Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada

Caio Cesar Carvalho Lima, Renato Leite Monteiro

Resumo

Introdução: Considerando-se o movimento mundial relativo à segurança jurídica e aos marcos regulatórios para a proteção de dados pessoais expõe o atual panorama no Brasil e analisa o Anteprojeto Brasileiro de Proteção de Dados Pessoais. Discorre sobre distintos aspectos referentes à privacidade, à intimidade e aos dados de pessoas naturais e estabelece uma análise comparada com legislação estrangeira. **Método**: Levantamento de legislação, de doutrina e de jurisprudência nacional e internacional. **Resultados**: Atualmente o Brasil dispõe de uma proteção dispersa e não específica sobre o tema proteção de dados. Menções aparecem em capítulos, artigos, parágrafos e incisos de diferentes normas legislativas e em decisões jurisprudenciais. Ao se analisar o Anteprojeto Brasileiro de Proteção de Dados Pessoais verifica-se a necessidade de esclarecimentos e aprofundamentos em determinados artigos e incisos especialmente nos que tratam da titularidade dos dados, da segurança dos repositórios de dados públicos e privados, da necessidade de criação de criação de entidade regulatória autônoma, e da ausência, no momento, de aplicação de penas em âmbito criminal. A Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense são as normativas que inspiraram o Anteprojeto. **Conclusões**: A proliferação de novas tecnologias e, principalmente, da Internet no país pressiona para a existência de marcos legais. Considerando-se que o objetivo do texto do Anteprojeto não é somente a proteção dos dados pessoais, mas também o estabelecimento de um paradigma jurídico - que possa servir de sustentáculo para investimentos econômicos e desenvolvimento tecnológico - o dispositivo também poderia contemplar as proteções de ordem econômica e das relações de consumo que envolvem o cidadão.

Palavras-chave

Proteção de dados. Dados pessoais. Acesso à informação. Lei de proteção de dados. Segurança da informação.

Introdução

O Brasil, na contramão a muitos de seus pares no cenário mundial, ainda não dispõe de proteção adequada para dados de natureza pessoal. Ainda que se considerem as proteções à intimidade e à privacidade estabelecidas pela Constituição Federal de 1988 (CF/1988), pelo Código Civil (CC), pela Lei de Acesso à Informação (Lei nº 12.527/11); e o amparo aos dados relativos a processos de consumo (nos ditames trazidos pelo Código de Defesa do Consumidor/CDC), ainda se está muito distante do nível de adequação garantido por legislações alienígenas, como as da Comunidade Europeia, do Canadá, da Argentina, do México, do Uruguai, do Peru, do Chile e dos Estados Unidos da América.

Em razão disso, e vislumbrando a necessidade de legislação nacional com o objetivo de estipular um marco regulatório adequado, idealizou-se o Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP), fruto do trabalho da Fundação Getúlio Vargas e do Ministério da Justiça. Tais instâncias tomaram por base diversas leis já em vigência no âmbito internacional, tais como a Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense, as quais são analisadas na sequência deste trabalho.

Questiona-se se realmente é necessário tal marco legal. Essa dúvida pode ser respondida de forma mais eficaz por meio de um viés pragmático. O atual estágio tecnológico chega a tornar quase que onipresente a utilização da Internet. Diante disso, considerando-se que essa ferramenta utiliza maciçamente dados de natureza pessoal –

muitos destes de caráter sensível, tais como cor, sexo e orientações políticas – há um imperativo para o correto tratamento de tais informações.

Diariamente, a mídia veicula notícias relativas ao vazamento de dados pessoais, cadastrais ou financeiros. Uma compilação das chamadas *data breaches* (violação de dados), iniciada em 2005, revela que estas já ultrapassam mais de três mil casos, ou aproximadamente 600 milhões de registros divulgados sem consentimento (PRIVACY RIGHTS CLEARINGHOUSE, 2013) em países que já regulam a matéria relativa a estes incidentes (o que não inclui o Brasil). Bancos de dados públicos voltados ao monitoramento de vazamentos de dados, tais como o *DataLossDB*, reportam diversos casos reais de prejuízos decorrentes da liberação não autorizada ao público de elementos que deveriam ter ficado restritos àqueles a quem eles foram confiados, incluídos aí dados bancários, números de documentos pessoais, endereço pessoal, dentre outros (OPEN SECURITY FOUNDATION, 2013). Tais situações explicitam um viés econômico, pois ao serem trazidas balizas legais mais contundentes – em decorrência do princípio da segurança jurídica – podem servir como uma forma de atração de investimentos. Neste aspecto, Ascenção (2002, p. 71) destaca que na atual sociedade da informação, na qual os dados são os ativos de maior valor, cresce a exigência da rápida efetivação de um regramento. Tancer (2009), ao discutir as principais condições de utilização de tais dados, observa que mesmo coletados à exaustão estes ainda são subaproveitados.

Assim, o maior beneficiário da estipulação de um marco legal é o cidadão, que é elo mais frágil, mormente quando posto diante de conglomerados empresariais e do Estado. Em um marco regulatório, o usuário (ou seja, o jurisdicionado) tem as informações que compõem suas esferas de intimidade e de privacidade tratadas adequadamente e, apenas o que é do seu interesse pode ser revelado ou utilizado por terceiros; o que garante a aplicação de seus direitos fundamentais.

Uma normativa que garanta o nível de proteção aludido não engessará ou impedirá o caráter autorregulatório da maioria das iniciativas tecnológicas. Pelo contrário, incentivará a criatividade e a novidade, assim como a neutralidade da rede, na medida em que estabelecerá regras claras para todos os jogadores do mercado.

Sob este contexto, o artigo objetiva analisar o atual cenário legislativo brasileiro, investigando a necessidade de um marco legal específico a reger a matéria. O estudo tem caráter documental-analítico voltado para a abordagem dos principais aspectos do Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP), encerrando-se com um breve estudo da legislação em vigor em demais países, em especial daqueles que serviram como fonte para a elaboração da norma brasileira.

Breve discussão do cenário brasileiro sobre privacidade e proteção de dados

O Brasil atualmente dispõe de uma proteção dispersa e não específica sobre o tema proteção de dados. A proteção maior se dá no âmbito da privacidade e da transparência, e não da proteção de dados em si.

A Constituição Federal de 1988 (CF) estabelece em seu Art. 5º um rol não exaustivo de direitos fundamentais garantidos a todo cidadão. Entre eles encontram-se diversos provimentos sobre privacidade e sobre proteção de dados, como a inviolabilidade das comunicações e o direito ao *habeas data*, este último regulado – em parte e recentemente – pela Lei de Acesso à Informação.

Dispõe o inciso X do referido artigo da CF, 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". Essa proteção geral dada no âmbito da privacidade é alvo de diversas interpretações e não se trata de um texto específico sobre a proteção de dados.

