ARTICLE 19

Proteção de dodos pessoais no Brasil

ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL

(Novembro de 2016)

FICHA TÉCNICA

Título: Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional

Realização: ARTIGO 19

Supervisão: Paula Martins
Coordenação executiva e editorial: Laura Tresca
Revisão: Paula Martins e Renato Leite
Texto e pesquisa: Dave Banisar, Gabrielle Guillemin e Marcelo Blanco
Design gráfico: MOOA estúdio

Apoio: Fundação Ford

Licença: Creative Commons - 3.0.

Caso tenha comentários ou sugestões sobre essa publicação, escreva para
comunicacao@artigo19.org

Sumário executivo

O direito à proteção dos dados pessoais é derivado do direito à privacidade. Uma legislação sobre esse tema deve regular o modo como informações públicas ou privadas sobre os indivíduos são coletadas, processadas, armazenadas e retidas eletronicamente ou analogicamente por órgãos públicos ou privados. Os dados pessoais devem ser tratados para finalidades determinadas ou específicas e com base no consentimento do titular dos dados ou com alguma base legítima e legal que transcenda tal necessidade. Ainda, todos devem ter o direito de acesso aos próprios dados que estejam nas mãos de terceiros ou de se opor ao tratamento, além de ter o direito de retificá-los ou excluí-los.

Um desafio comum e assunto frequente nos debates sobre proteção de dados pessoais é a relação do tema com o direito à liberdade de expressão — que também é um direito humano fundamental. Ambos os direitos visam proteger liberdades fundamentais que podem ser mitigadas se houver um tratamento indevido dos dados pessoais, tais como o direito à moradia, à saúde e à mobilidade urbana. Os tratados internacionais mais importantes, assim como variadas leis nacionais de proteção de dados, tentam equilibrar esses dois direitos, incluindo exceções e provisões sobre considerações relativas ao interesse público.

Atualmente, são três projetos de lei em tramitação no Congresso Nacional para proteção de dados pessoais — são eles, o PL 5276/2016, o PLS 330/2013 e o PL 4060/2012. Cada um oferece diferentes garantias ou riscos ao direito à privacidade e a outras liberdades fundamentais. Em todos os projetos, em diferentes graus, ainda existem pontos que precisam harmonizar a proteção de dados pessoais com os direitos fundamentais da liberdade de expressão e o direito à informação. Esta publicação tem o intuito de realizar uma análise e fazer recomendações nesse sentido.

RECOMENDAÇÕES GERAIS AOS PROJETOS DE LEI

1. O projeto de lei deve estipular a criação de um órgão regulatório independente, inclusive do ponto de vista orçamentário. As funções do órgão em relação à proteção de dados pessoais devem ser a de fiscalizar e regular a implementação da lei e das práticas adotadas por responsáveis pelo tratamento de dados, para que os titulares não fiquem com o ônus da iniciativa, assim como diminuir o tempo necessário para a plena implementação da lei a partir das ações do órgão. Além disso, a ARTIGO 19 defende que esse órgão não se limite à proteção de dados, mas se destine também à regulação de temas mais amplos, relacionados à sociedade da informação como um todo.

2. A menção expressa à Lei nº 12527/2011, conhecida como Lei de Acesso à Informação (LAI)é necessária, pois o direito de acesso à informação eventualmente pode conflitar com o direito à proteção de dados pessoais em algumas situações específicas. Os projetos de lei não podem criar obstáculos aos avanços obtidos com a LAI e devem conter dispositivos que assegurem o acesso a dados pessoais quando o interesse público for maior que a necessidade de sigilo, como a divulgação de salários de servidores públicos, por exemplo.

3. Interpretações que possibilitem que o "direito ao esquecimento" possa ser reivindicado para o cancelamento dos dados pessoais devem ser evitadas. O direito ao esquecimento não deve ser alvo do texto de uma lei geral de proteção de dados pessoais, pois se trata de um tema diverso ao objeto da lei e que ainda necessita de um debate maior na sociedade.Dessa forma, os projetos de lei não devem permitir a solicitação de exclusão de informações que sejam de comprovado interesse público. Para isso, é necessário que eles tragam em seu texto uma ressalva explícita sobre a questão do interesse público quando se tratar do cancelamento dos dados pessoais.

4. Uma lei geral de proteção de dados pessoais deve se aplicar ao setor público como um todo, inclusive às forças de segurança. É importante que forças de segurança não sejam excluídas do escopo da lei, pois é notório que nos últimos anos têm crescido os programas de vigilância implantados por polícias estaduais, forças armadas e outros órgãos desta área, o que requer protocolos e garantias de proteção aos cidadãos que involuntariamente têm seus dados tratados.

5. Os projetos de lei devem especificar e delimitar o que se entende por pesquisa estatística, tendo em vista que essa atividade está prevista nos três projetos e não necessitaria do consentimento dos titulares dos dados para sua realização. Uma pesquisa estatística pode abarcar um número grande de tipos de pesquisa, feitas pelos mais diversos atores com variadas finalidades. Por essa razão, os projetos de lei, quando especificarem a exceção às pesquisas estatísticas, também devem oferecer uma delimitação dos tipos de atores e finalidades para que uma pesquisa seja considerada estatística.

Índice

I.
Introdução

Números de documentos pessoais, informações sobre saúde, filiações políticas, dados financeiros. Essas são só algumas das informações pessoais manuseadas por terceiros, por meio do armazenamento em bancos de dados em empresas e órgãos públicos. Dessa forma, como garantir que nossa privacidade e outros direitos estejam protegidos?

No Congresso Nacional, há três projetos de leis tramitando relacionados à proteção de dados pessoais. Em geral, eles visam regular as dinâmicas de consentimento entre os titulares dos dados e os responsáveis pelos seus tratamentos, estabelecendo normas claras de quando se pode compartilhá-los com terceiros, excluí-los ou transferi-los de país, citando apenas algumas de suas atribuições. Trata-se de práticas já usuais e que somente agora são alvo de regulamentação de forma abrangente, transversal e multissetorial.

O projeto mais antigo e menos protetivo aos direitos individuais é o 4060/2012, de autoria do deputado federal Milton Monti, do PR-SP. O texto do projeto é bastante problemático, pois permite o tratamento de dados pessoais sem as devidas autorizações de seus titulares ou garantias na transferência e na segurança desses dados.

O segundo projeto é o PLS 330/2013, cujo autor é o senador Antônio Carlos Valadares, do PSB-SE — em 2015, o senador Aloysio Nunes, do PSDB-SP, como relator do projeto na CCT - Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, apresentou um projeto de lei substitutivo, versão que atualmente está sob análise no Congresso. O projeto estabelece garantias mais contundentes à proteção de dados dos cidadãos, aborda de forma mais detalhada cada aspecto do tratamento de dados pessoais, e considera o consentimento "livre, expresso, inequívoco e informado" como necessário para o tratamento de dados pessoais.

O terceiro projeto de lei que tramita no Congresso é o 5276/2016, elaborado no interior do Ministério da Justiça, no âmbito da Secretaria Nacional de Defesa do Consumidor (SENACON), a partir de diversas consultas públicas online que envolveram empresas, governos e a sociedade civil organizada. Trata-se de um projeto mais robusto que aborda o consentimento, a transferência internacional de dados e um órgão competente para lidar com o tema[1].

Para a ARTIGO 19, os direitos à privacidade e à liberdade de expressão e de informação são direitos humanos complementares, concebidos para empoderar o cidadão e auxiliá-lo na proteção aos seus demais direitos. Servem ainda para aumentar a transparência de órgãos públicos e privados que detêm e exercem poder na sociedade. Por isso, é fundamental que os projetos de lei sejam bem elaborados e protejam o direito individual de privacidade enquanto assegurem transparência governamental e liberdade de expressão.

Nesta análise, a ARTIGO 19 expõe suas preocupações relativas aos projetos de lei e suas compatibilidades com as obrigações internacionais sob a égide dos direitos humanos para a proteção da liberdade de expressão e do acesso à informação. O estudo também analisa outros aspectos dos projetos e propõe mudanças para torná-los mais fortes e coerentes com os padrões internacionais de direitos humanos.

1 O projeto de lei 4060/2012 tramitou lentamente por quatro anos até que houve uma movimentação maior na Câmara sobre o tema, avivado pela elaboração do PL 5276/2016, que foi enviado ao Congresso Nacional pelo Poder Executivo federal em regime de urgência e ganhou precedência sobre seu congênere mais antigo. Com a instabilidade política e o diagnóstico dos congressistas de que a matéria mereceria maior tempo de discussão, o regime de urgência foi retirado. Assim, atualmente, o PL 5276/2016 não tem mais precedência e encontra-se apensado ao PL 4060/2012. O projeto gerou interesse de diversas comissões na Câmara, que reivindicaram a oportunidade de discutir o tema. Quando isso ocorre, cria-se uma Comissão Especial, que substitui a discussão individualizada em cada comissão por um debate integrado sobre as propostas em um foro único. Em relação ao PLS 330/2013, em novembro de 2016, ele ainda se encontra no Senado. Seu texto já foi aprovado na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, assim como na Comissão de Meio Ambiente, Defesa do Consumidor e Fiscalização e Controle. Agora, encontra-se na Comissão de Assuntos Econômicos. Após sua provável aprovação, o projeto irá seguir para a Comissão de Constituição e Justiça e então será encaminhado à Câmara dos Deputados, onde será analisado na já referida Comissão Especial junto aos outros dois projetos já citados.

II. Privacidade, proteção de dados e liberdade de expressão e informação

O direito à liberdade de expressão é um direito humano reconhecido pela jurisdição internacional, cuja plena realização é fundamental para a obtenção de liberdades individuais e o desenvolvimento da democracia. A garantia desse direito é condição necessária para a realização dos princípios da transparência e da prestação de contas por parte de governos, que, por sua vez, são essenciais para a promoção e a proteção de todos os direitos humanos.

Simultaneamente, o direito à privacidade também é reconhecido nos tratados de direitos humanos internacionais, incluindo a Declaração Universal dos Direitos Humanos[2], a Declaração Americana dos Direitos e Deveres do Homem[3] e a Convenção Americana de Direitos Humanos[4]. Sob esses tratados, a privacidade é um termo amplo relacionado à proteção da autonomia individual e o relacionamento entre indivíduo e sociedade, incluindo governos, empresas e outros indivíduos.

O direito à privacidade é comumente reconhecido como um direito chave que sustenta a dignidade humana e outros valores, como a liberdade de associação e a liberdade de opinião. Ele também assegura o espaço individual privado, que é o primeiro passo para a realização de outros direitos, como o da liberdade de expressão.

A proteção de dados pessoais é reconhecida pelo Conselho de Direitos Humanos da ONU como parte fundamental da privacidade pelo Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos., Em seu Comentário Geral 16, o órgão declarou que:

> *A coleta e a manutenção de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por autoridades públicas ou indivíduos ou órgãos privados, devem ser regulados por lei. Medidas efetivas devem ser tomadas pelos Estados para assegurar que informações relativas à vida privada de uma pessoa não fiquem em mãos de pessoas que não estão autorizadas por lei para recebê-las, processá-las e usá-las, assim como nunca serem usadas para propósitos incompatíveis com o Pacto.*[5]

Em 1990, a Assembleia Geral da ONU aprovou uma resolução de princípios para a proteção de informações pessoais mantidas em bancos de dados computadorizados[6]. As diretrizes destacam seis princípios básicos de proteção de dados pessoais baseados em práticas de "informação justa", ou seja aquela que respeita os princípios de tratamento como finalidade, adequação e necessidade, por exemplo. Os direitos de proteção de dados pessoais também foram adotados em procedimentos legais e administrativos ao redor do globo.[7]

Essas normas sobre privacidade e proteção de dados pessoais também foram adotadas no continente americano. O artigo 11 da Convenção Americana de Direitos Humanos estipula as proteções básicas sobre privacidade pessoal. A Corte Interamericana de Direitos Humanos reconheceu a importância da prote-

2 UDHR, Art 12.
3 Artigos 5, 9 e 10.
4 Artigo 11.
5 Comentaŕio Geral 16, ibid, §10.
6 Diretrizes para a regulação de arquivos de dados pessoais computadorizados, G.A. res. 45/95, 14 de Dezembro de 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.
7 Veja OCDE "Princípios sobre proteção à Privacidade e fluxos transfronteiriços de Dados Pessoais (1980); Canadian Standards Association (CSA) International, "Código Modelo para Proteção de Informações Pessoais, 1996; APEC Privacy Framework, 2005; A declaração sobre privacidade de Madri,Padrões Globais de Privacidade para um Mundo Global, 3 November 2009.

ção à privacidade na era digital no caso "Escher vs Brasil", situação que envolveu interceptações telefônicas, mas que pode ser igualmente aplicada à proteção de dados:

> *Hoje, a fluidez das informações coloca o direito à privacidade do indivíduo em maior risco, devido a novas ferramentas tecnológicas, como a internet, e seu uso cada vez maior. Esse progresso, especialmente no caso de interceptações e gravações telefônicas, não significa que o indivíduo deva ser colocado em uma situação de vulnerabilidade quando trata com o Estado ou outros indivíduos. Além disso, o Estado deve aumentar seu compromisso em adaptar as formas tradicionais de proteção ao direito à privacidade para novos modelos.*[8]

A Organização dos Estados Americanos (OEA) está cada vez mais ativa na definição de normas mais detalhadas nessa área[9], tanto que o Comitê Jurídico Interamericano, ligado ao organismo, lançou um documento em 2012 intitulado "Proposta de Declaração de Princípios para Privacidade e Proteção a Dados Pessoais na América"[10], que reúne 12 princípios fundamentais que devem balizar a elaboração de leis e práticas nacionais.

Globalmente, mais de cem países adotaram leis abrangentes de proteção de dados pessoais.[11] Alguns deles estão nas Américas, como Argentina, Bahamas, Canadá, Chile, Colômbia, Costa Rica, Curaçao, República Dominicana, México, Nicarágua, Paraguai, Peru, Santa Lúcia, Ilha de São Martinho, São Vicente e Granadinas, Trinidade e Tobago e Uruguai. No continente, outros países da região também têm projetos de leis em fase tramitação.

8 Corte Interamericana de Direitos Humanos, Caso Escher et al. contra. Brasil, Julgamento de 6 de Julho de 2009.

9 Veja, por exemplo, Assembleia geral da OEA., AG/RES. 2661 (XLI-O/11)Acesso à Informação Pública e Proteção de Dados Pessoais, 7 de Junho de 2011.

10 Comitê Jurídico Interamericano, Proposta de Declaração de Princípios para Proteção à Privacidade e Dados Pessoais nas Américas, CJI/RES. 186 (LXXX-O/12), 9 de Março de 2012;Comitê Jurídico Interamericano, Princípios da OEA sobre Proteção à Privacidade e de Dados Pessoais com anotações, CJI/doc. 474/15 rev.2, 26 de Março de 2015.

11 Veja Greenlaf, Graham, Global Data Privacy Laws 2015: 109 countries, with European Laws Now a Minority (January 30, 2015). (2015) 133 Privacy Laws & Business International Report, Fevereiro dey 2015; UNSW Law Research Paper No. 2015-21. Disponível em SSRN: http://ssrn.com/abstract=2603529; Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (4 ed.,Janeiro 2015) (30 de Janeiro de 2015). (2015) 133 Privacy Laws & Business International Report, 18-28; UNSW Law Research Paper No. 2015-28. Available at SSRN: http://ssrn.com/abstract=2603502; Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (8 de dezembro, 2014). Disponível em SSRN: http://ssrn.com/abstract=1951416 ou http://dx.doi.org/10.2139/ssrn.1951416.

PRIVACIDADE E LIBERDADE DE EXPRESSÃO E DE INFORMAÇÃO

A privacidade e a liberdade de expressão são direitos complementares que aparecem entrelaçados na legislação sobre direitos humanos. Elas costumam aparecer juntas nos instrumentos internacionais, constituições nacionais e leis. Unidas, asseguram a prestação de contas por parte do Estado e de outros poderosos atores.

