3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Sumaré, 4 de julho de 2015.

Assunto: Contribuições à Consulta Pública sobre o Anteprojeto de Lei para a Proteção de Dados Pessoais

I. INTRODUÇÃO

3M do Brasil

Somos uma empresa baseada na ciência e aplicada à vida. Nossas soluções são usadas nas empresas e lares, melhorando a vida das pessoas. Reconhecida globalmente pela sua inovação e forma ética de conduzir negócios, a 3M está presente no Brasil há quase 70 anos, atualmente com 7 plantas fabris. Com forte desenvolvimento nacional, 70% de nossas vendas são de produtos manufaturados localmente.

A 3M orgulha-se de ter entre os seus valores o respeito ao ambiente físico e social, a partir do desenvolvimento de produtos e soluções sustentáveis com o objetivo de promover o bem estar da sociedade. Além disso, somos reconhecidos no Brasil e no mundo por nossos valores éticos, agindo com honestidade e integridade em todos os países em que estamos presentes. Atuamos mundialmente com cinco grandes grupos de negócios, nos mercados Industrial, de Consumo, de Eletrônicos e Energia, de Gráficos e Segurança Ocupacional e Viária, e de Saúde.

Nossas soluções são produzidas nos mais altos padrões de qualidade, seguindo os critérios exigidos pelas agências normalizadoras e reguladoras locais. Ademais, alinhados às políticas públicas para os setores nos quais atuamos, buscamos também oferecer nossas contribuições para o aperfeiçoamento institucional do ambiente de negócios.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

II. Da Legislação Brasileira Acerca da Proteção à Privacidade e do Anteprojeto de Lei para a Proteção de Dados Pessoais

II.a) Da Legislação Brasileira Vigente Acerca de Proteção à Privacidade

Inicialmente, cumpre apontar que, mesmo antes da entrada em vigor do Marco Civil da Internet, o ordenamento jurídico brasileiro já possuía dispositivos acerca da proteção às informações pessoais. A própria Constituição Federal de 1988 prevê a garantia da vida privada[1] como um dos direitos fundamentais, conforme estabelecido em seu artigo 5º, inciso X:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
> X - 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;

Do mesmo modo, a Constituição Federal prevê, no mesmo artigo 5º, inciso XII, a inviolabilidade do sigilo das comunicações[2]. Tal inciso é regulamentado pela Lei nº 9.296/1996, que prevê como crime a interceptação de comunicação informática, se não precedida de autorização judicial ou se realizada com objetivos não autorizados em lei[3].

O Código Civil, da mesma forma que a Constituição, inclui a privacidade entre os direitos de personalidade, determinando a inviolabilidade da vida privada da pessoa natural. Neste sentido: "art. 21. 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".

---

[1] Privacidade será aqui interpretada como incluindo o direito à vida privada e à intimidade, conforme adotado por José Afonso da Silva: "O direito à intimidade é quase sempre considerado como sinônimo de direito à privacidade. Esta é uma terminologia do direito anglo-americano (right of privacy), para destacar aquele, mais empregada no direito dos povos latinos. Nos termos da Constituição, contudo, é plausível a distinção que estamos fazendo, já que o inciso X do artigo 5º separa intimidade de outras manifestações da privacidade: vida privada (...), que trataremos, por isso, em tópicos apartados. (...) Abrange, nesse sentido mais restrito, a inviolabilidade do domicílio, o sigilo da correspondência, o segredo profissional. (...) É também inviolável a vida privada. (...) A vida das pessoas compreende dois aspectos: um voltado para o exterior, outro para o interior. A vida exterior, que envolve a pessoa nas relações sociais e nas atividades públicas, pode ser objeto das pesquisas e das divulgações de terceiros, por que é pública. A vida interior, que se debruça sobre a mesma pessoa, sobre os membros de sua família, sobre seus amigos, é a que integra o conceito de vida privada, inviolável nos termos da Constituição". (SILVA. José Afondo da. Curso de Direito Constitucional Positivo. 32ª edição. São Paulo: Malheiro, 2009, pp. 206 – 208).

[2] Constituição Federal: "Art. 5º: (...)XII - 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".

[3] Lei nº 9.296/1996: Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Neste aspecto, importante apontar que nos termos do artigo 52 do Código Civil, "aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade". Desse modo, o direito à privacidade alcança também a pessoa jurídica, conforme entendimento de Renato Opice Blum:

> O direito à privacidade no Brasil visa resguardar tanto os aspectos pessoais e familiares, bem como os empresariais. Ressalte-se que a pessoa jurídica não está excluída do direito à preservação de sua vida interna, vedando-se, pois, a divulgação de informações de âmbito particular. Existem, inclusive, normas legais que proíbem a divulgação de dados de natureza confidencial da empresa, excetuados os casos das companhias abertas que, por exigência do mercado, são obrigadas a divulgar informações pertinentes, em certos casos.[4]

Ainda, a Lei nº 8.078/1990, o Código de Defesa do Consumidor ("CDC"), contém previsões relacionadas à privacidade dos consumidores, na Seção VI de seu Capítulo V, dedicada a regular a criação de banco de dados cadastrais de consumidores, estabelecendo regras e restrições para mencionada situação, em prol do consumidor[5]. No entanto, o CDC não prescreve procedimentos específicos para a utilização de dados de consumidores, pelo fornecedor, ou restrições ao acesso às informações constantes de tais bancos de dados.