Isso não significa que o Poder Judiciário brasileiro está completamente ausente de discussões sobre o assunto. Por exemplo, as cortes brasileiras têm ampliado o conceito de espaço público

em diversos casos, ao mesmo tempo em que têm aplicado limitações à liberdade de expressão e garantido o direito à privacidade. Em um destes[1], relativo a dano moral, a súmula foi relata como segue:

> RESPONSABILIDADE CIVIL - DANO MORAL – Colocação de fotos em comunidade virtual – Cerceamento de defesa inocorrente – Preliminares rejeitadas – Exposição indevida da pessoa não configurada – Canal de comunicação mantido entre moradores do condomínio onde residem as partes – Retratação do dia a dia e eventos ocorridos no residencial – Inexistência de comentários relacionados às fotos, de modo a emprestar conotação espúria visando denegrir ou difamar – Dinâmica dos fatos que não denotam intenção de atingir a honra ou personalidade – Reconvenção – Inexistência do alegado excesso na ação ou abuso de poder da parte, ao exercer seu legítimo direito de ação – Decisão que analisou a questão de forma sucinta e coesa, não havendo falar em sentença '*citra petita*' – Recursos desprovidos.

Por meio da leitura da súmula do acórdão acima transcrita, consegue-se evidenciar que as cortes pátrias estão atentas a algumas das noviças questões que a utilização da internet trouxe, especificamente acerca do uso e da divulgação de informações pessoais.

No escopo do referido inciso constitucional, o Código Civil em seu Art. 21 estabelece que o judiciário, a pedido do ofendido, pode adotar providências para cessar as ofensas, uma vez que a "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".

Diferentemente de alguns países, como os Estados Unidos, no Brasil o direito ao anonimato não é garantido de forma irrestrita ao cidadão no âmbito da liberdade de expressão. A CF, no Art. 5º., inciso IV, esclarece que "é livre a manifestação do pensamento, sendo vedado o anonimato". Esta orientação jurídica é uma das causas mais comuns de limitação de conteúdos publicados, principalmente na Internet. Todavia, em contraponto ao texto constitucional, o Código Civil garante em seu Art. 19 que, desde que para fins lícitos, há proteção ao pseudônimo da mesma forma que se protege o nome da pessoa natural.

Uma menção direta da CF sobre proteção de dados se dá no inciso XII do já mencionado Art. 5º. Neste, determina-se a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas, salvo por ordem judicial para fins de investigação criminal e instrução processual penal. Este mandamento constitucional foi regulado pela Lei Federal nº 9.296/96 que, em seu Art. 1º, parágrafo único, afirma que a proteção dada aos sistemas de telefonia também se aplica à interceptação de fluxo de comunicações em sistemas de informática e telemática. Todavia, o texto legal, ao utilizar a palavra "fluxo de comunicações", trouxe consigo divergência doutrinária e jurisprudencial em face da diferença entre dados estáticos e dados "em movimento". Contudo, pelo fato da Lei nº Federal 9.472/97, conhecida como Lei Geral de Telecomunicações (LGT), conceituar telecomunicação como transmissão, emissão ou recepção de informações de qualquer natureza, apenas o fluxo de comunicações estaria protegido pelo inciso XII da CF/88 e pelo Art. 1º da Lei nº 9.296/96[2].

Entretanto, o entendimento sobre a confidencialidade de dados estáticos tem mudado, e a estes é imposto o véu da proteção dada à privacidade. Neste gênero é possível incluir, por exemplo, meros dados cadastrais em posse de empresas como registros eletrônicos de comunicação, tais como os endereços de Protocolo de Internet (IP). O Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP) pretende colocar um fim a essa divergência, conceituando dados pessoais e afirmando que estes somente podem ser fornecidos mediante ordem judicial. A referida proteção também é garantida pelo Projeto de Lei nº 2.126/2011, conhecido como "Marco Civil da Internet" que, caso aprovado com a redação atual, estipulará que tais dados somente podem ser for-

[1] Vistos, relatados e discutidos estes autos de Apelação n. 0007814-20.2008,8.26.0152, da Comarca de Cotia/SP, em que é apelante/apelado H.M.B. sendo apelado/apelante W.C.S.C.

[2] Por cuidar-se de meros registros cadastrais, desmerece confundida com interceptação telefônica em sentido estrito, escuta telefônica, ou até mesmo com os dados documentados pela concessionária referentes às ocorridas chamadas telefônicas. (Mandado de Segurança nº 293.304-3 – Ribeirão Preto – 3ª. Câmara Criminal – Relator Gonçalves Nogueira)

necidos mediante ordem judicial. Neste, há uma abordagem explícita ao tema, como segue:

> O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos:
> I – à inviolabilidade da intimidade e da vida privada, assegurado o direito à sua proteção e à indenização pelo dano material ou moral decorrente de sua violação;
> II – à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Neste particular, o texto do Código de Defesa do Consumidor (CDC) já explicita uma proteção extensa a dados relativos às relações de consumo. A Seção VI do CDC trata especificamente sobre bancos de dados e cadastro de consumidores garantindo, no seu Art. 43, que "o consumidor, sem prejuízo do disposto no Art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". O mesmo artigo garante em seus parágrafos que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" e que "o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção".

Em consonância com o Art. 43 do CDC, a Portaria número 05 de 2002 do Ministério da Justiça alargou o rol de cláusulas abusivas do Art. 51 do CDC, considerando:

> Art. 1º [...] abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que:
> I – autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia;
> II – imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor;
> III – autorize o fornecedor a investigar a vida privada do consumidor;

É importante frisar o inciso III desta Portaria, que considera cláusula abusiva aquela que autoriza ao fornecedor a investigar a vida privada do consumidor. Esta orientação é frequentemente desrespeitada, em especial quando se utilizam meios eletrônicos, pois a coleta de dados e a transferência destes para terceiros é quase uníssona, mesmo que explicitada nos "termos de uso" dos serviços (quando existentes).

O Art. 43, § 4º, do CDC considera os bancos de dados de consumidores algo de caráter público. Desta forma, em uma interpretação integrativa da lei, o acesso aos bancos de dados de registros pessoais das relações de consumo é igualmente assegurado por meio de *habeas data*.

A Lei Federal nº 9.507/97, que regulou o direito ao *habeas data* determina em seu Art. 1º, parágrafo único que se considera "[...] de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações". Desta forma, será concedido o *habeas data*:

> Art. 7º (...)
> I – para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;
> II – para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
> III – para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável e que esteja sob pendência judicial ou amigável.

O inciso XXXIII do Art. 5º da CF afirma que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". Este inciso foi regulamentado pela Lei Federal nº 12.527/11, que estabeleceu procedimento específico para que o cidadão requisite dados que estejam em posse da Administração Pública, além de classificar os documentos do Estado em níveis diferentes de sigilo, em consonância com o Decreto nº 5.301/04. Tais graus de sigilo variam desde o ultrassecreto, que somente pode ser acessado após vinte cinco

anos, até o reservado, que se torna público após cinco anos.

