEÇÃO DE DADOS

5.1 DESTAQUES COMENTADOS DA LEGISLAÇÃO APRESENTADA

A grande importância dada à privacidade como direito fundamental expresso na *Constituição* e considerado como inviolável no Art. 5º, X (BRASIL, 1988) pode ser avaliada pelo sentido e alcance amplo em que é empregada, *erga omnes*, e pela garantia da indenização por dano material ou moral pela sua violação, que pode ocorrer na busca e apreensão ilegal de informações armazenadas, uso não autorizado de fotos, abuso de mandados para realização de devassa, etc.

A *Constituição* apresenta de forma mais específica, no Art. 5º, XI (idem), a inviolabilidade material de espaços importantes para a manifestação da individualidade, no qual o termo "casa" deve ser entendido em sua acepção mais ampla e passível de ser defendida pelo próprio ofendido, em caso de tentativa de violação ilegal, sem que seja caracterizado o crime de resistência.

Quanto ao Art. 5º, XII, *CF* (idem), que trata do sigilo de correspondência e comunicações telegráficas, de dados e comunicações telefônicas, uma interpretação seria que as três primeiras contariam com inviolabilidade quanto à sua interceptação, que somente poderia ser quebrada por decretação de estado de defesa e de sítio, enquanto a última poderia ser por autorização judicial (LENZA, 2012).

Consequentemente, a combinação dos incisos X e XII do Art. 5º, *CF* (BRASIL, 1988), consiste em sólida base constitucional para a proteção de dados, mesmo que ponderável com outros direitos, pois nenhum deles é considerado absoluto em relação a outro.

Apesar da força com que se reveste a garantia constitucional da privacidade enquanto dados estão sendo comunicados, e apesar de autoaplicável, ela apresenta um caráter genérico, carente de uma especificidade maior a ser suprida por legislação infraconstitucional, de maneira a conferir maior efetividade à sua proteção.

Isto pode ser melhor compreendido quando pensamos nas diversas questões tecnológicas e jurídicas que a proteção de dados vem apresentando e que continuarão surgindo, tanto no Brasil como no mundo. Elas são um desafio que, em nosso entender, deve ser enfrentado o quanto antes, de forma séria e abrangente.

Analisando o *Código Civil*, verificamos que a privacidade é encarada como um direito fundamental da personalidade, o qual, além da indenização já prevista constitucionalmente pela sua violação, é cumulável com multa, caso determinada por descumprimento de ordem judicial ou sentença. Mas aqui a responsabilidade quanto à violação de dados e da privacidade é subjetiva, pois devem ser provados o dano e nexo de causalidade com o fato, o que é difícil para o usuário comum.

Em casos de relação de consumo, pode-se pensar em utilizar a responsabilidade pelo fato do serviço do CDC (BRASIL, 11 set. 1990), Art. 14, e daí teremos a responsabilidade objetiva do fornecedor.

A proteção ao nome e imagem deve ser entendida em sentido mais amplo, compreendendo, assim, a proteção da honra, à intimidade, ao recato e segredo pessoal, indenizáveis em caso de lesão, devido ao fato de serem direitos da pessoa, em regra, indisponíveis, somente podendo ser utilizados comercialmente quando autorizados expressamente, assim como seus escritos, publicações, etc.

Podemos considerar que, mesmo de forma não expressa, a proteção de dados no meio digital estaria contemplada, e não apenas quanto aos dados pessoais *stricto sensu* (nome, imagem, dados físicos, palavra, etc.) e os dados sensíveis, mas também à infinidade de dados e metadados gerados pelo usuário quando navega na internet e usa serviços de provedores, ou, ainda, quando coletados por outros sistemas interligados, pois, processados, podem gerar perfis extremamente acurados da pessoa.

Certamente isto dependeria de hermenêutica jurídica e a parca jurisprudência brasileira sobre o tema não ajuda para tornar este um direito realmente protegido. Este é um ponto cuja definição passa ao largo no *Código Civil* . Atualmente, a conceituação sobre dados já está resolvida pelo Decreto nº 8.771.

Como o usuário deve provar dano e nexo de causalidade, e talvez fosse necessário amplo conjunto probatório, incluindo perícia para isso, ele necessitaria ingressar com ação judicial de procedimento ordinário, o que ocasionaria demora na reparação, que normalmente é indenizatória. Entretanto, o Art. 12, CC (BRASIL, 10 jan. 2002), deixa clara a possibilidade de exigência por parte do usuário de cessação de ameaça ou lesão a seus direitos da personalidade, o que pode ser manejado através de pedido liminar de obrigação de não-fazer.

Como pode ser impossível saber se o direito à privacidade está sendo violado no meio digital, caso o usuário não seja apoiado por fiscalização prévia eficiente por uma agência regulatória, associações especializadas e Ministério Público, ele pode ficar sem meios para defender-se.

Assim, fica claro que, sem uma agência regulatória de proteção de dados, que possa fiscalizar previamente a violação de dados através de código, no sentido exposto por Lessig (2006), e de definição de padrão tecnológico e ético para proteção de dados, a situação atual perdurará.

A solução dada pela regulamentação do *Marco Civil,* através do Decreto nº 8.771/2016, não parece ser a mais eficaz, como será visto mais adiante, e acreditamos este ser um dos principais pontos a serem discutidos na formulação de lei específica para a privacidade *on-line*.

O *Código de Defesa do Consumidor* é, talvez, o diploma mais efetivo existente hoje na legislação brasileira para as violações à privacidade que puderem ser identificadas pelo consumidor. Sua aplicação prática é decorrente de ser lei principiológica e cogente, com regras imperativas, obrigatórias e inderrogáveis, mas, para que desfrute-se de sua proteção, deve-se estar na condição de consumidor.

Mesmo assim, o *CDC* cobre uma parcela considerável de interações estabelecidas no meio virtual, desde que, segundo suas definições, a interação seja considerada como de consumo e, como lei especial, prevalece sobre as demais no que contrariar suas disposições.

O *CDC* apresenta espectro protetivo maior do *Código Civil*, pois tutela mais do que interesses meramente individuais, como também individuais homogêneos, difusos e coletivos de algo que é considerado cláusula pétrea, a defesa do consumidor.

Conceitua abrangentemente o fornecedor e o consumidor (inclusive por equiparação), bens e serviços, e a própria relação de consumo pode ser a simples exposição a práticas comerciais e contratuais.

De especial importância são as disposições do *CDC* sobre contratos de adesão e cláusulas abusivas, o que abrange as políticas de privacidade[36], que dispõem sobre as principais questões sobre a proteção de dados unilateralmente. Determina, inclusive,

---

[36] Esquema desenvolvido por SCRIBBINS (2001), para a análise de políticas de privacidade, que verifica se as mesmas apresentam requisitos mínimos desejáveis:

1) Identificação da empresa que opera o site/fabrica produto;
2) Especificação em relação aos tipos de informação coletados;
3) Razão pela qual os dados são coletados e armazenados ou utilizados;
4) Com quem as informações são compartilhadas e se o usuário tem opções com relação a isso;
5) Por quanto tempo as informações são armazenadas;
6) Como a segurança é garantida;
7) De que forma os usuários podem acessar, alterar e apagar as suas informações;
8) Informação sobre o uso de cookies e outros meios;
9) Possibilidade da mudança de política no futuro e de que forma isto irá acontecer;
10) Detalhes para contato com a pessoa ou setor responsável na empresa pela privacidade das informações;
11) Informações de contato para as pessoas ou departamentos pertinentes no corpo da empresa

como devem ser apresentadas as informações: de forma clara, ostensiva, legível, com destaque para cláusulas que representam limitação de direito ou risco.

É comum encontrar problemas nas cláusulas constantes desses contratos, mas, aparentemente, os consumidores estão mais preocupados em reclamar judicialmente sobre defeitos de produto, sua entrega, qualidade diversa da anunciada, etc., do que em relação à proteção de seus dados e da sua privacidade, que são intangíveis.

Aliás, com relação a dados pessoais, eles são equivocadamente considerados como desimportantes por grande parte dos consumidores brasileiros, e a ocasião de maior interesse para reclamação é quando ocorre inscrição indevida da pessoa, ou não comunicada, em cadastros restritivos de crédito, sobre o que trata boa parte da jurisprudência.

Fato importante é que o *CDC* possibilita a inversão do ônus da prova em favor do consumidor e responsabiliza solidariamente o fornecedor e outros responsáveis pela caracterização do dano, o que facilita a alcançar as empresas terceirizadas.