Cumpre apontar, no entanto, que o Ministério da Justiça já se manifestou no sentido de que é dever do fornecedor proteger os dados e as informações pessoais dos consumidores:

> 07. Pode o site fornecer meus dados cadastrais para terceiros?
> **É dever do fornecedor proteger os dados e informações pessoais dos consumidores,** não podendo divulgar ou repassá-los para terceiros, salvo se expressamente autorizado pelo consumidor, sendo abusiva cláusula contratual que imponha ao consumidor a obrigação de

---

[4] OPICE BLUM, Renato M.S. **A Privacidade e os Tribunais**. Disponível em: http://www1.serpro.gov.br/publicacoes/tema/166/materia15.htm. Acesso em 04.05.2015.

[5] CDC: SEÇÃO VI - Dos Bancos de Dados e Cadastros de Consumidores: "Art. 43. 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. §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. §4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. §5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores; Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.
§1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. §2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código".

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

> manifestar-se contra a transferência de seus dados cadastrais a terceiros, nos termos da legislação em vigor (Constituição Federal e CDC) e da Portaria SDE nº 5, de 27 de agosto de 2002.
> Vale lembrar que o consumidor tem direito ao acesso às informações existentes a seu respeito em qualquer cadastro, banco de dados, fichas ou de dados pessoais a seu respeito, bem como sobre suas respectivas fontes, podendo exigir a correção de qualquer informação total ou parcialmente equivocada (conforme o artigo 43 do CDC).[6] (g.n.)

Desse modo, verifica-se que o ordenamento jurídico brasileiro, mesmo antes da entrada em vigor do Marco Civil da Internet, já previa a proteção à privacidade e à proteção a dados, como uma das garantias constitucionais e em disposições esparsas constantes da legislação.

II.b) A Privacidade após o Marco Civil da Internet

As previsões do Marco Civil da Internet vão ao encontro do quanto já estabelecido pelo ordenamento jurídico brasileiro, anteriormente à entrada em vigor de referida Lei, conforme se pode observar do artigo 3º, incisos II e III, que trazem a proteção da privacidade e dos dados pessoais como princípios do uso da Internet no Brasil:

> Art. 3o A disciplina do uso da internet no Brasil tem os seguintes princípios: (...)
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;

Ainda, o Marco Civil estabelece, como garantia dos usuários de serviços de Internet, a inviolabilidade da intimidade e da vida privada, bem como a inviolabilidade e o sigilo do fluxo das comunicações privadas armazenadas, a não ser mediante ordem judicial específica para a quebra de sigilo:

> 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.

Com relação a mencionado artigo 7º, I, cumpre apontar que este possui fundamento na proteção à privacidade constante do artigo 5º, X, da Constituição Federal, conforme indicado no parecer proferido

---

[6] Disponível em http://portal.mj.gov.br/main.asp?View={EE12C917-745A-44C1-B980-95849D45F794}&BrowserType=IE&LangID=pt-br. Acesso em 04.05.2015.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

em plenário[7], quando da discussão do projeto de lei que originou o Marco Civil na Câmara dos Deputados:

> Com relação ao artigo 7º, optamos por inserir novo inciso I, fundamentado no inciso X do artigo 5º da Constituição Federal. Ressalta-se, assim, a inviolabilidade da intimidade e da vida privada também no âmbito da Internet. Outro aperfeiçoamento que propomos é a previsão, além do direito à indenização, que a Constituição já garante (no próprio artigo 5º, inciso X, em relação à inviolabilidade da intimidade e privacidade), do direito de proteção, significando direito à sustação da violação, atuando na prevenção, não só na reparação. Isto complementa o texto constitucional sem contrariá-lo, porque se alinha ao mesmo espírito do direito à indenização.

Deste modo, o Marco Civil prevê a proteção dos dados pessoais dos usuários, bem como dos registros de conexão à Internet[8] e de acesso a aplicações de Internet[9], que permitem a identificação do usuário, por meio de previsões específicas sobre coleta, uso, tratamento, armazenamento e compartilhamento de tais informações, como forma de proteção à privacidade. Neste sentido:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Por sua vez, o artigo 7º, VII a IX, do Marco Civil[10], estabelece regras para a coleta, uso, tratamento, armazenamento e compartilhamento de dados pessoais e de registros de conexão e acesso a

---

[7] Disponível em http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1240240&filename=PPP+2+PL21261 1+%3D%3E+PL+2126/2011. Acesso em 04.05.2015.