Na esfera do alargamento do conceito de privacidade, a Lei Federal nº 7.232/84 – que estabeleceu a Política Nacional de Informática – define que, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, se deve ter como princípio o Art. 2º, inciso VIII desta Lei que estabelece "[...] mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas". O conceito de privacidade e de dados pessoais que se infere desta normativa estimulou projetos de lei, tais como relativo à proteção de dados e, anteriormente, o Estatuto da Criança e do Adolescente (ECA). Neste, um dos princípios a serem seguidos na aplicação de medidas socioeducativas é o da privacidade, garantindo o respeito à intimidade, ao direito de imagem e a reserva da vida privada das crianças e adolescentes. Textualmente, o Art. 100 do ECA explicita:

> Art. 100. – Na aplicação das medidas levar-se-ão em conta as necessidades pedagógicas, preferindo-se aquelas que visem ao fortalecimento dos vínculos familiares e comunitários.
> Parágrafo único. São também princípios que regem a aplicação das medidas:
> V – privacidade: a promoção dos direitos e proteção da criança e do adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada.

O mesmo Estatuto determina a preservação da identidade destes, nos seguintes termos:

> Art. 17. – O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais.

Em relação à privacidade na Internet, a Agência Nacional de Telecomunicações (ANATEL) e o Comitê Gestor da Internet Brasileira (CGI.br) estabelecem o princípio da neutralidade como um dos seus fundamentos. O provedor tem o dever de manter o sigilo dos dados de seus usuários perante terceiros, mesmo quando aqueles cometam supostos atos ilícitos, não podendo revelá-los senão mediante ordem judicial.

Ainda, o Art. 37, do Projeto de Lei nº 4.906/01 (que reuniu os Projetos de Lei nº 1.483/99 e 1.589/99), estabelece que "o provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas". O provedor de Internet é, assim, mero fornecedor de meios físicos, permitindo que mensagens e conteúdos sejam transmitidos entre um remetente e um destinatário, não os produzindo e não exercendo qualquer controle ou juízo de valor sobre eles.

O acesso ao tráfego de dados do usuário pelos provedores pode ser caracterizado como quebra de sigilo comunicacional e invasão de privacidade, nos moldes de Lei Federal e da Constituição Federal Brasileira. A eventual responsabilidade sobre o conteúdo transmitido é, portanto, do usuário que utilizou a infraestrutura de provimento de acesso à Internet, cuja identificação poderá ser requerida mediante ordem judicial, devido ao direito fundamental à privacidade e ao sigilo das comunicações.

Convém esclarecer que o e-mail corporativo (aquele utilizado como ferramenta de trabalho) não é considerado sigiloso para o empregador, que pode acessá-lo desde que com prévia ciência do empregado. Este é o entendimento pacífico na doutrina e na jurisprudência, como indica o exemplo abaixo:

> PROVA ILÍCITA. 'E-MAIL' CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO. 1. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual ('e-mail' particular). Assim, apenas o 'e-mail' pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade. 2. Solução diversa impõe-se em se tratando do chamado 'e-mail' corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim

> do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço. (...) 4. Se se cuida de 'e-mail' corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar a Internet e sobre o próprio provedor. Insta ter presente também à responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, Art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de 'e-mail' de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido). (...) (BRASIL. Tribunal..., 2005).

Duas outras legislações merecem destaque: A Medida Provisória 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) visando "garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras"; e a Lei Complementar nº 105/2001, que dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

No que diz respeito ao sistema de chaves públicas brasileiro, este é mantido pelo Instituto Nacional de Tecnologia da Informação (ITI) que é uma autarquia federal vinculada à Casa Civil da Presidência da República. A obrigatoriedade do uso de certificado digital nos moldes da ICP-Brasil já foi corroborada pelo Código de Processo Civil em modificações levadas a efeito pela Lei nº 11.419/2006 ("Lei do Processo Eletrônico").

Sobre o sigilo de operações de instituições financeiras, mesmo que a Lei determine a conservação do sigilo, este texto normativo confere exceções, tais como a troca de informações entre as próprias instituições, o atendimento a requisições da Receita Federal ou de autoridades competentes para verificar a existência de atividades ilegais ou a suspeita destas. Além a troca entre agências governamentais e as financeiras, a quebra de confidencialidade depende de ordem judicial nos termos indicados no Art. 1º, parágrafo 4º, a saber:

> § 4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes:
> I – de terrorismo;
> II – de tráfico ilícito de substâncias entorpecentes ou drogas afins;
> III – de contrabando ou tráfico de armas, munições ou material destinado a sua produção;
> IV – de extorsão mediante sequestro;
> V – contra o sistema financeiro nacional;
> VI – contra a Administração Pública;
> VII – contra a ordem tributária e a previdência social;
> VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores;
> IX – praticado por organização criminosa.

Todavia, até o momento, ainda não existe um terreno certo sobre a temática. Essa situação leva a diversas decisões judiciais diferentes em casos estritamente similares. Recentemente, o Poder Judiciário brasileiro iniciou um debate profundo sobre questões como privacidade e intimidade na Internet e alguns pontos, tais como a responsabilidade dos intermediários e como os dados pessoais devem ser processados ainda se encontram em um cenário incerto. As discussões abertas à sociedade, a regulação da Internet e uma lei sobre proteção de dados são passos necessários para estabelecer a segurança jurídica para os cidadãos e empresas no Brasil.

Comentários gerais ao Anteprojeto de Lei Brasileiro sobre a Proteção de Dados Pessoais

Antes de se adentrar especificamente na análise dos principais pontos do ALPDP, que "dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências", se deve destacar que a referida norma também discorre sobre dados sensíveis, os quais podem estar dentro da própria esfera de segredos. Assim, se faz necessário

incluir o aspecto da intimidade, em confluência com o Art. 5º, inciso X da Constituição Federal de 1988, e uma discussão com base na 'teoria dos círculos concêntricos da esfera da vida privada', o qual faz a separação entre privacidade, segredo e intimidade. (HUBMANN *apud* COSTA JÚNIOR, 2007).

No Art. 4º do Anteprojeto são trazidos conceitos-chave para o entendimento do texto em alusão, incluindo-se o que se deve considerar como "dado pessoal", "banco de dados", "dados sensíveis", "comunicação", "difusão", dentre outros. É sobremaneira arriscada a criação de conceitos paralisantes, em se tratando de tecnologia, tendo em vista que o Direito não acompanha *pari passu* a sociedade (CASTELLS, 2003).

O Art. 6º apresenta importante previsão acerca da responsabilidade objetiva daqueles que procedem ao tratamento de dados pessoais, atribuindo a essa prática o enquadramento como "atividade de risco". Interessante verificar que o presente artigo coloca em xeque a discordância jurisprudencial e doutrinária sobre se o simples fato de as empresas exercerem atividade de risco ensejaria responsabilidade objetiva. Em muitos *decisuns* dos tribunais pátrios, a responsabilidade objetiva vem sendo mitigada em contraponto ao Art. 927, parágrafo único do Código Civil, em face da natureza específica exercida pela atividade (como no caso de controle prévio de conteúdo gerado por usuários em redes sociais).