Entretanto, o ponto crucial é que a autonomia da vontade contratual ainda prepondera, mesmo em um contrato que dispõe unilateralmente um direito da personalidade, o uso dos dados do consumidor.

No afã de utilizar recursos tecnológicos cada vez mais essenciais, o usuário ou consumidor não lê as políticas de privacidade, seja pelo tamanho, dificuldade de sua leitura causada pelo seus termos e formato, como e onde é exposta ou, ainda, por desinteresse, devido ao fato de sentir-se impotente para mudar essa situação.

A publicidade dirigida ou abusiva através de métodos comerciais coercitivos fica assim possibilitada, mesmo que o *CDC* proíba exigir do consumidor vantagem manifestamente excessiva.

Quanto ao fornecimento de informações para conhecimento e retificação de dados, isso é seguido pelos cadastros restritivos como SERASA e SPC, ao menos em regra, inclusive o respeito do período máximo de cinco anos para sua exclusão. O que ocorre muitas vezes é a inserção do nome sem comunicação à pessoa, ou a permanência dele por mais tempo do que o necessário, devido à falta ou atraso de ordem de exclusão pelo credor após a regularização da dívida

Quanto a outros bancos de dados empresariais, ainda não há como saber verdadeiramente se respeitam o limite temporal para a eliminação dos dados, se foram apresentados integralmente ou sua forma de aquisição, a não ser por via judicial, apesar

de, certamente, estarem abertos à retificação, por motivos óbvios, quanto ao endereço, número de cartão de crédito, renda, etc.

Grandes corporações, como o Facebook, começaram a disponibilizar, a pedido do próprio titular, arquivos que, a princípio, devem conter todos os seus dados, assim como a sua eliminação após o encerramento da relação do usuário com o serviço, embora não se possa afirmar que isto efetivamente ocorra, menos ainda pelos terceirizados ou parceiros aos quais houve repasse de dados, que pode ser internacional.

Já o *Marco Civil da Internet* possui uma abrangência subjetiva maior que o *CDC*, pois o conceito de usuário, embora não definido naquela lei, é mais amplo do que o de consumidor, apenas, e dispõe de maneira expressa sobre a impossibilidade de monitoramento ou fiscalização de pacotes.

Entretanto, também é referido expressamente no *Marco Civil* que os negócios desenvolvidos no ambiente virtual gozam de liberdade em sua formulação. Isso é um problema, já que, para a proteção de dados, é necessária a limitação do modelo de negócio que coleta e manipula dados, pois ele se choca com outros princípios estabelecidos em lei,

Uma demonstração da necessidade de lei que disponha sobre proteção de dados decorre do próprio *Marco Civil*, quando assinala que sua regulamentação será realizada na forma da lei. Porém, a sua regulamentação pelo Decreto nº 8.771/2016, apesar de incluir uma seção sobre proteção de dados, não inclui diversos dos temas anteriormente discutidos no presente estudo, o que reforça a ideia da necessidade de lei específica para proteção de dados pessoais.

O *Marco Civil* reafirma a proteção dos direitos do consumidor, mas, infelizmente, adota o mesmo critério do *CDC* (BRASIL, 11 set. 1990), que considera suficiente o "consentimento expresso" do usuário, após recebimento de "informações claras e completas" e da "publicidade e clareza de eventuais políticas" utilizadas (notórios problemas), o que acaba reforçando a possibilidade de acesso a registros de aplicações na internet, a coleta, armazenamento, tratamento e uso de dados pessoais, incluindo a dos registros a outras aplicações.

Dessa forma, assim como o *CDC*, apesar da importância da qual se revestem na defesa conjunta de direitos do usuário do meio virtual, essas leis deixam brecha importante que acaba comprometendo o direito à privacidade.

Uma questão já resolvida é a prevalência da lei do foro brasileiro em qualquer demanda que envolva dados e registros pessoais ou de comunicações pela internet para

julgar causas que atentem contra o direito à privacidade, obedecidos os requisitos do Art. 11 do *Marco Civil* (op. cit.).

A questão sobre a guarda e disponibilização de dados pessoais e de conexão já está regulamentada pelo Decreto nº 8.771/2016, que estabelece de forma genérica requisitos que deverão ser adotados nessa tarefa, e sobre as soluções que devem ser tomadas para a segurança e controle sobre quem manipula os dados. Indica também que o Comitê Gestor da Internet – CGIbr será quem estabelecerá os padrões técnicos.

Complementando o *Marco Civil*, a regulação determina que deve ser retida a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos tão logo atingida a finalidade de seu uso ou se encerrado o prazo determinado por obrigação legal, no caso, seis meses.

A exigibilidade do fornecimento de informações sobre dados pessoais e privacidade, pelos provedores, que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, guarda, armazenamento e tratamento de dados, disposta no *Marco Civil*, é medida importante. As informações deverão ser mantidas em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal.

Porém, verificamos que, atualmente, o Poder Judiciário tem encontrado grandes dificuldades em fazer respeitar suas decisões quando o réu é empresa estrangeira, principalmente quando não há representação dela no Brasil.

A falta de fiscalização quanto à proteção de dados, comentada anteriormente, é parcialmente resolvida pela regulamentação, pois atribui responsabilidade à Anatel – Agência Nacional de Telecomunicações, para regular, fiscalizar e apurar infrações, em conjunto com a Secretaria Nacional do Consumidor, ficando a apuração de infrações à ordem econômica a cargo do Sistema Brasileiro de Defesa da Concorrência, em conjunto com órgãos e a outras entidades da administração pública federal com competências específicas.

É difícil crer que tal arranjo descentralizado dê conta de uma tarefa da dimensão que é a proteção de dados no ambiente virtual. A atitude integrada ou colaborativa de órgãos estatais é sempre bem-vinda, entretanto, sem uma agência específica para o assunto, dificilmente a tarefa será bem-sucedida.

Além disso, a Anatel já enfrenta dificuldades para regular e fiscalizar o serviço de telecomunicações, haja vista a qualidade deficiente e o alto custo dos serviços que são disponibilizados ao usuário pelas operadoras de telefonia e conexão à internet.

Recentemente (2016), inclusive, esta agência colocou-se em posição atrelada aos interesses de provedores, contra interesses legítimos dos consumidores/usuários, e em clara afronta ao *Marco Civil*, na questão da neutralidade da rede, assunto que foi momentaneamente resolvido, mas que merece o maior cuidado da sociedade civil quanto à sua condução.

Também deve-se considerar que, por opção política sobre o tema, a internet não é considerada telecomunicação, mas simplesmente um serviço de valor agregado, o que ajuda na justificativa para segregar essa grande tarefa a uma agência regulatória própria.

5.2 ASPECTOS JURISPRUDENCIAIS SOBRE PROTEÇÃO DE DADOS

Enfrentamos, em geral, conhecimento deficiente sobre proteção de dados, tanto por parte de advogados como pelos magistrados. Essa é uma matéria que envolve direito e tecnologia e que, certamente, ainda carece de mais estudo para um verdadeiro entendimento das suas possibilidades e limites.

A jurisprudência brasileira referente à proteção de dados caracteriza-se pela sua falta de consolidação.

Quanto à diversidade de pontos abordados nesses processos, ela está aumentando paulatinamente, mas ainda não é suficiente para o amplo balizamento deste campo de estudo.

Estamos, portanto, em evolução; não chegamos a um amadurecimento sobre a proteção de dados pessoais ou sobre como fazer respeitar a autonomia informativa de maneira prática, prévia e efetiva – e, de preferência, coletivamente. Esse fato, por outro lado, possibilita uma revisão dos conceitos e dos problemas sobre proteção de dados com análise mais profunda, pois estamos em estágio anterior ao da edição de lei específica que dê conta de abordar amplamente suas facetas.