[8] Lei 12.965/2015: Art. 5o Para os efeitos desta Lei, considera-se: (...)VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

[9] Lei 12.965/2015: Art. 5o Para os efeitos desta Lei, considera-se: (...)VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[10] Lei 12.965/2015: Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)II - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
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 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;

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

aplicações de Internet, prezando pela privacidade dos usuários. Conforme afirma a doutrina, "em síntese, pois, prevalecem para todos os registros as regras de inviolabilidade e de sigilo"[11].

Importante apontar que o Marco Civil da Internet como consta de seu artigo 1º, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil[12]. Neste sentido:

> Em análise à Lei do Marco Civil da Internet nota-se que a lei estabelece princípios, direitos e deveres de usuários da Internet. Alguns textos sobre a referida lei, com maior destaque para os jornalísticos, expressa, que esta lei seria uma espécie de "Constituição da Internet" e que a elaboração de um projeto desse porte e tema surgiu pelo fato de que após 18 anos de uso da Internet no Brasil, não havia qualquer lei que regulasse e estabelecesse diretrizes para proteger seus direitos.[13]

Em consequência, na medida em que o Marco Civil regula, primordialmente, as relações desenvolvidas por meio da Internet, as disposições constantes de tal Lei são aplicáveis a todas as situações em que haja a coleta, utilização ou tratamento de dados por meio da Internet, ou seja, utilizando-se de Protocolo TCP/IP.[14]

Desse modo, entre outros aspectos, a partir da entrada em vigor do Marco Civil, em 23 de junho de 2014, os dados coletados, utilizados, tratados ou armazenados por meio da Internet passaram a possuir proteção específica, com o intuito de garantir, entre outras questões, a privacidade dos usuários. No entanto, em não havendo a utilização de protocolo TCP/IP para qualquer uma de tais atividades, não é possível a aplicação das disposições de tal Lei, sendo, portanto, necessária a criação de norma mais abrangente, que regule o tratamento de dados pessoais no Brasil.

Isto posto, passamos, a seguir, a verificar os principais aspectos referentes ao Anteprojeto de Lei para a Proteção de Dados Pessoais.

---

[11] LIMA, Caio César Carvalho. *Garantia da Privacidade e Dados Pessoais à Luz do Marco Civil da Internet*. In *Marco Civil da Internet*. Coord. LEITE, George Salomão; LEMOS, Ronaldo. São Paulo: Atlas, 2014.

[12] Lei 12.965/2014: Art. 1o Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

[13] GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini. Metodologia Jurídica Político-Constitucional e o Marco Civil da Internet: Contribuição ao Direito Digital. *In* DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (Coords.). *Marco Civil da Internet*. São Paulo: Revista dos Tribunais, 2014, p. 23.

[14] "Em sua essência, a Internet funciona graças ao sistema TCP/IP, acrônimo de *Transmission Control Protocol/Internet Protocol*, o qual permite que diferentes computadores se comuniquem entre si, bastando, para tanto, que transmitam informações utilizando pacotes de dados. O Protocolo TCP/IP funciona da seguinte forma: o Protocolo de Controle de Transmissão (TCP) divide os dados a ser transmitidos em pequenos pedaços chamados de pacotes e, após efetuada a transmissão, reúne-os para formar novamente os dados originalmente transmitidos. O Protocolo de Internet (IP) adiciona a cada pacote de dados o endereço do destinatário, de forma que alcancem o endereço correto. (...) Cada pacote é enviado a seu destino pela melhor rota possível, a qual pode ou não ter sido utilizada pelos demais. Com isso, ainda que os pacotes de informações não trafeguem pelos mesmos caminhos, todos chegarão ao mesmo destino, onde serão reunidos." (LEONARDI, Marcel. *Internet: Elementos Fundamentais*. In *Responsabilidade Civil na Internet e nos demais Meios de Comunicação*. Coord. SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos. 2ª ed. São Paulo: Saraiva, 2012).

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

II.c) Anteprojeto de Lei para Proteção de Dados Pessoais

O Anteprojeto de Lei para a Proteção de Dados Pessoais ("APL"), que se encontra em fase de consulta pública até 05 de julho de 2015, tem por objeto dispor sobre e regular o tratamento de dados pessoais, para proteger a personalidade e a dignidade da pessoa humana.

Ao contrário do Marco Civil, cujas regras referentes à privacidade e ao tratamento de dados são aplicáveis exclusivamente no âmbito da Internet, o APL visa regular o tratamento de dados de forma generalizada, como apontado na página do Ministério da Justiça destinada ao debate público sobre o Anteprojeto:[15]

> O Marco Civil da Internet já não trata da proteção da privacidade e de dados pessoais? Por que mais uma lei sobre o mesmo assunto?
> A Lei 12.965/2014, conhecida como Marco Civil da Internet, possui diversas garantias para o usuário da internet em relação à proteção de sua **privacidade** e dos seus **dados pessoais** – algumas delas, inclusive, bastante semelhantes a alguns direitos previstos pelo anteprojeto de lei de Proteção de Dados Pessoais.
> O Marco Civil da Internet, no entanto, aplica-se **somente à internet**, enquanto que o anteprojeto regula os tratamentos de dados de forma generalizada – **dentro ou fora** da internet.
> No Marco Civil, a privacidade e a proteção de dados são alguns dos direitos assegurados na internet, entre outros. O anteprojeto trata **especificamente da proteção de dados** e, para a sua garantia, estabelece um **conjunto de ferramentas** especialmente talhado para esta finalidade.
> Tanto é assim que o próprio Marco Civil, em seu art. 3º, III, ao estabelecer a proteção de dados pessoais como um dos princípios do uso da internet no Brasil, refere-se a ela "na forma da lei", isto é, implicitamente reconhecendo a possibilidade de que uma **lei geral de proteção de dados** venha a disciplinar de forma mais ampla a matéria.

Desse modo, a redação do APL busca estabelecer os princípios que nortearão o tratamento de dados pessoais no Brasil[16], bem como as regras que regularão referido tratamento, sendo exigido, como regra, consentimento livre, expresso, específico e informado do titular dos dados para seu tratamento[17], complementando o sistema de proteção de dados estabelecido pelo Marco Civil, abrangendo o tratamento de dados dentro ou fora da Internet.

---

[15] Disponível em http://participacao.mj.gov.br/dadospessoais/2015/02/o-marco-civil-da-internet-ja-nao-trata-da-protecao-da-privacidade-e-de-dados-pessoais-por-que-mais-uma-lei-sobre-o-mesmo-assunto/. Acesso em 06.05.2015.

[16] Conforme consta do artigo 6º do APL, constituem princípios que regerão o tratamento de dados pessoais: (i) o princípio da finalidade; (ii) princípio da adequação; (iii) princípio da necessidade; (iv) princípio do livre acesso; (v) princípio da qualidade dos dados; (vi) princípio da transparência; (vii) princípio da segurança; (viii) princípio da prevenção; e (ix) princípio da não discriminação.

[17] APL: Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Dentre os princípios elencados no artigo 6º do APL, cumpre destacar os princípios da segurança e da prevenção, que determinam, respectivamente, que o responsável pelo tratamento de dados pessoais deve adotar medidas técnicas para proteger os dados de acessos não autorizados e que este deve contemplar medidas capazes de prevenir a ocorrência de danos em razão do tratamento de dados pessoais:

> Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais: (...)
> VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Tais princípios, inclusive, norteiam as disposições da Seção IV do APL, o qual estabelece que o operador que realizar o tratamento de dados pessoais deve adotar medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados:

> Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito. (...)
> Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

Ainda, o artigo 45, §1º, constante da mesma Seção, determina que, em caso de incidentes envolvendo segurança do tratamento de dados pessoais, será considerado, no juízo de gravidade do incidente, a adoção de medidas técnicas que dificultem o acesso aos dados: "§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los".

Importante apontar que o APL prevê o dever de indenizar daquele que, pelo tratamento de dados pessoais causar dano a outrem[18], bem como sanções administrativas a infrações às regras previstas no Anteprojeto.[19]

---

[18] APL: Art. 35: Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.

[19] APL: Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente: I – multa simples ou diária; II – publicização da infração; III – dissociação dos dados pessoais; IV – bloqueio dos dados pessoais; V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos; VI – cancelamento dos dados pessoais; VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

O APL, no entanto, assim como as leis brasileiras vigentes que tratam da proteção de dados e da privacidade, não faz menção ao conceito de privacidade visual de dados. Destacamos, entretanto, que tal conceito não é incompatível com a legislação brasileira, sendo, inclusive, por ela amparado, como melhor detalhado no item IV da presente análise.

III. A PRIVACIDADE E A PROTEÇÃO DE DADOS NO DIREITO COMPARADO

Enquanto no Brasil o Anteprojeto de Lei para Proteção de Dados Pessoais ainda se encontra em discussão junto à sociedade, outras nações já possuem normas específicas sobre o tema, regulando o tratamento de dados pessoais em suas respectivas jurisdições, sendo relevante para a presente análise verificar as disposições de algumas delas.

Dentre tais normas, cumpre destacar a Diretiva 95/46/CE do Parlamento Europeu e do Conselho ("Diretiva")[20], de 24 de outubro de 1995, que trata da proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados na União Europeia, bem como da transferência destes dados para outros países.

Tal Diretiva estabelece regras para o tratamento de dados pessoais, exigindo, como regra, a necessidade de consentimento do titular para tratamento dos dados, salvo em situações específicas em que o consentimento pode ser dispensado[21]. Além disso, a Diretiva contém disposições que visam garantir a segurança dos dados tratados:

> Artigo 17º
> Segurança do tratamento
> 1. Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.

---

[20] Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em 06.05.2015.

[21] Diretiva: Artigo 7º: Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:
a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou
b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou
e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou
f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

> Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

Desse modo, a Diretiva, de forma semelhante ao APL, prevê a obrigação de adoção de medidas técnicas com o intuito de garantir a segurança dos dados tratados, sem, no entanto, abordar expressamente o conceito de proteção visual de dados e possíveis efeitos práticos dele decorrentes.

Além da União Europeia, diversos países possuem leis específicas acerca da proteção de dados e da privacidade, que instituem regras sobre a necessidade de adoção de medidas técnicas que garantam a segurança e a confidencialidade de dados pessoais, como, por exemplo, a Lei nº 25.326/2008 da Argentina[22] e a Lei nº 18.331/2008[23] do Uruguai, sem, entretanto, fazer referência expressa à proteção visual da privacidade.

Por sua vez, o México, em sua "Ley Federal de Protección de Datos Personales en Posesión de los Particulares"[24], além de prever a necessidade de adoção de meios técnicos para garantir a segurança dos dados[25], reconhece, em seu artigo 17, II, a possibilidade de coleta de dados por meio visual:

> *Artículo 17.- (...) II. **Cuando los datos personales sean obtenidos directamente del titular por cualquier medio** electrónico, óptico, sonoro, **visual**, o através de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.* (g.n.)

---

[22] Lei Argentina nº 25.326/2008: "ARTICULO 9° — (Seguridad de los datos).
1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado." Disponível em http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf. Acesso em 06.05.2015.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

[23] Lei Uruguaia nº 18.331/2008: "Artículo 10. Principio de seguridad de los datos.- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad." Disponível em: http://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html. Acesso em 06.05.2015.

[24] Disponível em http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Acesso em 06/05/2015.

[25] Lei Mexicana: Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para elmanejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Ainda, a Austrália, por meio de sua autoridade nacional de proteção de dados, *Privacy Commissioner under the Office of the Australian Information Commissioner*, já reconheceu a importância de criar barreiras físicas com o intuito de proteger visualmente informações, como consta de guia para proteção de dados pessoais[26] desenvolvido por esta entidade, destacando, inclusive, a necessidade de proteção de telas e monitores, com o intuito de evitar a visualização indevida de informações. Neste sentido:

> ***Physical security***
> ***Physical security is an important part of ensuring that personal information is not inappropriately accessed****. You need to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, you should consider whether the workspace itself is designed to facilitate good privacy practices. (…)*
> - *Have privacy and security been considered when designing the workspace?*
>
> o ***Are workstations positioned so that computer screens cannot be easily read by unauthorised third parties?***
> o *Do visitors have access to general workspaces or are there designated areas for them?*
> o *Are employees working on sensitive matters able to do so in a private/secure space, particularly in open plan workplaces?*
> o *Do employees have access to secure storage spaces near their workstations to secure documents temporarily?* (g.n.)

No mesmo sentido, em documento intitulado *Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information*[27], emitido pelo Ministério da Economia, Comércio e Indústria do Japão, há previsão acerca da proteção física de equipamentos eletrônicos para prevenção de furtos de dados pessoais:

> *Physical security control measures*
> *The physical security control measures mean the measures of the control for entering and leaving a building (room) and of the prevention of personal data theft, etc.*
> *[Matters to be taken as physical security control measures]*
> *1) Implementing the control for entering and leaving a building (room)*
> *2) Preventing theft, etc.*
> *3)* ***Physically protecting equipments and devices****, etc. (…)*
> *3) Exemplifications of the means which are preferable to be taken for the practice of "Physically protecting equipments and devices, etc."*
> *• Physical protection of the equipments and devices, etc. handling personal data from the security control threat (for instance, theft, destruction, and damage) and from the environmental threat (for instance, water leakage, fire, and power stoppage)* (g.n.)

Desse modo, embora, em pesquisa realizada a legislações estrangeiras acerca da proteção de dados pessoais, não tenhamos localizado menção ao conceito expresso de privacidade visual de dados, é possível verificar que diversas das leis e normativas estabelecem a necessidade de adoção de medidas técnicas para a proteção dos dados tratados, de modo a garantir a privacidade do titular de tais dados. Ainda, alguns países reconhecem em sua legislação a possibilidade de obtenção de dados

---

[26] Disponível em http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Guide_to_securing_personal_information.pdf. Acesso em 07.05.2015.
[27] Disponível em http://www.meti.go.jp/policy/it_policy/privacy/0708english.pdf. Acesso em 07.05.2015.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

por meio visual e a importância de adotar medidas protetivas que impeçam fisicamente a visualização de dados por terceiros não autorizados a acessá-los.

IV. DA PRIVACIDADE VISUAL DE DADOS E DA NECESSIDADE DE SUA REGULAMENTAÇÃO

Verificadas, nos itens anteriores, as previsões constantes da legislação brasileira acerca da proteção da privacidade e de dados pessoais, bem como de algumas normas de ordenamentos jurídicos estrangeiros, passamos, a seguir, a analisar a extensão do conceito de privacidade visual de dados e a necessidade de sua regulamentação.

Inicialmente, cumpre apontar que, entendendo dado como qualquer informação disponível para análise[28], o conceito de privacidade visual de dados pode ser delimitado, de forma ampla, como a proteção conferida a quaisquer informações visualmente perceptíveis, com o intuito de resguardar o sigilo e a confidencialidade de tais conteúdo, ou a intimidade e/ou vida privada do titular destas.

Tal conceito pode, no entanto, ser restringido de acordo com o que se deve entender por "dado pessoal", conforme indicado em cada norma específica, especialmente no caso do APL, que faz referência genérica, nos termos do inciso I do artigo 5º.[29]

Por esta conceituação, é evidente, diante das tecnologias atuais, amplamente difundidas no cotidiano de diversas pessoas naturais e jurídicas, que a privacidade visual de informações tem sido constantemente ignorada, o que pode e tem resultado, por exemplo, no vazamento de informações confidenciais de valor estratégico ou na exposição ao público da vida privada da pessoa, natural como é facilmente verificável por meio de notícias frequentemente divulgadas na mídia.[30]

Além disso, a popularização de tecnologias como *smartphones*, *tablets* e *notebooks* levou ao aumento de prática conhecida como BYOD (*Bring Your Own Device*), pela qual os colaboradores de empresas utilizam seus próprios dispositivos eletrônicos para o desenvolvimento de funções profissionais, aumentando a circulação de informações confidenciais e estratégicas e facilitando a visualização destas por terceiros não autorizados.

---

[28] "**dados** (...) 1 Conjunto de material (= informações) disponível para análise. 2 Cib Representação de fatos, conceitos e instruções, por meio de sinais de uma maneira formalizada, possível de ser transmitida ou processada pelo homem ou por máquinas." Dicionário Michaelis. Editora Melhoramentos. Disponível em http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=dados. Acesso em 07/05/2015.

[29] APL: Art. 5º Para os fins desta Lei, considera-se: I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

[30] Matéria: "Exclusivo: Vaccarezza troca mensagens comprometedoras com Cabral". Disponível em http://www.sbt.com.br/jornalismo/noticias/?c=19887&t=Exclusivo:+Vaccarezza+troca+mensagens+comprometedoras+com+Cabral#.VUuRTPlVhBc. Acesso em 07.05.2015.
Matéria: "Fiorella Mattheis é flagrada conversando com Pato no telefone". Disponível em http://ego.globo.com/famosos/noticia/2014/10/fiorella-mattheis-e-flagrada-conversando-com-pato-no-telefone.html. Acesso em 07.05.2015.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Resta evidente, portanto, que o acesso indevido a informações visualmente perceptíveis, decorrente, principalmente, da difusão de tecnologias, é situação fática presente, que não pode ser ignorada pelo legislador, sendo especialmente relevante o presente momento, em que a sociedade civil discute os termos do APL.

Desse modo, entendendo-se o Direito como fenômeno social, que não constitui mera abstração estática, mas o resultado da interação entre fato, valor e norma, conforme ensinado por Miguel Reale em sua Teoria Tridimensional do Direito[31], faz-se necessário regulamentar a privacidade visual de dados. Isto porque, de acordo com tal Teoria, a norma jurídica deverá decorrer do valor conferido pela sociedade a situação fática, com o intuito de regulamentá-la. Neste sentido:

> A norma, por exemplo, representa para o jurista uma integração de fatos segundo valores, ou, por outras palavras, é expressão de valores que vão se concretizando na condicionalidade dos fatos histórico-sociais. (...)
>
> A análise fenomenológica da experiência jurídica, confirmada pelos dados históricos sucintamente lembrados, demonstra que a estrutura do Direito é tridimensional, visto como elemento *normativo*, que disciplina os comportamentos individuais e coletivos, pressupõe sempre uma dada situação de fato, referida a valores determinados.[32]

Assim, considerando-se a necessidade fática de proteção à privacidade visual de dados, conforme acima apresentado, bem como o valor atribuído pelo ordenamento jurídico brasileiro à privacidade, garantida pela Constituição Federal como direito fundamental, ratificado pelo Marco Civil da Internet, torna-se evidente a grande relevância da regulamentação de referida proteção no âmbito da legislação brasileira.

No mesmo sentido, cumpre apontar que Silvio de Salvo Venosa já destacou a necessidade de proteção à privacidade, diante das inovações tecnológicas, sendo sua intimidade um dos bens mais preciosos ao indivíduo:

> Deve haver sempre posição firme do jurista no sentido de defender a preservação da intimidade, tantos são os ataques que sofre modernamente. Não se pode permitir que a tecnologia, os meios de comunicação e a própria atividade do Estado invadam um dos bens mais valiosos do ser humano, que é seu direito à intimidade (...) Os fatos comezinhos da vida de cada um não devem interessar a terceiros.[33]

Como apontado anteriormente, o APL, bem como as demais leis estrangeiras de proteção de dados pessoais, incluindo a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, que serviu como fonte de inspiração ao Anteprojeto brasileiro, além do Marco Civil, contêm previsão acerca da adoção de medidas técnicas adequadas para a proteção de dados.

---

[31] "Segundo esta teoria, o ordenamento jurídico é, sem dúvida, normativo, mas não é apenas um conjunto gradativo de normas e muito menos um sistema de proposições lógicas. As normas representam o momento culminante de um processo que é, essencialmente, inseparável dos fatos que estão em sua origem (neste sentido é certo dizer que *ex facto oritur jus*) e dos valores ou fins que constituem sua razão de ser." (REALE, Miguel. Lições Preliminares de Direito. São Paulo: Saraiva, 2003. P. 194-195.

[32] REALE, Miguel. *Filosofia do Direito*. 19ª Ed. São Paulo: Saraiva, 1999.

[33] VENOSA, Sílvio de Salvo. *Direito Civil*. Vol. I. 9ª ed. São Paulo: Atlas, 2009, p.179.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Neste sentido, entendemos que a regulamentação da privacidade visual de dados, inclusive pela previsão de exigências técnicas a serem adotadas para garantir a preservação de referido direito, vão ao encontro do já estabelecido pelo ordenamento jurídico brasileiro atual e ao quanto disposto no Anteprojeto de Lei para Proteção de Dados Pessoais.

Inclusive, o Direito à privacidade garantido pela Constituição e pelo Código Civil, bem como outras previsões legais, como a proteção aos segredos de negócio, constante da Lei nº 9.279/1996, a Lei de Propriedade Industrial[34], bem como a tipificação do crime de divulgação de segredo, constante do Código Penal[35], ratificam referido entendimento, sendo evidente, portanto, em análise sistemática do ordenamento jurídico brasileiro, que este tem por intuito proteger a privacidade das pessoas e o sigilo das informações tidas por confidenciais, sendo adequadas ao ordenamento jurídico brasileiro previsões que reforcem este posicionamento.

Desse modo, verificada a adequação da proteção à privacidade visual de dados ao ordenamento jurídico brasileiro, passamos, a seguir, a sugerir alterações na legislação brasileira, de modo que ela passe a abarcar expressamente referido conceito.

V. SUGESTÕES DE ALTERAÇÕES ÀS NORMAS BRASILEIRAS

Verificada assim, a adequação jurídica da proteção à privacidade visual de dados ao ordenamento jurídico brasileiro, passamos, a seguir, a sugerir possíveis alterações, tanto no Anteprojeto de Lei de Proteção de Dados quanto no Marco Civil da Internet, com o intuito de incluir expressamente referido conceito na legislação brasileira.

Destacamos que, para além dos diplomas legais aqui especificamente abordados, é possível, entre outros aspectos, defender a alteração da legislação consumerista atualmente vigente, com o intuito, por exemplo, de determinar que equipamentos bancários ou aparelhos eletrônicos comercializados no Brasil utilizem mecanismos técnicos de proteção à privacidade visual de dados, com o intuito de garantir maior segurança aos dados dos consumidores, na utilização dos produtos ou serviços comercializados.

Além disso, ainda no âmbito da defesa do consumidor, é possível defender a necessidade de utilização de filtros físicos de segurança em todos os equipamentos utilizados internamente por fornecedores, nos quais circulem informações de consumidores, com o intuito de evitar visualizações indevidas por funcionários não autorizados a acessar estas informações.

Isto posto, passamos a verificar especificamente as possíveis alterações ao APL e ao Marco Civil:

---

[34] Lei nº 9.279/1996: Art. 195. Comete crime de concorrência desleal quem: (...) XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

[35] Código Penal: Divulgação de segredo
Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis.

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

a) Anteprojeto de Lei de Proteção de Dados Pessoais

Com relação ao Anteprojeto, sugerimos as seguintes alterações à redação de referido documento, com o intuito de regulamentar a proteção à privacidade visual de dados, especificamente no âmbito da proteção aos dados pessoais:

 Artigo 5º - Sugerimos a inclusão de inciso com o conceito de privacidade, da forma que este deve ser entendido no âmbito do APL. Neste sentido:

XIX – privacidade – direito conferido ao titular de que seus dados pessoais não serão tratados ou acessados, por qualquer meio, virtual ou físico, mesmo que apenas para mera visualização, fora das situações consentidas ou permitidas pela legislação brasileira.

 Artigo 6º: Recomendados a inclusão, no inciso VII do artigo 6º, de que devem ser adotadas as medidas físicas e eletrônicas necessárias para garantir a segurança dos dados:

Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais: (...)
VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas, **físicas e eletrônicas**, e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

 Artigo 42 – Sugerimos a alteração de referido artigo para a inclusão de §2º, que determine expressamente a necessidade de proteção da privacidade visual de dados:

§2º: Os agentes de tratamento ou qualquer outra pessoa ou entidade responsável pelo tratamento ou armazenamento de dados pessoais deverão adotar todos os meios técnicos eletrônica e fisicamente necessários para garantir a proteção de dados visualmente perceptíveis, de modo a evitar a visualização de dados pessoais perceptíveis, por terceiros não autorizados, com o intuito de respeitar o direito à privacidade do titular dos dados.