Todavia, no caso de tratamento de dados pessoais, o texto da norma vem ao encontro do atual Código Civil, pois determina que a atividade aqui descrita seja atividade de risco e, portanto, sob os auspícios da responsabilidade objetiva, na qual não se faz necessária a prova da existência de culpa, negligência ou imperícia, mas apenas do nexo causal e do dano.

Feita essa abordagem inicial, passa-se a traçar os principais aspectos do Anteprojeto que merecem ser ressaltados, a fim apresentar uma ideia ampla do seu escopo, uma vez que não se pretende a análise detalhada de todos os dispositivos.

Dos princípios e requisitos do Anteprojeto: alguns comentários

O Anteprojeto abordado, em seu Art. 8º, traça dez princípios que seriam a base sobre a qual repousam as demais previsões trazidas na norma. A leitura dos dispositivos tem um caráter didático, destacando apenas o que toca aos princípios da boa-fé objetiva e da responsabilidade (incisos VIII e IX respectivamente). A aplicação destes princípios decorre da Constituição Federal e do Código Civil, não sendo necessária uma previsão específica no Anteprojeto.

Contudo, é necessário verificar com atenção os requisitos mínimos exigidos a serem seguidos por aqueles que almejam realizar o tratamento de dados acerca da necessidade de aceitação expressa do titular dos dados pessoais, como se observa no Art. 9º do ALPDP.

O conceito de consentimento, para fins da presente normativa, merece tratamento mais detalhado, visto que, mesmo com o disposto no Art. 12 - que determina que o *opt-in* "é a permissão prévia concedida pelo destinatário e comprovável pelo remetente, autorizando o envio de e-mail marketing por um determinado remetente" – esta permissão deve estar em declaração apartada, considerando-se diversas formas possíveis de anuência do titular (muitas delas obscuras) e mesmo que estas não violem diretamente qualquer dispositivo de lei. Deve-se observar que tal aquiescência pode ser revogada a qualquer momento, em obediência aos termos do Art. 10 do diploma.

Igualmente, a norma em debate, *verbi gratia*, não discorre sobre a possibilidade de *opt-in* prévio por meio de mensagem não requisitada com o objetivo de conseguir a anuência para o tratamento dos dados. Alguns países da Europa já estabeleceram o *double opt-in* (dupla checagem acerca do desejo do destinatário de receber certos e-mails) como forma mais efetiva de proteção. Prática comum no mercado, por exemplo, é a pré-seleção dos *checkbox* de *opt-in* como forma diversa de adesão, sem probabilidade de modificação.

Mcdonald e Cranor (2008) demostram que poucos são os usuários que têm conduta ativa diversa do fornecimento de dados quando da contratação de um serviço *online*, o que traz em si forma automática de consentimento, metodologia divergente do pretendido pelo Anteprojeto.

Entende-se que o consentimento para utilização dos dados com fins comerciais deve ser colocado em tópico específico, garantido sua correta utilização e explicitado nos contratos de adesão, os quais são normalmente expostos como declarações de isenção de responsabilidade/*disclaimers* existentes em sítios virtuais. Interessante diferenciar, ainda no escopo do Art. 9, os termos "criança" e "adolescente" de forma a incluir este último aspecto visando consonância com o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990). Tal ajuste vai ao encontro das mais recentes discussões que vêm sendo tratadas acerca da reformulação da Diretiva 95/46, que discorre sobre proteção de dados no âmbito da Comunidade Europeia.

Quanto a esse aspecto, em específico, importa esclarecer que existem exceções à necessidade de consentimento, especialmente aquelas expostas no exercício do direito de defesa em sede judicial – em referência a dados provenientes de atos ou registros públicos – para a execução de obrigações e de outras situações prescritas no Art. 13. Quanto ao dispositivo elencado, há previsão do inciso IV no sentido de que o consentimento será dispensado quando se estiver diante de tratamento de dados para fins estatísticos. Atualmente, pesquisas de análise comportamental têm por base exatamente dados coletados de indivíduos que tiveram suas informações dissociadas (BAKER, 2009). Chamada de *behavioral analysis*, essa metodologia utiliza dados coletados durante a navegação de usuários em sítios virtuais obtidos por meio de *cookies* ou mesmo de registros de pesquisas que permitem traçar perfis de grupos específicos e podem levar à individualização com base em cruzamento de informações (ECKERSLEY, 2009). A análise estatística de comportamento virtual pode influenciar toda uma coletividade e atingir diretamente os hábitos de indivíduos, principalmente aqueles voltados a interesses comerciais, tais como o número de usuários de determinada região; usuários que acessam o sítio virtual em certo horário; usuários que utilizaram determinado serviço. Tais dados são relevantes quando não dissociados (BARKER, 2009) sendo, portanto, necessária à estipulação sobre qual tipo de análise estatística prescinde de anuência para ser tratada.

No Art. 13 igualmente se faz diferenciação entre os meios físicos e escritos. Contudo, uma crítica deve ser feita ao inciso VII – mesmo que esteja nos moldes do Art. 43 do CDC – pois, como em outras partes do Anteprojeto é necessário rever a metodologia de diferenciação ou determinar os casos em que a comunicação pode ser processada de forma totalmente eletrônica. Acerca da diferenciação, convém esclarecer que algumas leis não distinguem se a comunicação deve ser feita em formato eletrônico ou por escrito. Tal se dá no presente caso, no qual se observa que o inciso em referência se limita a afirmar que a comunicação deve ser feita por escrito para o titular, no caso de inadimplemento de obrigação, sem diferenciar o que pode ser considerado como "por escrito".

Cumpre observar no Art. 14 (o qual traz boas condutas sobre o tratamento das informações pessoais), que o inciso V (que dispõe sobre o tempo de armazenamento dos dados pessoais) recai sobre a mesma problemática enfrentada atualmente pelos tribunais, tanto pela doutrina, como pelo Projeto de Lei nº 2.126/2011: ao determinar que os dados não devam ser conservados por período de tempo superior ao necessário para as finalidades que justificaram sua coleta, o texto repassa para a Autoridade de Garantia (AG) ou para as instituições cabíveis a determinação deste prazo.

O Art. 11 do Projeto de Lei nº 2.126/2011 determina que os registros eletrônicos de conexão devam ser armazenados pelo período de um ano, podendo este prazo ser aumentado deste que motivado e requisitado por autoridade. Essa regulamentação dá fim à lacuna existente sobre o prazo de armazenamento, a qual permite que existam práticas diversas no mercado.

Desta forma, seria de bom alvitre constar menção expressa também na futura Lei de Dados Pessoais a menção a um prazo de armazenamento, limitando este ao prazo em que cesse o motivo pelo qual a coleta foi realizada, respeitando o princípio da finalidade.