Para exemplificarmos julgados que tangenciam a proteção de dados com base na atual legislação, mostraremos algumas decisões:

- Coleta de dados indevida causou cobrança indevida ao autor por empresa de cartão de crédito – parcial provimento ao recurso dos autores (Recurso Inominado nº 71002932101/RS);
- Indeferimento de inicial referente à inconformidade do autor com a comercialização de seus dados pessoais e sensíveis – provimento da apelação do autor (Apelação Cível nº 70060251816/RS, nº 70059939777/RS, nº 710029332101/RS, nº 70061683454/RS);

- Falta de segurança do Facebook permitiu invasão à conta do autor com exclusão de dados e possibilidade de seu uso ilícito – desprovimento da apelação do autor (Apelação Cível nº 70066407776/RS);
- Falha administrativa possibilitou indevida divulgação de dados cadastrais do autor na internet - desprovimento da apelação do autor (Apelação Cível nº 70064382591/RS, nº 70061012050/RS, nº 70057259145/RS);
- Ilicitude de sistema de atribuição de escore para avaliação de risco de crédito ao autor baseado em cadastro de dados pessoais - desprovimento da apelação do autor (Apelação Cível nº 70066177759/RS, ver REsp n° 1.419.697/RS – Recurso Especial Repetitivo)
- Ilicitude de comercialização cadastro de dados pessoais de consumidores – desprovimento da apelação do autor (Apelação Cível nº 70068799634/RS, nº 70068799634/RS /RS, nº 70065967432/RS, nº 70060118239/RS, nº 70065983132/RS, nº 70063665228/RS, nº 70064583412/RS, Agravo Regimental nº 70065946022/RS)
- Divulgação não autorizada de dados pessoais do autor a terceiros pela OI Brasiltelecom S/A e posterior importunação comercial – provimento do recurso do réu (Recurso Inominado nº 71006183941/RS)
- Bloqueio de site violador da privacidade e dados pessoais Tudosobretodos – provimento da cautelar do autor (Cautelar inominada nº 0805175-58.2015.4.05.8400/RN).

A informação mais chocante quanto à proteção de dados pessoais, e que demonstra uma opinião atual e forte jurisprudencialmente, ao menos no TJ/RS, é a apresentada abaixo (RIO GRANDE DO SUL, 20 set. 2016), reiterada em diversos outros recursos repetitivos:

> Atualmente, não mais se consideram sigilosos os dados cadastrais de consumidores quando no dia-a-dia das relações negociais e comerciais são fornecidos a todo momento, seja de forma pessoal ou por outro meio (telefone e Internet) [...] a parte autora não efetuou qualquer prova no sentido de que a divulgação de dados pela requerida tenha lhe causado qualquer prejuízo de ordem moral [...] apenas uma ferramenta de consulta para análise do perfil do consumidor, não se sujeita ao dever de notificação prévia.

Os exemplos de decisões apresentados acima incluíram os temas mais representativos e recorrentes com relação à proteção da privacidade e de dados pessoais, mas não foi encontrada jurisprudência específica sobre o ponto que considera-se a maior fonte de violação: a ampla coleta de dados dos usuários através de meios tecnológicos, como os *cookies*, de forma a sustentar o *big data*, o que prejudicou uma análise

jurisprudencial “por dentro” pela não localização de decisões e acórdãos específicos sobre o tema.

Esta falta de jurisprudência talvez seja explicada pelo fato de ser uma coleta praticamente invisível ou ignorada, como já abordado anteriormente, o que apoia a ideia de legislação que contemple este tema, e também uma fiscalização que tenha o condão de prevenir o dano antes que ele aconteça.

Além do TJ/RS, a pesquisa jurisprudencial foi realizada nos *sites* do STF[37], STJ[38] e TJ/SP[39], nos quais foi encontrada a mesma dificuldade para achar jurisprudência específica sobre coleta de dados realizada virtualmente por aplicações de internet tendo em vista o modelo de negócios criticado nesta monografia.

Questões como a transferência internacional de dados, políticas de privacidade, ponderação sobre limites a determinados modelos de negócio *versus* privacidade e falta de fiscalização por agência específica, por exemplo, também não foram localizadas[40].

5.3 TENDÊNCIAS LEGISLATIVAS SOBRE PROTEÇÃO DE DADOS

Segundo Teixeira (2014), antes da promulgação da lei do *Marco Civil da Internet*, em 2014, e da sua regulamentação, em 2016, já tramitaram no Congresso diversos projetos de lei visando a um tratamento jurídico específico para questões relacionadas à internet, e, dos que foram pesquisados, foram selecionados os considerados mais representativos para ilustração:

- Projeto de Lei nº 3.356/2000 (BRASIL, 28 jun. 2000 [a]), do Deputado Osmânio Pereira, dispõe sobre a aquiescência que deverá ser dada pelo usuário para a coleta e distribuição de informações pessoais, entre outros assuntos. Foi desarquivado em 09 de fevereiro de 2015, mas seu conteúdo, praticamente, foi todo superado pela legislação existente;
- Projeto de Lei nº 3.360/2000 (BRASIL, 28 jun. 2000 [b]), do Deputado Nelson Proença, dispõe sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas, de apenas seis artigos. Arquivado em 11 de março de

[37]Disponível em: <http://www.stf.jus.br/portal/principal/principal.asp>.

[38] Disponível em: <http://www.stf.jus.br/portal/principal/principal.asp>.

[39] Disponível em: <http://www.tjsp.jus.br/>.

[40] A busca de processos foi realizada utilizando diversas palavras e expressões, como internet, dados de aplicações, dados de conexão, big data, proteção de dados, uso de dados pessoais, coleta de dados, etc., com variação de operadores lógicos; isto não exclui a possibilidade de sua existência, existindo a hipótese de não terem sido encontrados por imperícia na execução da pesquisa.

2008, possui importante aspecto contemplado, pois dispõe que deverá ser informado em que momentos as informações serão coletadas e sua finalidade, em aparição legível e destacada, sempre com a opção de aceitação ou não da coleta, mas, devido à sua redação, não fica claro se o provedor possui ou não a opção de recusar a prestação do serviço, caso o usuário não aceite a coleta;

- Projeto de Lei 4.249/2001 (BRASIL, 13 mar. 2001), do Deputado João Caldas, que acrescenta dispositivo ao *CDC*, dispondo sobre o estabelecimento da inviolabilidade de informações pessoais e patrimoniais em posse do fornecedor, proibindo sua comercialização para terceiros. Foi apresentado em 13 de março de 2001 e arquivado em 31 de janeiro de 2007.
- Projeto de Lei nº 6541/2002 (BRASIL, 11 abr. 2002), do Deputado Paulo Rocha, inclui como crime passível de pena a divulgação ou a comercialização de endereços e dados pessoais sem a devida autorização, acrescentando Art. 152-A ao Código Penal. Foi apresentado em 11 de abril de 2002 e teve parecer positivo da CCJC em 04 de outubro de 2007.
- Projeto de Lei nº 1.589/1999 (BRASIL, 31 ago. 1999.), baseado no anteprojeto de lei realizado pela OAB/SP, que procura dar proteção à privacidade, determinando que o ofertante somente possa exigir do consumidor dados de caráter privado que estejam relacionados com a negociação em vista, com a inovação de que, além de devê-las manter em sigilo, salvo se autorizado pelo titular para divulgá-las ou cedê-las, não pode condicionar esta autorização à aceitação do negócio. Dispõe também sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, de forma abrangente e com boa técnica legislativa. Foi apresentado em 31 de agosto de 1999 e, desde 24 de setembro de 1999, foi apensado ao PL 1483/99 e, sucessivamente, ao PL 4906/2001. Foi a plenário em 20 de março de 2013, mas a matéria não foi apreciada por acordo de líderes partidários.
- Projeto de Lei nº 4.060/2012 (BRASIL, 13 jun. 2012), do Deputado Milton Monti, dispõe sobre dados pessoais de forma abrangente, mas parece retroceder em termos de privacidade, se comparado com o anterior, por ser mais orientado à livre iniciativa, liberdade de comunicação e à ordem econômica, reforçando valor contratual das políticas de privacidade e dando mais destaque à autorregulamentação e descentralização de responsabilidade em outros órgãos, em vez de propor uma agência própria para o assunto. Apresentado em 13 de junho de 2012, em 18 de agosto de 2016 recebeu despacho para análise por comissão especial criada para o assunto.

- Projeto de Lei n° 330/2013 (BRASIL, 2013), do Senador Antonio Carlos Valadares, dispõe sobre a proteção, o tratamento e o uso dos dados pessoais; é bastante completo e é um dos importantes projetos atualmente no Senado que trata sobre proteção de dados. Apresentado em 13 de agosto de 2013, está em tramitação, aguardando parecer da Secretaria de Apoio à Comissão de Assuntos Econômicos.
- Projeto de Lei n° 181/2014 (BRASIL, 2014 [a]), do Senador Vital do Rêgo, estabelece princípios, garantias, direitos e obrigações para a proteção de dados pessoais no Brasil; elenca os direitos do titular; determina o regime jurídico do tratamento de dados pessoais; estabelece regras para a tutela administrativa dos dados pessoais. Apresentado em 20 de maio de 2014, está em tramitação, aguardando parecer da Secretaria de Apoio à Comissão de Assuntos Econômicos.
- Projeto de Lei n° 131/2014 (BRASIL, 2014 [b], da CPI da Espionagem do Senado Federal, dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros. Foi apresentado em 16 de abril de 2014, encontrando-se em tramitação, aguardando parecer da Secretaria de Apoio à Comissão de Assuntos Econômicos.
- Projeto de Lei nº 5276/2016 (BRASIL, 13 maio 2016), de autoria do Poder Executivo, foi baseado em anteprojeto realizado pelo Ministério da Justiça[41]. Teve lançada consulta pública para discussão em 28 de janeiro de 2015. Possui texto baseado em eixos: o âmbito de aplicação da norma, a definição do dado protegido (dados pessoais, anônimos e sensíveis), os princípios norteadores e o consentimento, segurança, sigilo, boas práticas e sanções administrativas; cria, inclusive, a figura do agente responsável pelo tratamento dos dados. Este projeto foi apresentado em 13 de maio de 2016, encontra-se em tramitação e foi devolvido pela Comissão de Constituição e Justiça e de Cidadania à Coordenação de Comissões Permanentes.

A Secretária Nacional do Consumidor, Juliana Pereira, acredita que a proteção de dados inova ao redefinir as fronteiras da privacidade e afirma que "Uma das principais bases da nossa mobilização social é que o titular deve sempre ser o detentor da vontade sobre o uso de seus dados" (BRASIL, 29 jan. 2015).

[41]http://www2.camara.leg.br/camaranoticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html

O texto debatido (PENSANDO..., [s./d.]), elaborado pelo Ministério da Justiça, é o mais completo até agora, quanto ao assunto da proteção de dados pessoais e da privacidade, e possui diversas contribuições da sociedade civil.

O PL 5276/2016 (BRASIL, 13 maio 2016), quando da sua apresentação na Câmara dos Deputados, apresentou texto com diferenças em relação ao texto do anteprojeto que consta na internet, e desde já pode-se dizer que houve retrocesso importante em relação ao tema do consentimento, crucial para a proteção de dados pessoais ou sensíveis, que será visto adiante.

Apesar disso, o PL possui uma redação com boa qualidade técnica e é bem estruturado, e no qual pode-se encontrar os pontos até agora não contemplados pelo ordenamento em relação à proteção de dados e da privacidade, já identificados em capítulos anteriores. Como esses temas são necessários à adequada tutela daqueles direitos fundamentais, a sua inclusão em projeto de lei, e a própria existência e tramitação deste diploma legislativo são autojustificativos de sua necessidade, o que corrobora a hipótese desta monografia.

Avaliaremos a seguir seus principais destaques, de forma a ilustrar o afirmado.

Seu Capítulo I, referente às Disposições Preliminares, apresenta no Art. 1º o seu objeto, a proteção de direitos fundamentais em relação aos dados pessoais, e são enunciados em seu Art. 2º os seus fundamentos.

O Art. 3º especifica o escopo do tratamento de dados a que se destina (coleta e tratamento de dados no território nacional, ou com a finalidade de oferta de bens e serviços ou tratamento de dados de indivíduos localizados em território nacional), deixando claro em seu parágrafo primeiro que considera os dados como coletados no território nacional quando o seu titular ali se encontrar no momento da coleta.

Já o Art. 4º define os casos de tratamento aos quais ela não se destina, e em seu § 3º faz menção pela primeira vez a um “órgão competente” quanto ao assunto proteção de dados, dando a entender ser necessário a criação de um órgão específico para a tarefa.

Seu Art. 5º apresenta um glossário de termos bastante completo, suplementando a falta de alguns conceitos não apresentados no CDC, Marco Civil ou sua regulamentação.

No Art. 6º é apresentada a conceituação dos diversos princípios pelos quais deve-se pautar a atividade de tratamento de dados, não contemplados pela legislação

existente, dos quais podemos ressaltar o da finalidade, adequação, necessidade e segurança.

No Capítulo II, Requisitos para o Tratamento de Dados Pessoais, o Art. 7º apresenta *numerus clausus* as hipóteses em que o tratamento de dados poderá ser realizado[42].

O Art. 8º complementa *CDC, MCI* e regulamentação quanto às informações necessárias que devem ser disponibilizadas ao usuário, referentes ao tratamento de seus dados, e em seu § 4º [43] é que ocorre o retrocesso anteriormente comentado quanto ao consentimento do usuário à coleta e tratamento de dados pessoais, pois abre a possibilidade do estabelecimento de condição da sua aceitação para o fornecimento de produto ou serviço ou para o exercício de direito.

Ora, este é justamente o cerne de toda a problemática que envolve o negócio *big data* e suas variantes, pois quando é dito que "*Quando* o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço ou para o exercício de direito...", o mercado entenderá que *sempre* poderá exigir isto, desde que informe o titular "com destaque sobre tal fato e sobre os meios pelos quais poderá exercer o controle sobre o tratamento dos seus dados. "

42

I - mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco;

II - para o cumprimento de uma obrigação legal pelo responsável;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;

IV - para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial ou administrativo;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

43

§ 4º Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados.

O Art. 7º, §1º [44], do anteprojeto do Ministério da Justiça, solucionava esta questão estratégica dizendo claramente que o estabelecimento de condição para fornecimento de produto ou serviço não poderia ser realizado, a não ser em casos excepcionais. Esta mudança substancial provavelmente ocorreu para atender a interesses que não são os da população brasileira, e devem ter sido usados expedientes políticos de baixíssimo nível para sua operacionalização.

Nesta toada, deve-se ficar preparado para, quando da sua aprovação, após passar pelas diversas comissões, receber uma lei de dados completamente descaracterizada e que atenda apenas a interesses privados.

O "consentimento livre, informado e inequívoco", que aparece no Art. 7º e 9º, de nada adianta como garantia ao usuário, mas sim à empresa, pois se ele não concordar com os termos ela estará autorizada a não fornecer o produto ou serviço.

Apesar da defesa dos princípios da finalidade e necessidade nos §§ dos Art. 9º e 10, do dever da garantia de transparência, dos meios eficazes para os titulares manifestarem a sua oposição, etc., parece que tudo isto restou irremediavelmente enfraquecido pela infeliz redação do Art. 8º.

O Art. 11 aborda a vedação ao tratamento de dados sensíveis, exceto uma série de situações, que podem se transformar em qualquer situação, dependendo apenas de consentimento, em alguns casos. Em outros casos os dados sensíveis podem ser tratados sem o consentimento do titular, obedecidos alguns requisitos.

Aparentemente o Art. 12 tenta dar um reforço à proteção dos dados sensíveis, pois fala que o órgão competente *poderá* estabelecer medidas adicionais de segurança, ou ainda solicitar relatório de impacto à privacidade ao responsável. Fácil verificar que isto é uma faculdade, e não uma obrigação.

O Art. 13, e seus §§, possui importantes disposições sobre considerar dados pessoais os dados anonimizados que foram revertidos ou que possam ser revertidos ao estado inicial, assim como os dados utilizados para formação de perfil comportamental de uma determinada pessoa natural, ainda que não identificada. É relatado ainda que o "órgão competente *poderá* dispor sobre padrões e técnicas" do processo de anonimização e de sua segurança, falando ainda sobre o uso e compartilhamento deste

[44] Art. 7º, §1º - O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.

tipo de dado ser objeto de publicidade e transparência, podendo ser solicitado ao responsável relatório de impacto do referido processo e tratamento.

Acredita-se, apesar da forma verbal *poderá*, que é uma verdadeira obrigação do órgão responsável estabelecer uma arquitetura de controle e protocolos que garantam a anonimização, tendo em vista que os dados não nascem anônimos, e que pelas brechas do texto será possível continuar condicionando o uso de produtos dos dados à aceitação da sua coleta e tratamento, mesmo que com atenuantes.

A questão temporal dos dados, muito importante, e que não fora tangenciada ainda pela legislação, é tratada no Art. 15, que dispõe sobre as hipóteses do término do tratamento dos dados pelo responsável, sendo complementada pelo Art. 16, que afirma que os dados pessoais serão eliminados após o tratamento, sendo autorizada sua conservação para as finalidades elencadas, às quais podem ser acrescentadas hipóteses específicas de conservação pelo órgão competente.

O Capítulo II, Dos Direitos do Titular, inicia com o Art. 17 que assegura a toda pessoa natural a titularidade dos seus dados, e o Art. 18 complementa informando o que tem direito de obter, em relação a seus dados, o titular dos dados pessoais.

A confirmação da existência ou o acesso aos dados pessoais pelo titular são abordados pelo Art. 19, que também explicita os formatos em que poderão ser solicitadas as informações. Trata-se de direito complementar, pois abordado de formas diversas em outros dispositivos legais, como no CDC, e constitucionais, como o *Habeas Data.*

O Art. 20 comenta sobre o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Já foi comentado nesta monografia anteriormente (p. 28) que na União Europeia este direito ao esclarecimento pelo usuário da causa de determinada avaliação quanto à sua pessoa deveria dar inclusive ao usuário a possibilidade de ter o seu caso reavaliado por um ser humano.

O Art. 21 diz que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo, e o Art. 22 trata da possibilidade de tutela individual e coletiva dos direitos dos titulares de dados, como ocorre em outras situações.

O Capítulo IV, Do Tratamento de Dados pessoais pelo Poder Público, segue do Art. 23 ao Art. 30, abrangendo a administração direta e indireta no trato com a questão de dados pessoais.

O Capítulo V, Da Transferência Internacional de Dados, começa com o Art. 33 indicando as hipóteses de possibilidade de transferência de dados pessoais a outros países, que, entre outros pontos, levará em consideração o nível de proteção de dados do país estrangeiro.

É abordado no Art. 34, entre outros pontos, que o órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos que constem em documentos ou realizadas diligências de verificação quanto às operações em andamento que fundamentem a transferência internacional de dados, que podem ser requeridas informações suplementares.

Já o Art. 35 é taxativo quanto à responsabilidade solidária e objetiva pelo tratamento de dados tanto pelo cedente como pelo cessionário, independentemente do lugar em que se localizem e em qualquer hipótese.

O Capítulo VI, Dos Agentes do Tratamento de Dados, possui seção que corresponde aos Art. 36 a 40, que tratam, em rápida síntese, de que estes agentes são o Responsável e o Operador, sendo que este último deverá realizar as operações de acordo com as instruções repassadas pelo primeiro, que deverá verificar a observância de suas próprias instruções e da legislação aplicável, e que a comunicação de dados entre eles deve ser autorizada pelo titular, salvo hipóteses de dispensa de consentimento previstas.

A segunda seção corresponde ao Art. 41, que trata da indicação pelo responsável de um encarregado pelo tratamento de dados pessoais, cuja identidade deve ser publicada preferencialmente no site do responsável, e que terá como atividades o relacionamento com titulares e órgão competente, para resolução de problemas, e na orientação de funcionários e contratados da entidade a respeito das práticas a serem adotadas em relação à proteção de dados, que podem ser complementadas pelo órgão competente.

Aparentemente trata-se de pessoalização e responsabilização por tarefa importante, dando um rosto humano, uma tangibilização maior para o relacionamento necessário com titulares, funcionários e fiscalização.

A questão da responsabilidade e ressarcimento de danos é abordada na terceira seção, do Art. 42 ao Art. 44, dispondo sobre a obrigatoriedade de reparação de danos causados a outrem em vista da atividade de tratamento de dado pessoais, da possibilidade de inversão do ônus da prova, que eventual dispensa de consentimento não dispensa as demais obrigações previstas nesta lei, e da obrigação solidária entre cedente e cessionário, observadas exceções previstas.

O Capítulo VII, Da Segurança e das Boas Práticas, em sua primeira seção, que vai do Art. 45 ao Art. 49, trata sobre a segurança e sigilo de dados, das medidas técnicas e administrativas que o operador deve tomar na prevenção de acidentes e ilícitos, que o órgão competente poderá dispor sobre padrões técnicos e organizacionais para as tarefas, e que deverão obedecer ao estado atual da tecnologia, principalmente no caso de dados sensíveis.

Os agentes de tratamento possuem dever de sigilo quanto aos dados pessoais, e o responsável deverá comunicar ao órgão competente qualquer incidente de segurança relevante, cuja comunicação deverá ser realizada em prazo razoável e contendo uma série de informações estabelecidas na lei. De acordo com a gravidade do incidente serão determinadas providências pelo órgão competente. A pronta comunicação aos titulares independe de determinação do órgão competente, sempre que seja identificado risco de segurança pessoal ou de dano aos titulares.

A segunda seção refere-se às boas práticas, que podem ser formuladas individualmente pelas empresas ou por associações, tendo em vista o escopo, natureza, finalidade do tratamento dos dados, e a probabilidade/gravidade dos riscos dos danos aos titulares, e o órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

O Capítulo VIII, Da Fiscalização, é talvez um dos mais importantes, pois estabelece em seu Art. 52 as sanções administrativas para as infrações realizadas pelas pessoas jurídicas de direito privado, aplicáveis pelo órgão competente[45], que serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com o caso concreto.

O Art. 53 dispõe sobre as atribuições do órgão competente para a fiscalização do disposto na lei, bastante extensas, incluem, entre outras, a elaboração de uma Política Nacional de Dados Pessoais e Privacidade, realizar auditorias nos tratamentos de dados pessoais, e estabelecer normas complementares para as atividades de comunicação de dados pessoais e sobre proteção de dados pessoais e privacidade.

I - multa simples ou diária;

II - publicização da infração;

III - anonimização dos dados pessoais;

IV - bloqueio dos dados pessoais;

V - suspensão de operação de tratamento de dados pessoais;

VI - cancelamento dos dados pessoais; e

[45] VII - suspensão de funcionamento de banco de dados.

O Art. 54 fala sobre a composição do Conselho Nacional de Dados Pessoais e da privacidade, composto por 15 representantes titulares e seus suplentes, com mandato de 2 anos, permitida a recondução. Indicados pelo Ministro da Justiça.

O Art. 55 indica a competência do referido Conselho, que inclui fornecimento de subsídios para a formação da Política Nacional de Proteção de Dados Pessoais e da Privacidade, assim como elaborar relatórios anuais e avaliação das ações desta sugestão de ações a serem tomadas pelo órgão competente, realização de estudos e debates sobre o tema, e a disseminação de conhecimento sobre proteção de dados e privacidade à população em geral.

A inclusão no texto do PL 5276/2016 (BRASIL, 13 maio 2016) de diversos pontos considerados como lacunas observadas na legislação é, além de grata surpresa pela absoluta necessidade de que se revestem, prova de que o exame levado a cabo nesta monografia foi acertado, corroborando a sua falta em nosso ordenamento e comprovando a hipótese apresentada.

Como relatado no início desta monografia, a União Europeia já possuía legislação sobre a proteção de dados e o direito fundamental à privacidade, como as Diretivas 95/46/CE e a 2002/58/CE, que tratam amplamente sobre o tema proteção de dados pessoais no âmbito da União Europeia.

Além disso, os países-membros também possuem legislações próprias, complementares às leis comunitárias, e podem declarar inconstitucionalidade de determinados artigos destas, quando entrarem em conflito.

Recentemente reformou esta legislação anterior através da edição da Regulamentação Geral de Proteção de Dados - *Regulation (EU) 2016/679* e da Diretiva de Proteção de Dados – *Directive (EU) 2016/680*, de forma a avançar na questão, e os países-membros deverão incorporá-las em sua legislação até 2018.

Pode-se verificar, pelo exposto, que a tendência é a continuação da utilização de soluções legais para o problema da proteção de dados pessoais, embora fosse interessante o estudo, criação e a utilização conjunta de recursos tecnológicos que assegurassem o cumprimento das eventuais leis aprovadas sobre a matéria através da arquitetura da informação.

Com base nos diversos projetos de lei encontrados, fica evidente que a questão da proteção de dados no Brasil vem sendo discutida, pelo menos, desde o ano de 2000, ou seja, aguardamos há dezesseis anos por um marco sobre o assunto, o qual já deveria ter sido regulado.

A tramitação do PL 5276/2016 (BRASIL, 13 maio 2016) deve contar com uma fiscalização atenta da sociedade civil organizada, para que não seja desfigurado por emendas e substitutivos que lhe alterem negativamente a substância, o que já ocorreu com a questão do consentimento, mas que ainda pode ser revista.

Entretanto, mesmo com um cenário favorável, devido ao regime de urgência constitucional pelo qual tramita, pode ser afetado pelo atual cenário político e econômico (2016), que devido à sua instabilidade, poderá influenciar o ritmo dos trabalhos negativamente.

Dessa forma, talvez tenhamos de aguardar ainda algum tempo para que se transforme em realidade, em nosso país, a existência de uma legislação sobre proteção de dados adequada ao tempo e à situação tecnológica em que vivemos.

6 CONCLUSÃO

Após percorrermos o *iter* escolhido para estruturar esta monografia, tivemos a oportunidade de conhecer, passo a passo e de forma sucinta, o desenvolvimento do cenário digital, desde sua origem até o momento atual.

Foram também apreciados os conceitos básicos relativos à proteção de dados e da privacidade virtual, além de certificar qual é o entendimento doutrinário sobre o tema e adquirir conhecimento acerca do que já existe em nosso ordenamento jurídico para amparar e garantir aqueles direitos fundamentais da personalidade.

Da mesma forma, através de pesquisa sobre a jurisprudência existente, cuja hermenêutica é lastreada pelo atual acervo legislativo, dentro do possível foram apresentadas sentenças proferidas pelo poder judiciário que mostram a opinião corrente de nossos julgadores e que representam precedentes a serem considerados sobre o tema.

Assim, partindo-se de aspectos gerais para chegar aos aspectos específicos da questão, finalmente foi possível concluir pela real necessidade da criação de uma lei de proteção de dados para nosso país, esperando que, se editada, acompanhe em seu conteúdo o estado da arte mundial sobre a matéria, principalmente as resoluções e diretivas emanadas pela União Europeia.

A conclusão foi deduzida pela verificação da existência de diversas situações em que o usuário fica em assimetria jurídica, técnica e econômica em relação aos agentes que dominam o espaço virtual e pelo fato de existirem lacunas legislativas sobre questões importantes, o que dá suporte à validação de nossa tese, sobre as quais iremos discorrer a seguir.

Partindo da constatação de que a privacidade é um direito fundamental, que além de expressamente constar da *Constituição* também é respaldada por outros diplomas legislativos, ela deveria ser efetivamente garantida no ciberespaço, o que não ocorre.

A garantia existente pela legislação quanto à matéria é apenas parcial, pois deixa pontos importantes fora de sua apreciação e, mesmo nos que estão incluídos, deixa margem para a ocorrência de violação da privacidade e de danos ao usuário.

Na ausência de legislação específica, o que acaba prevalecendo são as práticas de mercado, que atendem a interesses comerciais privados e não ao interesse público.

Então, como o desenvolvimento de novas formas de negócio é livre e ocorre de forma permanente na internet, o que acaba acontecendo é que o usuário fica totalmente vulnerável à prática que exige contratualmente a cessão de seus dados. Este é um ponto

nevrálgico, de grande peso na validação da hipótese deste trabalho, pois carece de equacionamento e ocasiona diversas outras violações, em cascata, aos direitos da personalidade, problema que somente será sanado com uma lei de proteção de dados adequada.

Este ponto importantíssimo continua carente de tutela, pois como vimos no capítulo anterior, a redação do PL 5276/2016 não é das mais felizes.

Imbricada com este fato está a inexistência de uma política pública geral para a proteção de dados, por meio da qual sejam tomadas as iniciativas necessárias à informação e educação dos usuários, à adequação de conduta de provedores, à segurança tecnológica necessária, à fiscalização prévia e atuante para sua obediência e à cooperação internacional – tarefas cuja realização deveria ser deixada sob responsabilidade de agência reguladora específica para o assunto. O Decreto nº 8.777, de 11 de maio de 2016, refere-se unicamente à instituição da Política de Dados Abertos do Poder Executivo Federal.

Estes dois pontos, uma política pública e um órgão competente específico estão contemplados no PL 5276/2016, com o acréscimo da criação de um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

A *Constituição* solidamente embasa o direito à privacidade, no Art. 5º, X, XI e XII. Essas garantias, apesar de fundamentais, são de caráter genérico demais para dar solução aos diversos pontos específicos que necessitam ser avaliados para a proteção de dados pessoais.

O *Código Civil* de 2002 discorre, logo em seu início, sobre a personalidade e capacidade da pessoa natural (art. 1º ao art. 10) e sobre os direitos da personalidade decorrentes (art. 11 ao art. 21), o que demostra a importância de que se reveste a disciplina desta matéria para o restante de seu conteúdo, e em seu art. 21, dispõe sobre a privacidade individual, em termos similares aos constitucionais.

Entretanto, da mesma forma que a *Constituição*, o *Código Civil* discorre sobre direitos da personalidade de forma genérica, sem abordar especificamente a proteção de dados e como ela seria realizada, a não ser indicar que, a requerimento do interessado, o juiz adotará providências necessárias para impedir ou fazer cessar ato contrário à inviolabilidade da vida privada.

Pelas características das relações virtuais pela internet, influenciadas pela sua instantaneidade, internacionalização, replicação de dados e a própria arquitetura da rede, a simples indenização para reparação de danos ou mesmo a tutela liminar da obrigação de não-fazer podem ser insuficientes – até porque estas soluções são posteriores à

violação da privacidade, cujo dano causado pode continuar ocorrendo, inclusive por terceiro, a partir de outro servidor, até mesmo localizado em outro país.

A questão do conhecimento restrito sobre a matéria, por parte dos advogados e magistrados, e a dificuldade de fazer cumprir sentenças no exterior, quanto à internet, também não deve ser desconsiderada.

Portanto, mesmo a combinação da proteção dada pela *Constituição* e pelo *Código Civil* não é suficiente para o desafio que é a proteção de dados e da privacidade na internet, preferencialmente de maneira prévia à ocorrência de sua violação e da ocorrência de dano ao usuário, sob pena não atingir seus objetivos.

A flexibilização dos direitos da personalidade, quando possível por lei, sempre deve privilegiar o interesse e benefício do usuário, e não o empresarial. Defende-se a tese de que os direitos da personalidade possuem *status* superior à autonomia da vontade contratual, como questão de ordem pública.

Já a garantia dada pelo *Código de Defesa do Consumidor* apresenta o senão de abranger apenas o consumidor, embora, através do conceito de consumidor equiparado, consiga estender sua abrangência. Quanto aos contratos de adesão, o *CDC* é mais exaustivo e efetivo que o *Código Civil*, porque garante não somente a inversão do ônus da prova, mas também o foro brasileiro ao usuário nacional, obedecidos alguns requisitos.

Apesar da adoção pelo *CDC* da interpretação de cláusulas ambíguas ou contraditórias de forma mais favorável ao consumidor e da garantia contra as cláusulas abusivas, continuamos a enfrentar o problema da imposição de consentimento para a prática da utilização de *cookies* e outras tecnologias para a coleta de dados.

Some-se a este fato as hipóteses anteriormente aventadas de o consumidor não saber que sua privacidade está sendo violada, de não ter lido a política de privacidade, de considerar-se impotente para reagir e que, caso não aceite essa situação, tenha que ir ao Judiciário para resolvê-la. Portanto, continuamos com a necessidade de uma lei específica para a proteção de dados e da determinação de maneiras práticas para resolver a questão.

Com o *Marco Civil da Internet* não temos melhor sorte, pois, apesar de proteger qualquer usuário, não há qualquer restrição na formulação de novos modelos de negócio no ambiente virtual e ele não trata do detalhamento das garantias nem disciplina as matérias da proteção de dados e privacidade; entretanto, apresenta dispositivo de suma importância: os provedores deverão prestar “informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao

armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações".

A regulamentação do Marco Civil foi expedida recentemente (Decreto 8.771, de 11 de maio de 2016), indicando a Anatel para fiscalização e apurações de infrações quanto aos requisitos técnicos e que o Comitê Gestor da Internet – CGIbr expedirá as diretrizes quanto a esses. Mas, como diz que o CGIbr deve apenas *recomendar* procedimentos e normas sobre proteção de dados, isso nada garante quanto à implementação e o seu cumprimento.