 Artigo 45 – Sugerimos a inclusão, no atual §1º do artigo 45, de que serão avaliadas, em caso de incidentes de segurança, todas as medidas físicas e eletrônicas adotadas que não só tornem os dados ininteligíveis como também impeçam sua visualização:

§1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas **físicas e eletrônicas** adequadas que tornem os dados pessoais afetados ininteligíveis **ou impossíveis de serem visualizados** para terceiros não autorizados a acessá-los.

b) Marco Civil da Internet

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

No que diz respeito ao Marco Civil, por sua vez, indicamos as seguintes alterações na redação da Lei atualmente em vigor:

 Artigo 7º - Com relação ao artigo 7º, que estabelece os direitos assegurados aos usuários de Internet, sugerimos a inclusão de inciso ao artigo em questão, tendo por intuito exigir a utilização de meios técnicos, em instalações de provedores de serviços de Internet nas quais haja tratamento ou armazenamento de dados, que impeçam o acesso visual indevido a tais dados por terceiros não autorizados, como, por exemplo, funcionários cujas atividades desenvolvidas não exijam acesso à referidas informações. Dessa forma, indicamos a seguinte redação:

Artigo 7º: O acesso à internet é essencial ao exercício da cidadania, e a usuário são assegurados os seguintes direitos: (...)

XIV – adoção, por provedores de serviços de Internet, internamente, em suas instalações nas quais haja tratamento ou armazenamento de dados, ou nas de terceiros contratados para esta finalidade, de meios físicos e eletrônicos de proteção de dados visualmente perceptíveis, com o intuito de evitar o acesso indevido a dados de usuários por terceiros não autorizados.

 Artigo 13 – Em complementação ao acima disposto, importante esclarecer que o conceito de "ambiente controlado e de segurança" inclui também a vedação de acesso visual não autorizado, conforme abaixo:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, **visualmente não acessível a terceiros não autorizados**, pelo prazo de 1 (um) ano, nos termos do regulamento.

 Artigo 15 – Em complementação ao acima disposto, as previsões também devem se aplicar aos provedores de aplicação, com o objetivo de manter a isonomia no tratamento entre os diversos entes que atuam no cenário da internet:

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, **visualmente não acessível a terceiros não autorizados**, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Acreditamos que com essas previsões, os usuários da internet terão garantidos, de forma mais específica, a proteção aos seus dados, por parte dos provedores que atuam na internet, especialmente no que concerne à possibilidade de vazamento visual, que apesar de extremamente relevante, tem sido alvo de pouca atenção, por parte dos legisladores nacionais.

IV – DA CONCLUSÃO E DO ENCERRAMENTO

3M do Brasil Ltda.
Relações Governamentais
SHIS QI 05, Chácara 27
71600-540 – Brasília/DF
Tel./Fax: (61) 3248-4836

Diante de todo o exposto, entendemos, **s.m.j.**, que:

a) O ordenamento jurídico brasileiro, mesmo antes da entrada em vigor da Lei nº 12.965/2014, conhecida como Marco Civil da Internet, já possuía dispositivos destinados à proteção da privacidade, tendo o Marco Civil sistematizado respectiva proteção no âmbito na Internet, sendo necessária a elaboração de lei para proteção de dados pessoais também fora da rede, como pretendido pelo Anteprojeto de Lei para Proteção de Dados Pessoais;

b) Embora o APL, da mesma forma que a legislação anterior, não faça referência expressa ao conceito de privacidade visual de dados, este exige a adoção de medidas técnicas de segurança aos dados pessoais tratados, por parte dos responsáveis pelo tratamento, o que está de acordo com a proteção conferida por respectivo conceito;

c) De forma semelhante, diversos países, em sua legislação de proteção de dados pessoais, exigem a adoção de medidas técnicas de segurança, sendo que, em alguns deles, a possibilidade de obtenção visual de informações é reconhecida, bem como a necessidade de adoção de barreiras físicas com o intuito de garantir a proteção visual de dados;

d) Desse modo, o conceito de privacidade visual de dados, como a proteção conferida a informações visualmente perceptíveis, com o intuito de resguardar o sigilo destas e a intimidade e vida privada de seu titular, encontra-se amparado pelo ordenamento jurídico brasileiro, sendo importante sua regulamentação, diante da necessidade fática e do valor concedido à privacidade pela legislação brasileira; e

e) Desse modo, sugerimos as alterações de artigos constantes da APL, bem como do Marco Civil da Internet, com o intuito de regular expressamente o conceito de privacidade visual de dados no ordenamento jurídico brasileiro, como descrito nesta análise.

Colocamo-nos à disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

Atenciosamente.