Deve-se, contudo, conduzir o processo de coleta e de tratamento dessas informações mantendo-se todos os direitos garantidos no ALPDP em análise, nos termos abordados abaixo.

Dos direitos dos titulares dos dados

Os direitos atinentes àquele que terá seus dados tratados encontram-se dispostos no Art. 15 do ALPDP. Neste, há consonância com os moldes do Art. 43 do CDC, inclusive em relação ao prazo de cinco dias para informar ao titular dos dados pessoais a existência de qualquer informação ao seu respeito na base de dados do responsável por seu tratamento. A parte final do *caput* do artigo determina que o acesso ao banco de dados possa ser feito tanto por meio do remédio constitucional do *habeas data* como, dependendo de onde os dados estejam armazenados, invocando-se a Lei de Acesso à Informação. O Art. 43, parágrafo 4º do CDC, considera os bancos de dados de consumidores algo de caráter público. Em uma interpretação integrativa da Lei, o APLDP – ao possibilitar o acesso aos bancos de dados de registros pessoais por meio de *habeas data* – confere caráter público a estes, mesmo que não tenham natureza de relações de consumo.

Nesse cenário, nada obsta a que sejam imaginadas situações como a da impetração desse remédio, em face de uma pequena Organização Não Governamental (ONG), *verbi gratia*, pelo simples fato de ela lidar com dados de natureza pessoal. Neste particular, convém ser necessária maior explicitação desse artigo.

Igualmente, para fins de requisição das informações e alteração destas, é importante notar que em nenhum momento se limita a atuação em tais procedimentos por meio de um advogado constituído, o que leva a se inferir que o cidadão, *sponte propria*, poderá propor tais procedimentos.

No caso de alteração de dados, convém serem observados os procedimentos trazidos pelo Art. 16 do Anteprojeto, sendo certo que o titular dos dados poderá oferecer oposição, total ou parcial, ao tratamento de suas informações – nos casos previstos nos incisos do Art. 17 do ALPDP – cabendo suscitação de eventual descumprimento da norma perante a Autoridade de Garantia (AG).

Caso se esteja diante de dados sensíveis, incluindo-se até mesmo informações genéticas, consoante se deflui do Art. 4º, IV, impende observar que, nos termos do Art. 20 do APL, ninguém poderá ser obrigado a fornecê-los. Ainda sobre informações sensíveis delineou-se que é vedada a formação de banco de dados que os contenham, salvo disposição legal expressa (ALPDP, Art. 21). Contudo, o parágrafo 1º, I do mesmo dispositivo afirma que o tratamento de tais dados será permitido quando o titular tiver confirmado o seu consentimento livre, sempre e quando tal for necessário para a realização de suas atribuições legais ou estatutárias.

Entende-se, *data maxima venia*, que nesse trecho há possibilidade de ato particular suplantar comando legal, no caso das atribuições legais ou estatutárias não discorrerem expressamente sobre a possibilidade de fornecimento de dados sensíveis. É necessária, portanto, uma sincronia de textos legais para a viabilidade do tratamento de dados sensíveis, em relação aos quais, também, deve ser dada atenção quanto ao manuseio e segurança destes dados, evitando-se o acesso por terceiros não autorizados.

Do tratamento, segurança dos dados e códigos de boas práticas

Deve-se reforçar a atenção quanto à segurança no tratamento de dados, a fim de que eles não caiam em mãos desautorizadas, causando prejuízos que podem trazer impacto sobremaneira elevado. Justamente a fim de evitar a ocorrência dessas situações, o Cap. VI do Anteprojeto trata especificamente da segurança dos dados em ambiente

eletrônico, trazendo-se de modo claro que isso se dará com a adoção de medidas que visam à redução máxima da quantidade de falhas.

Importante lembrar a atenção que se teve com o assunto, ao se elaborar o diploma em alusão, tendo-se criado princípio próprio, chamado de "Princípio da Segurança Física e Lógica" (Art. 8º, VII), tema que, com a elevação do uso dos sistemas de tecnologia, vem adquirindo cada vez mais importância (MANDARINO JUNIOR, 2010, p. 35-37).

Cumpre ter em mente o que diz respeito aos bancos de dados (principais repositórios de informações), que precisam ser desenhados de modo a impedir a captura por terceiros não autorizados, privilegiando-se a utilização de criptografia. Deve ser permitido o acesso a essas informações armazenadas nos casos expressamente permitidos no Anteprojeto, consoante incluído no Cap. V, o qual alude ao "tratamento de dados sensíveis". A previsão do parágrafo único deve ser analisada de modo a se evitar a perpetuação de desproporções em termos de exigência. Isto é, caso se esteja diante de grandes instituições financeiras – que lidam com informações que são frequentemente alvo de criminosos – certamente atentará de forma mais constante e elevada neste aspecto do que uma pequena loja que apresente estruturas de dados menos complexas, tais como o nome e a preferência de compra de seus clientes.

Deve-se ter em mente que isso implicará um monitoramento pela organização dos dados, com especial atenção às novidades trazidas pelas normas da Associação Brasileira de Normas Técnicas (ABNT), Organização Internacional para Padronização (ISO), mais especificamente as já publicadas ISO/IEC 27001 (Tecnologia da informação – técnicas de segurança – sistemas de gerência da segurança da informação – requisitos) e ISO/IEC27002 (Gerenciamento da Segurança da Informação), as previsões da *RSA Data Security* e seus *Request for Comments* (RFC), dentre outros. Nessa esteira, as Políticas de Segurança da Informação, bem como os Regulamentos Internos de Segurança da Informação (RISI) e os Termos de Uso de Segurança da Informação (TUSI), presentes em inúmeras corporações, precisarão ser sistematicamente atualizadas em conformidade com as distintas normas.

O Art. 45 traz específica determinação acerca do que se deve atentar ao se elaborar o RISI e o TUSI, denominados de "Código de Boas Práticas", sendo importante a observação de que eles deverão ser depositados e tornados públicos perante a Autoridade de Garantia (AG), consoante expressa determinação do parágrafo 4º, que poderá desaprová-los.

Necessário se faz, igualmente, analisar mais profundamente o que consta no parágrafo 5º do Anteprojeto definindo a quem caberá a publicidade do Código mencionado: se à Autoridade ou à parte que elaborou o documento, mormente se levando em conta que se está diante de documento obrigatório.

Por derradeiro, no parágrafo único do Art. 25, verifica-se que o subcontratado (entende-se que o termo "administrador do banco de dados" seja melhor cabível) deverá realizar o tratamento consoante as instruções fornecidas "por escrito". Tal anacronismo já mencionado é recorrente ao longo do texto da norma, que aborda os documentos eletrônicos de forma distinta dos textos escritos, como fica evidente no Art. 15, parágrafo 3º, por exemplo.

Sobre o tema, o Anteprojeto do Novo Código de Processo Civil, Projeto nº 166/2010 destacou a Seção VIII do Cap. XI para abordar a questão sem prejuízo de diversos outros dispositivos que se posicionam favoravelmente à plena validade dessa documentação gestada em ambiente eletrônico (Art. 225 do Código Civil, Medida Provisória nº 2.200-2/2001, Lei nº 11.419/2006, dentre outros).