As liberdades de expressão e de informação permitem aos indivíduos investigar e desafiar abusos contra os direitos humanos, incluindo violações de privacidade. Ambas as liberdades são afetadas quando limites são colocados sobre o direito à privacidade, causando sérios prejuízos, por exemplo, à imprensa. Nessa situação, jornalistas não são capazes de desenvolver efetivamente suas investigações e receber informações confidenciais e de outras fontes.[12]

Assim, leis que disponham sobre a questão da privacidade podem estimular a liberdade de expressão ao estabelecer limites sobre a coleta ilegal de informações pessoais com propósitos políticos, como, por exemplo, a coleta de informações realizadas por órgãos públicos que depois servirão de base para a criação de dossiês usados para pressionar jornalistas, defensores dos direitos humanos, entre outros.

A Comissão Europeia, em uma avaliação recente sobre seu regime de proteção de dados, notou que:

> *Privacidade e proteção de dados pessoais [...] "têm um papel chave para o exercício de direitos fundamentais em um sentido mais amplo. Muitas das liberdades fundamentais só podem ser plenamente exercidas se o indivíduo está assegurado de que não é objeto de vigilância permanente e observação por autoridades e outras organizações poderosas. Liberdade de pensamento, liberdade de expressão, liberdade de assembleia e associação, mas também liberdade de conduzir um negócio não serão exercidas plenamente por todos os cidadãos em um ambiente em que o indivíduo sinta que cada um dos seus movimentos, atos, expressões e transações estão sujeitos ao escrutínio de outros que tentam controlá-lo. O exercício dessas liberdades é crucial para a manutenção dos direitos fundamentais."*[13]

12 Veja, por exemplo, IFEX Alert, Thirty IFEX members call on governments to respect fundamental human rights of free expression and privacy of communications, 5 de Junho de 2009. http://www.ifex.org/international/2009/06/05/ja_gm/.

13 Comissão Europeia,Acompanhamento de Avaliação de Impacto. O documento "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" e 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, SEC (2012)" , 25 de janeiro de 2012.

Sendo dois direitos humanos complementares (privacidade e liberdade de expressão) é essencial que os governos e a justiça os equilibrem de maneira justa sem dar precedência a um sobre o outro. A jurisdição internacional de direitos humanos não reconhece uma "hierarquia" de direitos. Como descrito pela Corte Interamericana de Direitos Humanos em "Fontevecchia vs Argentina":[14]

> *A justiça deve encontrar um balanço entre a vida privada e a liberdade de expressão que, não sendo absolutos, são dois direitos fundamentais garantidos pela Convenção Americana e são de grande importância em uma sociedade democrática. A Corte recorda que todo direito fundamental deve ser exercido em relação a outros direitos fundamentais. Esse é um processo de harmonização no qual o Estado tem papel chave na tentativa de determinar as responsabilidades e a imposição de sanções que possam ser necessárias para atingir tal propósito.*

De forma similar, o direito à informação, que é reconhecido pela Corte Interamericana como um elemento essencial para a liberdade de expressão[15], também precisa ser harmonizado com o de proteção de dados pessoais. A Assembleia Geral da OEA em uma resolução publicada em 2013 declarou:

> *"Reiterando que o acesso à informação pública, por um lado, e a proteção de dados pessoais, por outro, são valores fundamentais que devem operar em harmonia a todo momento".*[16]

É a partir dessa noção de complementaridade que projetos de lei sobre proteção de dados pessoais devem ser elaborados. Na próxima seção, analisaremos os três projetos que atualmente tramitam no Congresso brasileiro.

14 Corte Interamericana de Direitos Humanos,Caso de Fontevecchia and d'Amico v. Argentina, Julgamento de 29 de Novembroer 29, 2011.

15 Corte Interamericana de Direitos Humanos, Claude Reyes et al. v. Chile, Julgamento de 19 de Setembro, 2006; IACtHR, Caso de Gomes Lund et al. ("Guerrilha do Araguaia") v. Brazil. Julgamento de 24 de Novembro, 2010.

16 OEA, AG/RES. 2811 (XLIII-O/13), Acesso à Informação Pública e Proteção de Dados Pessoais. (adotada na quarta sessão do plenário, realizado em 6 de Junho,2013); AG/RES. 2842 (XLIV-O/14), Acesso à Informação Pública e Proteção de Dados Pessoais. (Adotada na segunda sessão plenária,realizada em 4 de Junho, 2014).

III. Comparativo dos projetos de lei

Em um contexto de pressão constante por informações, incluindo as pessoais, é imperativo que os Estados adotem boas leis de proteção de dados dos cidadãos, e que sejam equilibradas com o direito humano à liberdade de expressão. O tratamento de dados pessoais é feito para os mais diversos fins, por atores privados e públicos, online ou offline, e com interesses econômicos, políticos, de segurança, jornalísticos, artísticos, entre outros.

No Brasil, constantemente são noticiados casos de vazamento de dados pessoais, tratamentos sem consentimento, coleta de dados excessiva, entre outras ameaças à privacidade. A proteção de dados pessoais, portanto, é um problema já presente na sociedade brasileira que necessita de uma regulação adequada urgentemente.

Nesta seção, foram selecionados aspectos relacionados à liberdade de expressão e à garantia de outros direitos fundamentais que deveriam estar presentes nos projetos de lei a fim de estabelecer o correto equilíbrio entre os vários direitos concorrentes. Os campos foram marcados com satisfatório, parcialmente satisfatório, ausente e insatisfatório, conforme avaliação dos projetos de lei.

A seguir, detalhamos a metodologia para a atribuição dessas classificações:

SATISFATÓRIO
O projeto de lei aborda o tópico de maneira adequada.

PARCIALMENTE SATISFATÓRIO
O projeto de lei aborda o tópico de maneira incompleta.

AUSENTE
O projeto de lei não aborda o tópico.

INSATISFATÓRIO
O projeto de lei aborda o tópico de maneira inadequada.

Os aspectos[17] avaliados durante a análise feita a cada um dos projetos de lei estão enumerados abaixo, assim como os critérios levados em consideração para a classificação de cada um deles:

1) MENÇÃO EXPRESSA À PROTEÇÃO DA LIBERDADE DE EXPRESSÃO

Uma lei de proteção de dados pessoais deve garantir o equilíbrio entre o direito à privacidade e o direito à liberdade de expressão, de forma a evitar eventuais conflitos. Por isso, é importante que a expressão "liberdade de expressão" seja mencionada de maneira expressa no texto da lei

2) EXCEÇÃO À ATIVIDADE JORNALÍSTICA E OUTRAS FORMAS DE EXPRESSÃO

Uma lei de proteção de dados pessoais deve prever uma lista de exceções para alguns casos em que os dados pessoais não devem estar sujeitos à proteção por lei, Essas exceções devem abranger atividades com fins jornalísticos, artísticos, acadêmicos e literários, de modo a assegurar o livre fluxo de informações de interesse público ou com fins legítimos.

3) MENÇÃO EXPRESSA À LEI DE ACESSO À INFORMAÇÃO

Dados relacionados a atividades públicas de autoridades ou de outras pessoas que atuem utilizando dinheiro público ou desempenhem ações de interesse público não devem estar protegidos na lei tais quais os demais dados pessoais. A exceção deve se basear na Lei de Acesso à Informação, que deverá ser mencionada de forma expressa.

4) CUIDADO COM INTERPRETAÇÕES QUE POSSIBILITEM REIVINDICAÇÕES DO DIREITO AO ESQUECIMENTO

O "direito ao esquecimento" é um tema complexo e controverso, sendo que sua inclusão na lei sobre proteção de dados pessoais seria precipitada e prejudicial nesse momento, já que o tema merece um debate mais aprofundado e específico. O direito ao esquecimento contrapõe-se ao direito à liberdade de expressão em diversas ocasiões e, por isso, deve sempre ser avaliado em relação a ele quando e se for aplicado[18]. Por essa razão, o texto da lei não deve dar margens à institucionalização do direito ao esquecimento em seu conteúdo.

17 Muitos outros aspectos poderiam ser analisados, mas a ARTIGO 19 optou por pontuar aqueles que consideramos ter maior impacto para o direito à liberdade de expressão.

18 A ARTIGO 19 é contrária à positivação do direito ao esquecimento. Se legislações sobre o tema venham a ser discutidas, elaboramos os seguintes critérios para avaliação dos casos concretos:

- Se a informação em questão é de natureza privada;
- Se o requerente tinha uma expectativa razoável de privacidade, incluindo a consideração de questões como a conduta anterior, autorização para publicação ou prévia existência da informação em acesso público;
- Se as informações em causa são de interesse público;
- Se as informações em causa referem-se a uma figura pública;
- Se a informação é parte do registro público;
- Se o requerente demonstrou danos substanciais;
- Quão recente é a informação e se mantém o valor de interesse público;
- Ter uma definição clara do que é informação de acesso público;
- Assegurar que todas as regras sobre exclusão de informação pública sejam balanceadas com a liberdade de expressão.

5) ÓRGÃO REGULATÓRIO

O projeto de lei deve criar e determinar competências e atribuições do órgão regulatório que ficará responsável por sua aplicação e implementação, assim como agir com mandato fiscalizador. Esse órgão regulatório deve ser independente tanto do ponto de vista administrativo quanto orçamentário.

6) MECANISMO DE PARTICIPAÇÃO E CONTROLE SOCIAL

O projeto de lei deve apresentar algum mecanismo de participação e controle social, seja por meio de conselhos consultivos no âmbito do órgão regulatório ou no interior de empresas que fazem o tratamento de dados pessoais. Mecanismos de participação social são ferramentas que proporcionam às pessoas o direito de opinar e construir em conjunto os rumos de um processo político, além de permitir o exercício da liberdade de expressão.

7) PROTEÇÃO AOS DADOS SENSÍVEIS

Os dados sensíveis são aqueles que podem gerar discriminação caso se tornem públicos. Trata-se, por exemplo, de dados que informem a orientação sexual, ideológica, política, religiosa ou a raça de um indivíduo. Dados relativos à saúde, vida sexual, assim como dados genéticos ou biométricos, também são considerados sensíveis. Uma lei de proteção de dados pessoais deve criar um regime de tratamento diferenciado a esses dados, requerendo o consentimento expresso para o seu tratamento, pois seu vazamento pode gerar graves consequências aos titulares e pessoas próximas, podendo, inclusive, causar restrições ao exercício da liberdade de expressão (um exemplo seria quandoalguém não declara sua religião ou orientação sexual com medo de sofrer represálias). As exceções para o tratamento de dados sensíveis deve ter como referência a Lei de Acesso à Informação, Nº12.597. No artigo 31 desta são listadas cinco situações nas quais o consentimento poderá ser relevado, sendo elas:

I à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III ao cumprimento de ordem judicial;

IV à defesa de direitos humanos; ou

V à proteção do interesse público e geral preponderante.

8) GRAUS DE CONSENTIMENTO

O consentimento proporciona ao titular dos dados um momento no qual ele pode expressar sua vontade. Trata-se da principal fase do processo de tratamento de dados pessoais do ponto de vista do direito à liberdade de expressão, uma vez que é quando uma pessoa pode decidir, de movo livre e informado, o que será feito de seus dados. Dessa forma, uma pessoa pode a

qualquer momento, e baseada somente em seu julgamento próprio, aceitar ou recusar o tratamento de seus dados ou, ainda, dizer quais dados podem e quais não podem ser tratados.

É importante lembrar que o consentimento não deve ser tratado pela lei como uma mera autorização. A graduação do consentimento em categorias é necessária para mostrar como este deve ser obtido e quais informações devem ser providas para que o titular dos dados tome uma decisão que reflita realmente sua vontade. Assim, o consentimento para o tratamento de dados pessoais deve ser:

- LIVRE, ou seja, deve se dar sem nenhum tipo de pressão ou coação sobre o titular dos dados;

- INFORMADO, sendo que o titular deve ter a ciência sobre o que é o tratamento de dados pessoais e as implicações do tratamento;

- INEQUÍVOCO, o que garante a ciência do titular sobre a possibilidade de seus dados serem tratados, mesmo que indiretamente- Ele se refere ao comportamento do titular no contexto em que está inserido, ou seja de que ele está ciente de todas implicações a que está sujeito, sem ainda deixar dúvidas de que o titular consente com a prática do tratamento naquela situação;

- ESPECÍFICO, ou seja, que os dados pessoais que sejam alvo do tratamento tenham seu destino devidamente detalhado para o titular;

- DETERMINADO, evitando o consentimento genérico e obrigando a delimitação clara dos tipos de dados que serão alvo do tratamento;

- EXPRESSO, isto é, a pessoa deve apresentar uma indicação clara e objetiva de que concorda que seus dados sejam tratados e com as implicações decorrentes.[19]

9) CONSENTIMENTO DO TITULAR PARA COMPARTILHAMENTO A TERCEIROS

O projeto de lei não pode permitir o compartilhamento de dados pessoais com terceiros sem o consentimento do titular, a não ser nos casos das exceções previstas em lei. É imprescindível que no momento de apresentar seu consentimento, o titular seja informado, de forma específica, sobre as ações de transferência de seus dados a terceiros e as possíveis implicações dessa transferência. Toda pessoa deve ter o direito de escolher os atores que farão o tratamento de seus dados, assim como ter o direito de acessar as informações sobre essa operação.

19 Para mais informações sobre os graus de consentimento para tratamento de dados pessoais, consulte a publicação: "XEQUE-MATE, O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil", desenvolvida pelo GPOPAI-USP. Acessível em: https://gpopai.usp.br/?p=520.

10) PROTEÇÃO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados é assunto complexo, pois os dados de um cidadão de determinado país serão tratados em outra nação, na qual seus direitos podem ser menores e os mecanismos de fiscalização, mais escassos. Em caso dessa operação ocorrer sem consentimento, o titular dos dados tem uma série de direitos violados, pois perde o controle sobre dados que dizem respeito à sua intimidade. Por essa razão, o titular dos dados deve sempre ser consultado antes da realização desse tipo de operação, exercendo seu direito à "autodeterminação informativa".
A transferência internacional de dados deve envolver algumas condições como:

- O país ao qual os dados serão transferidos deve contar com uma legislação de proteção de dados de nível similar à nacional;

- O órgão regulatório nacional deve autorizar a transferência;

- O titular deve consentir prévia e especificamente sobre a transferência internacional, compreendendo que seus dados estarão sob uma jurisdição diversa e sujeitos a todas as implicações decorrentes desse tipo de operação.

11) PROTEÇÃO DE DADOS EM ACESSO PÚBLICO

Dados que estejam em acesso público requerem o mesmo nível de autorização requerido para o tratamento dos outros tipos de dados pessoais, independentemente da vontade do titular. O direito à privacidade deve ser levado em consideração, pois nem todo dado que tenha se tornado público pode ser tratado indiscriminadamente. Pelo contrário, um dado pessoal não perde sua condição por estar em acesso público e deverá sempre contar com o consentimento do titular para seu tratamento, a não ser que se enquadre nas exceções previstas em lei, isto é, que seja de comprovado interesse público.

12) ADOÇÃO DE MEDIDAS DE SEGURANÇA E DE MANUSEIO DOS DADOS PESSOAIS

É fundamental que a segurança na administração de bancos de dados pessoais seja objeto do projeto de lei, que, por sua vez, deve estabelecer medidas a serem adotadas caso ocorram vazamentos de informações ou quebras de protocolos de segurança. Tais medidas devem envolver o órgão regulatório na solução desses incidentes. A garantia de que seus dados pessoais estejam seguros no local de armazenamento e que somente pessoas autorizadas e responsáveis terão acesso a eles é essencial para a aquisição do consentimento dos titulares e para a confiança no processo de tratamento de dados em geral.

13) APLICAÇÃO AO SETOR PÚBLICO COMO UM TODO, INCLUINDO FORÇAS DE SEGURANÇA

A lei de proteção a dados pessoais deve ter aplicação ao setor público de forma abrangente, sem exceções a órgãos de segurança ou inteligência, visto que eles têm capacidade técnica e operacional de lidar com grandes bases de dados pessoais em território nacional, assim como, historicamente, já violaram o direito à privacidade e à liberdade de expressão com base no uso de dados pessoais sem o consentimento de titulares.[20] Uma eventual exclusão desses atores do escopo da lei inibe os usuários de inserir seus dados pessoais na internet, tendo em vista que órgãos de segurança e inteligência podem estar coletando e tratando seus dados de forma indiscriminada e sem nenhum tipo de sanção prevista.

14) DELIMITAÇÃO DE PESQUISA ESTATÍSTICA

Os três projetos de lei sobre proteção de dados pessoais apresentam exceções para as atividades com fins de pesquisa estatística. Apesar de serem exceções válidas, essas atividades devem ter uma definição precisa no texto da lei, delimitando claramente quais atividades não se encaixam nessa definição, e assim evitando casos, por exemplo, em que empresas realizem tratamento de dados pessoais para fins comerciais e definam tal atividade como "pesquisa e desenvolvimento". Um exemplo de pesquisa que pode minar o direito à liberdade de expressão é o perfilamento de indivíduos de acordo com as preferências pessoais. A categorização indiscriminada leva a mapeamentos de grupos ideológicos, com fortes impactos para a livre circulação de informações, ideias e opiniões. Para a realização de pesquisa estatística sem o consentimento dos titulares, deve-se ter como referência a Lei de Acesso à Informação, mais precisamente o inciso II, §3º artigo 31, que afirma que este tipo de pesquisa deve contar com evidente interesse público ou geral para a realização deste tipo de pesquisa, ficando vedada a identificação da pessoa a que as informações se referirem.

20 Para mais informações sobre as violações à liberdade de expressão e à privacidade, acesse os relatórios da ARTIGO 19, disponíveis em: http://artigo19.org/blog/2016/03/10/da-ciberseguranca-a-ciberguerra-o-desenvolvimento-de-politicas-de-vigilancia-no-brasil/; http://artigo19.org/blog/2015/09/10/relatorio-as-ruas-sob-ataque-protestos-2014-e-2015/; http://protestos.artigo19.org/.

15) PRAZO PARA A LEI ENTRAR EM VIGOR

A proteção de dados pessoais é um tema urgente já que a operação envolvendo dados pessoais já ocorre massivamente, em especial na internet, e sem uma regulação necessária que garanta os direitos dos usuários. Por essa razão, uma lei geral de proteção de dados pessoais deve entrar em vigor o quanto antes.

Pela tabela comparativa, o projeto de lei que traz mais garantias de proteção de dados pessoais aos cidadãos é o 5276/2016, elaborado no

ASPECTOS DA LEI	PL 5276/2016	PLS 330/2013	PL 4060/2012
Menção expressa à proteção da liberdade de expressão	🟢	🔴	🟡
Exceção à atividade jornalística e outras formas de expressão	🟢	🟡	🟢
Menção expressa à Lei de Acesso à Informação (LAI)	🟢	🔴	🔴
Evita interpretações que possam ensejar reivindicações do direito ao esquecimento	🔴	🔴	🔴
Órgão regulatório	🟡	🟡	🔴
Mecanismo de participação e controle social	🟡	🟡	🔴
Proteção aos dados sensíveis	🟢	🟢	🟡
Graus de consentimento	🟢	🟢	🔴
Consentimento do titular para compartilhamento a terceiros	🟢	🟢	🔴
Proteção para transferência internacional de dados	🟢	🟢	🔴
Proteção de dados em acesso público	🟡	🔴	🔴
Adoção de medidas de segurança e de manuseio dos dados pessoais	🟢	🟢	🟡
Aplicação ao setor público como um todo, incluindo forças de segurança	🔴	🔴	🔴
Delimitação de pesquisa estatística	🔴	🔴	🔴
PRAZO PARA A LEI ENTRAR EM VIGOR	180 dias	120 dias	90 dias

interior do Ministério da Justiça, porque atende plenamente a oito aspectos de 15 analisados. Entretanto, para trazer melhores garantias aos cidadãos, o projeto precisa ainda sanar algumas lacunas, como: dirimir as brechas existentes que permitem a aplicação do "direito ao esquecimento"; propor a criação de um órgão independente que trate da proteção de dados pessoais; propor um mecanismo de controle social; prever a aplicação de seus dispositivos a órgãos de segurança e inteligência; delimitar qual o escopo do que seria uma "pesquisa estatística"; e ter um prazo mais reduzido para a entrada em vigor da lei.

O projeto que poderíamos classificar como intermediário é o PLS 330/2013, do senador Antônio Carlos Valadares (PSB-SE), que atende a cinco dos 15 aspectos analisados. Ele não se sobressai ao seu congênere anterior em nenhum aspecto. Todas as sugestões de melhorias feitas ao PL 5276/2016 também valem para o PLS 330/2013, que carece ainda de uma menção explícita em seu texto à liberdade de expressão e à Lei de Acesso à Informação (LAI) e de um artigo que determine que o tratamento de dados de acesso público não possa ocorrer sem o consentimento dos titulares dos dados.

Criado pelo deputado federal Milton Monti (PR-SP), o PL 4060/2012 foi o pior avaliado dentre os projetos analisados porque contemplou somente um dos 15 pontos listados acima. O projeto atenta contra a maioria dos direitos dos titulares de dados pessoais, não tendo sequer abordado a discussão sobre os graus de consentimento. Também não toca na questão de transferência internacional de dados e permite um compartilhamento praticamente livre entre os donos de bases de dados, excluindo o titular de qualquer participação nessas operações.

A seguir, detalharemos como os aspectos listados acima são tratados por cada projeto de lei em tramitação no Congresso Nacional.

IV.
PL 5276/2016

Este projeto, que atualmente tramita na Câmara dos Deputados, contém importantes aspectos que asseguram direitos no processo de tratamento de dados pessoais dos cidadãos brasileiros, seja ele realizado por órgãos públicos ou privados. A construção do texto do PL 5276/2016 foi aquela que contou com maior participação social. Uma série de reuniões e consultas públicas organizadas pelo Ministério da Justiça envolveram empresas, organizações da sociedade civil e representantes do poder público na discussão sobre as melhores formulações para o texto. A plataforma recebeu mais de 50 mil visitas e mais de 1.100 contribuições. Inclusive, no próprio Poder Legislativo, o texto foi alvo de consulta pública online na plataforma *e-democracia*[21], que recebeu um total de 452 contribuições de 79 participantes de diferentes setores da sociedade. O resultado final ficou ao nível do debate internacional moderno sobre o tema.

Ainda que o projeto precise de aprimoramentos, o principal ponto positivo e diferencial em relação aos outros projetos de lei é a atribuição a um órgão competente da responsabilidade pela implementação e fiscalização das disposições da lei. A seguir, apresentaremos os pontos do projeto que consideramos satisfatórios, bem como aqueles que deveriam ser aprimorados.

21 A ARTIGO 19, em 03 de junho de 2016, escreveu carta endereçada aos parlamentares reivindicando que o projeto de lei fosse colocado em consulta pública online a fim de consolidar todo o processo participativo realizado pelo poder Executivo. A carta foi entregue pessoalmente a mais de dez deputados e, no dia 23 de junho, um dos relatores da proposição na Câmara, o deputado Alessandro Molon, abriu a consulta pública online.

ASPECTOS SATISFATÓRIOS DO PROJETO DE LEI

Menção expressa à proteção da liberdade de expressão

O artigo 2, inciso II, insere as liberdades de expressão, de comunicação e de opinião como fundamentos da proteção de dados pessoais. Essa inserção é de suma importância, pois a proteção de dados pessoais necessita ser contrabalanceada ao direito à liberdade de expressão e ao interesse público no acesso à informação.

Exceção jornalística e outras formas de expressão

Além da menção explícita à liberdade de expressão como um de seu fundamentos, o inciso II do artigo 4 do projeto afirma que atividades exclusivamente jornalísticas, artísticas, literárias ou acadêmicas estariam fora do escopo da lei.

Essa é uma garantia importante, pois tais atividades requerem, por vezes, o tratamento de dados para fins legítimos, como o desenvolvimento de uma reportagem investigativa ou a análise de dados para uma pesquisa acadêmica. Tais atividades não têm um fim meramente econômico e podem ter uma função social de denúncia ou, ainda, de acúmulo de conhecimento.

As práticas exclusivamente artísticas e literárias também não podem ser alvo de limitações, pois são pura demonstração da liberdade de expressão de seus autores. Nesse ponto, seria bom esclarecer que a atividade deve ser exclusivamente para esses fins, não podendo ter impactos econômicos ou políticos. O projeto de lei, no parágrafo 3 do artigo 4, ainda confere ao órgão competente a função de emitir opiniões técnicas ou recomendações referentes às exceções previstas a essas atividades, o que visa evitar possíveis abusos e mau usos.

Menção expressa à Lei de Acesso à Informação

São três citações do projeto 5276/2016 à Lei de Acesso à Informação (LAI). A primeira ocorre no artigo 23, tornando o tratamento de dados pessoais realizado por pessoas jurídicas de direito público (por exemplo, os órgãos integrantes da administração direta do Executivo, Legislativo, Judiciário, Ministério Público, das autarquias, das fundações públicas, das empresas públicas, das sociedades de economia mista e das demais entidades controladas direta ou indiretamente pela União, pelos Estados, pelo Distrito Federal e pelos municípios) submetido ao atendimento de sua finalidade pública, conforme já prevê o artigo 1º da LAI.

A segunda menção ocorre no primeiro parágrafo do artigo 26, e determina que o compartilhamento de dados pessoais com pessoas de direito privado é vedado, podendo somente ocorrer em casos de execução descentralizada de política pública, com um fim específico e determinado, sempre observando o que é disposto na LAI.

Por fim, o primeiro parágrafo do artigo 44 exime de responsabilidade solidária do cessionário que esteja atuando "no exercício dos deveres de que trata a Lei nº 12.527, de 2011, relativos à garantia do acesso à informações públicas."

Proteção aos dados sensíveis

O projeto de lei traz em seu artigo 7, inciso I, a obrigação do consentimento livre, informado e inequívoco para o tratamento de dados pessoais. Para o tratamento de dados sensíveis, o texto ainda prevê uma autorização mais restrita: o consentimento específico do titular para o tratamento. Essa é uma garantia necessária, pois os dados sensíveis hoje são utilizados para finalidades que podem impactar diretamente na classificação de alguém para a realização de atividades como: obtenção de crédito, aquisição de seguro, compra de produtos e entrada em um posto de trabalho.

No artigo 11, o projeto de lei proíbe o tratamento de dados sensíveis, estipulando exceções limitadas e razoáveis, sendo a condição principal o fornecimento de consentimento "livre, inequívoco, informado, expresso e específico" pelo titular. Já o artigo 12 define que o órgão competente estabeleça medidas adicionais de segurança e de proteção aos dados sensíveis.

Graus de consentimento

O capítulo I, que aborda os requisitos para o tratamento de dados pessoais, dá ampla importância para o tipo de consentimento do titular sobre seus dados. O artigo 7 define que o processo só poderá ser realizado mediante um consentimento livre, informado e inequívoco. Tais qualificações reforçam os modos de permissão necessários.

O parágrafo 1 do artigo 7 estipula que mesmo sendo permitido o tratamento de dados pela administração pública para o cumprimento de obrigações legais ou por conta da necessidade para execução de políticas públicas, esse tratamento deve ser informado ao titular. Sobre o mesmo ponto, o parágrafo 2 ainda exprime que a autoridade competente pode regular essa ação, estabelecendo diretrizes que protejam o titular. O artigo 8 dispõe que o acesso às informações do tratamento de dados deve ser facilitado e deve incluir pontos como:

- a finalidade específica do tratamento
- a forma e a duração do tratamento
- a identificação do responsável

Esses direitos garantem a transparência do processo de tratamento que poderá ser avaliado e supervisionado, além do órgão competente, pelos próprios titulares.

No artigo 8, inciso VII, são descritos os direitos que o titular dos dados têm sobre o tratamento. Fica assegurado que ele pode:

- acessar, retificar ou revogar seu consentimento para o tratamento de seus dados
- denunciar possíveis atos em desacordo com essa lei
- não oferecer o consentimento mediante o fornecimento de informações sobre as consequências da negativa

O parágrafo 3 do mesmo artigo determina que em casos de coleta de dados continuada, o responsável pela operação deve informar periodicamente sobre as principais características do tratamento — prática conhecida como "consentimento granular" —, ou seja, deve haver prestação de contas em serviços duradouros, o que permite o acompanhamento regular e perene do titular sobre os seus dados.

Consentimento do titular para compartilhamento a terceiros

O artigo 40 da lei prevê que "a comunicação de dados pessoais entre responsáveis ou operadores de direito privado dependerá do consentimento do titular, com exceção das hipóteses de dispensa do consentimento previstas nesta lei". Em relação ao uso compartilhado de dados pessoais pelo poder público, o artigo 26 afirma que essa ação só é permitida quando "atende finalidades específicas de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas". O parágrafo 1º ainda veda o compartilhamento para entidades privadas.

Proteção para a transferência internacional de dados

Os artigos 33, 34 e 35 tratam da transferência internacional de dados. Atualmente, com a internet, grande parte do tratamento de dados pessoais de cidadãos de determinado país é realizada em um país estrangeiro. O artigo 33 prevê que essa transferência se dará somente junto a países que possuam um nível de proteção de dados semelhante, apresentando cinco critérios específicos de como será feita a comparação; quando o órgão competente autorizar a operação; e quando o titular tiver fornecido seu consentimento, com informação prévia e específica sobre o caráter internacional da operação. O artigo 35 ainda garante que tanto o responsável pelo tratamento quanto o operador respondam pelo tratamento de dados, independentemente de onde a operação se realize.

Adoção de medidas de segurança e de manuseio dos dados pessoais

Outro importante ponto que o projeto prevê são as medidas de proteção e segurança que o responsável pelo tratamento deve estabelecer sobre os dados pessoais que tem controle.

No artigo 6, inciso VII, a lei afirma que a segurança é um dos princípios que regem seu texto. Segundo a redação, "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."

No artigo 16, do capítulo I, da seção II, é abordado o momento de término do tratamento, assegurando ao usuário que seus dados serão eliminados após o fim do processo.

O capítulo IV se refere ao tratamento de dados pessoais pelo poder público. No artigo 32, fica estabelecido que o órgão competente pode requerer relatórios aos órgãos públicos sobre o impacto das suas práticas de tratamento na privacidade, assim como sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

O capítulo VI, da seção I, dispõe sobre as funções do responsável e do operador sobre os dados tratados. No artigo 39, há a menção de que o órgão competente possa determinar que o responsável pelo tratamento dos dados elabore um relatório de impacto à privacidade referente às suas operações. No artigo 40, fica expresso que a comunicação de dados pessoais entre responsáveis e operadores de direito privado dependerá do consentimento do titular tendo como ressalvas as hipóteses previstas em lei. No artigo 41, é designada a figura do encarregado.

Já o capítulo VII inicia-se com o artigo 45, que determina que "o operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração de comunicação ou qualquer forma de tratamento inadequado ou ilícito."
O artigo 46 complementa o anterior e estipula a obrigatoriedade de sigilo também aos responsáveis pelo tratamento de dados, mesmo após o fim do período da operação.

ASPECTOS PARCIALMENTE SATISFATÓRIOS OU AUSENTES NO PROJETO DE LEI

Órgão regulatório

O PL 5276/2016, do Ministério da Justiça, designa um órgão competente para zelar pela implementação e pela fiscalização da lei, apesar de não criar um órgão regulatório independente para a proteção de dados pessoais. Mais especificamente, como mecanismo de participação e controle social, sugere a criação de um conselho nacional de proteção de dados pessoais, que será constituído, em sua maioria, por representantes públicos e com pequena participação da sociedade civil e da iniciativa privada. A independência desse órgão deveria ser inclusive orçamentária, que definisse o modo de aplicação de sanções e evoluísse para um órgão relacionado aos temas da sociedade da informação. Entendemos ser necessário que o tal órgão aumente seu escopo de atuação para além da proteção aos dados pessoais e passe a ser responsável por todas as problemáticas relativas à constituição da sociedade da informação, como a crescente conectividade de dispositivos com o advento da internet das coisas. Mesmo o texto que está posto poderia ser aprimorado, prevendo, por exemplo, a eleição entre os pares para compor o referido conselho.

Mecanismo de participação e controle social

O projeto de lei aborda timidamente a adoção de mecanismos de participação e controle social. O artigo 10, parágrafo 2º, que apresenta situações de tratamento de dados baseados no legítimo interesse dos responsáveis, prevê um mecanismo que garanta a transparência sobre o processo e o fornecimento da possibilidade aos titulares de manifestarem sua oposição ao tratamento de seus dados. O artigo 51 também define que o órgão competente deve estimular "a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais." Apesar de reconhecermos esses pontos como benéficos, acreditamos que a lei deveria trazer mais detalhes sobre mecanismo de participação e controle social sobre o tratamento de dados pessoais.

Proteção de dados em acesso público

O artigo 7, parágrafo 4º, supõe que o mesmo tratamento concedido aos dados em domínio priva-

do deve ocorrer com dados tornados públicos. Ou seja, não há um relaxamento das normas por conta da origem dos dados pessoais, o que é um ponto positivo. Por outro lado, ao impor o mesmo processo para o tratamento de dados em acesso público, admite hipóteses nas quais o consentimento do titular não seja requerido no tratamento desses dados, como para o uso de forças de segurança e inteligência, que já praticam esse tipo de tratamento de dados em acesso público há algum tempo.

Delimita pesquisa estatística

O artigo 7, inciso IV, afirma que o tratamento de dados pessoais é permitido para a realização de pesquisas estatísticas independentemente do consentimento dos titulares, impondo a condição de que sempre que possível os dados devem estar sob anonimato. No entanto, a proposta não se preocupa em delimitar o que se enquadraria como uma pesquisa estatística, se qualquer pessoa de direito ou público ou privado pode fazer esse tipo de pesquisa e com quais finalidades tais pesquisas podem ser realizadas.

Prazo para a lei entrar em vigor

Entre os três, este projeto de lei tem o mais longo período entre a publicação e sua entrada em vigor. A ARTIGO 19 acredita que por se tratar de um assunto urgente, a lei de proteção de dados pessoais necessita entrar em vigor assim que for publicada.

ASPECTOS INSATISFATÓRIOS DO PROJETO DE LEI

Evita interpretações que possam ensejar reivindicações do direito ao esquecimento

Avaliamos que o projeto de lei pode ser mal interpretado, de modo a permitir a exclusão de informações que, embora pessoais, são de interesse público, sob a alegação do direito ao esquecimento. É importante deixar claro que o direito ao cancelamento e à exclusão de dados pessoais não pode se confundir com o direito ao esquecimento. Essas práticas devem ser sempre ponderadas com interesses legítimos na manutenção dos dados, especialmente o interesse público subjacente. Ou seja, a exclusão de dados pessoais que tenham relevante interesse público nem sempre deve ser realizada, pois, por muitas vezes, a supressão dessas informações pode funcionar como um meio de acobertamento de informações.

No artigo 7, parágrafo 4, a lei determina que "o tratamento de dados pessoais cujo acesso é público deve ser realizado de acordo com essa lei, considerando a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização." Fica estabelecido, portanto, que não há diferenças em relação às regras do tratamento entre dados de acesso público e privado.

Já o artigo 18 acrescenta o direito do titular em pedir anonimato, portabilidade ou eliminação de seus dados, de acordo com a situação. Dessa forma, público ou não, todos os dados pessoais estão sujeitos às requisições dos titulares pela retirada, exclusão ou alteração. Os riscos dessa disposição são os abusos que podem ocorrer, especialmente por parte de figuras públicas que possuem vasta quantidade de dados relativos à sua imagem na internet e em outros meios, e podem tentar caracterizar como dado pessoal informações que são, na realidade, informações de utilidade pública e devem ser de acesso público.

Para que esse dispositivo legal não sofra de tais abusos, a ARTIGO 19 recomenda que haja uma ressalva explícita ao interesse público quando se tratar do cancelamento ou da exclusão dos dados pessoais.

Aplica-se ao setor público como um todo, incluindo forças de segurança

O artigo 4, inciso III, exclui da aplicação da lei o tratamento de dados pessoais "realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais." Essa exceção feita aos órgãos de segurança é recorrente nos três projetos de lei e aprofundada nas recomendações gerais a todos os projetos feitas mais adiante nesta análise.

A única diferença entre o PL 5276/2016 para os demais é que, mesmo com a citada exceção, o parágrafo primeiro do artigo 4 prevê que os princípios gerais de proteção e os direitos do titular continuam sendo aplicados para as atividades de segurança, além de demandar uma legislação específica para a regulação da atividade por esses atores.

V.

PLS 330/2013

O PLS 330/2013, de Antônio Carlos Valadares (PSB-SE), que atualmente tramita no Senado, também contém importantes aspectos que asseguram direitos no processo de tratamento de dados pessoais dos cidadãos brasileiros, como o respeito à liberdade de expressão. As premissas deste projeto são muito similares às adotadas no PL 5276/2016, da Câmara dos Deputados, apesar de não ter o mesmo nível de proteção de dados. Em novembro de 2016, este projeto encontra-se na última comissão do Senado e em breve será reunido na Comissão Especial na Câmara dos Deputados, junto aos PLs 5276/2016 e 4060/2012.

ASPECTOS SATISFATÓRIOS DO PROJETO DE LEI

Proteção aos dados sensíveis

O projeto de lei, em seu artigo 15, proíbe o tratamento de dados pessoais sensíveis, estabelecendo sete possíveis exceções a essa regra:

- a primeira delas se refere a possibilidade do tratamento de dados sensíveis com o consentimento específico e expresso do titular;
- a segunda para quando for necessário para o cumprimento das obrigações e dos direitos do responsável no domínio da legislação do trabalho;
- a terceira quando se tratar de entidades de caráter político, filosófico, religioso ou sindical, que trate dados de seus membros, vedando o acesso de terceiros a esses dados;
- a quarta exceção permite o tratamento quando necessário para o cumprimento de obrigação legal pelo responsável;
- a quinta quando realizado exclusivamente no âmbito da pesquisa jornalística, histórica ou científica sem fins lucrativos e desde que sejam tomadas medidas adicionais de proteção;
- a sexta quando necessário para a realização de atividades específicas de pessoas jurídicas de direito público, mediante decisão motivada, e desde que a obtenção do consentimento represente obstáculo à consecução do interesse público;
- a sétima quando necessário para tutela da saúde ou proteção da integridade física do titular ou de terceiro.

As exceções estabelecidas no artigo são razoáveis, no entanto dois pontos merecem maior atenção. Na quinta exceção, é necessária a delimitação das atividades consideradas como pesquisa jornalística, histórica ou científica, impossibilitando que práticas comerciais ou com outros fins não sejam enquadradas nessa exceção. Já na sexta exceção, é fundamental atenção e fiscalização sobre as atividades das pessoas jurídicas de direito público, já que o termo "atividades específicas" podem abarcar diversas ações e uma "decisão motivada" deve ser alvo de avaliação do órgão competente.

Graus de consentimento

A graduação do consentimento é importante em um projeto de lei sobre proteção de dados, pois dá maior informação e poder de escolha ao titular dos dados sobre o tratamento a ser realizado com eles. O projeto 330/2013, em seu artigo 4, inciso V, prevê que um dos princípios para o tratamento de dados é o consentimento livre, específico, inequívoco e informado do titular dos dados —em se tratando de dados sensíveis, o consentimento deve ser ainda mais prévio e expresso. O artigo 6, inciso IV, reforça esse princípio e requer que a concordância deva se dar de maneira destacada. No artigo 13, define que o consentimento prestado de forma apartada do restante das declarações deve apontar uma finalidade legítima, específica e delimitada. Esses três artigos dão uma base sólida ao consentimento como um princípio fundante de qualquer relação de tratamento de dados pessoais.

Consentimento do titular para compartilhamento a terceiros

Os artigos 13 e 20 estabelecem o consentimento como base para o compartilhamento de dados pessoais a terceiros por parte do responsável pelo tratamento dos dados. No artigo 13, o primeiro parágrafo expressa que o titular deve ter acesso a todas as informações relativas ao tratamento antes de dar sua autorização, inclusive sobre se seus dados serão comunicados a terceiros. No artigo 20, que trata especificamente da questão da comunicação dos dados, fica estabelecido que a ação somente ocorrerá com o consentimento específico e próprio do titular, ou por conta das exceções previstas nos incisos III a VI do artigo 12 da lei, que são:

"II na execução de um contrato ou na fase pré-contratual de uma relação em que o titular seja parte;

III quando necessário para o cumprimento de obrigação legal pelo responsável;

IV quando realizado exclusivamente no âmbito da pesquisa jornalística, histórica ou científica sem fins lucrativos e desde que sejam tomadas medidas adicionais de proteção;

V quando necessário para a realização de atividades específicas de pessoas jurídicas de direito público, mediante decisão motivada, e desde que a obtenção do consentimento represente obstáculo à consecução do interesse público;

VI quando necessário para tutela da saúde ou proteção da integridade física do titular ou de terceiro".

As exceções são poucas, mas devem ser bem delimitadas, por exemplo, com uma clara definição sobre quais atividades podem ser consideradas de fins exclusivamente de pesquisa histórica ou científica.

Proteção para transferência internacional de dados

Os artigos 26, 27 e 28 abordam a questão da transferência internacional de dados. O artigo 26 estabelece alguns critérios para que essa operação possa ser realizada, dos quais destacam-se dois:

1 A transferência internacional de dados só poderá ser feita a países que ofereçam o mesmo grau de proteção de dados.

2 O titular dos dados deve ter ser informado sobre todos os aspectos que envolvem a atividade, inclusive os riscos que ele deve consentir de forma específica e própria.

As medidas protegem os dados de cidadãos brasileiros, pois impedem que empresas baseadas em países sem legislação forte de proteção envie os dados de brasileiros e requer que o indivíduo tome uma decisão informada e específica sobre o caráter internacional dessa operação.

Estipula medidas de segurança técnicas e de manuseio durante o período de tratamento dos dados pessoais

Os artigos 18, 22, 23 e 24 expõem as medidas que deverão ser adotadas pelos donos ou responsáveis pelos bancos de dados pessoais para a segurança dos dados tratados. O artigo 18 impede o acesso não autorizado "aos equipamentos, instalações e suportes de tratamento de dados", assim como impede o tratamento de dados sensíveis em locais que não reúnam condições de segurança mínimas, a serem definidas pelo regulamento da lei.

O artigo 22 prevê que os responsáveis pelo tratamento adotem "medidas técnicas atualizadas e compatíveis com os padrões internacionais, conforme estabelecido em regulamento, com a natureza dos dados tratados e com a finalidade do tratamento", assim como define que deve ser guardado sigilo sobre os dados durante e após o tratamento. Essa obrigação de sigilo tem a abordagem estendida no artigo 23, que presume uma pena aos responsáveis que descumprirem a disposição. O artigo 24 estabelece que o responsável deve sempre comunicar incidentes de segurança ao órgão competente com o maior nível de detalhamento possível sobre o acontecido e sua implicações, permitindo ao órgão qualificado avisar aos titulares sobre o ocorrido, divulgar amplamente a notícia e buscar a reversão da situação.

A segurança dos dados é essencial para que os titulares se sintam confortáveis com o tratamento de suas informações. Somente a partir da garantia de que os dados são manuseados apenas por pessoas autorizadas e em pequeno número, de que os incidentes de segurança serão prontamente comunicados e solucionados, seja pelo responsável ou pelo órgão competente, que o titular confiará no processo de tratamento de dados.

ASPECTOS PARCIALMENTE SATISFATÓRIOS OU AUSENTES NO PROJETO DE LEI

Existem alguns pontos que podem ser melhorados no projeto de lei. Ressaltamos os seguintes:

Menção expressa à proteção da liberdade de expressão

O projeto de lei, em nenhum momento, faz o necessário contrabalanço do direito à proteção de dados pessoais ao direito à liberdade de expressão. A importância da menção expressa à liberdade de expressão em projetos de lei sobre proteção de dados pessoais é abordada mais detalhadamente na seção de recomendações a todos os projetos analisados.

Exceção à atividade jornalística e outras formas de expressão

O projeto de lei inclui somente a atividade jornalística no rol de exceções à necessidade de consentimento para o tratamento de dados pessoais, exigindo, por exemplo, consentimento para atividades artísticas, literárias e acadêmicas.

O artigo 3, inciso II, exclui do escopo de aplicação da lei somente as atividades de cunho puramente jornalístico. A ARTIGO 19 acredita que a lei deve contrabalançar o direito à proteção de dados pessoais com o direito à liberdade de expressão e informação, incluindo o tratamento de dados pessoais para fins jornalísticos, acadêmicos, artísticos ou de expressão literária.

Menção expressa à Lei de Acesso à Informação

No projeto de lei não há nenhuma menção ao direito de acesso à informação. Tema que está diretamente implicado na proteção de dados pessoais, como foi bem percebido pelo projeto 5276/2016. A ausência de disposições sobre o conteúdo gera um vácuo legislativo que pode dar margem a interpretações favoráveis a uma cultura de sigilo nos órgãos públicos em relação aos dados pessoais de funcionários ou autoridades públicas, por exemplo.

Órgão regulatório

O projeto não avalia a criação de um órgão independente responsável pela fiscalização e normatização do tratamento de dados pessoais no país. No entanto, o artigo 5 da lei prevê que o poder público é responsável por assegurar os direitos do titular no tratamento de seus dados. Porém, o texto é paradoxal, pois estabelece que também será designado um órgão capaz de aprovar normas para lidar com o tema. O artigo 11 também admite o direito do titular em buscar o órgão autorizado, caso venha a ocorrer alguma violação durante o tratamento de seus dados.

Por sua vez, o artigo 24 obriga o responsável pelo tratamento reportar todo incidente de segurança que possa acarretar prejuízo aos titulares do órgão competente, delegando a eles a responsabilidade de adotar providências quanto aos incidentes de segurança, de acordo com a gravidade do ocorrido. O artigo 26 também prevê que será função da autoridade competente o gerenciamento de autorizações para transferências de dados internacionalmente.

O artigo 33 versa sobre o poder do órgão competente em relação aos responsáveis e determina que poderá adotar medidas preventivas caso haja suspeita sobre a atuação do responsável e possíveis danos aos titulares, estabelecendo multas diárias, na hipótese das ordens serem descumpridas.

Mecanismo de participação e controle social

O PLS 330/2013 prevê a criação de mecanismos de participação do titular em um programa de governança em privacidade criado pelo responsável do tratamento em seu artigo 29, em especial no inciso I (e). Essa foi a maneira encontrada pelo legislador para fazer valer o princípio estabelecido no inciso X, do artigo 4, sendo ele: "responsabilização e prestação de contas pelos agentes que tratam dados pessoais, de modo a demonstrar a observância e o cumprimento das normas de proteção de dados pessoais".

Proteção de dados em acesso público

O projeto de lei não faz menção ao tratamento específico de dados que estejam em acesso público. Contudo, uma leitura em conjunto do artigo 3, inciso I, e do artigo 12 nos leva a uma interpretação de que esses dados estão submetidos ao mesmo tratamento de dados pessoais de acesso privado. O artigo 3, inciso I, prevê que dado pessoal é "qualquer informação referente a pessoa natural identificável ou identificada", ou seja, um dado pessoal continua a ser assim classificado independentemente da fonte em que foi coletado. Por sua vez, o artigo 12 determina as únicas ocasiões em que poderá ocorrer o tratamento de dados pessoais e não faz menção ao tratamento de dados em acesso público. Ou seja, como o tratamento de dados pessoais em acesso público não está entre as situações em que é permitida a execução de tratamento, a lei proíbe o tratamento desses dados, a não ser que haja o "consentimento livre, específico, inequívoco e informado concedido pelo titular dos dados" (art 12,I).

Delimitação de pesquisa estatística

O parágrafo único do artigo 4 prevê que a conservação dos dados e identificação dos seus titulares poderá ocorrer quando se tratar de pesquisas estatísticas. Apontamos o problema de que a pesquisa estatística pode abarcar variadas atividades, realizadas por um número incontável de atores e com diversas finalidades. Ao permitir essa exceção, sem a delimitação necessária apontando o que deve ser considerada um fim estatístico, o projeto cria, na verdade, uma brecha para que entes públicos e privados possam conservar dados pessoais e a identificação de cidadãos brasileiros.

Prazo para a lei entrar em vigor

A partir da data da publicação da lei, caso venha a ser aprovada, serão necessários 120 dias para que ela entre em vigor. Nossa recomendação é de que a lei sobre proteção de dados pessoais deveria entrar em vigor imediatamente após sua publicação no Diário Oficial, pois trata-se de um problema já muito difundido nas práticas comerciais e sociais e necessita urgentemente de regulamentação. O país encontra-se muito atrasado nesse tema e os dados dos cidadãos brasileiros necessitam imediatamente da proteção legislativa e de mecanismos de fiscalização e regulação que reforcem o direito à autodeterminação informativa.

ASPECTOS INSATISFATÓRIOS DO PROJETO DE LEI

Evita interpretações que possam ensejar reivindicações do direito ao esquecimento

O projeto de lei 330/2013 não faz referência a situações nas quais o direito do titular de exclusão definitiva de dados pessoais —direito assegurado no artigo 6, inciso VII— entra em conflito com o direito de acesso à informação e ao de interesse público, por exemplo. Uma lei de proteção de dados pessoais não pode dar margens a interpretações que permitam a institucionalização do direito ao esquecimento. Os artigos 8 e 9 da lei tratam dos casos nos quais podem ocorrer correção, bloqueio, cancelamento ou dissociação dos dados. Em nenhum momento se faz o contrapeso dessas ações com o interesse público, o que é problemático, pois há casos em que os dados pessoais publicizados têm efetivamente um grande interesse público por trás, como em casos de denúncias de corrupção ou então de irregularidades em órgãos públicos.

Aplicação ao setor público com um todo, inclusive às forças de segurança

O parágrafo 3º, do artigo 2, afirma que a lei não se aplica "aos bancos de dados mantidos pelo Estado exclusivamente para fins de defesa nacional e segurança pública", ou seja, a proteção de dados pessoais de cidadãos brasileiras não estará garantida quando forem manuseadas pelo órgão cujo dever é zelar pela defesa e segurança pública. Tal contradição é encontrada nos três projetos analisados e mais aprofundada na seção de recomendação a todos os projetos de lei.

VI.
PL 4060/2012

Entre todas as proposições em análise pelo Congresso Nacional, este PL, de autoria do deputado federal Milton Monti (PR-SP), é o mais problemático, porque seu teor é mais vago, dispondo mais sobre o tratamento dos dados pessoais do que sua proteção. A linguagem do texto do projeto não incorpora as discussões mais relevantes dos últimos anos sobre o tema e não assegura padrões mínimos de proteção aos titulares dos dados pessoais, em total desacordo com os padrões internacionais de direitos humanos.

ASPECTO SATISFATÓRIO DO PROJETO DE LEI

Exceção à atividade jornalística e outras formas de expressão

O projeto, assim como o PL 5276/2016, faz a necessária exclusão da atividade jornalística de sua aplicação no artigo 6. Conforme explicado anteriormente, a exclusão da atividade jornalística é importante, pois garante a liberdade de imprensa e de expressão. Sem essa garantia, os jornalistas seriam privados de desenvolver importantes atividades como a produção de jornalismo investigativo e o cruzamento de dados que podem ser relevantes para a opinião pública sobre agentes públicos ou privados de grande influência social.

ASPECTOS PARCIALMENTE SATISFATÓRIOS OU AUSENTES NO PROJETO DE LEI

Caso avance, seria necessário reformular o projeto de lei a fim de garantir os direitos dos cidadãos e não apenas legitimar o tratamento de dados pessoais que já é realizado no país. Especificamente, recomendamos:

Menção expressa à proteção da liberdade de expressão:

O projeto possui uma única menção ao princípio constitucional da liberdade de comunicação em seu artigo 3º. Em nenhum momento ele cita expressamente o direito à liberdade de expressão, necessário para qualquer discussão que envolva questões de privacidade.

Menção expressa à Lei de Acesso à Informação

O PL 4060/2012 não faz nenhuma referência à Lei de Acesso à Informação. Essa menção é de importância ímpar, pois reforça a aplicação dos princípios de transparência e controle social da LAI no escopo da proteção dos dados pessoais, especificamente em casos de tratamento de dados pessoais pelo poder público.

Órgão regulatório

Por sua origem no Poder Legislativo, o projeto de lei não estipula um órgão competente para fiscalizar e implementar a proteção de dados pessoais. Apesar dessa designação poder ser feita por meio de decreto regulamentador, seria importante ter uma disposição na lei, que tem um grau de hierarquia superior. Os artigos 21, 22 e 23 tratam da tutela fiscalizatória e sancionatória. Há uma observância especial ao Código de Defesa do Consumidor, enfatizando o caráter econômico do processo de tratamento de dados em detrimento da ótica dos direitos humanos, assim como uma menção a dispositivos autorregulatórios no artigo 23, sem antes estabelecer quais órgãos públicos seriam responsáveis por essa regulação. Ou seja, a proposta da lei é que a atividade de tratamento de dados pessoais seja basicamente autorregulada.

Mecanismo de participação e controle social

O projeto não estipula nenhum modelo que promova o controle social sobre o tratamento de dados pessoais na sociedade e que envolva as pessoas nas tomadas de decisão relativas à aplicação da lei em questão.

Proteção aos dados sensíveis

A proposta de lei só faz duas menções ao tratamento de dados sensíveis. A primeira no parágrafo único do artigo 11, que prevê a adoção de medidas tecnológicas "proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis." Uma disposição vaga que não se aprofunda sobre a defnição de "natureza dos dados" e "características específicas do tratamento" e inclui o tratamento especial a dados sensíveis como um apêndice do texto.

A segunda menção ao termo ocorre no artigo 12, que se refere ao tratamento de dados sensíveis e permite que a autorização do titular para esse tipo de tratamento se dê por qualquer meio que permita a manifestação de sua vontade. Fica patente que tal disposição visa manter a prática já comum de incluir tal autorização em contratos longos e complexos, os quais poucas pessoas leem com atenção, o que limita a capacidade de negociação dos focos do tratamento de dados pessoais e a autodeterminação informativa dos cidadãos.

Adoção de medidas de segurança e de manuseio dos dados pessoais

O texto não possui uma seção para lidar especificamente com o tema da segurança dos dados. A única disposição sobre o assunto está no artigo 11, no qual se estabelece que o responsável deve "adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular." O texto não prevê medidas específicas de proteção e segurança dos dados, como fazem os outros dois projetos de lei. Não há menção sobre prevenção a acessos não autorizados, possibilidade de verificações periódicas dos dados tratados ou a garantia de que dados só serão acessados pelos usuários.

Prazo para a lei entrar em vigor

A lei só será implementada após 90 dias de sua publicação. A ARTIGO 19 acredita que o tema da proteção de dados pessoais é urgente e uma lei que trate da questão deve valer já na data de sua publicação.

ASPECTOS INSATISFATÓRIOS NO PROJETO DE LEI

Evita interpretações que possam ensejar reivindicações do direito ao esquecimento

O artigo 13 do projeto de lei prevê que fica assegurado aos titulares o bloqueio do registro de seus dados para tratamento ou interconexão. O artigo 19 reforça esse direito, afirmando que o titular pode pedir o bloqueio a qualquer momento, salvo se a manutenção dos dados for necessária para a execução de obrigações contratuais ou legais. Nenhuma dessas disposições reprime o direito do titular em bloquear seus registros com o interesse público. Assim, a depender da interpretação feita pelo magistrado da lei, pode ficar configurado o direito que qualquer pessoa tem sobre a exclusão de seus dados, sem que haja mais condicionamentos a essa exclusão, além da própria vontade do titular, o que dá margem a execução do direito ao esquecimento.

Graus de consentimento

O artigo 9 se limita a estabelecer que os dados pessoais serão tratados com "lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares". O artigo 12 prevê que o tratamento de dados pessoais só poderá ser iniciado após a autorização do titular, no entanto, essa autorização poderá ser dada por qualquer meio. Não há menção ao conceito de consentimento e seus graus da maneira que é feita pelos outros dois projetos. Os conceitos de lealdade, boa-fé e legítimos interesses são amplos e difusos, não possuem conceituação específica no próprio projeto e não permitem uma fiscalização minuciosa sobre o tratamento que será realizado. O artigo 10 também é limitador da proteção dos dados pessoais, pois não inclui os direitos humanos, em especial o direito à liberdade de expressão e à privacidade, e do rol de objetivos fundamentais que disciplinam juridicamente o tratamento de dados pessoais, limitando-se aos direitos do consumidor e direitos econômicos.

Consentimento do titular para compartilhamento a terceiros

No artigo 14, permite-se aos responsáveis compartilhar os dados pessoais, inclusive para fins de comunicação comercial, com qualquer um que contribua direta ou indiretamente para a realização de tratamento de dados pessoais. Esse ponto é extremamente crítico. O que se autoriza a partir dessa disposição é, em seu extremo, a livre circulação de dados pessoais por uma rede enorme de empresas, órgãos públicos ou qualquer um que tenha interesse em tratar dados pessoais, mediante a autorização e o consentimento do titular a um único responsável por tratamento de dados.

Proteção para transferência internacional de dados

Quanto ao compartilhamento internacional de dados, o projeto de lei não tem uma seção específica que regule essa ação, ou seja, o compartilhamento internacional é tratado da mesma maneira que o compartilhamento realizado dentro das fronteiras brasileiras, o que é uma falha do legislador, tendo em vista as diversas implicações jurisdicionais desse assunto e em comparação aos outros dois projetos.

Proteção de dados em acesso público

O projeto de lei não se aplica a dados que estejam em acesso público, de acordo com o artigo 6, inciso IV. A lei deveria levar em consideração que, frequentemente, dados tornados públicos não tiveram o consentimento do titular para tanto ou, então, foram publicizadas de forma ilegal, tornando público uma grande quantidade de dados pessoais. Mesmo quando as informações foram tornadas públicas pelo próprio titular, é necessário considerar a expectativa de privacidade contextual. Por essa razão, ao se tratar de um dado pessoal de acesso público, deveria ser necessário o consentimento do titular.

Aplicação ao setor público como um todo, incluindo forças de segurança

O artigo 6, inciso III, exclui os "bancos de dados utilizados para a pesquisa histórica, científica ou estatística, de administração pública, investigação criminal ou inteligência" da aplicação do texto. A exclusão das atividades de investigação criminal ou inteligência da aplicação das regras sobre proteção de dados pessoais é um sério risco aos direitos individuais dos titulares de dados pessoais e é uma das recomendações que elaboramos a todos os projetos de lei mais adiante em nossa análise.

Delimitação de pesquisa estatística

No mesmo trecho citado no item anterior, as pesquisas estatísticas ficam de fora da aplicação do projeto de lei. Essa é outra disposição problemática, pois não é feita a delimitação do que se entende por pesquisa estatística, quem pode realizá-la e com quais finalidades, sendo também uma das recomendaçẽos a todos os projetos mais à frente neste estudo.

VII. Recomendações a todos os projetos de lei

Os projetos de leis gerais em tramitação no Congresso Nacional para proteção de dados pessoais —nomeadamente PL 5276/2016, PLS 330/2013 e PL 4060/2012— oferecem diferentes garantias ao direito à privacidade. Como visto anteriormente, em todas as propostas, ainda é necessário harmonizar a proteção de dados pessoais com os direitos fundamentais da liberdade de expressão e o direito à informação. Neste capítulo, apresentamos recomendações gerais aos três projetos de leis analisados. São pontos que as propostas não trataram de maneira adequada e deveriam constar em uma boa lei de proteção de dados pessoais.

Aprofundar o órgão regulatório

Nenhum dos projetos de lei cria um órgão público específico e independente para lidar com a questão da proteção de dados pessoais. Aquele que mais se aproxima de tal determinação é o PL 5276/2016, que estabelece atribuições e responsabilidades bastante específicas para a regulação e a fiscalização da implementação da lei por um órgão competente a ser designado na regulamentação da lei. Tais disposições são um bom começo, no entanto, logo não serão suficientes. A ausência de um órgão independente levanta sérias preocupações sobre as possibilidades da lei ser implementada consistentemente e efetivamente sobre todos os setores. Cerca de 90% das leis de proteção de dados ao redor do mundo possuem uma autoridade independente para proteção de dados[22].

São dois os principais problemas resultantes da ausência de um órgão independente. Primeiramente, os titulares dos dados serão abandonados com o ônus da iniciativa, sem a expertise adequada, e tendo que enfrentar uma distribuição desigual de interesses, pois estão limitados à iniciativa individual. Em segundo lugar, como resultado, o tempo para que a lei se torne efetiva será muito mais longo, tomando um tempo maior para que os princípios e as medidas se tornem claros para que tenham algum impacto preventivo.

Além disso, a ARTIGO 19 defende que o Estado crie um órgão relacionado à sociedade da informação, que regule a proteção aos dados pessoais, mas que se estende em suas atribuições, tornando-se responsável por todas as questões que surgem com a ocupação do ciberespaço e a crescente importância dele na vida das pessoas.

Menção expressa à Lei de Acesso à Informação

Somente o PL 5276/2016, elaborado no interior do Ministério da Justiça, no âmbito da Secretaria Nacional de Defesa ao Consumidor, refere-se explicitamente à Lei de Acesso à Informação. Tal menção é necessária quando o tratamento de dados pessoais é feito por órgãos da administração pública, mesmo que a aplicação da LAI já esteja subentendida, pois reforça a obrigação de transparência. De acordo com o artigo 31, parágrafo 3, inciso V, da LAI, informações pessoais podem ser publicadas sem consentimento se forem necessárias para a proteção do bem público e o interesse geral. Esse dispositivo da lei tem gerado bons resultados, como a divulgação de remunerações de funcionários públicos que recebem

22 Graham Greenleaf, Global data privacy laws 2015: DPAs and their organisations, Privacy Laws & Business. International Report, maio de 2015.

supersalários ilegalmente. A lei de proteção de dados pessoais prestes a ser aprovada não pode obstaculizar os avanços obtidos com a LAI, como por exemplo, impedir que dados como os desse exemplo só possam ser publicados com o consentimento dos funcionários que recebem esses salários, fato que iria impedir a publicização por completo.

A Declaração de Princípios sobre a Liberdade de Expressão da OEA, por exemplo, prevê que "leis sobre privacidade não devem inibir ou restringir a investigação e a disseminação de informação de interesse público" e que " autoridades públicas estão sujeitas a um escrutínio mais rigoroso da sociedade." [23]

Em análises anteriores, a ARTIGO 19 propôs a seguinte definição sobre a "questão de interesse público", a qual propomos, novamente, por entender que se aplica também a este caso:

A expressão "questão de interesse público" é definido expansivamente de modo a incluir todos os tópico relativos ao interesse público. Isso inclui, mas não só: os três poderes constituídos —e, em particular, assuntos relacionados a figuras e autoridades públicas— política, saúde pública e segurança, aplicação da lei e a administração da justiça, interesses consumeristas e sociais, o meio ambiente, assuntos econômicos, o exercício do poder, arte e cultura. Contudo, ele não inclui, por exemplo, assuntos puramente privados, sobre os quais o interesse público é meramente de curiosidade ou sensacionalista.

Por fim, a ARTIGO 19 tem duas principais recomendações para conciliar a LAI a um projeto de lei de proteção de dados pessoais:

- O projeto de lei de proteção de dados pessoais deve isentar especificamente informação sobre atividades públicas e funções de autoridades públicas e daqueles que exercem qualquer tipo de função pública;

- O projeto deve reconhecer o trecho que trata do interesse público na lei de nº 12.527/2011 sobre acesso à informação mantidas por órgãos públicos e assegurar que o interesse público seja sempre considerado.

Evitar interpretações que possam ensejar reivindicações do direito ao esquecimento

O conceito de autodeterminação informativa — presente especialmente nos projetos 5276/2016 e 4020/2012— não deve legitimar interpretações que operacionalizam o direito ao esquecimento, assunto que deve ser tratado de forma independente da discussão de um projeto de lei sobre proteção de dados pessoais e que necessitaria de um tratamento específico. O direito ao esquecimento geralmente se refere a uma solução que, em algumas circunstâncias, permite aos indivíduos demandarem a buscadores o cancelamento da lista de informações que aparecem sobre eles após uma pesquisa por seu nome. Soluções existentes devem ser aplicadas, como as oferecidas por leis de proteção à honra e também soluções baseadas nos termos e condições dos provedores, ao invés de reconhecer o direito ao esquecimento. Além disso, qualquer direito ao esquecimento deve ser estritamente limitado, com certos requisitos mínimos que devem ser cumpridos para que tal direito seja compatível com o direito à liberdade de expressão, tanto em termos materiais como processuais.

Aplicação ao setor público como um todo, incluindo forças de segurança

Todos os projetos possuem exceções para as atividades de investigação das forças públicas de segurança. Mesmo o PLS 330/2013, do senador Antônio Carlos Valadares (PSB-SE), que aborda o assunto, cria uma possibilidade de tratamento de informação tão ampla para "fins de segurança do Estado e da sociedade", que basicamente permite às autoridades de segurança enquadrarem qualquer motivação nessa hipótese. Não há porque estabelecer essa exceção. Justifica-se que ela seria necessária para as atividades de investigação de casos que precisam de agilidade na resolução. No entanto, nos últimos anos, constatou-se a construção de aparatos de vigilância pelos governos nacionais ao redor do mundo, incluindo o Brasil, no qual os alvos são todas as pessoas que estiverem ao alcance. O vigilantismo indiscriminado é uma realidade e é necessário que se imponham limites razoáveis para o tratamento de dados pessoais pelos órgãos públicos, em especial os de segurança. O consentimento do titular é primordial, assim como a possibilidade de acompanhar o tratamento que se faz. A privacidade é um direito humano fundamental, e como tal, só pode ser limitado pelo que é claramente estabelecido por lei, para propósitos limitados, sendo necessários e proporcionais. A criação de regulações paralelas, que não se incorporam completamente aos cuidados estabelecidos em lei, enfraquece a proteção dos titulares dos dados.

Delimitação de pesquisa estatística

Todos os projetos de lei permitem o tratamento de dados pessoais para a realização de pesquisa estatística. No entanto, não há uma delimitação precisa sobre os alcances e limites dessas atividades no texto da lei, podendo gerar brechas que permitam entidades privadas ou o setor público justificar ilegalmente atividades de tratamento de dados sem o consentimento dos titulares baseando-se nessa prerrogativa. Por essa razão, os projetos de lei devem definir o que se entende por pesquisa estatística, os possíveis atores que executam este tipo de atividade e as finalidades de tais pesquisas.

23 https://www.cidh.oas.org/basicos/portugues/s.Convencao.Libertade.de.Expressao.htm.

VIII. Garantias dos projetos de lei face aos casos concretos

O uso indevido de dados pessoais já é recorrente no Brasil. Nesta seção, a proposta é simular a aplicação de cada um desses projetos de lei em casos reais de violações à privacidade já ocorridos no Brasil, ou que têm reflexos no contexto nacional, e comparar os diferentes níveis de proteção aos dados pessoais oferecidos aos usuários[24]. Foram selecionados diversos casos, desde vazamento de informações de um banco de dados pessoais à discussão sobre o uso de criptografia em aplicativos de mensagens instantâneas, passando por ações de vigilância estatal e as configurações das Smart TVs que atualmente são comercializadas.

24 Claramente, as possibilidades de interpretações de uma lei pode ocorrer de diversas maneiras e nossa simulação é apenas uma das diversas análises possíveis.

SMART TV

O caso e os projetos de lei

As Smart TVs vendidas no Brasil captam o áudio das conversas ao seu redor. As fabricantes alertam seus clientes por meio da política de privacidade e dos termos de uso que acompanham o produto a não conversarem perto do aparelho sobre temas confidenciais ou íntimos, já que o aparelho, além de gravar os sons à sua volta, também pode enviá-los a terceiros, como empresas terceirizadas que são responsáveis pela ferramenta de áudio do dispositivo. Isso muda o modo de interação tradicional dos telespectadores. De certo modo, agora o televisor também assiste ao telespectador.

Em 2013, um blogueiro do Reino Unido realizou testes na sua Smart TV LG e constatou que a televisão estava enviando dados para os servidores da LG, inclusive arquivos de um pen drive que ele conectou ao dispositivo. Um detalhe interessante é que mesmo quando a opção para a transferência de dados havQWia sido desligada, a Smart TV continuou a transmitir os dados para os servidores da companhia. Ao questionar a fabricante sobre os fatos, o blogueiro recebeu uma simples resposta de que ele havia assinado os termos de uso e serviço quando comprou o televisor e que esse tipo de reclamação deveria ser feita ao vendedor do aparelho.

(Fontes da notícia: http://doctorbeet.blogspot.com.br/2013/11/lg-smart-tvs-logging-usb-filenames-and.html; http://noticias.r7.comrecord-news/jornal-da-record-news/videos/rosana-hermann-comenta-caso-de-invasao-de-privacidade-atraves-de-smart-tv-17102015; http://exame.abril.com.br/tecnologia/noticias/samsung-pede-que-clientes-evitem-discutir-assuntos-pessoais-em-frente-de-sua-smarttv)

PL 5276/2016

A constatação de que as Smart TVs repassam a terceiros as informações por ela coletadas, mesmo os dados pessoais de um pendrive conectado a ela, vai contra o princípio da necessidade, que o PL 5276/2016 prevê em seu artigo 6. Segundo o projeto, o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. O conteúdo do pendrive do usuário claramente não é necessário para a funcionalidade da Smart TV. Mas não somente essa ação pode ser considerada desproporcional. O simples fato da coleta de aúdio já viola os princípios da finalidade e da adequação, expostos no artigo 6 da lei. O primeiro prevê que "o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades". O segundo presume que "o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento" , ou seja, a compra de um televisor, ao menos em princípio, não deve implicar na cessão dessa quantidade de dados pessoais, tendo em vista que o televisor consegue realizar suas funções normalmente sem gravar tudo o que acontece ao seu redor, o que ultrapassaria sua finalidade. Por sua vez, muitos consumidores não esperam que, ao comprar um um aparelho de TV, sejam monitorados de forma ostensiva como demonstrado, o que viola a questão das legítimas expectativas do titular, sob o princípio da adequação.

PLS 330/2013

No artigo 4, inciso I, este projeto estabelece como princípio que "a coleta, armazenamento e processamento de dados pessoais devem ser limitados a finalidades determinadas". Além disso, o PL prevê responsabilização e prestação de contas por parte dos responsáveis pelo tratamento. O artigo 29 estabelece que os responsáveis por esses dados devem implementar um programa de governança em privacidade que demonstre as práticas adotadas pelo responsável e sua adequação à lei, com garantias de supervisão das atividades e que conte com mecanismos de participação dos titulares de dados. Essas disposições protegem os consumidores que não concordam com a transferência de dados realizada pelas Smart TVs, permitindo-lhes agir judicialmente contra as configurações que a fabricante da Smart TV implementou nos aparelhos, assim como participar de mecanismos no interior dessa empresa que promovam melhores políticas de privacidade em seus aparelhos.

2 RASTREADOR DE NAMORADO

Em 2013, um app chamado "Rastreador de Namorado" chamou a atenção por permitir monitorar as principais atividades de outra pessoa pelo celular, a partir das mensagens enviadas e recebidas, o registro de chamadas, e se o aparelho esteve desligado ou em modo avião. Para tanto, o app tem de ser instalado no aparelho do "namorado" e configurado para notificar o celular da "namorada". Todas as atividades relacionadas acima eram notificadas diretamente à namorada por meio de mensagens SMS.

(Fonte da notícia: http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/08/sem-consentimento-app-rastreador-de-namorado-e-ilegal-diz-advogado.html; http://rastreadordenamorado.com.br/app)

O caso e os projetos de lei:

PL 4060/2012

No artigo 14, fica permitido que responsáveis pelo tratamento realizem o compartilhamento dos dados tratados com parceiros do mesmo grupo econômico ou ainda para terceiros. Além disso, não há no PL uma discussão aprofundada sobre consentimento, desdobrando-o como fazem os outros projetos em diversos tipos de autorização que o usuário pode fornecer ao responsável pelo tratamento. Isso limita a moderação sobre quais dados devem ser tratados pela Smart TV nos termos de uso e serviço que a fabricante estabelece com o cliente.

PL 5276/2016

Segundo o PL5276/2016, no artigo 9, o consentimento do titular dos dados deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique. O app permite que qualquer pessoa com acesso ao celular de terceiros faça o download e torne o aparelho rastreável, ou seja, mesmo que o aplicativo requeira em seus termos de uso o consentimento de ambas as partes para seu funcionamento, é um risco claro que um dos namorados instale o aplicativo sem que o outro saiba. Para evitar

tal desídia, a implementação do consentimento granulado, aquele que estende no tempo, periodicamente informando o titular do tratamento dos seus dados, pode ser uma saída.

PLS 330/2013

O PLS 330/2013, no artigo 4, inciso V, requer o consentimento livre, específico, inequívoco e informado do titular de dados como requisito à coleta de dados e ainda prévio e expresso em caso de dados sensíveis, o que pode ocorrer nesse caso, já que o aplicativo "Rastreador de Namorado" permite um monitoramento completo das comunicações desenvolvidas no aparelho. Dessa maneira, caso o aplicativo de rastreamento fosse instalado sem o consentimento do dono do celular, a vítima estaria coberta pela lei de proteção de dados pessoais.

PL 4060/2012

Já o PL 4060/2012 não possui uma disposição clara sobre o consentimento para tratamento de dados pessoais. Suas únicas ressalvas sobre o assunto estão presentes nos artigos: 17, o único a utilizar a palavra consentimento, no qual se dispõe que o tratamento de dados pessoais de crianças só será permitido com o consentimento de seus pais; e 12, no qual se requer a "autorização" para o tratamento de dados pessoais sensíveis, exclusivamente. Portanto, o membro do casal que tivesse instalado em seu aparelho o aplicativo de rastreamento estaria menos resguardado sob a lei de proteção de dados pessoais, caso o PL 4060/2012 seja aprovado.

3 TUDO SOBRE TODOS

Em 2015, surgiu na rede um site de nome Tudo sobre Todos, no qual era possível consultar dados pessoais a partir de seu nome ou CPF. O modo de obtenção dessas informações é obscuro e provavelmente ilegal. A publicação desses dados na internet de forma desprotegida e sem consentimento dos titulares se trata de um ataque frontal contra a privacidade dos cidadãos brasileiros.

A analista de planejamento Aline Oracic teve seus dados vazados e conta que ficou "bem assustada" ao ver expostas informações sobre ela, seus vizinhos e pessoas com quem mora. "Veja bem, se a pessoa precisa usar uma ferramenta como essa é porque eu não quero que ela tenha essas informações. Uma ferramenta dessas não foi desenvolvida para fins legais e não traz benefícios nenhum à população. Perigosíssimo esse site", diz.

(Fonte da notícia: http://renatoleitemonteiro.jusbrasil.com.br/artigos/217037831/protecao-de-dados-10-motivos-porque-o-site-tudo-sobre-todos-e-ilicito)

O caso e os projetos de lei:

PL 5276/2016

O funcionamento do site Tudo sobre Todos viola uma série de princípios de proteção a dados pessoais, tais quais a proteção à privacidade (caput art 2), a inviolabilidade da intimidade, da vida privada, da honra e da imagem (art. 2,III), a finalidade (art. 6, I), a adequação (art. 6, II), a necessidade (art. 6, III), o consentimento (art. 7, I) e basicamente todos os outros princípios da lei.

PLS 330/2013

O site Tudo Sobre Todos estaria em flagrante ilegalidade de acordo com o texto desse projeto de lei. Os artigos 4 e 5 estabelecem princípios e determinações sobre o tratamento de dados pessoais e dados pessoais sensíveis, respectivamente. As práticas da página vão contra diversas dessas disposições, a destacar: "coleta, armazenamento e processamento de forma lícita, com observância do princípio da boa-fé e adstritos a finalidades determinadas" (art.4, I); "consentimento livre, específico, inequívoco e informado do titular de dados como requisito à coleta de dados pessoais e, ainda, prévio e expresso, quando se tratar de dados sensíveis "(art.4,V)".

O artigo 31 da lei expõe as sanções administrativas possíveis em casos de infrações à lei, prevendo desde advertências aos responsáveis até a intervenção judicial. Nesse caso específico, além das sanções administrativas, também pode ser tratado na esfera criminal, tendo em vista o tamanho dos danos possivelmente causados pela plataforma.

PL 4060/2012

O PL 4060/2012 em seu artigo 6, inciso IV, coloca como exceção à lei, o tratamento de dados pessoais de informações de acesso público, ou seja, o projeto corrobora a defesa do site Tudo Sobre Todos, que afirma que não estaria violando nenhuma lei, pois as informações publicizadas estariam em acesso público.

CRIPTOGRAFIA E LEGALIDADE

4 O Ministério Público Federal está realizando uma investigação sobre a legalidade da criptografia utilizada pelo WhatsApp, já que ela estaria em violação do inciso XII do artigo 5º da CF, que afirma que o sigilo da correspondência dos cidadãos brasileiros é inviolável, exceto quando se tratar de uma ordem judicial. Ou seja, a criptografia do WhatsApp estaria atentando contra o direito da Justiça de investigação com base na quebra de sigilo das correspondências. A intenção do órgão investigativo é barrar o uso da criptografia, para que a Justiça tenha acesso facilitado às conversas no aplicativo quando estiver investigando casos criminais.

(Fonte da notícia: http://www.tecmundo.com.br/whatsapp/104522-mpf-investida-possivel-inconstitucionalidade-criptografia-whatsapp.htm)

O caso e os projetos de lei:

PL 5276/2016

A criptografia é reconhecidamente a melhor maneira para manter a segurança das comunicações no contexto digital, sendo esta última um dos princípios do PL 5276/2016, no artigo 6, inciso VII, que afirma que "devem ser utilizadas medidas técnicas constantemente atualizadas" para a proteção dos dados pessoais. O artigo 47, parágrafo 1º, inciso III, é o único que explicita a possibilidade de encriptação, classificando-a como uma possível medida de segurança utilizada para a proteção de dados em casos de incidentes de segurança, o que contraria a posição adotada pelo Ministério Público Federal. A proposta do MPF de tornar a criptografia ilegal parece desproporcional sob a ótica deste projeto, pois mais enfraquece a privacidade e segurança de dados pessoais durante o período de tratamento do que resolve o problema de investigação criminal de casos específicos.

PLS 330/2013

O PLS 330/2013 também prevê a possibilidade da utilização de procedimentos de encriptação em casos de incidentes de segurança que acarretem prejuízos aos titulares no artigo 24, parágrafo 1º, inciso I, harmonizando-se com a disposição anterior do artigo 22 que estabelece que o responsável deve adotar medidas técnicas atualizadas e compatíveis com os padrões internacionais. Assim como no PL 5276/2016, o PLS não só não condena o uso da criptografia, como entende que procedimentos de encriptação podem ser utilizados de maneira a dar mais segurança aos titulares de dados pessoais.

PL 4060/2012

A única menção à proteção dos dados pessoais sob a perspectiva do indivíduo se encontra no artigo 2 de forma vaga e imprecisa no qual se afirma genericamente que: todos têm "direito à proteção de seus dados pessoais." A lei só faz referência a medidas técnicas que possam assegurar maior proteção aos dados das pessoas no artigo 11, no qual o "responsável pelo tratamento de dados, bem como eventuais subcontratados, deverão adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular." Apesar de não parecer uma preocupação primordial da lei, há nela algum subsídio que pode ser usado para a defesa de técnicas de criptografia.

OI E VAZAMENTO DE DADOS

5 Em 2013, a operadora Oi foi acusada de entregar dados cadastrais de seus clientes aos provedores de conteúdo UOL e Terra. O MPF do Mato Grosso do Sul foi quem entrou com ação para investigar essa transferência de dados pessoais. A suspeita se iniciou após diversas denúncias de que os provedores citados acima começavam a ligar para oferecer seus serviços logo após a contratação da Oi. Mais do que isso, segundo a reportagem: "nas ligações feitas pelos representantes das empresas, os atendentes se passavam por funcionários da Oi e coletavam dados bancários e número do cartão de crédito dos clientes. Os consumidores eram, então, compelidos a contratar o serviço privado, para que, enfim, tivessem liberados login e senha de acesso à internet."

(Fontes da notícia: http://www.viomundo.com.br/denuncias/mpf-diz-que-oi-vazava-dados-sigilosos-de-clientes-para-uol-e-terra.html; http://www.otempo.com.br/cidades/procon-apura-fraudes-e-repasse-ilegal-de-cadastro-envolvendo-oi-uol-e-terra-1.711715)

O caso e os projetos de lei:

PL 5276/2016

Atividades como a praticada pela Oi estão proibidas de acordo com o PL de dados pessoais. A transferência a terceiros deve estar especificada e precisa contar com o consentimento do titular dos dados, segundo o caput do artigo 27.

PLS 330/2013

Os artigos 20 e 21 tratam especificamente da comunicação no tratamento de dados pessoais. A lei deixa claro que esse tipo de ação necessita do consentimento específico e próprio para ser realizada, o que já tornaria proibida as ações da Oi. Além disso, o parágrafo 2º do artigo 20 prevê que os responsáveis por causarem danos aos titulares devem responder solidariamente às acusações. O artigo 21 estabelece que em situações como essa, os órgãos competentes devem fiscalizar a comunicação e a interconexão de dados pessoais e entre outros aspectos "podendo determinar, mediante processo administrativo, que sejam assegurados o contraditório e a ampla defesa, o cancelamento dos dados, o fim da interconexão ou outras medidas que garantam os direitos dos titulares". O artigo 31 determina algumas sanções administrativas que poderiam caber à Oi neste caso, de acordo com o que o órgão competente viesse a decidir sobre as acusações. No caso mais grave, a empresa poderia até mesmo ficar proibida de realizar tratamento de dados por cinco anos, sem prejuízo de sanções de natureza civil e penal.

PL 4060/2012

A prática de transferência de dados pessoais entre empresas fica autorizada de acordo com este projeto de lei. O artigo 14 é enfático afirmando que "os responsáveis pelo tratamento de dados poderão compartilhá-los, inclusive para fins de comunicação comercial, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais."

FALHA NO APP DO BANCO DO BRASIL

Em dezembro de 2013, clientes do Banco do Brasil que utilizam o aplicativo da instituição para gerenciarem suas contas bancárias vivenciaram, por um período de quase uma hora, uma falha que permitia a visualização de dados de outros clientes do banco. O BB afirmou que o problema foi prontamente corrigido, mas isso nos mostra que, mesmo os sistema financeiros, que costumam ter protocolos de segurança elevados, podem possuir brechas graves que permitem episódios como esse para usuários comuns, que nem mesmo tentaram invadir ou quebrar a segurança do banco. Novamente, em 2016, a segurança dos sistemas de acesso online do BB, Caixa Econômica e Itaú mostraram novamente serem falhas. Um plugin "de segurança" utilizado pelos portais de acesso desses bancos revelou ter uma brecha que permite a criminosos acessarem os dados dos clientes. Segundo reportagem, "chamado de Warsaw, o plugin defeituoso em questão é utilizado por empresas como Caixa Econômica Federal, Banco do Brasil e Itaú." A falha permite que criminosos utilizem a tecnologia para instalar um malware que enganaria o internauta fazendo-o ceder seus dados para hackers.

(Fontes da notícia: http://www.ebc.com.br/noticias/economia/2013/12/banco-do-brasil-suspende-aplicativo-que-provocou-vazamento-de-dados; http://olhardigital.uol.com.br/fique_seguro/noticia/plugin-de-seguranca-dos-bancos-permite-vazamento-de-dados-dos-internautas/58113; http://meiobit.com/273531/falha-em-apps-expoe-dados-dos-clientes-do-banco-do-brasil)

O caso e os projetos de lei:

PL 5276/2016

No artigo 45, este PL afirma que o responsável pelo tratamento dos dados deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Além disso, quando uma falha ocorrer, o PL prevê no artigo 47 que o responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares. Em episódios como esses, o banco teria que prestar contas ao órgão competente, que seria o responsável pela apuração e resolução do problema e por apontar possíveis prevenções a serem adotadas para casos futuros.

PLS 330/2013

O artigo 24 deste projeto de lei prevê que na ocorrência de incidentes de segurança o responsável pelo tratamento deve comunicar imediatamente o órgão competente, mencionando no mínimo cinco pontos:

"**I** descrição da natureza dos dados pessoais afetados;

II informações sobre os titulares envolvidos;

III indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV riscos relacionados ao incidente;

V medidas que foram ou que serão adotadas para reverter ou aliviar os efeitos de prejuízo."

Por sua vez, analisando a situação, o órgão competente poderá adotar três medidas em resposta:

I pronta comunicação aos titulares;

II ampla divulgação do fato em meios de comunicação;

III medidas para reverter ou diminuir os efeitos de prejuízo.

Essa determinação de procedimentos é vital em uma sociedade da informação, pois os incidentes de segurança são rotineiros e somente com um processo institucional bem definido e robusto será possível enfrentar incidentes de segurança que efetivamente assegurem a proteção do sigilo dos dados pessoais em tratamento.

PL 4060/2012

O projeto de lei não aborda os tipos de medidas técnicas que devem ser adotadas pelos responsáveis, assim como não atribui a responsabilidade a um órgão competente ou cria um órgão para tratar da proteção a dados pessoais. Sua única disposição quanto a isso está no artigo 11, no qual se afirma que o responsável pelo tratamento deve adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular." Tais brechas de segurança ocorridas com os bancos poderiam ser interpretadas como uma falta de responsabilidade das instituições com os dados de seus clientes.

COLÉGIO BANDEIRANTES E VAZAMENTO DE DADOS DE ALUNOS

Em 2015, o tradicional Colégio Bandeirantes, de São Paulo, sofreu um vazamento de dados. Eles foram expostos em redes sociais e tinham registros de alunos, desde sua performance acadêmica até avaliações emocionais, feitas por professores e pela direção. A publicização desse conteúdo gerou mal-estar em toda a comunidade da escola, que rapidamente teceu críticas duras à direção por não ter um sistema de segurança eficiente para o armazenamento dessas informações. Muitos alunos e pais se sentiram lesados com alguns comentários feitos nas avaliações vazadas. Uma delas diz, por exemplo: "tem olheiras, boca de ódio, cara de criança de filme de suspense". O Bandeirantes sofreu fortes críticas e teve de mudar seu sistema de armazenamento. Esse episódio revela como a segurança da informação é importante em todos os âmbitos.

(Fonte da notícia: http://www.trrsecuritas.com.br/blog/2015/03/19/vazamento-de-dados-do-colegio-bandeirantes-causa-polemica/)

O caso e os projetos de lei:

PL 5276/2016

O PL requer que os responsáveis pelo tratamento de dados pessoais adotem "medidas técnicas e administrativas [...] aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão." (art 6, inciso VII), assim como medidas de prevenção (art. 6, inciso VIII), além de estabelecer um responsável pelo tratamento (art. 8, inciso III) que responda aos titulares dos dados. Ademais, por se tratar de um caso que envolve adolescentes como titulares, a lei indica em seu artigo 7, inciso IX, que o tratamento deve ser especial, com maior ênfase na proteção, segurança e sigilo. Por fim, o artigo 14 afirma que o tratamento de dados pessoais de crianças e de adolescentes deve se dar no seu melhor interesse, de acordo com a legislação pertinente, a ver o Estatuto da Criança e do Adolescente. Esta disposição é interessante, pois além de incluir a proteção dos dados pessoais na lei mais geral sobre o tratamento à criança e ao adolescente, o princípio do melhor interesse nega a concepção clássica de que o menor de idade deva ser completamente tutelado por seus responsáveis e tenta dar voz ao interesse do menor na questão, ou seja, a vontade do jovem passa também a ser levada em consideração.

PLS 330/2013

O artigo 14 da lei se refere ao tratamento de dados pessoais de criança e pessoa absolutamente incapaz, que só poderá ser realizado com consentimento dos pais ou responsáveis e no melhor interesse do jovem, e deve levar em consideração outras duas condições:

"**I** autorização condicionada à supervisão, assistência ou anuência do responsável legal;

II respeito à sua condição pessoal, podendo os responsáveis legais revogar o consentimento para tratamento de dados pessoais a qualquer tempo."

Portanto, de acordo com este projeto de lei, as escolas que tratam dados de seus alunos devem explicitar este procedimento no ato da matrícula e a qualquer momento os responsáveis estariam autorizados a revogar seu consentimento sobre a operação.

PL 4060/2012

O artigo 17 deste projeto estabelece que o tratamento de dados pessoais de crianças só poderá ser realizado mediante o consentimento de seus pais, responsáveis legais ou por imposição legal. É importante dar tratamento especial para o tratamento de dados pessoais de menores de idade, no entanto, o tratamento dado não leva em consideração a vontade do titular, como é feito no PL 5276/2016, que utiliza o princípio do melhor interesse da criança e do adolescente.

ACESSO NÃO AUTORIZADO DE FUNCIONÁRIOS

Outra situação que o acesso a grandes bases de dados possibilita é o assédio por parte de funcionários de empresas que oferecem, entre outros, serviços como internet, telefonia e TV a cabo a clientes ou a possíveis clientes. Em 2015, várias pessoas, em especial mulheres, relataram casos nos quais atendentes entraram em contato com elas após ter oferecido um pacote de serviços, utilizando o número da base de dados da empresa. Alguns, mesmo depois pedidos para encerrar a conversa, insistiam em continuar. Esse acesso a um grande número de telefones e e-mails a pessoas sem a devida responsabilidade e competência pode gerar inúmeros casos de abusos, assédios ou até mesmo perseguição. Por isso, é necessária uma política criteriosa sobre o acesso a bases de dados cadastrais dentro das empresas.

(Fontes da notícia: http://taedai.com.br/quando-o-perigo-bate-a-porta; http://www.administradores.com.br/noticias/negocios/consumidores-denunciam-assedio-de-atendentes-de-telemarketing/101538/)

O caso e os projetos de lei:

PL 5276/2016

No artigo 5, incisos VIII,IX e X, o projeto de lei prevê três figuras distintas que fazem parte da operação do tratamento:

- O responsável (a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais);
- Operador (a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável);
- E o encarregado (pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente).

A figura do encarregado é parte da resposta a casos como esse, pois atua como ponte entre o titular e o órgão que realiza o tratamento dos dados e seus operadores. O encarregado, em casos como esse, deve ser ágil em responder a essas práticas de violação e vazamento de dados, indicar responsáveis e auxiliar os titulares.

No capítulo VII, sobre segurança e boas práticas, está expresso que o responsável pelo tratamento dos dados pessoais, no artigo 45, deve adotar medidas de segurança técnicas e ad-

ministrativas aptas a proteger os dados pessoais de acessos não autorizados; no artigo 46, estipula-se que "o sigilo sobre os dados é obrigatório a todo agente de tratamento ou pessoa que teve acesso aos dados"; no artigo 47, torna-se dever do responsável a "comunicação ao órgão competente de qualquer incidente de segurança que acarrete risco ou prejuízo aos titulares"; o artigo 48 prevê que o órgão competente é responsável por "averiguar o ocorrido e determinar ao responsável a adoção de providências", sendo possível até uma determinação de adoção de medidas técnicas que evitem que terceiros voltem a acessar os dados pessoais de titulares.

PLS 330/2013

O artigo 18 deste projeto de lei estipula alguns cuidados que os proprietários e gestores de bancos de dados devem ter em relação ao sigilo e ao acesso às informações. O inciso I deste artigo prevê que o responsável deve impedir "que pessoas não autorizadas tenham acesso aos equipamentos, instalações e suportes de tratamento de dados." O inciso II pede a garantia de que "somente pessoas autorizadas tenham acesso aos dados transmitidos". Dessa forma, de acordo com este projeto, um atendente de serviços não poderia reter dados pessoais de clientes da empresa para qual trabalha. Também sobre essa questão, o artigo 24, parágrafo 3º, impõe ao órgão encarregado a responsabilidade de verificar se foram adotadas medidas técnicas adequadas para evitar o acesso não autorizado. Essas medidas propostas pelo projeto parecem indicar um bom caminho para o combate e a prevenção de novos casos de acessos não autorizados a dados pessoais por funcionários de empresas com grandes bancos de dados pessoais.

PL 4060/2012

O artigo 20 do projeto de lei prevê que os responsáveis pelo tratamento devem assegurar aos titulares amplo acesso à política de privacidade adotada, com informações acerca da utilização dos dados coletados. O projeto ainda permite a um grande fluxo de trocas e compartilhamentos de dados entre os responsáveis de dados sem o consentimento específico dos titulares para cada um deles no artigo 14. A permissão conferida aos responsáveis pode desencadear um cenário no qual os dados pessoais dos titulares serão dificilmente monitorados por estarem compartilhados em um grande número de bases de dados pessoais, o que aumenta a possibilidade de vazamentos e assédios como visto no caso acima.

CASO ESCHER E ESCUTAS TELEFÔNICAS

9 Para demonstrar que as violações à privacidade não se encerram somente ao contexto digital, citamos na coletânea o caso Escher, no qual o Brasil foi condenado pela Corte Interamericana de Direitos Humanos (CIDH), em julho de 2009, a indenizar trabalhadores rurais de cooperativas ligadas ao Movimento Sem-Terra em razão de interceptações telefônicas irregulares realizadas no Paraná em 1999. As interceptações, que duraram 49 dias, foram autorizadas judicialmente em decisões não fundamentadas, após requerimento de autoridade não competente (Polícia Militar), fora do âmbito de uma investigação criminal corrente e sem notificação do Ministério Público, em flagrante desrespeito à Lei das Interceptações Telefônicas.

O caso e os projetos de lei:

PL 5276/2016

Apesar do tratamento de dados que trata o PL 5276 não se aplicar ao tratamento de fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais (art 4, inciso III), ele é importante, pois eleva os parâmetros de proteção e segurança aos dados pessoais, estabelecendo princípios (art 6) que também devem ser levados em conta pelas autoridades da área da segurança, como a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção e a não discriminação.

PLS 330/2013

O PLS 330/2013, em seu artigo 2, parágrafo 3º, determina que esta lei não se aplica aos bancos de dados mantidos pelo Estado exclusivamente para fins de defesa nacional e segurança pública. No entanto, à frente, no artigo 19 do projeto, são estabelecidos limites à atuação nesse âmbito, da seguinte maneira:

"**I** exercício de competência prevista em lei;

II prevenção ou repressão de infração penal, administrativa ou tributária;

III compartilhamento de informações para fins de segurança do Estado e da sociedade;

IV atendimento dos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte."

Por conta dessa exceção feita aos órgãos de segurança, o projeto não teria aplicação direta no caso em questão, sendo que as violações cometidas estariam sujeitas a outras normas e regulamentos, como a lei de interceptações telefônicas.

PL 4060/2012

Segundo o artigo 6, o projeto de lei não se aplica a bancos de dados de administração pública, investigação criminal ou inteligência. Ou seja, uma ação similar a essa, caso se repita, teria de levar em consideração outros marcos regulatórios.

(Fonte da notícia: http://terradedireitos.org.br/wp-content/uploads/2009/08/Cronologia_Interceptacoes.pdf)

PRIVACIDADE DO "POKÉMON GO"

10 O "Pokémon Go" tornou-se um dos jogos mais populares no Brasil na metade de 2016. Seu lançamento foi o mais aguardado do ano e sua jogabilidade transformou a experiência do uso de aparelhos móveis para muitos usuários. O jogo de realidade aumentada permite aos jogadores andarem pelas ruas e calçadas de suas cidades "caçando" pokémons. O mapa do jogo é o mapa da cidade. Logo, começaram as questões sobre a possibilidade do jogo estar espionando ou monitorando seus jogadores, os lugares aonde vão e, ainda, as imagens que cedem enquanto estão jogando, já que é necessário estar sempre com a câmera do aparelho celular ligada para jogar. Houve uma polêmica logo no lançamento do "Pokémon Go",

pois ele solicitava informações e permissões excessivas do usuário e de seu aparelho, como saber a página da web que o usuário acessou antes de abrir o app, assim como ler e escrever e-mails por você. A Niantic, empresa desenvolvedora do game, logo diminuiu o nível de acesso do "Pokémon Go" aos dados e aplicações após a má repercussão, tornando os termos da política de privacidade do jogo mais aceitáveis e equiparáveis a outras aplicações de jogos. Contudo, nem todas as questões são abordadas nessa política e duas delas nos interessam neste estudo. A primeira se refere ao item 5 da política de privacidade do "Pokémon Go", em que está expresso que, após o término ou desativação da conta ou contrato, a Niantic, seus clientes, afiliados ou provedores de serviço podem reter informações e conteúdo de usuário por um período comercialmente razoável para fins de fazer uma cópia de segurança, arquivamento ou auditoria. Já a segunda se relaciona à transferência internacional dos dados feita pelo aplicativo e na qual fica autorizada a transferência de dados para países que possuem uma política de proteção de dados inferior a do país de origem.

O caso e os projetos de lei:

PL 5276/2016

Este projeto de lei aborda as duas questões levantadas na política de privacidade destacada. O artigo 18, inciso VI, diz que é direito do titular requerer a eliminação, a qualquer momento, de dados pessoais que tenham sido cedidos por ele. Ou seja, a política de privacidade do "Pokémon" estaria em desacordo com a lei nacional caso o projeto de lei fosse aprovado. O segundo ponto, referente à transferência internacional de dados, é abordado pelo capítulo V da lei. No artigo 33, inciso I, fica determinado que a transferência internacional de dados só é permitida para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta lei. Um terceiro ponto interessante que faz parte do debate diz respeito ao princípio da necessidade, pois não fica claro o porquê da política de privacidade do "Pokémon Go" requerer tantos dados e por tanto tempo. O PL 5276/2016 limita o tratamento somente aos dados pertinentes, proporcionais e não excessivos.

PLS 330/2013

O projeto de lei, em seu artigo 6, inciso VII, prevê a "exclusão definitiva, a seu requerimento e ao término da relação entre as partes, dos seus dados pessoais em quaisquer bancos de dados, ressalvadas outras hipóteses legais que incidem sobre a guarda de dados." Não há mais detalhes sobre o que seria entendido como outras hipóteses legais, portanto, não há como definir se a cláusula na política de privacidade do "Pokémon Go" estaria em desacordo com a lei ou não.

Sobre a transferência internacional de dados, o projeto estabelece no artigo 26 que ela só se realizará para países com mesmo grau de proteção de dados, com aval do órgão competente, o que torna ilegal a cláusula existente na política de privacidade do "Pokémon Go".

PL 4060/2012

O artigo 16 do projeto prevê que quando ocorra a cessão ou o bloqueio do tratamento dos dados, o responsável só poderá compartilhá-los ou conservá-los para finalidades históricas, estatísticas ou de pesquisa científica. Ou seja, não seria permitida a conservação dessas informações para fazer cópia de segurança, arquivamento ou auditoria, como está expresso na política de privacidade do Pokémon Go. Contudo, a lei autoriza o tratamento de dados em território estrangeiro no artigo 4, sem muitas restrições, o que autorizaria o procedimento em países que tenham um nível de proteção de dados pessoais inferior.

WHATSAPP INTEGRADO AO FACEBOOK

11 Em 25 de agosto de 2016, o aplicativo de mensagens instantâneas WhatsApp anunciou que mudaria sua política de privacidade, compartilhando sua base de dados com a plataforma do Facebook, empresa que comprou o aplicativo em 2014. Dessa maneira, os usuários foram instados a escolher entre aceitar ou não o compartilhamento de seus dados, tendo como prazo limite para optar pelo não compartilhamento o dia 25 de setembro de 2016. Aqueles que não responderam até essa data tiveram seus dados compartilhados. A transferência de dados é um assunto que os três projetos de lei deste estudo abordam de formas diferentes.

O caso e os projetos de lei:

PL 5276/2016

Este PL autoriza a transferência de dados a terceiros com o consentimento do titular. No entanto, em seu artigo 16, inciso III, a lei permite que, após o término da relação de tratamento de dados, a conservação das informações poderá ocorrer caso a finalidade seja transferência a terceiros. Ou seja, caso um usuário do WhatsApp deixe de usar a ferramenta, seus dados poderiam ser conservados no Facebook, caso todos os requisitos estivessem de acordo com o restante da lei. Esse é um ponto problemático, pois abre possibilidade para que as empresas transfiram dados para conservá-los a despeito dos objetivos originais.

PLS 330/2013

O PLS 330 estabelece que a comunicação ou interconexão de dados somente será realizada quando o titular consentir de forma específica no artigo 20. Além disso, o segundo parágrafo prevê que, em caso de dano decorrente da comunicação, os responsáveis pelo tratamento devem responder solidariamente, o que permite aos titulares que se sentirem lesados com esta ação do Facebook possam levar a cabo suas reclamações. Por fim, o artigo 21 prevê que as autoridades administrativas competentes devem fiscalizar toda comunicação e a interconexão de dados pessoais. Ou seja, caso este projeto de lei estivesse em vigor, o processo de comunicação entre bases de dados pessoais feito de forma independente teria uma fiscalização.

PL 4060/2012

O artigo 14 permite que ocorra a transferência e o compartilhamento dos dados pessoais pelos responsáveis "a terceiros que, direta ou indiretamente, contribuam para a realização de seus tratamentos."

APLICATIVOS PARA CONTROLE DO CICLO MENSTRUAL

12 Dentre os vários aplicativos desenvolvidos diariamente, uma nova tendência tem se mostrado particularmente preocupante. Os aplicativos que prometem a mulheres um maior controle sobre o ciclo menstrual e suas implicações no organismo têm acumulado um número significativo de dados sensíveis que estão sendo comercializados com empresas de vendas de dados. As informações fornecidas pelas usuárias do aplicativo variam desde os dias de seu período menstrual até informações como a última vez e em que posição tiveram relações sexuais ou se estiveram doentes, quais sintomas tiveram e como se trataram. Estes dados são de extremo valor para empresas que anunciam produtos e serviços de saúde, como fabricantes de remédio ou seguradoras.

O caso e os projetos de lei:

PL 5276/2016

O artigo 7, inciso IX desta lei prevê que o tratamento de dados pessoais é permitido "quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade." Os aplicativos de controle sobre o ciclo menstrual atuam claramente na intersecção apontada pelo inciso, sendo que o interesse das usuárias pela utilização e compartilhamento de seus dados sensíveis devem prevalecer ante o interesse do responsável. No artigo seguinte, também está expresso que o responsável deve disponibilizar de forma clara, adequada e ostensiva a finalidade do tratamento (I), os sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão (V).

O artigo 11 se refere ao tratamento de dados pessoais sensíveis, que fica proibido, exceto em casos nos quais haja o consentimento livre, inequívoco, informado, expresso e específico em quase todos os casos, com raras exceções. Dessa maneira, os aplicativos de controle do ciclo menstrual teriam de informar detalhadamente a suas usuárias cada possibilidade de tratamento dos dados que foram inseridos, inclusive as atividades de terceiros. Além disso, mesmo com o consentimento das mulheres, o tratamento de dados pessoais sensíveis deve contar com um modo de segurança mais robusto e tecnologicamente atualizado.

PLS 330/2013

No artigo 15, o projeto prevê que o tratamento de dados pessoais sensíveis é proibido, exceto nos casos que se tenha o expresso e específico consentimento de seu titular ou representante legal, e em outros casos mais específicos e excepcionais. Essa obrigação forçaria o aplicativo a obter o consentimento de suas usuárias, descrevendo todas as possibilidades de tratamento e atores envolvidos no processo. Isto é, o que hoje ocorre de forma implícita, deverá ser feito com a certeza de que as usuárias leram e estão informadas sobre todas as possibilidades de tratamento de seus dados.

PL 4060/2012

O artigo 14 deste projeto permite o compartilhamento de dados pelos responsáveis de forma irrestrita, dentro do próprio grupo econômico do qual fazem parte ou a terceiros, inclusive para fins de comunicação comercial. Ou seja, não haverá restrições ao funcionamento dos aplicativos caso esta lei seja aprovada.

Há uma ressalva para o tratamento de dados pessoais sensíveis. O artigo 12 deste PL requer a autorização do titular dos dados. Contudo, ele permite que a licença seja dada por qualquer meio, e não da maneira como é feita nos outros dois projetos —em relação ao grau de consentimento. Ou seja, a autorização pode ser dada da maneira com que estamos hoje acostumados: somente clicando em um botão, aceitando qualquer proposição que esteja nos termos de uso e serviço do aplicativo.

CADASTRO ÚNICO DE PESSOAS PRIVADAS DE LIBERDADE

13 Em 24 junho de 2016, o Conselho Nacional de Política Criminal e Penitenciária (CNPCP) criou e regulamentou o Cadastro Único de Pessoas Privadas de Liberdade da Unidade Penal, o CadUPL. A ideia do cadastro, segundo o órgão, é a criação de um "instrumento de transparência e uniformização de dados estatísticos mínimos, a ser avaliado quando das inspeções e fiscalizações jurídicas das unidades penais." Além do Cadastro Único, que permitirá às polícias e aos poderes Judiciário e Executivo um controle maior sobre as informações relativas às pessoas privadas de liberdade, um grande banco de dados pessoais será estruturado. Nesse caso, diversos órgãos públicos terão acesso a essas informações, como fica explícito nos artigos 4º, 5º, 6º da Resolução nº 2/2016, que tratam das obrigatoriedades de compartilhamento desse cadastro com órgãos do poder Executivo estadual (parágrafo único, art 4º), ao próprio CNPCP (artigo 5º) e a possibilidade a do auxílio de preenchimento do cadastro pela Defensoria Pública. Além disso, o parágrafo único do artigo 5º requer que o CNPCP publique em seu site oficial um relatório trimestral do cadastro, como um "instrumento de Transparência em Estatística e Indicadores da execução penal". Apesar da importância do controle estatístico e de transparência sobre o cadastro de pessoas privadas da liberdade, em nenhum momento da resolução se trata da questão da privacidade e do sigilo dos dados dessas pessoas. É importante lembrar que estão sendo tratados dados pessoais sensíveis, que requerem um procedimento especial, pois a depender de como sejam preenchidos ou por quem forem acessados ou alterados, podem causar impactos diretos na vida da pessoa em privação de liberdade, seja enquanto ela ainda estiver restrita ou já ressocializada. Além disso, deve-se apontar funcionários responsáveis em cada um destes órgãos com autorização de acesso ao cadastro, que serão os únicos a lidar com a tabela e responderem por seu preenchimento.

O caso e os projetos de lei:

PL 5276/2016

O projeto de lei prevê que o órgão competente pela fiscalização e implementação das medidas para proteção de dados pessoais tem responsabilidade também sobre o nível de privacidade com que órgãos de segurança tratam dados pessoais. O parágrafo 3º, do artigo 4, prevê que "o órgão competente emitirá opiniões técnicas ou reco-

mendações referentes às exceções previstas nos incisos II e III e poderá solicitar aos responsáveis relatórios de impacto à privacidade." O inciso III trata precisamente dos órgãos de segurança. Por sua vez, não há nenhuma menção à privacidade no teor da Resolução nº2/2016 do CNPCP.

Também há uma seção do projeto de lei 5276/2016 que trata exclusivamente do tratamento de dados pessoais pelo poder público. O artigo 24 prevê que os órgãos públicos devem publicar os detalhes sobre o tratamento de dados que realizam, preferencialmente em seus sites. Essa medida é contemplada no parágrafo único do artigo 5º da Resolução nº2/2016 da CNPCP que obriga a entidade a publicar na página oficial um "relatório trimestral intitulado CadUPL Trimestral por UF, como instrumento de Transparência em Estatística e Indicadores da execução penal." Vale ressaltar que este relatório deve ser publicado com dados anonimizados, ou seja, que não permitam a identificação das pessoas privadas de liberdade.

PLS 330/2013

Diferentemente do PL 5276/2016, o PLS 330 não tem uma seção específica para o tratamento de dados realizado por pessoas de direito público. No artigo 5, fala-se da não aplicação deste projeto de lei para órgãos de segurança pública prevista no artigo 2, parágrafo 3º, que permite que o CadUPL seja operacionalizado sem a garantia das proteções previstas no projeto, desde que seja respeitado o que é estabelecido no artigo 19, como as obrigações de realizar o tratamento considerando as seguintes hipóteses:

"I exercício de competência prevista em lei;

II prevenção ou repressão de infração penal, administrativa ou tributária;

III compartilhamento de informações para fins de segurança do Estado e da sociedade;

IV atendimento dos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte.

Infelizmente, interpretamos que o projeto de lei é insuficiente para garantir a proteção necessária dos dados pessoais de apenados incluídos no CadUPL.

PL 4060/2012

O artigo 6º, inciso III, exclui os bancos de dados de administração pública do escopo do projeto. Portanto, o caso não seria objeto desta lei, caso o PL vier a ser aprovado.

VIGILÂNCIA ESTATAL

14 Em 2013, ocorreram centenas de manifestações populares em todo o país. Iniciou-se com a organização de um movimento contra o aumento das tarifas do transporte público, mas ganhou proporções que extrapolaram em muito esse tópico. Naquela época, uma reportagem[25] publicada no jornal O Estado de S.Paulo revelou que a Agência Brasileira de Inteligência havia montado uma equipe para monitorar as organizações dos protestos no Facebook, Twitter, Instagram e até no WhatsApp, um aplicativo de mensagens que não possui interface pública, e que por isso requer uma quebra de sigilo de comunicação dos usuários. Esse tipo de ação não é permitida pela legislação brasileira e seria como a prática de um grampo telefônico sem ordem judicial, uma violação do artigo 5, inciso XII da Constituição Federal e da lei 9.296/96, que regulamenta esta questão. Além disso, o monitoramento de dados pessoais que estejam em acesso público não dá o direito a forças policiais ou de inteligência de processar, analisar e autorizar operações com base neles, pois, mesmo estando em acesso público, os titulares destes dados deveriam forneceram seu consentimento para que seus dados fossem assim utilizados.

25 Abin monta rede para monitorar internet. 19/06/2016 Disponível em:http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500 Acesso em:17/10/2016.

O caso e os projetos de lei:

PL 5276/2016

O artigo 7, §4º, relativo aos dados que estão em em acesso público, estipula que tais dados devem ter o mesmo tipo de tratamento que aqueles que se encontrem em acesso privado, necessitando, portanto, de consentimento do titular. No entanto, este projeto de lei, no artigo 4, inciso III, já havia determinado que esta lei não se aplica ao tratamento de dados realizado "para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais". Ou seja, o sistema Mosaico não estaria violando nenhuma lei enquanto estivesse monitorando somente dados pessoais de acesso público.

PLS 330/2013

Este projeto de lei não se aplica aos "bancos de dados mantidos pelo Estado exclusivamente para fins de defesa nacional e segurança pública", segundo o artigo 2, parágrafo 3º, o que já torna difícil analisar outros pontos desta lei. Entretanto, desconsiderando esse primeiro impeditivo, analisamos que não há menção explícita sobre o tratamento de dados pessoais em acesso público no projeto de lei. Ou seja, o projeto não diferencia dados pessoais pela maneira como são coletados, levando-nos à conclusão de que todo dado pessoal, esteja em acesso público ou não, está sujeito ao consentimento do titular para a autorização do início do tratamento. Isso poderia significar que órgãos públicos não poderiam realizar varreduras online e começar a tratar dados pessoais das pessoas no Brasil sem que elas consentissem.

PL 4060/2012

Este PL não se aplica aos banco de dados utilizados para investigação criminal ou inteligência nem ao tratamento de informações de acesso público, conforme expresso no artigo 6, incisos III e IV, respectivamente. Ou seja, estariam autorizados os tipos de monitoramento praticados pela ABIN sobre o Facebook, Instagram e Twitter.

Sobre o ARTIGO 19

A ARTIGO 19 é uma organização não-governamental de direitos humanos nascida em 1987, em Londres, com a missão de defender e promover o direito à liberdade de expressão e de acesso à informação em todo o mundo. Seu nome tem origem no 19º artigo da Declaração Universal dos Direitos Humanos da ONU.

Com escritórios em nove países, a ARTIGO 19 está no Brasil desde 2007 e tem se destacado por impulsionar diferentes pautas relacionadas à liberdade de expressão e informação. Entre as quais, estão o combate às violações ao direito de protesto, a descriminalização dos crimes contra a honra, a elaboração e a implementação da Lei de Acesso à Informação e a construção e defesa do Marco Civil da Internet.

Contando com especialistas de diferentes campos, a organização atualmente se divide em quatro áreas: Acesso à Informação, Centro de Referência Legal, Direitos Digitais e Proteção e Segurança.

Se você quiser entrar em contato para discutir esta análise, por favor, envie um e-mail para **comunicacao@artigo19.org.br.**

ARTIGO 19 Brasil
Edifício das Bandeiras Rua João Adolfo, 118 - Conjunto 802
Centro - São Paulo – SP - 01050-020, Brasil

T: +55 (11) 3057 0042
E: comunicacao@artigo19.org
www.artigo19.org