Importante fato é que o próprio CGIbr (COMITÊ..., 01 out. 2016) e o Núcleo de Informação e Coordenação do Ponto BR – NIC.br posicionam-se como fortemente favoráveis a uma lei de proteção de dados, e que a regulamentação reforça que os provedores devem reter a menor quantidade de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos tão logo atingida a finalidade do seu uso ou se encerrado o prazo por obrigação legal.

A indicação da Anatel para fiscalização, em conjunto com a Secretaria Nacional do Consumidor e o Sistema Brasileiro da Defesa da Concorrência, com a colaboração de órgãos e as entidades da administração pública federal com competências específicas quanto aos assuntos, *a priori* não parece ser a melhor opção.

Esta arquitetura aparenta ser excessivamente descentralizada, de difícil coordenação e resultados efetivos, e a sua característica principal parece ser a defesa da concorrência e do consumidor, e não a proteção de dados e do usuário.

Além disso, a Anatel já possui um grande espectro de abrangência, e apresenta dificuldades em conseguir o atingimento do padrão de qualidade dos serviços fornecidos pelos seus administrados. Além disso, recentemente trabalhou contra a neutralidade da rede e os interesses dos seus usuários, fatos que apontam uma agência para a proteção de dados como uma opção mais interessante, pois, além de ser uma tarefa gigantesca, manteria uma segregação de matérias que talvez fossem de maior interesse ao usuário.

Quando o *Marco Civil*, art. 3º, III, diz que a proteção de dados pessoais será exercida na "forma da lei", indica a criação de norma específica para este fim, ponto importante na validação de nossa hipótese.

Quanto à jurisprudência analisada, o que sobressai são alguns aspectos repetitivos como exibição de dados, sigilo bancário, escutas, fraudes na internet, coleta

de dados históricos ou técnicos, informação sobre servidores, etc., enquanto que os abordados neste trabalho não foram verificados.

Como apresentado anteriormente, causa espécie a posição de alguns magistrados de não considerarem mais sigilosos os dados cadastrais dos consumidores, apenas pelo fato de serem fornecidos para relações negociais, e que a parte é que deveria demonstrar o prejuízo sofrido.

A produção de prova de utilização indevida de dados pode ser tarefa tecnologicamente difícil, e a alegação, por um magistrado, que uma ferramenta de análise de perfil do consumidor construída nessas bases não violaria a privacidade é realmente desconcertante. (RIO GRANDE DO SUL, 20 set. 2016).

O fato de determinadas informações acabarem na internet, com ou sem consentimento, não retira o direito do usuário sobre elas, e o seu uso fere o princípio da finalidade, caso utilizadas para outros objetivos que não aqueles para os quais elas foram fornecidas, ou cruzadas com outros bancos de dados ou, ainda, utilizadas por período indefinido.

A questão do princípio da finalidade, entre outros importantes à proteção de dados, assim como um melhor equacionamento do controle temporal dos dados, já estão contemplados no PL 5276/2016.

A amostra jurisprudencial encontrada reitera a situação atual de descontrole quanto à autonomia informacional, devido ao entendimento equivocado da questão e à ineficiente proteção de dados, e assim é considerado por parcela dos magistrados como fato normal dos “novos tempos”.

Entretanto, como contraponto a essa visão equivocada, foram apresentadas, a partir do início do novo milênio, diversos projetos de lei sobre proteção de dados, sendo possível identificar uma genuína preocupação de alguns parlamentares com a situação atual no Brasil.

A regulação bastante incisiva quanto à proteção de dados e a defesa do usuário já é realidade em inúmeros países, em consonância como que pensa a maioria da doutrina analisada.

Apesar da demora na tramitação destes projetos (BIONI; MONTEIRO, 01 out. 2016), muitos já arquivados, verifica-se que a preocupação ainda persiste por parte da classe política, e a apresentação do Projeto de Lei nº 5.276/2016 (BRASIL, 13 maio 2016), é um bom sinal.

Embora esta a iniciativa regulatória concorra com outras[46], ela teve seu regime de tramitação fixado como de urgência constitucional, e apesar da previsão de que este projeto já pudesse ter sido votado, hoje existe a real possibilidade de aprovação de uma lei de proteção de dados para o Brasil.

É um projeto que contempla as principais preocupações expressadas neste trabalho, o que corrobora não somente os pontos apontados no mesmo, como também a hipótese que a necessidade de legislação específica para a proteção de dados não é uma opção, mas uma necessidade para o enfrentamento dos problemas causados pela sua violação.

Infelizmente a redação quanto à questão do consentimento a ser fornecido pelo usuário, pedra angular do problema da proteção de dados, teve mudança que implicou em retrocesso quando o anteprojeto transformou-se no PL 5276/2016, ponto no qual espera-se mudança até sua conversão em lei.

Finalmente, não somente conclui-se pela necessidade de uma lei de proteção de dados para o Brasil, como espera-se que exista a vontade política para a tramitação célere e a aprovação de um projeto de lei desta natureza, pois ele é necessário para que possam ser utilizados todos os recursos que a rede mundial nos disponibiliza, sem que sucumbamos a um estado de vigilância constante sobre nosso comportamento *on-line,* que certamente causa efeitos negativos na esfera mais íntima da personalidade individual.

[46] PL n° 4060/2012, PL n° 330/2013, PL n° 181/2014 e PL n° 131/014.

REFERÊNCIAS

ALMEIDA JR., Vitor de Azevedo; FURTADO, Gabriel Rocha. A tutela do consumidor e o comércio eletrônico coletivo. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 399-430.

AMARAL, Francisco. **Direito Civil:** introdução. 6 ed. rev. e aum. Rio de Janeiro: Renovar, 2006.

BARCELOS, Jorge. Cuidado: você está sendo vigiado. **Zero Hora**, Porto Alegre, 02 ago. 2015. Caderno PrOA, p. 3.

BARRAL, Welber Oliveira. **Metodologia da pesquisa jurídica**. 4 ed. rev., atual. e ampl. Belo Horizonte: Del Rey, 2010.

BIONI, Bruno Ricardo; MONTEIRO, Renato Leite. O Brasil caminha rumo a uma Lei Geral de Proteção de Dados Pessoais? Carta Capital, São Paulo, 25 maio 2016, 18:52. Disponível em: <http://www.cartacapital.com.br/politica/o-brasil-caminha-rumo-a-uma-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 01 out. 2016, 18:40.

BITTENCOURT, Daniel. O que podemos aprender com o caso WhatsApp**. Zero Hora**, Porto Alegre, 20 dez. 2015. Caderno PrOA, p. 3.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BRASIL. Câmara dos Deputados. **Consulta pública será base para projeto de lei sobre proteção de dados pessoais**. 29 jan. 2015, 20:43. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html>. Acesso em: 01 dez. 2016, 18:50.

_____. Câmara dos Deputados. **PL 1589/1999**: apresentação em 31 ago. 1999. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=16943>. Acesso em: 01 dez. 2016, 18:36.

_____. Câmara dos Deputados. **PL 3356/2000**: apresentação em 28 jun. 2000 [a]. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=19529>. Acesso em: 01 dez. 2016, 18:29.

_____. Câmara dos Deputados. **PL 3360/2000**: apresentação em 28 jun. 2000 [b]. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=19533>. Acesso em: 01 dez. 2016, 18:31.

_____. Câmara dos Deputados. **PL 4060/2012**: apresentação em 13 jun. 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 01 dez. 2016, 18:38.

BRASIL. Câmara dos Deputados. **PL 4249/2001**: apresentação em 13 mar. 2001. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=26637>. Acesso em: 01 dez. 2016, 18:32.

_____. Câmara dos Deputados. **PL 5276/2016**: apresentação em 13 maio 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 01 dez. 2016, 18:46.

_____. Câmara dos Deputados. **PL 6541/2002**: apresentação em 11 abr. 2002. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=48659>. Acesso em: 01 dez. 2016, 18:34.

_____. **Constituição** (1988). Disponível em :<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: jul./nov. 2016.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: set.-dez. 2016.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: set.-dez. 2016.

_____. **Lei Nº 13.105, de 16 de março de 2015**. Institui o Código de Processo Civil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: set.-dez. 2016.

_____. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm>. Acesso em: set.-dez. 2016.

_____. **Lei Nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: set.-dez. 2016.

_____. Senado Federal. **Projeto de lei do Senado nº 131, de 2014** [b]. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/116969>. Acesso em: 01 dez. 2016, 18:44.

_____. Senado Federal. **Projeto de lei do Senado nº 181, de 2014** [a]. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/117736>. Acesso em: 01 dez. 2016, 18:42.

_____. Senado Federal. **Projeto de lei do Senado nº 330, de 2013**. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 01 dez. 2016, 18:40.

CASTELLS, Manuel. **A galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

COMITÊ GESTOR DA INTERNET. **Iniciativas de proteção de dados pessoais são analisadas em Seminário do NIC.br e CGI.br**. 26 ago. 2016. Disponível em: <http://www.cgi.br/noticia/releases/iniciativas-de-protecao-de-dados-pessoais-sao-analisadas-em-seminario-do-nic-br-e-cgi-br/>. Acesso em: 01 out. 2016, 19:06.

CONPEDI/UFMG/FUMEC/Dom Helder Câmara (org.). **Direito, governança e novas tecnologias** [Recurso eletrônico on-line] Florianópolis: CONPEDI, 2015.

DONEDA, Danilo. Os direitos da personalidade no código Civil. In: TEPEDINO, Gustavo (coord.). **A parte geral do novo Código Civil:** estudos na perspectiva civil-constitucional. Rio de Janeiro: Renovar, 2002.

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

_____. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 61-78.

DUARTE, Nestor. Parte Geral. In: PELUSO, Antônio César (coord.). **Código Civil comentado:** doutrina e jurisprudência – Lei n. 10.406, de 10.01.2002: contém o Código Civil de 1916. 4. ed. rev. e atual. Barueri/SP Manole, 2010. p. 15-182.

EUROPEAN COMISSION. **Reform of EU data protection rules**. Last update 24 nov. 2016. Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>. Acesso em: 24 nov. 2016.

FONSECA, Caue; MINOZZO, Paula. Entre o livre arbítrio e o algoritmo. **Zero Hora**, Porto Alegre, 17 maio 2015. Caderno PrOA, p. 6.

GAERTNER, Adriana. **Privacidade da informação**: um estudo das políticas no comércio eletrônico. Salvador, 2006. 187 f. Dissertação (Mestrado). Instituto de Ciência da Informação. Universidade Federal da Bahia. 2006.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2006.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**: contratos e atos unilaterais. 9 ed. São Paulo: Saraiva, 2012. Vol. 3.

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

LEMOS, Ronaldo. **Algoritmos**. Programa Estúdio i, Canal Globonews, 28 set. 2016, 14:40.

LENZA, Pedro. **Direito constitucional esquematizado**. 16 ed. atual. e ampl. São Paulo: Saraiva, 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, 2011.

LESSIG, Lawrence. **Code**. New York: Basic Books, 2006.

LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre os seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 109-146.

MARTIN, Guilherme Magalhães. O direito ao esquecimento na internet. In: _____ (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 3-28.

MATTOS, Nelson. A internet não esquece. **Zero Hora**, Porto Alegre, 19 abr. 2015. Artigos, p. 26.

MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira.; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. (Org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205-230. V. 1.

MIETNIK, Kevin. **Fantasma no sistema**: minhas aventuras como hacker mais procurado do mundo. Rio de Janeiro: Alta Books, 2013.

MODENESI, Pedro. Contratos eletrônicos de consumo: aspectos doutrinário, legislativo e jurisprudencial. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014. p. 301-370.

MÜLLER, Nicolas. **O começo da internet no Brasil**. 23 ago. 2008. Disponível em: <https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil>. Acesso em: 18 nov. 2016, às 14:38.

NUNES, Luis Antonio Rizzatto. **Curso de direito do consumidor.** 7 ed. rev. e atual. São Paulo: Saraiva, 2012.

OLSON, Parmy. **Nós somos Anonymous**: por dentro do mundo dos hackers – LulzSec, Anonymous e o poder revolucionário do ativismo na internet. São Paulo: Novo Século, 2014.

PARANHOS, Felipe. **O que é política de privacidade ou termos de segurança?** 11 nov. 2013. Disponível em: <https://www.oficinadanet.com.br/post/11863-o-que-e-politica-de-privacidade-ou-termos-de-seguranca>. Acesso em: 27 nov. 2016, 10:56.

PELUSO, Cezar (coord.). **Código Civil comentado:** doutrina e jurisprudência – Lei n. 10.406, de 10.01.2002: contém o Código Civil de 1916. 4 ed. rev. e atual. Barueri, SP: Manole, 2010.

PENSANDO O DIREITO. **Anteprojeto de lei para a proteção de dados pessoais**. [s./d.] Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 03 dez. 2016, 19:06.

PINHEIRO, Patrícia Peck. **Direito digital**. São Paulo: Saraiva, 2013.

REALE, Miguel. **A Constituição e o Código Civil**. 08 nov. 2003. Disponível em: <http://www.miguelreale.com.br/artigos/constcc.htm>. Acesso em: 24 nov. 2016, 19:55.

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível: AC 70071021711 RS**. Disponível em: <http://tj-rs.jusbrasil.com.br/jurisprudencia/391663911/apelacao-civel-ac-70071021711-rs/inteiro-teor-391663929>. Acesso em: 20 set. 2016, 20:13.

SAMSUNG. **Política de privacidade local.** Disponível em: <http://www.samsung.com/br/info/privacy.html>. Acesso em: 14 set. 2016, 18:31.

SANTI, Alexandre de. **O lado negro do Facebook**. Superinteressante, ed. 348, p. 28-39, jun. 2015.

SAWAYA, Márcia Regina. **Dicionário de informática e internet**. São Paulo: Nobel, 1999.

SCRIBBINS, Kate. **Privacy@net:** an international comparative of consumer privacy on the internet. London: Consumers International, 2001. Disponível em: <http://www.consumers international.org/media/304817/privacy@net- an international comparative study of consumer privacy on the internet.pdf>. Acesso em: 27 nov. 2016, 16:07.

SEDESTMIDH – Secretaria Adjunta de Desenvolvimento Social de Brasília. **O que são informações pessoais?** Disponível em: <http://www.sedest.df.gov.br/publico-alvo/familias/item/1594-o-que-s%C3%A3o-informa%C3%A7%C3%B5es-pessoais>. Acesso em: 19 nov. 2016, às 14:58.

SILVA, José Afonso da. **Direito constitucional positivo**. 10 ed. São Paulo: Malheiros, 1994.

SIQUEIRA, André. **Por que é importante e como montar uma política de privacidade para seu site**. 08 out. 2013. Disponível em: <http://resultadosdigitais.com.br/ blog/como-montar-uma-politica-de-privacidade/>. Acesso em: 27/11/2016, 10:57.

SORDI, Jaqueline; ROSO, Larissa. Horas de silêncio no WhatsApp. **Zero Hora**, Porto Alegre, 18 dez. 2015. Editoria, p. 40.

SUPREMO TRIBUNAL FEDERAL. **A Constituição e o Supremo:** Constituição da República Federativa do Brasil (Versão completa). Disponível em: <http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfSobreCorte_pt_br&idConteudo=175946>. Acesso em: 27 nov. 2016, 21:10.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n. 22.337/RS**, rel. Ministro Ruy Rosado de Aguiar, DJ. 20 mar. 1995, p. 6119.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 2 ed. São Paulo: Saraiva, 2014.

TRIBUNAL DE JUSTIÇA do Distrito Federal e dos Territórios. **Consumidor segundo a teoria finalista aprofundada**. Disponível em: <http://www.tjdft.jus.br/institucional/jurisprudencia/jurisprudencia-em-foco/cdc-na-visao-do-tjdft-1/definicao-de-consumidor-e-fornecedor/mitigacao-da-teoria-finalista-para-o-finalismo-aprofundado>. Acesso em: 21 nov. 2016, 12:00.

VADE MECUM OAB e Concursos. 9 ed. atual. e ampl. São Paulo: Saraiva, 2016. Obra coletiva de autoria da Editora Saraiva com a colaboração de Lívia Céspedes e Fabiana Dias da Rocha.

VANCIM, Adriano Roberto; MATIOLI, Jeferson Luiz. **Direito & internet**: contrato eletrônico e responsabilidade civil na Web. Franca, SP: Lemos & Cruz, 2014.

ZALIS, Pieter. A maior revolução em 300 anos. **Veja**, São Paulo, ed. 2416, n. 2416, p. 17-21, *11 mar. 2015*. Entrevista com Alex Pentland, Páginas Amarelas.

ZERO HORA**. Bloqueio desarrazoado**. Porto Alegre, 20 dez. 2015. Editorial, p. 26.