Essas questões, entretanto, sofrem algumas diferenciações quanto ao tratamento em se estando diante de banco de dados do setor público ou privado.

Do tratamento de dados no setor público e no setor privado

Acerca do tratamento de dados especificamente no setor público é importante ler as prescrições trazidas nos artigos 32 e 33 do Anteprojeto. O primeiro dispositivo aborda a comunicação e a interconexão de dados entre pessoas jurídicas de direito público. Ademais, os conceitos inseridos no *caput* e em seu parágrafo único (de "matérias distintas" e de "competências institucionais") são sobremaneira abertos, fornecendo margem para ampla liberdade de atuação do ente público, o que pode ter efeitos negativos que podem trazer graves consequências.

Não se exige, pois, qualquer autorização do titular dos dados para a comunicação deles entre tais entes públicos, o que confirma a ampla liberdade para troca dessas informações, ampliando as chances de vazamento, o que vem se tentando evitar ao longo de toda a norma em análise.

As emanações do inciso III do Art. 33, contudo, podem ser interpretadas como mecanismos para mitigar o risco aludido, na medida em que são estreitadas as situações nas quais os responsáveis pelos bancos de dados públicos poderão atuar, ainda sendo sobremaneira alargadas as possibilidades, sugerindo-se que tais especificações sejam reduzidas.

Já no que diz respeito ao tratamento de dados no setor privado, tal tema é abordado no Art. 35 do ALPDP, o qual se manifesta no sentido de que apenas empresas que possuam mais de duzentos empregados deverão apontar diretor responsável pelo tratamento dos dados. Não se entende a razão da estipulação desse valor, que deve ser alterado para abarcar todas as empresas com atuação em âmbito eletrônico, independentemente do número de colaboradores, tendo em vista as consequências que poderão advir da perda das informações por elas tratadas. Pode-se tornar o dispositivo mais maleável quanto a estas, com exceção da necessidade de se ter empregado destacado especificamente para esta tarefa.

Chama-se atenção para a ligação direta da pessoa ou do departamento designado junto à Autoridade de Garantia (AG), como forma de garantir um canal efetivo de comunicação e de conformidade/*compliance* com as regras impostas pela organização. Deve-se atentar também para a inclusão dessas responsabilidades no RISI e no TUSI, a fim de que as empresas também se resguardem quanto às funções do gestor do banco de dados.

Neste contexto, a AG apresenta-se como de papel fundamental para a gestão eficiente dos aspectos apresentados no ALPDP. Existem ainda, contudo, alguns aspectos principais que precisam de melhor enfoque.

Da Autoridade de Garantia

Apesar de entendimentos em sentido contrário, pensa-se ser salutar a criação de Conselho específico para tratar da proteção de dados pessoais tendo em vista a necessidade de especialização daqueles que cuidarão do tema. Sem dúvida, as organizações que hoje lidam com isso o fazem de modo esparso e como atividade secundária, constatando-se amadorismos que refletem, dentre outros, em demora excessiva para responder questionamentos básicos.

A criação de entidade regulatória autônoma no âmbito da proteção de dados pessoais é natural em legislações alienígenas, tendo por origem o Direito Italiano. A Europa detém entidades nacionais e supranacionais que têm por função primordial a conformidade das leis estatais que introduzem em seus territórios as Diretivas da Comunidade.

Com a instituição de célula específica nesse sentido espera-se que esses entraves referidos sejam solucionados, tendo-se célere e efetiva atuação do órgão, quando suscitado a se manifestar e atuando de igual modo em prestígio da segurança jurídica.

A primeira referência específica à Autoridade de Garantia é observada no Art. 18 do ALPDP, atribuindo-se a ela a função de garantia da lei,

a quem os titulares poderão recorrer no caso de violações. No Art. 22 tem-se que a tal órgão cabe delimitar as medidas de segurança e de proteção ao titular dos dados sensíveis.

Importante observar que, no Art. 24 há previsão no sentido da necessidade de constantes adaptações às alterações tecnológicas por parte daqueles que lidam com dados pessoais, sendo função da AG explicitar quais os critérios que deverão ser considerados.

À Autoridade de Garantia também se atribuiu o encargo de receber notificações, conjuntamente com os titulares, quando se verificar acesso indevido, perda ou difusão acidental de informações, e sempre que se vislumbrar possibilidade de risco à privacidade dos titulares. Cabe a AG tomar as medidas que julgar convenientes, inclusive podendo determinar seja dada ampla divulgação ao fato; decidir, de igual modo, sobre a possibilidade da transferência internacional, perscrutando se os termos prescritos no Art. 35 são seguidos pela nação a quem os dados serão repassados, havendo exceções a essa regra, nos moldes confirmados pelo Art. 37. Ademais, no Art. 38 traz-se disposição acerca da criação do Conselho Nacional de Proteção de Dados Pessoais, atuando como Autoridade de Garantia e gozando de relativa autonomia. As competências cabíveis da AG estão declinadas no Art. 39.

O Art. 40 se manifesta no sentido de que podem ser instituídas diversas autoridades de proteção de dados pessoais, por parte dos Estados, do Distrito Federal e dos Municípios. Como se observa, não há maiores previsões acerca da forma de atuação de cada uma delas, limitando-se a prever que elas terão competência concorrente – dentro de seus respectivos territórios – e, com base no princípio da simetria, ter competência e atuação semelhantes à Autoridade de Garantia de âmbito nacional.

À Autoridade de Garantia é atribuída à função de aplicar as sanções administrativas previstas nos artigos 41 e seguintes do ALPDP, sem prejuízo de determinar as medidas corretivas que julgar necessárias para reverter os efeitos danosos causados.

Importante observar que o Anteprojeto em referência não trouxe qualquer previsão de aplicação de penas em âmbito criminal, sequer de instituição de tipos penais, limitando-se a traçar consequências administrativas e cíveis do descumprimento das normas trazidas.

Feitas essas considerações sobre o marco nacional, adiante são trazidas incursões breves sobre o tratamento levado a efeito em outras nações, verificando-se os aspectos mais marcantes, os quais, inclusive foram tomados como inspiração pelos elaboradores do diploma analisado.

O Anteprojeto de Lei Brasileiro de Proteção de Dados Pessoais e legislações estrangeiras: Direito Comparado

O Art. 3º do ALPDP determina que esta Lei seja aplicada aos tratamentos de dados pessoais realizados no território nacional por pessoa física ou jurídica de direito público ou privado. A abrangência deste artigo, incluindo bancos de dados ou base de dados que se encontrem no exterior, condiz com a atual tendência tecnológica da ubiquidade, mormente com a utilização de *Cloud Computing*, em que os dados podem estar armazenados nos mais diversos locais. É prática do mercado o não fornecimento dessas informações caso estejam alocadas em território alienígena, mesmo quando requisitadas judicialmente.

Dispõe o Art. 35 do Anteprojeto que "[a] transferência internacional de dados pessoais somente é permitida para países que proporcionem um nível de proteção de dados equiparável ao da presente lei", elencando as seguintes exceções:

> Art. 35 – A transferência internacional de dados pessoais somente é permitida para países que proporcionem um nível de proteção de dados equiparável ao da presente lei, salvo as seguintes exceções:
> I – quando o titular tiver manifestado o próprio consentimento livre, expresso e informado para a transferência;

> II – quando for necessária para a execução de obrigações derivadas de um contrato do qual o titular for parte;
> III – quando for necessária para a garantia de um interesse público relevante previsto em lei;
> IV – quando for necessária para a cooperação internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional a que o Brasil se vincule;
> V – quando for necessária para a defesa de um direito em juízo, se os dados forem transferidos exclusivamente para esta finalidade e pelo período de tempo necessário;
> VI – quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, se o titular não puder fornecer o próprio consentimento por impossibilidade física, por incapacidade de agir ou de compreender.

O Art. 36 e o Art. 39, XI discorrem sobre a competência da AG para atestar a equivalência entre os países com relação à proteção aos dados pessoais e permitir a transferência de dados entre estes países. É necessário, portanto, analisar as legislações estrangeiras para verificar se estas estão em nível adequado.

Como paradigma de leis de proteção de dados e privacidade, o panorama europeu deve funcionar como modelo, não somente por abordar questões cruciais, mas por ter sido um dos primeiros a estabelecer regulamentos abrangentes sobre o tema com a Diretiva de Proteção de Dados de 1995 (UNIÃO EUROPÉIA. Directive..., 1995). A entrada em cena da Diretiva foi um marco histórico na proteção de dados na União Europeia e em todo o mundo, uma vez que elevou ao nível de direito fundamental o direito à proteção de dados pessoais.

Todavia, novamente em contraponto ao cenário brasileiro, a Diretiva se encontra sob um processo extenso de revisão, adaptando-a aos avanços tecnológicos e da globalização, que trouxeram consigo novos desafios para a proteção de dados pessoais. Dentre as principais alterações, podem ser mencionadas as redes sociais e a computação em nuvem, bem como o fato de que as formas de coletar dados pessoais tornaram-se progressivamente mais elaboradas e difíceis de detectar (UNIÃO EUROPÉIA. European Commission, 2012). Este processo de reforma, no contexto da União Europeia, a Diretiva tem os seguintes objetivos principais:

a) reforçar os direitos das pessoas;
b) aprofundar a vertente relativa ao mercado interno;
c) rever as normas de proteção de dados no domínio da cooperação policial e judiciária em matéria penal;
d) observar a dimensão mundial da proteção de dados; e
e) traçar um quadro institucional mais forte para uma melhor aplicação das normas de proteção de dados.

E, no âmbito do reforço dos direitos pessoais, pode-se citar a necessidade de:

a) garantir a proteção adequada das pessoas em todas as circunstâncias;
b) aumentar a transparência para as pessoas;
c) aumentar o controle sobre os próprios dados;
d) garantir o consentimento informado e livre;
e) proteger dados sensíveis; e
f) tornar as soluções e as sanções mais eficazes.

O ALPDP teve clara inspiração nas Diretivas Europeias, mas também recebeu forte impacto da lei de proteção de dados canadense (*Protection and Electronic Documents Act* - PIPEDA)[3]. Esta abrange todos os tipos de informações pessoais, em todas as entidades privadas, estando em adequação com os padrões europeus e permitindo a transferência de dados entre países, tendo também estabelecido uma Autoridade de Garantia.

Os Estados Unidos da América, apesar do cenário de utilização massiva de tecnologias de processamento de dados, e de ser lar de grande parte das empresas privadas que lidam com informações pessoais, não têm uma regulação geral sobre proteção de dados, mas sim leis estaduais que va-

[3] Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/>. Acesso em: 24 maio 2013.

riam de protetivas até mais restritivas. Algumas normas federais tratam sobre temas específicos como saúde, crianças e instituições financeiras tais como a *Children's Online Privacy Protection Rule*, a *Federal Information Security Management Act* (FISMA), a *Gramm-Leach-Bliley Act* (GLBA) e a *Health Insurance Portability and Accountability Act* (HIPAA). Demais normas que tratam sobre a liberdade de expressão e o acesso estatal a informações são mais comuns, tais como o *Federal Privacy Act*, *Freedom of Information Act* e o *Patriot Act*. De acordo com o princípio da reciprocidade, as empresas americanas que desejarem estar de acordo com o nível de proteção dado na Europa devem aderir aos princípios do *US-EU Privacy Safe Harbour*. Muitos Estados americanos, como a Califórnia, detêm legislações compelindo a notificação dos titulares dos dados no caso de falhas de segurança.

Recentemente, os maiores provedores de acesso à Internet dos EUA adotaram como padrão a análise do tráfego de seus usuários na busca por conteúdo autoral indevidamente utilizado, em contraponto ao princípio da neutralidade (ESTADOS UNIDOS, 2011), e em similaridade a Lei Francesa HADOPI[4].

Na América Latina, alguns países promulgaram leis específicas de proteção de dados pessoais, tais como a Argentina, Uruguai, Paraguai, Chile e, recentemente o Peru. O Uruguai, devido ao seu avanço legislativo nesse sentido, foi incluído como Estado signatário da Convenção 108 da Organização para a Cooperação e Desenvolvimento Econômico (OECD) – que traz em seu corpo princípios básicos para proteção de dados – e é o único país não europeu a assinar o protocolo (POLAKIEWICZ, 2011).

O Art. 37 do Anteprojeto de Proteção de Dados Pessoais traz previsões de situações em que, mesmo não estando atendidas as disposições de conformidade de tratamento aos dados pessoais do país para o qual eles serão enviados, ainda assim, essa troca pode ocorrer desde que sejam dadas as mínimas garantias prescritas para tanto.

Conclusões

O ALPDP faz parte do movimento nacional para os estabelecimentos de marcos regulatórios necessários em face da proliferação de novas tecnologias e, principalmente, da Internet no país.

Não se pode confundir, todavia, a ideia de marco regulatório com regulação. A proposição de marco vai ao encontro na natureza autopoiética desse meio, ou seja, da criação intrínseca, por seus participantes, de normas de conduta, funcionando apenas como fatores limitadores de abuso, de forma a garantir a segurança jurídica a situações que recebem tratamentos diversos.

O atual estado da tecnologia, e a quantidade de dados que são coletados dos indivíduos, permitindo um conhecimento completo sobre as suas vidas, mesmo sem a sua anuência, não permite mais um cenário apático de proteção destes dados. O mero conceito de privacidade, elástico como tem sido, não é suficiente para evitar abusos e proteger o cidadão. É emergente, portanto, a promulgação do ALPDP na forma de Lei, assim como o debate sobre ela deve inserir os participantes/*stakeholders* nacionais também no âmbito do Poder Legislativo.

Considerando-se que o objetivo do texto do ALPDP não é somente a proteção dos dados pessoais, mas também o estabelecimento de um paradigma jurídico que possa servir de sustentáculo para investimentos econômicos e desenvolvimento tecnológico, o referenciado dispositivo também poderia contemplar as proteções de ordem econômica e das relações de consumo que envolvem o cidadão.

[4] Disponível em: <http://www.hadopi.fr/>. Acesso em: 24 maio 2013.

Referências

ASCENSÃO, J. de O. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

BAKER, S. **Numerati**. São Paulo: Saraiva, 2009.

BRASIL. Constituição da República Federativa do Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 11 jan. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 30 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 12 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do Art. 5° da Constituição Federal. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 25 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 17 jul. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9472.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial [da] República Federativa do Brasil, Brasília**, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 20 dez. 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 20 jun. 2013.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 27 ago. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 20 jun. 2013.

BRASIL. Projeto de Lei nº 2.126, de 2011. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, [em tramitação]. Disponível em: <http://www.planalto.gov.br/ccivil_03/Projetos/PL/2011/msg326-24ago2011.htm>. Acesso em: 20 jun. 2013.

BRASIL. Câmara dos Deputados. **Projeto de lei nº 4.906, de 2001**. Dispõe sobre o comércio eletrônico. Em tramitação. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=29955>. Acesso em: 20 jun. 2013.

BRASIL. Ministério da Justiça. **Portaria nº 5, de 27 de agosto de 2002**. Complementa o elenco de cláusulas abusivas constante do Art. 51 da Lei nº 8.078, de 11 de setembro de 1990. Disponível em: <http://portal.

mj.gov.br/main.asp?View={4521CE7B-732B-40EB-B529-F9200C365E93}>. Acesso em: 20 jun. 2013.

BRASIL. Senado. **Projeto de lei nº 166, de 2010**. Dispõe sobre a reforma do Código de processo civil. Em tramitação. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=79547&tp=1>. Acesso em: 20 jun. 2013.

BRASIL. Tribunal Superior do Trabalho. Recurso de Revista n° 613/2000-013-10-00. 1ª Turma. Relator: Ministro João Oreste Dalazen. **Diário da Justiça**, 10 jun. 2005.

CASTELLS, M. **A Galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade.. Rio de Janeiro: Jorge Hazar, 2003.

COSTA JUNIOR., P. J. da. **O direito de estar só**: tutela penal da intimidade. 4. ed. São Paulo: Revista dos Tribunais, 2007.

OPEN SECURITY FOUNDATION. Data Loss statistics. In: **DataLossdb**. 2013. Disponível em: <http://datalossdb.org/statistics>. Acesso em: 5 jun. 2013

ECKERSLEY, P. **How online tracking companies know most of what you do online**: and what social networks are doing to help them. San Francisco CA: Electronic Frontier Foundation, 21 Sept. 2009. Disponível em: <https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks>. Acesso em: 18 jun. 2013.

ESTADOS UNIDOS. Federal Bureau of Investigation. Operation Technology Division. Wireless evolution. **ETR Bulletin: emerging technology research**, v. 8, n. 1, March 2011. Disponível em: <http://www.wired.com/images_blogs/threatlevel/2011/07/FBI-Tech-Newsletter.pdf>. Acesso em: 25 maio 2013.

MANDARINO JUNIOR., R. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

MCDONALD, A. M.; CRANOR, L. F. The cost of reading privacy policies. **I/S: A Journal of Law and Policy for the Information Society**, v.4, n. 3, p. 540-565, 2008. Disponível em: <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf>. Acesso em: 18 jun. 2013.

POLAKIEWICZ, J. Current developments in privacy frameworks: towards global interoperability. In: OECD CONFERENCE, 2011. **Proceedings…** Mexico City, 2011. Disponível em: <http://www.oecd.org/sti/ieconomy/49154885.pdf>. Acesso em: 25 maio 2013.

PRIVACY RIGHTS CLEARINGHOUSE. **Chronology of Data Breaches**: Security Breaches 2005- Present. [USA], 2013. Disponível em: <http://www.privacyrights.org/data-breach>. Acesso em: 9 maio 2013.

TANCER, B. **Click**: o que milhões de pessoas estão fazendo on-line e por que isso é importante. São Paulo: Globo, 2009.

UNIÃO EUROPÉIA. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **Official Journal**, Luxemburgo, L 281, 23 Nov. 1995, p. 0031 – 0050. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 25 maio 2013.

UNIÃO EUROPÉIA. European Commission. Proposal for a directive of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - COM/2012/010. **EUR-Lex**: access to European Union law, Luxemburgo, 2012. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:HTML>. Acesso em: 25 maio 2013.

Brazilian legal landscape on protection of personal data: discussion and comparative analysis

Abstract

Introduction: Given the worldwide movement on the legal and regulatory frameworks for the protection of personal data the article exposes the current scenario in Brazil and analyzes the Protection of Personal Data Protection Project. Discusses aspects related to privacy, intimacy and the data of natural persons and provides a comparative analysis with foreign law. Method: Desk research evolving national legislation, doctrine and case law, as well as, international normatives. Results: Currently, Brazil has a dispersed and not specific laws on the issue of data protection. Specific and non specific mentions appear in chapters, articles, paragraphs and sections of different pieces of legislation and jurisprudence. When analyzing the Brazilian Personal Data Protection Project there is a need for clarification and insights on specific items, especially those dealing with ownership of data, the public data repositories security and privacy, and the need for creating an autonomous regulatory entity. Another concern is related with the absence of criminal penalties. The Bill was inspired by The European Directive on the Protection of Personal Data (EC 95/46) and the Canadian Data Protection Act. Conclusions: The proliferation of new technologies, especially the Internet, is pushing for the existence of legal frameworks. Considering that the aim of the text of the Bill's draft is not only the protection of personal data, but also the establishment of a legal paradigm, it can serve as a prop for economic investment and technological development and contemplate the protection of economic and consumer relations.

Keywords

Data protection. Personal data. Access to information. Data protection law. Information security.

Recebido em 30 de abril de 2013
Aceito em 23 de junho de 2013

Sobre os autores:

Caio Cesar Carvalho Lima
Bacharel em Direito - UFC, Especialista em Direito da Tecnologia da Informação - UGF/RJ, Mestrando em Direito Processual Civil - PUC/SP (bolsista CNPq).
ccesar@gmail.com

Renato Leite Monteiro
Bacharel em Direito - UFC, Mestre em Direito (Direito Constitucional) - UFC. Escola de Magistratura do Estado do Ceará - ESMEC, Escola Paulista de Direito (MBA) - EPD.
renatoleite@gmail.com

Como citar este artigo:

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada . **AtoZ: novas práticas em informação e conhecimento**, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <http://www.atoz.ufpr.br>. Acesso em: