Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais

Ao tratar da proteção de dados pessoais, o Brasil busca suprir uma demanda legislativa cada vez mais central, principalmente dado o crescimento dos fluxos de informação que ocorreu nos últimos anos e a importância que seu processamento adquiriu tanto para os setores público quanto privado.

O Anteprojeto de Lei (APL) de Proteção de Dados Pessoais, submetido à consulta pública pelo Ministério da Justiça, não surge em um contexto de completa ausência legal. O Brasil conta com normas difusas que regulam o direito à privacidade. Desde a Constituição Federal, que, por exemplo, considera inviolável a vida privada e a intimidade, até dispositivos presentes no Código Civil e Penal, no Código Brasileiro de Defesa do Consumidor, entre outros. Além disso, a aprovação do Marco Civil da Internet (Lei 12.965/2014) constituiu um importante avanço ao reforçar a necessidade de proteção no âmbito digital.

No entanto, o APL busca preencher lacunas importantes na legislação brasileira no que diz respeito à proteção de dados pessoais, que possui uma série de fundamentos e princípios específicos. Como recorda Doneda (2006),

> **[...] a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada a por esta, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento brasileiro.**

Os desafios que se apresentam para tal tarefa são muitos e, cabe destacar, não foram ainda solucionados pela academia ou por legisladores em outros países. A Europa, por exemplo, que conta com uma diretiva de proteção de dados pessoais aprovada em 1995 (a Diretiva 95/46/EC), discute, desde 2012, a reforma de seu marco legal buscando atualizar e fortalecer os seus princípios de proteção. Apesar de pioneira, essa norma se encontra em grande medida obsoleta em relação às novas tecnologias de informação e comunicação.

Ainda que siga sendo uma referência na área, a norma europeia atual não pode ser tomada como único modelo possível, sendo necessárias inovações que dêem conta dos novos desafios, considerando as particularidades do ordenamento jurídico e da história e cultura brasileiras. A consulta pública do Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais se mostra, assim, uma oportunidade única de envolver os diversos setores para pensar soluções que possam unificar e organizar o marco legal existente e que, ao mesmo tempo, considerem o cenário que se apresenta internacionalmente no que diz respeito ao processamento e transmissão de informações.

Nesse sentido, o Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (CTS-FGV), que tem colaborado com o Ministério da Justiça desde a elaboração do Marco Civil da Internet, considera fundamental a iniciativa e apresenta suas considerações sobre o texto colocado em debate público.

Conscientes dos diversos aspectos que poderiam ser discutidos no contexto do estabelecimento de um marco legal de proteção de dados pessoais, optamos por tratar de alguns temas centrais que - justamente pela dificuldade em se encontrar um modelo a ser seguido - têm sido alvo de intensos debates na academia e entre a sociedade civil e legisladores no âmbito internacional. Nos esforçamos para oferecer propostas concretas de alteração da redação atual sempre que possível, porém, dada a complexidade de certos assuntos, em outros casos apresentamos um panorama das diversas alternativas esperando, sempre, oferecer subsídios para as discussões futuras que ocorrerão no contexto da tramitação do futuro projeto de lei.

Na presente contribuição trataremos dos seguintes pontos:

- **A teoria do diálogo de fontes como orientadora para a harmonização da interpretação da futura lei de proteção de dados pessoais às demais normas que tratam o tema;**
- **O conceito de dados pessoais e o tratamento de dados dissociados;**
- **As obrigações do Estado como responsável pelo tratamento de dados;**
- **O modelo de autogerenciamento da privacidade, suas limitações e possíveis abordagens;**
- **A importância da criação de uma autoridade garantidora independente de proteção de dados pessoais;**
- **Os conceitos de *privacy by design* e *privacy by default* como princípios orientadores da proteção de dados pessoais;**
- **O direito à portabilidade.**

Teoria do diálogo de fontes e a vulnerabilidade do titular de dados

Uma das questões que se colocam com a futura Lei de Proteção de dados pessoais é como ela vai dialogar com outras normas que já regulam o tratamento de dados pessoais e o direito à privacidade. Cabe ressaltar que tal lei se encontrará inserida em um sistema de normas que, muitas vezes, aparentam ser inconciliáveis. A título de exemplo, as seguintes normas tratam, ao menos em algum aspecto, de temas relativos à privacidade e proteção de dados pessoais:

- **Código de Processo Penal[1] (Lei 3689/41)**
- **Código de Defesa do Consumidor[2] (Lei 8078/90)**
- **Estatuto da Criança e do Adolescente[3] (Lei 8.069/90)**
- **Lei de Interceptação das Comunicações Telefônicas (Lei 9296/96)**
- **Lei do Habeas Data[4] (Lei 9507/97)**
- **Lei Geral das Telecomunicações (Lei 9.472/97)**
- **Código Civil[5] (Lei 10.406/02)**
- **Lei de Acesso à Informação[6] (Lei 12.527/11);**
- **Bancos de Perfis Genéticos para fins de investigação criminal[7] (Lei 12.654/12 e Decreto 7.950/13)**
- **Lei das Organizações Criminosas (Lei 12.850/13)**
- **Marco Civil da Internet[8] (Lei 12.965/14)**
- **Lei de Identificação Criminal[9] (Lei 12.037/09)**
- **Lei do Processo Eletrônico[10] (Lei 11.419/06)**

A ideia de um possível conflito entre normas nos remete à Teoria do Diálogo de Fontes, que defende a ideia de que o ordenamento jurídico deve ser interpretado de forma unitária, afastando o entendimento de que as leis devem ser aplicadas de forma isolada uma das outras. Idealizada pelo jurista alemão Erik Jayme, foi trazida ao Brasil pela jurista Claudia Lima Marques, especialmente no contexto do Novo Código Civil de 2002 e sua relação com o Código de Defesa do Consumidor de 1990, e passou a orientar a aplicação das normas consumeristas no Brasil.[11]

---

[1] Disponível em http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm

[2] Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Os artigos 43, 44 e 51 guardarão relação com a futura lei.

[3] Disponível em http://www.planalto.gov.br/ccivil_03/Leis/l8069.htm. O artigo 100, V, prevê o direito a privacidade na aplicação de medidas de proteção sempre que os direitos das crianças e adolescentes forem violados ou ameaçados. Além disso, todos os direitos previstos na lei deverão nortear o tratamento de dados de crianças e adolescentes.

[4] Disponível em http://www.planalto.gov.br/ccivil_03/leis/l9507.htm

[5] Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm Ver artigos 19 e 21.

[6] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[7] Disponíveis em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12654.htm e http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7950.htm.

[8] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[9] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm

[10] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm

[11] A respeito do contexto em que a aplicação da teoria se fez necessária no Brasil, Claudia Marques (2004) afirmou que: "No Brasil de hoje, a construção de um Direito Privado com função social, proposta por Jhering e Gierke, e o futuro da

Naquela época, diante da coincidência de matérias abordadas no Novo Código Civil e no Código de Defesa do Consumidor, eventual sobreposição de uma norma sobre a outra representaria a diminuição de garantias ao consumidor e, ao invés de se construir um cenário de proteção e promoção de direitos, acabaria por representar retrocesso legal.

Com o objetivo de superar a insuficiência dos critérios clássicos de resolução das antinomias jurídicas (hierarquia, especialidade e cronologia), a Teoria do Diálogo de Fontes defende que as diferentes normas não excluam a aplicação umas das outras, mas se complementem. Assim, as normas com campos de aplicação convergentes devem ser interpretadas de forma coordenada, coerente e sistemática, em consonância com os preceitos constitucionais.

O exemplo do sistema de coexistência de leis desenvolvido no âmbito do direito do consumidor pode ser interessante para se pensar o contexto da proteção dos dados pessoais.[12]

A aplicação dessa teoria em relação à protetiva de dados pessoais afasta a ideia de que a futura lei consista em um microssistema jurídico isolado das demais normas que possuem campo de aplicação convergente. Almeja-se a aplicação coordenada e sistemática das normas jurídicas com o objetivo de proteger o titular de dados contra a violação de sua privacidade.

No caso das relações consumeristas, o diálogo entre normas tem como um dos parâmetros o princípio de reconhecimento da vulnerabilidade do consumidor no mercado de consumo estabelecido no Código de Defesa do Consumidor (art. 4°, inciso I), de forma que a aplicabilidade das normas deve ser aferida de acordo com o que representar maior proteção ao consumidor.

Para Moraes (2009):

> **Vulnerabilidade, sob o enfoque jurídico, é, então, o princípio pelo qual o sistema jurídico positivado reconhece a qualidade ou condição daquele(s) sujeito(s) mais fraco(s) na relação de consumo, tendo em vista a possibilidade de que venha(m) a se ofendido(s) ou ferido(s), na sua incolumidade física ou psíquica, bem como no âmbito econômico, por parte do(s) sujeito(s) mais potente(s) da mesma relação.**

Em relação ao titular de dados, da mesma forma, se pode dizer que existe uma relação assimétrica entre o responsável pelo tratamento e o titular. Essa vulnerabilidade pode se revelar em diversos aspectos[13], como:

- **Vulnerabilidade técnica - na medida em que o titular não possui conhecimentos específicos sobre o tratamento de dados a que suas informações pessoais estão sujeitas.**

Justiça para os mais fracos nos tribunais brasileiros está a depender do grau de domínio, que os aplicadores da lei conseguirem alcançar neste momento, sobre o sistema de coexistência do Direito do Consumidor, presente no CDC, e do Direito Civil e Direito Comercial das Obrigações, presente no CC/2002. A tarefa de especialização e de excelência no uso das normas de direito do consumidor renova-se.

[12] É verdade que em muitos casos o titular de dados estará inserido em uma relação de consumo e, de qualquer forma, protegido pela incidência do Código de Defesa do Consumidor. No entanto, os conceitos de titular de dados e consumidor não se confundem, na medida em que haverá ocasiões em que o titular de dados deverá ser protegido na categoria de cidadão, e não consumidor.

[13] Definições comumente apontadas em relação à vulnerabilidade do consumidor.

Diante da complexidade do mundo moderno, em que não é possível dominar todos os processos em que se está envolvido, o titular de dados acaba por ter como único aparato a confiança na boa fé da outra parte;

- **Vulnerabilidade jurídica - também entendida como inerente à vulnerabilidade técnica, diz respeito às dificuldades que o titular de dados enfrente na luta para a defesa de seus direitos, seja na esfera administrativa ou judicial;**
- **Vulnerabilidade política ou legislativa - decorre da falta de organização do titular de dados brasileiro, já que inexistem associações ou órgãos "capazes de influenciar decisivamente na contenção de mecanismos legais maléficos que acabam gerando verdadeiros monstrengos jurídicos" (Moraes, 2009);**
- **Vulnerabilidade psíquica ou biológica - o titular de dados é atingido por uma infinidade de estímulos que influenciarão na sua decisão de se comportar de determinadas formas em relação aos seus próprios dados pessoais. "Essa motivação pode ser produzida pelos mais variados e eficazes apelos de marketing possíveis à imaginação e à criatividade orientada pelos profissionais da área"[14];**
- **Vulnerabilidade econômica e social - especialmente no que diz respeito às organizações privadas, essa vulnerabilidade diz respeito às disparidades de força entre os agentes de tratamento de dados e os titulares.**

É nesse contexto que se reconhece a existência de uma heteronomia - a imposição de regras de uma parte à outra - e não a autonomia das vontades quando um dos participantes é vulnerável (Braga Netto, 2014). É o que acontece na relação entre responsável e titular de dados, em que a vulnerabilidade do titular impede que exista uma real autonomia das vontades. Assim, em substituição à heteronomia levada a cabo pelos responsáveis pelo tratamento de dados, o próprio Estado se adianta a regular, através de processo legislativo democrático, de forma a reequilibrar a relação de forças entre responsáveis e titulares de dados. Isso porque quanto maior for a desigualdade, mais intensa deverá ser a proteção ao direito fundamental em jogo, e menor a autonomia privada (Sarmento, 2004).

Diante dessa conjuntura, assim como se reconheceu na ocasião do advento do Novo Código Civil em relação ao Direito do Consumidor (consumidor x produtores), deixar o titular de dados desassistido (não intervenção estatal), apostando na autocomposição na relação com o responsável pelo tratamento de dados, seria uma medida que acabaria por contrariar o princípio de igualdade material. A relação entre os sujeitos envolvidos no tratamento de dados deve ser equilibrada com alguma intervenção do Estado. A própria regulação consiste em uma forma de intervenção com esse objetivo.

Nesse sentido, nos parece importante que a futura lei faça menção à vulnerabilidade do titular de dados, o que permitiria que tal princípio oriente a interpretação de normas nos casos em que haja eventual conflito com outras normas a fim de harmonizar as diversas leis que regulam matérias relativas a tratamento de dados.

O processo de harmonização deve permitir que normas anteriores sejam reinterpretadas a partir dos princípios de proteção de dados pessoais contidos na futura lei. Da mesma forma que, no

[14] Nesse sentido, vale lembrar a política de *pop-ups* de solicitações a respeito de cookies, em que, sobrecarregado diante de tantas solicitações, o titular de dados online sequer lia o que estava escrito e aceitava sem ponderações.

momento da inovação legislativa consumerista, a nova lei - mais geral - não revogou as anteriores nem as mais especiais se sobressaíram , sendo que todas passaram a integrar um único sistema de proteção do consumidor, defendemos que a nova norma atue no mesmo sentido: incrementando a proteção de dados em um sistema que reconheça a vulnerabilidade do titular de dados.

O diálogo de fontes permitirá, por exemplo, que o artigo 421 do Código Civil - que afirma que a liberdade de contratar será exercida nos limites da função social do contrato - seja plenamente aplicável nas situações de incidência da futura protetiva de dados. O mesmo vale para o imperativo da boa-fé (art. 422, CC) e o de que nenhuma convenção prevalecerá se contrariar preceitos de ordem pública ou a função social do contrato e da propriedade (art. 2035, CC).

O alerta de Claudia Lima Marques no momento do ineditismo de uma lei protetiva dos consuimidores também nos serve para o contexto do anteprojeto em discussão:

> Quem, neste momento, for ingênuo e seguir as primeiras visões do CC/2002 repetindo os preceitos do Direito Civil dos iguais do século XIX ou do CC1916, contribuirá para o fim do Direito Comercial e para um esvaziamento inconstitucional do Direito do Consumidor. Quem for ingênuo e seguir os modelos eruditamente colocados como definitivos de direito comparado, sem um distanciamento crítico e rigor científico, transformará o Código Civil em centro não só do Direito Privado, mas do direito econômico, desconstruindo as conquistas de tratamento diferenciado do Direito Comercial e da sociedade de consumo de massas no mercado brasileiro. A hora é de especialização e rigor, de atenção e estudo, pois a reconstrução do direito privado brasileiro identificou 3 sujeitos: o civil, o empresário e o consumidor, mesmo se os princípios do CC/2002 e CDC são - em geral - os mesmos! Vejamos.

A futura lei de proteção de dados pessoais, da mesma forma, deverá ter a capacidade de dialogar de forma harmônica com as demais leis, sob pena de ser esvaziada em diversos aspectos ou acabar por representar retrocesso em casos mais específicos em que já havia sido regulamentada a proteção em outras leis.

A lógica aqui proposta extrai de todo o ordenamento jurídico a proteção mais ampla e sistematizada possível e, ao reconhecer a vulnerabilidade do titular de dados, transfere o "peso" do dever de cautela contra eventuais violações ao responsável pelo tratamento de dados e não ao titular de dados.

Dessa forma, além da sugestão de que a Teoria do Diálogo de Fontes possa coordenar a harmonização entre leis aplicáveis quando a lei de proteção de dados pessoais for uma realidade, propomos a seguinte alteração ao Art. 1º da redação atual do anteprojeto, para instrumentalizar essa harmonização:

Texto atual	Texto sugerido
Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade,	Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural, atendido o

intimidade e privacidade da pessoa natural.	**princípio de reconhecimento da vulnerabilidade do titular de dados.**

A definição de dados pessoais e o tratamento dos dados dissociados

Existem diferentes perspectivas teóricas sobre o conceito de dados pessoais. Elas incluem abordagens reducionistas, expansionistas e até mesmo a defesa de que não se deve limitar a interpretação a uma definição específica, já que se trata de um conceito em constante transição. Essa discussão é central no âmbito legislativo, uma vez que envolve a compreensão sobre quais tipos de dados e atividades estariam cobertos pela norma.

Tanto o APL quanto o texto da reforma da legislação europeia atualmente em discussão trazem abordagens expansionistas quanto à definição de dados pessoais. No caso brasileiro, a redação do art. 5º, inciso I, afirma que trata-se de "dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos". Adiante, no inciso IV do mesmo artigo, afirma que dados anônimos são "dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular".

A partir da leitura conjunta das duas definições, pode-se inferir que a diferença entre dados pessoais e dados anônimos residiria na conceituação de quais seriam os "meios razoáveis". Ou seja, se a reidentificação puder ser feita utilizando-se um meio razoável, estaríamos falando de um dado pessoal. Caso contrário, o dado seria considerado anônimo. Uma vez que: a) a definição de dados pessoais afirma que esses dados são dados identificados ou identificáveis; b) a natureza dos dados anônimos é a de não serem identificáveis por meios razoáveis (mas podem ser identificados por meios "não-razoáveis", que empreguem recursos, expertises, etc., pouco acessíveis atualmente); então, é preciso concluir que dados anônimos devem ser considerados, por definição, identificáveis e, por isso, são dados pessoais, protegidos na forma da lei. Qualquer interpretação em contrário deixaria uma grande quantidade de dados potencialmente identificáveis desprotegidos.

Seria benéfico, por conseguinte, tornar ainda mais clara a leitura conjunta das definições de dados pessoais e dados anônimos, de modo a prevenir futura situação de insegurança jurídica. Isso se faz particularmente necessário porque o artigo 1º do anteprojeto define que "Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural". Dessa forma, poder-se-ia aventar que a lei se aplica a dados pessoais, mas não a dados anônimos. Entretanto, como mencionado anteriormente, dados anônimos são dados pessoais.

Na Europa, a Diretiva 95/46/CE define como dado pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável ('pessoa em causa')". Afirma ainda que "é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social."

Deriva-se da atual redação europeia que quaisquer dados que permitam identificar um indivíduo são protegidos pela Diretiva. Vale destacar que o termo "direta ou indiretamente" não encontra

correspondência no anteprojeto brasileiro, mas que pode servir como inspiração para a modificação da atual versão, a fim de fortalecer a esfera de proteção. O texto, porém, não define em maior detalhe quando se considera que um indivíduo pode ser identificado, valendo como regra geral que a possibilidade de identificação é suficiente para garantir a proteção.

Segundo o art. 5º, inciso XIV do anteprojeto de lei de proteção de dados pessoais, a dissociação seria:

> **XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;**

O processo de dissociação consiste em remover as informações pessoalmente identificáveis de um conjunto de dados, com a intenção de que as pessoas a quem os dados descrevem não sejam identificadas. Seriam dados em que, a princípio, não seria possível identificar o seu titular, ou seja, que "buscam alcançar o anonimato" e não "dados anônimos" de fato.[15]

A autoridade inglesa de proteção de dados Information Comissioner's Office (ICO) afirma em seu "Guia Prático de Anonimização: Gerindo o risco da proteção de dados" que como padrão de segurança para a proteção de dados pessoais, a dissociação consiste em uma ferramenta muito valiosa que permite que dados sejam compartilhados de forma a explorar seu enorme valor econômico e social, ao mesmo tempo que, garantida a eficiência do processo, é preservada a privacidade do titular de dados. [16]

Essa assunção permitiu que as técnicas de dissociação - tidas como instrumentos de proteção da privacidade dos titulares de dados - passassem a viabilizar a retenção e o compartilhamento indiscriminado de informações pessoais e fundamentou diversos debates, leis e outras formas de regulação da privacidade.[17]

Inicialmente, cabe destacar que o fato de um dado não estar relacionado a um nome não significa que não consista em dado pessoal. Isso porque a mera individualização de uma pessoa é capaz de afetar a sua privacidade, seja através de identificadores eletrônicos atribuídos pelo próprio responsável pelo tratamento de dados, por outras ferramentas como o IP do computador ou mesmo com a agregação de dados.

Por esse motivo, a organização European Digital Rights (EDRI) defende que:

> **Em muitos casos, não é necessário que o controlador de dados possa identificar uma pessoa específica para tomar atitudes que afetem a sua privacidade;**

---

[15] "We must also correct the rhetoric we use in information privacy debates. We are using the wrong terms, and we need to stop. We must abolish the word anonymize; let us simply strike it from our debates. A word that should mean, "try to achieve anonymity" is too often understood to mean "achieve anonymity," among technologists and nontechnologists alike. We need a word that conjures effort, not achievement." (Ohms, 2010)

[16] Anonymisation: managing data protection risk code of practice. Guia da Information Comissioner's Office (ICO), autoridade de proteção de dados inglesa. Disponível em https://ico.org.uk/media/1061/anonymisation-code.pdf.

[17] Nos Estados Unidos, os estatutos federais de privacidade apresentam exceções para aqueles que dissociam dados. Na União Europeia, a Directiva de Protecção de Dados fundamenta-se na garantia da tecnologia de anonimização ao definir "dados pessoais."

> **singularizar a pessoa pode ser suficiente. Isso deve refletir na definição do sujeito de dados, que deve incluir o aspecto de singularização. Por outro lado, a definição de "dados anônimos" deve ser evitada, na medida em que poderia aumentar o risco de se criar brechas, se a definição não for perfeita. Esse tipo de falha pode ser explorada por controladores para contornar as regras da regulação.**

Assim, dados inicialmente não definidos como dados pessoais podem ser utilizados para identificar um indivíduo, e, cada vez mais, é possível realizar a identificação usando menos dados. Apesar de o CEP não ser primordialmente um dado pessoal, por exemplo, pode assumir essa condição dependendo do contexto em que seja inserido. Um estudo recente demonstrou que o agregado das três informações de CEP, data de nascimento e gênero levam à individualização, ou seja: não existem dois indivíduos diferentes em que esses três dados coincidam.

Como destaca Paul Ohm, a ciência da reidentificação demonstrada em estudos recentes minou a fé depositada nas técnicas de dissociação, de forma que a partilha de dados de forma indiscriminada e o armazenamento perpétuo de dados já não se justifica pela garantia de privacidade. Dito isso, os elaboradores de lei deveriam, segundo o autor, reanalisar suas regulamentações e se perguntar se o poder de reidentificação e a fragilidade das técnicas de dissociação comprometem seus objetivos originais.

É nesse contexto, em que já se discute o "mal entendido"[18] a respeito dessa técnica em relação a proteção da privacidade, que o Brasil passa a discutir a regulamentação de proteção de dados. O atraso regulatório[19] em relação a diversos outros países pode ser, ao menos nesse aspecto, considerado positivo, na medida em que permite que o país se valha das experiências anteriores e possa partir de pontos mais avançados da discussão em relação aos dados dissociados. Sendo assim, considerando a definição de dados pessoais presente no Anteprojeto de Lei, que é abrangente o suficiente para alcançar os dados identificáveis, reconhecer os dados dissociados como identificáveis, como demonstram as pesquisas recentes, seria o suficiente para identificar o seu caráter de dados pessoais e garantir a proteção decorrente da incidência da futura lei.

Levando em consideração a necessidade de incluir os dados dissociados dentro do escopo da futura legislação, é preciso discutir a respeito da melhor estratégia legislativa para fazê-lo.

O Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPOPAI) apresentou contribuição em que apresenta a opção pela exclusão do termo dissociação e da definição de dados anônimos e a incorporação da definição do processo de anonimização como "o ato de tornar um dado não correlacionável ao seu titular, utilizando-se de técnicas que procurem não identificá-lo, direta ou indiretamente, com um indivíduo. Os dados anônimos são, para fins desta lei, dados pessoais em razão da reversibilidade de seu processo, ainda que disponham de regras próprias nos termos desta legislação."

---

18 Paul Ohm (2010) destaca que as recentes revelações a respeito da possibilidade de reidentificação de titulares de dados anonimizados por cientistas da computação mostrou que houve um mal entendido em relação ao poder dessa técnica como protetiva da privacidade, erro que fundamentou diversos debates, leis e outras formas de regulação da privacidade. Sendo assim, o autor busca fornecer ferramentas para responder a esse "fracasso".

19 Para consultar o mapa de países que já contam com legislações de proteção de dados, consultar o mapa de David Banisar: National Comprehensive Data Protection/Privacy Laws and Bills 2014, disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

Nos filiamos a essa posição, ainda que reconheçamos que o termo "anonimização" é controverso no âmbito internacional.[20] A utilização do termo dissociação, por sua vez, representaria apenas uma das formas de "anonimização"[21] e, por isso, Paul Ohm o considera inadequado, adicionando a preocupação de que muitos acabam assumindo os dados dissociados com promessas de solidez, quando, na realidade, métodos de dissociação podem ser robustos ou fracos. Nesse sentido, defende que sempre que o termo "dissociação" fosse empregado, se deveria perguntar se representa uma dissociação "robusta" ou "fraca".[22]

O Conselho da União Europeia chegou a adotar pelo termo "pseudonimização"[23] em sua proposta de reforma da diretiva europeia, tendo em conta que os pseudônimos, não consistem em dados anônimos e, pelos motivos já expostos, são identificáveis. No entanto, reconhece que o fato de previrem a pseudonimização como método de reduzir riscos não implica no afastamento das outras medidas de proteção de dados exigidas na legislação.[24]

Considerando o exposto em relação à definição de dados pessoais e ao processo de dissociação, propomos algumas alterações ao artigo 5, incisos I e IV:

> **Art. 5º Para os fins desta Lei, considera-se:**
>
> **I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, direta ou indiretamente, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;**
> **IV - Anonimização: ato de tornar um dado não correlacionável ao seu titular, utilizando-se de técnicas que procurem não identificá-lo, direta ou indiretamente, com um indivíduo.**
> **Parágrafo único: Os dados anônimos são, para fins desta lei, dados pessoais em razão da reversibilidade de seu processo, ainda que disponham de regras próprias nos termos desta legislação.**

[20] Como esclarece Latanya Sweeney, o termo anônimo implica que o dado não pode ser manipulado ou relacionado de forma a identificar um indivíduo. Nesse sentido, Paul Ohm critica o termo "anonimização" por ser suscetível a confundir com a ideia de dados anônimos que não seriam passíveis de reidentificação.
[21] Refere-se à forma de "anonimização" chamada por Paul Ohm (2010) de "release-and-forget anonymization".
[22] "Although "deidentify" carries less connotative baggage than "anonymize," which might make it less likely to confuse, I still find it confusing. "Deidentify" describes release-and-forget anonymization, the kind called seriously into question by advances in reidentification research. Despite this, many treat claims of deidentification as promises of robustness,227 while in reality, people can deidentify robustly or weakly.228 Whenever a person uses the unmodified word "deidentified," we should demand details and elaboration." (Ohm, 2010)
[23] A definição constante na proposta de reforma do Conselho afirma que a pseudonimização "é o tratamento de dados pessoais, de modo que não possam mais ser atribuídos a um titular específico, sem o uso de informações adicionais, desde que essa informação adicional seja mantida separadamente e sujeita a medidas técnicas e organizativas para assegurar a não-atribuição a uma pessoa identificada ou identificável.
[24] 23a) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of 'pseudonymisation' through the articles of this Regulation is thus not intended to preclude any other measures of data protection.

As obrigações do Estado como responsável pelo tratamento de dados (artigos 2º e 4º)

O Anteprojeto de Lei de Proteção de Dados Pessoais (APL) deixa claro, já em seu artigo 2º, que abrange o tratamento de dados tanto por agentes privados, quanto públicos.

> **Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:**
> **I – a operação de tratamento seja realizada no território nacional; ou**
> **II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.**

De acordo com o texto do APL, todas as garantias e obrigações presentes na lei, portanto, são igualmente aplicáveis às entidades públicas e privadas, desde que realizem qualquer operação de tratamento de dados pessoais por meio total ou parcialmente automatizado. Nesse ponto, cabe ressaltar que a limitação do escopo da lei aos tratamentos automatizados pode implicar a ausência de proteção em uma série de situações em que o tratamento ocorra de forma não automatizada, e pode resultar em violações aos princípios da legislação proposta e o objetivo expresso em seu art. 1º:

> **Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.**

A preocupação do legislador com o avanço tecnológico e o consequente crescimento dos fluxos de informação é compreensível. No entanto, dada a ausência de uma regulamentação unificada sobre o direito à privacidade e proteção de dados pessoais no Brasil, a limitação da proposta de lei ao tratamento automatizado poderia restringir significativamente sua aplicação. No âmbito internacional observa-se que o escopo das leis de proteção de dados pessoais inclui o tratamento não automatizado, como é o caso da Diretiva 95/46/CE, documento que orienta a adoção de normas de proteção de dados pessoais nos países membro da União Europeia, que no art. 3º afirma:

> **A presente directiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.**

Apesar do texto do APL explicitamente incluir as atividades do Estado em seu escopo de aplicação, ele contém exceções e especificações que merecem uma análise atenta e transversal, já que por vezes podem dar margem à relativização das obrigações do Estado e de agentes privados com relação a certos tipos de tratamento de dados pessoais.

No referido artigo 2º, por exemplo, o parágrafo 3º afirma o seguinte:

§ 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Abaixo sugerimos a alteração do texto de modo a deixar claro que tal tipo de transferência somente poderá ser feita quando previsto em concessão ou permissão para a realização de uma atividade específica que demande o compartilhamento de certos tipos de dados pessoais. Além disso, nos parece fundamental o acréscimo de uma limitação adicional para seu tratamento e retenção nos casos das exceções previstas no parágrafo 3º.

Texto atual	Texto sugerido
Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que: [...] § 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.	Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, bem como ao tratamento por meios não automatizados, de dados pessoais, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que: [...] § 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado. § 4º Os dados mencionados no § 3º devem ser definitivamente excluídos após o período de vigência do contrato de concessão ou permissão ou da prestação do serviço terceirizado que demandou o compartilhamento. § 5º As entidades privadas mencionadas no § 3º deverão comprovar a capacidade para garantir a segurança de dados a que se refere esta lei antes de sua contratação. § 6º Cabe ao órgão ou entidade pública comprovar a necessidade de transferência de

	dados pessoais para entidade privada, sob pena de responsabilização.

No artigo 4º, a lei exime o Estado e agentes privados de suas obrigações em relação ao cumprimento da lei em dois casos específicos: (i) fins de segurança pública, defesa e segurança do Estado e (ii) atividades de investigação e repressão de infrações penais. O parágrafo único especifica que o tratamento de dados nos dois casos mencionados anteriormente é vedado a entidades privadas a não ser que ocorram sob tutela de órgãos e entidades públicas.

> **Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.**
> **Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.**

Em primeiro lugar, parece importante destacar que o argumento da segurança pública, defesa e segurança do Estado não pode justificar o tratamento arbitrário de dados pessoais e que a existência de regras específicas para reger o acesso por parte das agências de inteligência não pode levar à erosão dos direitos e liberdades fundamentais, inclusive a privacidade, liberdade de expressão e pensamento e a presunção da inocência.

O grupo de trabalho Article 29 analisou a aplicabilidade dos princípios de proteção de dados pessoais às autoridades responsáveis pela realização de atividades relacionadas à segurança pública, defesa, segurança do Estado ou atividades de investigação e repressão de infrações penais. O relatório ressalta a importância de se determinar com clareza a finalidade do tratamento de dados nesse tipo de atividade, uma vez que isso afeta o cumprimento de outros princípios, como o de adequação e necessidade, na linguagem do texto brasileiro. Para o grupo, a limitação insuficiente dos propósitos, unida à ausência de evidências para demonstrar que determinada medida atende a uma necessidade social urgente, não se encontraria em consonância com os ditames da proteção de dados pessoais.

> **O princípio da limitação de propósitos se refere à compreensão do porquê certos dados pessoais são processados. [...] Isso permite o melhor cumprimento do princípio da minimização dos dados. O princípio da minimização existe para garantir que somente uma quantidade mínima de dados pessoais seja processada para se atingir o propósito determinado. Esses princípios da proteção de dados pessoais se relacionam de forma muito próxima com o conceito de proporcionalidade no contexto da privacidade.**[25]

[25] Article 29 Working Party. Opinion 01/2014 on the "Application of necessity and proportionality concepts and data protection within the law enforcement sector". Parágrafo 5.7, tradução nossa.

A ordem constitucional brasileira prevê a presunção de inocência, assim como o direito à privacidade, o sigilo das comunicações e dados dos cidadãos[26], como direitos fundamentais no Art. 5º. Tal sigilo somente pode ser quebrado mediante ordem judicial e, especificamente, para fins de persecução criminal. Em outros termos, até que se prove o contrário, todos são inocentes e a quebra do sigilo das comunicações e dados deve se dar somente mediante ordem judicial. A autorização judicial prévia é essencial porque os demais ramos do governo não podem conferir o grau de independência e objetividade necessário para evitar abusos de poder.

Um exemplo do uso de tecnologias para fins de segurança pública são os chamados cavalos de troia: softwares espiões que seriam instalados nos dispositivos tecnológicos para a coleta de informações que poderiam ir desde o conteúdo de comunicações privadas a imagens e fotos. Notícia publicada no jornal Folha de S. Paulo em 27/04/2015, por exemplo, relata que a Polícia Federal estaria estudando formas de obter informações de comunicações privadas em celulares grampeados[27]. Dada a permeabilidade das novas tecnologias na vida dos cidadãos, as implicações sobre a privacidade desse tipo de tecnologia podem ir muito além da interceptação telefônica. Como recorda Laura Schertel Mendes, Coordenadora do Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS/IDP)[28]:

> **[...] a infiltração permite uma coleta de dados mais ampla que a interceptação telefônica ou telemática, pois não se trata apenas de interceptar um determinado tráfego de dados, mas de coletar todos os dados de um determinado aparelho já armazenados ou que estão sendo produzidos em tempo real, sem qualquer conhecimento da pessoa afetada. Estamos a falar, portanto, de uma ação ainda mais invasiva e sensível do que a interceptação de mensagens de voz ou eletrônica. É sob esse olhar do alto grau de interferência na vida das pessoas e da sensibilidade de informações que podem ser coletadas que deve ser analisada juridicamente a instalação desse dispositivo em aparelhos pessoais.**

Caso se opte por tratar as atividades mencionadas no artigo 4º em legislação a ser discutida no futuro, é clara a necessidade de que haja regras específicas para o tratamento de dados pessoais para fins de segurança pública, defesa e segurança do Estado alinhadas aos padrões internacionais de direitos humanos e com os princípios da proteção de dados pessoais.

---

[26] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...] LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória; [...].

[27] Disponível em http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml (consultado em 10/06/2015).

[28] Mendes, L. S. "Uso de softwares espiões pela polícia: prática legal?". Jota, 04/06/2015. Disponível em http://jota.info/uso-de-softwares-espioes-pela-policia-pratica-legal (consultado em 10/06/2015).

Cabe ressaltar que estudo realizado pelo grupo de trabalho Article 29 no contexto da, já mencionada, Opinião 04/2014 identificou que em alguns países da União Europeia a legislação sobre dados pessoais prevê obrigações relacionadas às atividades de segurança pública, defesa, segurança do Estado, investigação e repressão de infrações penais e que, em certos casos, incluem a supervisão das atividades de inteligência por parte da autoridade garantidora independente (que pode ter diferentes formatos segundo o país). Assim, os diferentes modelos de legislação doméstica existentes poderiam servir como referência para uma proposta de tratamento integrado da proteção de dados pessoais no caso brasileiro. Além disso, texto da Comissão Europeia para a reforma do marco legal de proteção de dados pessoais prevê em seu artigo 9a que o processamento de dados relacionados à investigação e repressão de infrações criminais devem ser realizados pela autoridade competente e prover as proteções adequadas à garantia dos direitos e liberdades dos titulares.

Até a aprovação de legislação específica, prevista no art. 4º, portanto, garantias devem ser inseridas no corpo da lei. Dessa forma, fazemos a seguinte sugestão de alteração:

Texto atual	Texto sugerido
Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei. **Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.**	**Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.** **§1º Até a aprovação de uma lei específica alinhada aos princípios da proteção de dados pessoais, os tratamentos previstos no caput ficam sujeitos à presente legislação.** **§2º O tratamento dos dados a que se refere o caput deve ser realizado apenas sob supervisão das autoridades competentes, respeitando as proteções adequadas à garantia dos direitos fundamentais dos titulares de dados.** **§3º O acesso a dados pessoais, inclusive metadados, coletados e/ou armazenados por entidades privadas por parte de autoridades públicas para fins de investigação ou repressão de infrações penais somente será autorizado mediante ordem judicial, observando os princípios estabelecidos no artigo 6º.** **§4º Os dados mencionados no §4º não serão tratados de forma incompatível com as finalidades pelas quais foram originalmente obtidos, devendo ser definitivamente excluídos quando não forem mais necessários para os propósitos para os quais foram coletados.**

	§5º Cabe às autoridades públicas que detiverem os dados em questão garantir que serão adotadas medidas de segurança para evitar o acesso indevido, de acordo com as diretrizes previstas nessa lei e desenvolvidas pela autoridade garantidora independente.

Sobre o modelo de autogerenciamento da privacidade

A ideia de consentimento advém da compreensão de que somente o titular pode autorizar ou não o tratamento de seus dados pessoais e é considerada uma condição essencial para permitir que os indivíduos possam desfrutar plenamente o seu direito de autodeterminação. Seu objetivo é oferecer às pessoas o controle sobre seus dados pessoais e a possibilidade de tomar decisões sobre o tratamento considerando os custos e benefícios que pode trazer.[29]

Tanto na Europa, com a atual Diretiva 95/46/EC, quanto no Brasil, com o Marco Civil, o consentimento é uma das condições que legitimam o tratamento de dados pessoais e a sua expressão deve ser livre (ou seja, sem coação ou coerção), informada (o indivíduo deve estar munido de todas as informações necessárias para orientar sua decisão, de uma forma clara e inteligível) e específica (em relação a uma finalidade específica)[30]. Também nos Estados Unidos, prevalece desde os anos setenta a ideia de que os indivíduos possuem uma série de direitos que os permitem administrar seus dados pessoais e que incluem a notificação e o consentimento.[31] Daniel Solove (2013) denomina esse sistema presente nas distintas legislações de proteção da privacidade e dados pessoais de "autogerenciamento da privacidade" (*privacy self-management*).

O texto atual do APL de proteção de dados pessoais, em seu Capítulo II, estabelece que o tratamento de dados pessoais somente é permitido mediante consentimento (art. 7º) e apresenta as situações em que tal regra não se aplica (art. 11).

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

O condicionamento do tratamento de dados a um consentimento forte, como o previsto no referido artigo, dá ainda mais centralidade ao modelo de autogerenciamento de informações do que a legislação europeia e estadounidense[32]. Apesar de ter sido um avanço importante, o

---

[29] No contexto europeu, o grupo de trabalho Article 29, que reúne as autoridades de proteção de dados pessoais de todos os países que adotam a Diretiva 95/46/EC, emitiu uma opinião (15/2011) afirmando que o conceito de consentimento deve ser compreendido como uma indicação inequívoca de um desejo por meio do qual o indivíduo expressa sua anuência em relação ao tratamento de seus dados pessoais. Ela deve ser clara e afirmativa ou implicar uma ação que indique a aceitação de um tratamento específico dos dados pessoais.

[30] O art. 7°, inciso VII, do Marco Civil prescreve que os indivíduos têm direito ao "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". Ver também a Opinião 15/2011 do Grupo de Trabalho do Artigo 29. (2011), sobre a definição de consentimento. Bruxelas, 13 de julho de 2011, p. 14.

[31] Segundo Solove (2013), o sistema de privacy self-management aparece nos Estados Unidos pela primeira vez nos anos setenta quando o Departamento de Saúde, Educação e Bem Estar publicou uma série de princípios para regular o tratamento de dados digitalizados, que posteriormente inspiraram as Orientações de Privacidade da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Os chamados Fair Information Practices Principles (FIPPs) incluíam: (i) a transparência sobre os sistemas de registros de dados pessoais; (ii) o direito à notificação sobre a existência de tais sistemas; (iii) o direito a prevenir o uso de dados pessoais para novos fins sem o consentimento; (iv) o direito à correção e emenda dos registros e (v) responsabilidades dos detentores de dados de evitar o mal uso.

[32] No caso da Diretiva 95/46/EC, por exemplo, o tratamento de dados pessoais é permitido em seis situações, sendo apenas uma relativa ao consentimento: Artigo 7º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se: a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) O tratamento for necessário para cumprir

modelo do consentimento não se encontra livre de críticas. A opção do anteprojeto pela centralidade do consentimento pode acarretar alguns problemas tanto para a efetiva proteção de dados, quanto para a inovação tecnológica.

No caso das relações online, a solicitação do consentimento tem sido implementada pelo setor privado principalmente através de contratos de adesão que os usuários devem aceitar ao utilizar certas plataformas. São os chamados Termos de Serviço ou Termos de Uso. No entanto, se mesmo no mundo *offline* os contratos de adesão (o tipo de contrato mais comum para a maioria das transações econômicas) poucas vezes são lidos e, quando o são, são considerados difíceis de compreender (Bakos, Marotta-Wurgler & Trossen, 2013), no ambiente online essa situação se agrava. Segundo um estudo da Universidade de Carnegie Mellon, nos Estados Unidos, um usuário deveria reservar 8h diárias em 76 dias de um ano para ler somente as Políticas de Privacidade de uma média de 1.462 páginas visitadas (McDonald & Cranor, 2008). Uma pesquisa recente também constatou, com dados empíricos, que no mercado de compra e venda de software online são pouquíssimos os consumidores que leem as *End User License Agreements* ou EULAs: entre 0,22% e 0,5% (Bakos, Marotta-Wurgler & Trossen, 2013).

Por conta disso, o modelo de autogerenciamento baseado na informação e consentimento tem sido criticado internacionalmente como mecanismo capaz de proteger a privacidade, já que, em diversos casos, o titular se vê compelido à autorizar certos tratamentos para acessar os serviços ou obter os produtos desejados. Nesse sentido, é interessante observar que o modelo de negócios em que muitos dos serviços online se baseiam contradiz parte dos princípios de proteção de dados pessoais da União Europeia e mesmo assim seu número de usuários cresce constantemente[33], já que o consentimento tornou-se condição ou "o preço que se paga" para se ter acesso a diversos serviços e produtos (Joergensen, 2014).

No Brasil, o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990) busca prevenir que vendedores e prestadores de serviço elaborem os termos de seus contratos de modo a colocar consumidor em posição excessivamente desvantajosa por meio de uma interpretação restritiva do princípio de autonomia da vontade e da previsão de um rol de cláusulas abusivas que são nulas de pleno direito. O APL acertadamente incorpora essa regra no parágrafo 7º do artigo 7º, oferecendo maior proteção ao cidadão no contexto descrito acima.

> **§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.**

---

uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

[33] Na Europa, por exemplo, onde a necessidade de consentimento para certos tratamentos de dados pessoais está garantida há pelo menos uma década, apenas pouco mais de um quarto dos usuários de redes sociais acredita ter controle total de seus dados (TNS Opinion & Social, 2011).

O modelo de autogerenciamento da privacidade, reforçado pelas medidas previstas na redação atual do anteprojeto, como a de que o consentimento deve ser fornecido por escrito e de forma destacada das demais cláusulas contratuais, têm uma função importante de estimular as empresas a oferecerem informações relevantes a seus consumidores. Além disso, um importante impacto prático do modelo de *privacy self-management* é o de melhorar as práticas institucionais de gestão da privacidade, na medida em que a obrigação de oferecer informações faz com que as empresas ou órgãos públicos tenham que analisar suas atividades de tratamento de dados. Por conta disso, os mecanismos relativos ao consentimento não devem ser descartados em uma legislação de proteção de dados pessoais.

> **Oferecer notificação, acesso e a possibilidade de controle aos indivíduos sobre seus dados é chave para se oferecer alguma autonomia em um mundo em que decisões que os afetam são tomadas com base no uso de dados pessoais, processos automatizados e lógicas clandestinas e onde as pessoas têm habilidades mínimas de fazer qualquer coisa sobre tais decisões. Um mundo sem o autogerenciamento de privacidade claramente seria problemático, já que as pessoas não teriam o direito de saber como seus dados são utilizados e tomar decisões sobre tais usos. (Solove, 2013, tradução nossa[34])**

Não se pode pensar, no entanto, que somente o oferecimento de mais informações aos indivíduos solucionará o problema descrito anteriormente. Como alternativa, a proposta de a adoção de um mecanismo mais explícito e afirmativo de obtenção de consentimento - o que parece estar sugerido na linguagem atual do anteprojeto quando fala de consentimento específico e expresso - também tem sido discutida internacionalmente. Uma declaração de 2007 do comissário da Federal Trade Commission (FTC) nos Estados Unidos, Jon Leibowitz, afirma que as empresas deveriam adotar um sistema de *opt-in* quando se trata da coleta e compartilhamento de informações dos consumidores.

O problema deste tipo de solução, porém, é que principalmente as organizações que possuem um modelo de negócios baseado no tratamento de dados pessoais terminariam por desenvolver formas de estimular o consentimento, por exemplo, tornando-o condição para o acesso ou uso de determinados serviços ou produtos.

> **[...] apesar das melhores intenções do legislador, um sistema de opt-in ou uma requisição de consentimento afirmativo para a maioria dos novos usos de dados provavelmente levaria a mais botões para se clicar e mais formas de assinar, mas não a uma proteção mais significativa da privacidade. (Solove, 2013, tradução nossa[35])**

[34] "Providing people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data, automated processes, and clandestine rationales, and where people have minimal abilities to do anything about such decisions. A world without privacy self-management would clearly be troublesome, as people should have rights to know about how their data is being used and to make decisions about those uses."

[35] "[...] despite regulator's best intentions, an opt-in system or a requirement of affirmative consent for most new uses of data will likely lead to more buttons to click and more forms to sign, but not to more meaningful privacy protection."

Por conta disso, ainda que pareça uma proposta mais protetiva para os direitos dos indivíduos, confiar exclusivamente no modelo de autogerenciamento da privacidade pode por em risco a proteção dos dados pessoais caso se torne ferramenta para legitimar possíveis tratamentos abusivos. Sob o ponto de vista dos responsáveis pelo tratamento, a implementação técnica do consentimento previsto atualmente no art. 7º para cada um dos distintos tipos de tratamento pode se tornar complexa e restringir práticas que poderiam trazer benefícios sociais.

Por outro lado, o surgimento e avanço de novas tecnologias de processamento e de negócios baseados no tratamento intensivo de dados pessoais e no seu uso como forma de pagamento indireto dos serviços e produtos oferecidos também têm colocado novos desafios para o modelo do consentimento. Solove (2013) fala de problemas estruturais que incluem: (i) um problema de escala, no qual há uma quantidade imensa de entidades que realizam algum tipo de tratamento de dados pessoais, com ou sem conhecimento do titular fazendo a intermediação de certas operações; (ii) um problema de agregação, ou seja, de que se pode atualmente deduzir informações sobre uma pessoa a partir da combinação de dados a princípio inofensivos e (iii) um problema de avaliação dos danos, já que os impactos negativos do compartilhamento de certos dados podem ocorrer após um longo período de tratamento, enquanto os benefícios são geralmente imediatos.[36]

De fato, o modelo de "aviso e consentimento" se baseia na definição preliminar do uso dos dados pessoais pelo controlador associada à anuência do titular, e não consegue enquadrar os desafios decorrentes do uso de técnicas de big data, que buscam extrair inferências a partir da análise de grandes conjuntos de dados após a coleta. O responsável pelo tratamento não pode, nesse caso, definir - ou até mesmo ter uma compreensão clara - da finalidade do processamento dos dados no momento ou antes da coleta inicial. Por outro lado, a complexidade do tratamento de grandes volumes de dados muitas vezes não permite que os titulares realmente compreendam e possam avaliar suas consequências e potenciais efeitos negativos. Discutindo a agregação dos dados e as consequências de tal prática em um contexto de crescente disseminação de técnicas de mineração de dados, Solove (2013) sublinha que se torna praticamente impossível o gerenciamento dos dados pelo titular:

> **A dificuldade com o efeito de agregação é que ele torna praticamente impossível o gerenciamento dos dados. Os tipos de novas informações que podem ser obtidas da análise de informações existentes e os tipos de previsões que podem ser feitos a partir desses dados são muito vastos e complexos e estão evoluindo muito rapidamente para que as pessoas possam compreender totalmente os riscos e benefícios envolvidos. (Tradução nossa[37])**

[36] Cohen (2012) elenca alguns dos benefícios imediatos que a personalização pode trazer e que têm um apelo importante para os consumidores, independentemente dos danos que podem acarretar a longo prazo. Eles incluem, por exemplo, descontos, produtos e serviços aprimorados, um acesso a recursos mais conveniente e um aumento do status social.

[37] "The difficulty with the aggregation effect is that it makes it nearly impossible to manage data. The types of new information that can be gleaned from analyzing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved."

No caso da análise de big data, portanto, a ideia de um "consentimento informado" não parece ser realista. Uma das alternativas que se apresenta seria a adoção de medidas mais restritivas que, além de proteger o titular dos dados ao proibir certos tipos de tratamento, dariam conta da proteção da privacidade enquanto bem social ao retirar a centralidade das decisões do indivíduo.

Cohen (2012) argumenta que compreender a privacidade apenas como um direito individual é um erro e, por conta disso, sob seu ponto de vista, legitimar certas práticas através da obtenção de consentimento seria insuficiente. Ela critica a ideia de que a privacidade possa sempre ser trocada por outros bens e defende que os indivíduos não deveriam poder abrir mão de sua privacidade em certas circunstâncias. Solove (2013) também defende que o modelo de privacy self-management deve ir além de uma abordagem que se pretende neutra sobre o mérito de tratamentos de dados particulares.

> **Sob o autogerenciamento da privacidade, a maioria das formas de coleta, uso e compartilhamento de dados pessoais são aceitáveis, desde que consensuais. O consentimento muitas vezes se torna uma forma conveniente de se obter resultados sem se confrontar com os valores em questão. Para se ir além, esse tipo de neutralidade não pode ser sustentado. (Solove, 2013, tradução nossa[38])**

Ao estabelecer que o tratamento de dados pessoais somente é permitido mediante consentimento (art. 7º) e as exceções para a aplicação de tal regra, a redação do APL apresenta-se como mais próxima do modelo europeu (Solove, 2013)[39], buscando priorizar a proteção sem criar regras estáticas ao ponto de restringir tratamentos que poderiam se mostrar positivos para a sociedade a priori.

No entanto, a aposta no consentimento como única opção legítima para o tratamento de dados pessoais parece fragilizar a proteção pretendida. A experiência internacional em países com legislações de proteção de dados pessoais mais restritivas com relação às exigências para o tratamento indica que as empresas buscam legitimar o tratamento de dados com base em outros fundamentos, já que o consentimento - como o APL brasileiro reconhece - pode ser revogado a qualquer momento pelo titular. Somada à força do consentimento proposto no art. 7º - livre, expresso, específico e informado - e as possíveis dificuldades de implementação, essa tendência pode estimular agentes cujos modelos de negócios são altamente dependentes do tratamento de dados pessoais a buscar outras bases legais para legitimar suas atividades. Tal situação poderia resultar em interpretações excessivamente abrangentes das exceções previstas no parágrafo 1º do referido artigo e no art. 11 e em uma série de disputas judiciais, sempre que tais interpretações sejam questionadas.

---

[38] "Under privacy self-management, most forms of data collection, use, or disclosure are acceptable if consensual. Consent often becomes a convenient way to reach outcomes without confronting the central values at stake. To move forward, this kind of neutrality cannot be sustained."

[39] Solove (2013) aponta que o tratamento da proteção de dados pessoais e do autogerenciamento da privacidade é mais forte na União Europeia: "Eu privacy law has a self-management component, but it requires a much more stringent and explicit form of consent than US privacy law. Moreover, EU law is more restrictive of data collection, use, and disclosure - it requires a legal basis before personal data can be processed, whereas in the US data can generally be processed "unless a law specifically forbids the activity".

> **Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.**
> **§1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.**

Assim, nas situações em que o APL prevê o consentimento como forma de proteção salvo nas "hipóteses de dispensa do consentimento previstas nesta Lei" (por exemplo os artigos 23 e 24), ela poderia se tornar inócua dado que o foco das disputas estaria justamente centrado nas situações de dispensa de consentimento.

Além disso, parece importante considerar se a possibilidade de consentimento para o tratamento de dados pessoais sensíveis (art. 12, inciso I) e para a transferência internacional de dados para países que não possuem um nível de proteção equiparável ao brasileiro (art. 29) previstos no texto atual do APL seriam adequadas para a proteção da privacidade.

No referido inciso do art. 12, relativo ao consentimento para o tratamento de dados sensíveis, o texto fala em consentimento especial sem se especificar exatamente qual seria seu significado e a diferença entre o consentimento previsto no art. 7º. Além disso, se reproduz o modelo centrado no consentimento e suas exceções previsto na Seção I do Capítulo II e, consequentemente, seus problemas. Cabe se considerar também se, nesses casos, o cidadão, ao se deparar com uma notificação e solicitação de consentimento especial, teria condições de avaliar as consequências do tratamento.

> **Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:**
> **I – com fornecimento de consentimento especial pelo titular:**
> **a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e**
> **b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou**
> **II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para:**
> **a) cumprimento de uma obrigação legal pelo responsável;**
> **b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;**
> **c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;**
> **d) exercício regular de direitos em processo judicial ou administrativo;**
> **e) proteção da vida ou da incolumidade física do titular ou de terceiro;**
> **f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.**
> **§ 1º O disposto neste artigo aplica-se a qualquer tratamento capaz de revelar dados pessoais sensíveis.**

> **§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.**

Com relação à transferência internacional de dados, o texto traz uma opção restritiva ao proibir a transferência para países que não proporcionem um nível de proteção equiparável ao da lei (art. 28), mas a exceção caso haja consentimento - ainda que especial - parece fragilizá-la ao colocar sobre o indivíduo uma responsabilidade excessiva com relação à gestão de seus dados (art. 29), principalmente considerando as fragilidades do modelo de autogerenciamento da privacidade mencionadas anteriormente.

> **Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:**
> **I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;**
> **II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;**
> **III – quando órgão competente autorizar a transferência, nos termos de regulamento;**
> **IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;**
> **V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.**
> **Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:**
> **I – normas gerais e setoriais da legislação em vigor no país de destino;**
> **II – natureza dos dados;**
> **III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;**
> **IV – adoção de medidas de segurança previstas em regulamento; e**
> **V – outras circunstâncias específicas relativas à transferência.**
>
> **Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:**
> **I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e**
> **II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.**

Pensando no papel educativo que uma legislação de proteção de dados pessoais pode assumir no contexto brasileiro, uma lei que se propõe a fortalecer o direito à autodeterminação dos cidadãos, mas que, na prática, dá margem para uma série de situações em que ele não será efetivado (as hipóteses em que os dados forem indispensáveis para o oferecimento de serviços

ou produtos, por exemplo), pode fazer com que as pessoas deixem de acreditar na possibilidade de realização dos seus direitos fundamentais.

Por conta disso, e de todo o exposto acima, uma possibilidade seria se pensar em soluções para a proteção da privacidade dos indivíduos que complementem o modelo de autogerenciamento e, ao mesmo tempo, não limitem a priori usos sociais positivos do tratamento de dados pessoais. Como buscamos ressaltar acima, mesmo no âmbito internacional, ainda não há uma solução que dê conta dos desafios para a proteção de dados pessoais existentes no contexto atual.

A solução adotada pela Diretiva 95/46/EC estabelece um rol de condições para o tratamento legítimo e das quais o consentimento é apenas uma delas.

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

Essa opção pode tornar a legislação mais clara e garantir uma atenção mais aprofundada das diferentes situações de tratamento. Um dos problemas, porém, é que a tendência a disputas em torno das exceções permanece, por exemplo, quando se trata de interesse legítimo (item f). No entanto, nesse caso é possível se estabelecer garantias específicas para cada uma das situações em que o tratamento é legal.[40]

Pode-se dizer que a solução presente no texto atual do APL brasileiro incorpora a maioria das condições para o tratamento legítimo de dados pessoais prevista na diretiva como exceções ao consentimento (art. 11) e a amplia com o parágrafo 1º do art. 7º, discutido anteriormente.

[40] No caso europeu, por exemplo, o grupo de trabalho Article 29 emitiu uma opinião especificando como deve ser a compreensão do interesse legítimo e oferecendo parâmetros para a avaliação desses casos. Article 29 Working Party. Opinião 06/2014 sobre a "Noção de interesses legítimos do responsável pelo tratamento sob o Artigo 7º da Diretiva 95/46/EC".

> **Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:**
> **I – cumprimento de uma obrigação legal pelo responsável;**
> **II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;**
> **III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;**
> **IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;**
> **V – exercício regular de direitos em processo judicial ou administrativo;**
> **VI – proteção da vida ou da incolumidade física do titular ou de terceiro;**
> **VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.**
> **§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.**
> **§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.**
> **§ 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.**

Uma solução que poderia ser vislumbrada, portanto, seria a reorganização do capítulo sobre consentimento de acordo com o modelo europeu, dadas as vantagens apresentadas anteriormente. Nesse caso, os artigos 7º e 11 se combinariam, identificando todas as possibilidades de tratamento legítimo de dados: (i) consentimento livre, expresso, específico e informado do titular; (ii) cumprimento de obrigações legais; (iii) tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública; (iv) execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º; (v) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; (vi) exercício regular de direitos em processo judicial ou administrativo; (vii) proteção da vida ou da incolumidade física do titular ou de terceiro e (vii) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias. Artigos subsequentes tratariam de especificar e fornecer maiores garantias para a proteção em cada uma das situações.[41]

Caso contrário, sugere-se um maior detalhamento e limitação das exceções propostas, de modo a incorporar garantias que orientariam sua interpretação quando alvo de disputas. Um exemplo é a exceção para a "realização de pesquisa histórica, científica ou estatística, garantida, sempre que

[41] Se adotada essa opção, a harmonização com os dispositivos legais eventualmente em conflito com o estabelecimento de outras possibilidades de tratamento de dados legítimas e não baseadas exclusivamente no consentimento poderia ocorrer através de cláusula específica nas disposições transitórias ao final do texto.

possível, a dissociação dos dados pessoais;" (art. 11, inciso IV), que, pelo texto abrangente, poderia ser utilizada para legitimar certos tratamentos sem consentimento - inclusive o big data referido anteriormente. Uma opção, baseada nas discussões da Comissão Europeia para a reforma do marco de proteção de dados pessoais, seria especificar que dados pessoais podem ser tratados para fins de pesquisas históricas, estatísticas e científicas desde que (i) não possam ser realizadas sem o processamento de dados que não permitam a identificação do titular e (ii) sempre que possível para tais fins, os dados que permitam a atribuição de informações a um titular identificado ou identificável sejam mantidos em separado de outras informações.

No que diz respeito à exceção relativa ao cumprimento de obrigações legais ou ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública, o texto do Conselho da União Europeia apresentado no contexto das discussões sobre a reforma do marco legal de proteção de dados pessoais traz algumas especificações que poderiam também ser adotadas pela legislação brasileira. O órgão explicita que tais tipos de tratamento devem ser necessários ao exercício de funções de interesse público ou da autoridade pública de que está investida o responsável e afirma que podem ser apresentadas limitações quanto ao tratamento de certos tipo de dados, os titulares em questão, além de delimitar, por exemplo, prazos de armazenamento, entidades que poderão ter acesso a dados, etc.[42]

De todo modo, buscando equilibrar a proteção dos dados com o fomento à inovação em relação a novos tipos de tratamento, o texto brasileiro poderia atribuir competências a uma autoridade garantidora independente - com capacidade técnica, pessoal, recursos financeiros e poderes institucionais - de supervisionar as modalidades de coleta, armazenamento e tratamento dos dados pessoais. Cabe ressaltar que o papel de uma autoridade garantidora de dados pessoais no contexto das novas técnicas de processamento pode ser crucial ao analisar tratamentos inovadores ou de big data, por exemplo, atestando a atenção aos princípios do tratamento de dados pessoais (art. 6º) nos casos de exceções e avaliando o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.

Tal autoridade poderia avaliar casos concretos e no caso de boas práticas desenvolver uma espécie de selo de qualidade para determinado responsável e tratamento, certificando que a prática em questão atende aos princípios da proteção de dados. Isso não restringiria a possibilidade de revisão das práticas em questão após um certo período e a punição caso as práticas não sejam condizentes aos padrões desenvolvidos em consonância com os princípios do artigo 6º.

---

[42] "O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), deve ser estabelecido em conformidade com : a) O direito da União; ou b) A legislação nacional do Estado - Membro a que o responsável pelo tratamento dos dados se encontra sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento dos dados. Este fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento , nomeadamente as condições gerais de licitude do tratamento de dados pel o responsável pelo tratamento dos dados, o tipo de dados objeto de tratamento, os titulares em questão, as entidades a que os dados poderão ser comunicados e para que efeitos, os limites a que as finalidades do tratamento devem obedecer, os prazos de armazenamento e as operações e procedimentos de tratamento, incluindo medidas destinadas a garantir a legalidade e lealdade do tratamento, inclusive para outras situações de tratamento específicas previstas no Capítulo IX." Conselho da União Europeia, Artigo 6.3 (2015).

Autoridade Garantidora Independente

Na a ausência de um marco regulatório unificado para o tratamento da proteção de dados pessoais, o Brasil não conta atualmente com autoridades específicas para este fim. O texto do Anteprojeto de Lei de Proteção de Dados Pessoais , faz diversas referências a um "órgão competente" e delimita algumas de suas atribuições. Nota-se o uso do termo órgão competente com diferentes sentidos na redação atual: ora sugerindo referir-se a uma autoridade de proteção de dados pessoais, ora a um órgão qualquer que tenha competência para atuar em determinada situação.

Embora o texto não faça menção explícita a uma "autoridade garantidora", a importância da discussão acerca de questões institucionais necessárias para a efetivação dos objetivos do anteprojeto é nítida. Abaixo (i) abordaremos exemplos de experiências internacionais, (ii) explicamos questões jurídico-administrativas relacionadas com a proteção de dados pessoais; (iii) explicamos como o presente anteprojeto de lei aborda a questão, e quais poderes pretende conferir a um "órgão competente"; e (iv) descreveremos possíveis contornos que poderiam ser assumidos por uma autoridade com base no arcabouço jurídico-administrativo brasileiro existente.

Experiências Internacionais

Tendo em vista a inexistência de uma estrutura administrativa responsável pela proteção de dados no Brasil, é importante buscar referências de jurisdições que já debateram o assunto, principalmente, aquelas nas quais já existem autoridades de proteção de dados.

A análise comparada não deve ignorar as características do arcabouço jurídico, político e administrativo brasileiro. Contudo, por meio de experiências internacionais é possível inferir os desafios de diferentes modelos adotados, assim como suas principais vantagens. Abaixo serão exploradas experiências de autoridades de Estados-membro da União Europeia. Estas autoridades já existem há muitos anos e fazem parte de um sistema de proteção de dados que se assemelha ao que está sendo proposto no Brasil.

Em cumprimento aos requisitos estabelecidos pelo Artigo 28 da Diretiva de Proteção de Dados (Diretiva 95/46/CE), os Estados-membro da União Europeia criaram autoridades nacionais independentes de proteção de dados e um órgão supervisor, que é um órgão da União Europeia responsável pelo acompanhamento da aplicação das regras de proteção de dados. O órgão supervisor publica opiniões e orientações para a interpretação da Diretiva que devem ser seguidas pelas referidas autoridades. O modelo, contudo, pode variar em função da forma em que os diferentes países interpretam as diretivas. Além disso, há variações decorrentes de diferentes estágios de implementação das referidas regras em cada Estado-membro.

Alguns Estados possuem uma autoridade de supervisão geral, com a função de garantir o monitoramento e o respeito à legislação de proteção de dados dentro de seus territórios. Outros, possuem uma autoridade de competência geral que atua em paralelo a outras agências para setores específicos, como saúde, correios e telecomunicações. Em alguns casos, foram criadas autoridades em âmbito nacional que supervisionam autoridades regionais ou estaduais e, em

outros, existe ainda a figura do *ombudsman*, que exerce um papel complementar importante na proteção de dados pessoais (European Agency for Fundamental Rights, 2010).

A Agência de Direitos Fundamentais da União Europeia identificou os desafios enfrentados no âmbito do sistema de proteção de dados na União Europeia e incluiu entre eles a falta de independência como uma importante questão estrutural das Autoridades de Proteção de Dados. O estudo também apontou que alguns dos Estados-Membros reportaram dificuldades dos agentes públicos das Autoridades de Proteção de Dados para executarem suas funções de forma autônoma. A falta de recursos financeiros também foi apontada como um problema enfrentado pelas referidas autoridades. Por fim, nem todas as autoridades possuem plenos poderes de investigação, de intervenção em operações de processamento, prestação de aconselhamento jurídico e engajamento em processos judiciais, o que prejudica o desenvolvimento e a eficácia de suas atividades (European Agency for Fundamental Rights, 2010).

Cada um destes desafios será objeto de análise a seguir, no que se refere à (i) a autonomia e a independência das autoridades; (ii) seus poderes e limitações; e (iii) seu orçamento.

INDEPENDÊNCIA

A Diretiva de Proteção de Dados estabelece medidas relativas à independência funcional das autoridades nacionais de proteção de dados, assim como suas atribuições e poderes. De acordo com o art. 28 da Diretiva, as autoridades deverão ter, no mínimo, poderes de inquérito e de intervenção assim como de intervir em processos judiciais e de levar infrações ao conhecimento das autoridades judiciais. Além disso, as decisões da autoridade são passíveis de recursos judiciais.

É fundamental que a independência seja em relação à administração direta e que a autoridade tenha suas decisões revistas apenas pelo Poder Judiciário. Tal característica é fundamental para que as autoridades estejam protegidas contra influências político-partidárias que se revelem nocivas ao bom andamento de suas atividades. Assim, para que as autoridades possam exercer suas atribuições com isonomia e equidade, a independência é estabelecida como uma das garantias de que os objetivos das autoridades serão alcançados. Ademais, a questão da proteção de dados pessoais é complexa e envolve uma série de aspectos técnicos, além de diferentes interesses públicos e particulares.

A discussão sobre independência pode recair sobre diferentes aspectos, como o tipo de vinculação das autoridades com a administração direta, ao tempo de mandato e forma de indicação dos dirigentes das autoridades. A independência deve ser completa, no sentido de que seus poderes de decisão devem ser livres de quaisquer influências diretas ou indiretas, embora a diretiva não defina claramente os contornos desta independência. Não obstante, a reforma da Diretiva da União Europeia, em discussão atualmente, prevê que estes contornos sejam estabelecidos de forma mais clara.

Em alguns Estados-membro da União Europeia, por exemplo, falta de completa autonomia é relacionada principalmente ao processo de nomeação ou designação dos delegados, quando o governo tem o poder exclusivo de selecionar os membros da autoridade ou o pessoal de gestão. A designação dos membros da autoridade exclusivamente pelo governo aumenta significativamente o risco de subordinação dos controladores de dados ao poder executivo. Por

vezes a formação de um conselho multissetorial cujos membros sejam designados pelos diferentes setores e não somente pelo executivo serve como forma de mitigar este risco.

Um dos casos emblemáticos relacionados com o debate acerca da independência das autoridades de proteção de dados é o da Alemanha, que conta com autoridades em diferentes regiões (*Länder*) vinculadas à administração publica direta de tais regiões. O Tribunal de Justiça da União Europeia determinou que tal arranjo institucional viola a Diretiva de Proteção de Dados, por não contar com a completa independência no exercício de suas funções. A Alemanha alegou, em sua defesa, que o mecanismo de monitoramento interno da administração regional direta não constitui uma influência externa. Tal argumento, contudo, não foi aceito pelo Tribunal de Justiça. Em função desta decisão, as autoridades regionais passaram por alterações estruturais.

Na Espanha, a Autoridade de Proteção de Dados é um ente de direito público, com personalidade jurídica própria e que atua com plena independência da administração publica no exercício de suas funções, e se relaciona com o Governo por meio do Ministério da Justiça, que nomeia o Diretor da autoridade. A autoridade segue o regime jurídico das administrações públicas e o procedimento administrativo comum. Dinamarca e Letônia também são outros países que contam com autoridades com vínculo com o Ministério da Justiça de seus países.

Em um recente caso decidido em 2014[43], o Tribunal de Justiça da União Europeia determinou que a independência da autoridade de proteção de dados húngara foi desrespeitada. Em função de uma reforma no sistema de proteção de dados promovida pelo parlamento, o Supervisor da autoridade foi substituído antes do fim de seu mandato de seis anos. O Tribunal considerou que as autoridades não podem estar sujeitas a nenhum tipo de influência externa, e que a alteração da liderança da autoridade seria uma ofensa à independência da instituição.

Em diferentes países, a nomeação dos cargos da autoridade de proteção de dados é feita envolvendo o executivo, o legislativo, o judiciário e por vezes grupos da sociedade civil. Há casos em que se questiona a independência das autoridades tendo em vista que a indicação ou nomeação dos agentes é feita somente pelo Governo, sem que seja recebida a opinião, o consentimento ou a revisão do poder legislativo. Este é o caso da Lituânia, da Letônia, da Estônia, da Irlanda e do Reino Unido.

As autoridades de proteção de dados têm natureza de direito público e contam com o imperativo jurídico da independência. Os contornos de tal imperativo jurídico, contudo, admitem diferentes formas. Apesar de referirem à seara dos Direitos Humanos, os Princípios relativos ao Estatuto das Instituições Nacionais de Direitos Humanos (Princípios de Paris), adotados pela resolução 48/134 da Assembleia Geral das Nações Unidas, de 20 de Dezembro de 1993, podem propiciar elementos interessantes ao pensar a composição de orgãos independentes e plurais.

[43] Case C-288/12 - Commission v Hungary. Tribunal de Justiça da União Européia. Disponível em http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140053en.pdf.

Composição e garantias de independência e pluralismo

1. A composição da instituição nacional e a designação dos seus membros, quer por eleição quer por outros meios, deverão ser definidas em conformidade com um procedimento que preveja todas as garantias necessárias para assegurar a representação pluralista das forças sociais (da sociedade civil) que participam na promoção e protecção dos direitos humanos, particularmente competências que permitam o estabelecimento de uma cooperação entre, ou através da presença de representantes, de:
a) Organizações não governamentais com competências no domínio dos direitos humanos e na luta contra a discriminação, associações sindicais e organizações sócio-profissionais interessadas, nomeadamente de juristas, médicos, jornalistas e cientistas eminentes;
b) Correntes de pensamento filosóficas ou religiosas;
c) Universidades e peritos qualificados;
d) Parlamento;
e) Departamentos governamentais (caso sejam incluídos, estes representantes deverão participar nas deliberações apenas a título consultivo).

2. A instituição nacional deverá dispor de uma infra-estrutura adequada ao bom desempenho das suas actividades, e em particular de fundos suficientes. O seu financiamento deverá ter por objectivo permitir que a instituição disponha de pessoal e instalações próprias, a fim de garantir a sua independência face ao governo e evitar que fique sujeita a um controlo financeiro susceptível de afectar a respectiva independência.
3. A fim de assegurar a estabilidade do mandato dos membros da instituição, sem o qual não pode existir verdadeira independência, a nomeação de tais membros deverá ser efectuada mediante acto oficial que estabeleça expressamente a duração do mandato. Este mandato poderá ser renovável, desde que garantido o pluralismo na composição da instituição.

(Fonte: Resolução 48/134 da Assembleia Geral das Nações Unidas, de 20 de Dezembro de 1993)

PODERES

A Diretiva Europeia de Proteção de Dados estabelece os poderes gerais que devem ser conferidos às autoridades nacionais. Mais especificamente a Diretiva estabelece (i) o poder de assessorar autoridades legislativas e administrativas no processo legislativo e regulatório sobre a proteção de direitos e liberdades individuais que se relacionam com o processamento de dados pessoais; (ii) o poder de investigação, intervenção e engajamento em processos jurídicos e (iii) o poder de receber reinvindicações. Contudo, há diferentes níveis de implementação desses poderes pelos diferentes países da União Europeia.

Um estudo da Agencia Europeia de Direitos Fundamentais (2010), classificou os poderes das autoridades em ex-ante e ex-post. Países como Finlândia, Suécia, Irlanda e Reino Unido são mais focados em atividades preventivas - ex-ante - enquanto outros, como Grécia, Republica Checa e Letônia, estão mais focados em ações reativas e no cumprimento e monitoramento das regras relativas à proteção de dados - ex-post.

Com respeito aos poderes de investigação, a maioria das autoridades podem requisitar informações e documentos, acessar bancos de dados e sistemas, busca e apreensão sem autorização judicial e conduzir auditorias. Algumas autoridades, no entanto, apenas podem fazer a busca e apreensão por mandado judicial (e.g. Alemanha, França, Itália, Malta, e Reino Unido).

As autoridades também possuem poderes de intervenção, como a elaboração de pareceres jurídicos no âmbito de processos que envolvem dados sensíveis, como determinar que dados sejam bloqueados, deletados, ou destruídos. Além disso, as autoridades exercem seu poder de polícia administrativa, por exemplo, determinando que controlador de dados[44] seja banido, processado, notificado ou proibido, ou ordenando que medidas técnicas e organizacionais sejam tomadas com o objetivo de prevenir violações à legislação de proteção de dados.

As autoridades da União Europeia também têm poderes de receber reinvindicações e de se engajar em processos jurídicos. Tais reinvindicações podem ser feitas por quaisquer pessoas ou associação representando esta pessoa na defesa de seus direitos e liberdades referentes à proteção de seus dados. Ademais, as autoridades têm obrigação de iniciar processos jurídicos no caso de violação de direitos, ou trazer à atenção do judiciário tais violações. Além disso, as autoridades podem encaminhar casos para o legislativo ou outras instituições políticas. A Autoridade da Eslovênia, contudo, não apenas pode levar casos ao judiciário, mas também tem o poder de iniciar uma ação junto ao tribunal constitucional (European Agency for Fundamental Rights, 2010). Apenas parte das autoridades realmente podem levar diretamente casos ao judiciário ou encaminhar casos para o legislativo. Assim como ocorre em relação às demais características das agências, há diferentes estágios de implementação dos referentes poderes pelas autoridades.

As autoridades de proteção de dados devem ser consultadas quando da elaboração de medidas administrativas ou regulatórias por parte do legislativo e do executivo. Este papel de fonte de referência em questões de privacidade é essencial para dar interpretação homogênea aos diferentes documentos, regras e posicionamentos dos governos. Na Irlanda, a autoridade de proteção de dados pode inclusive elaborar códigos de conduta para associações de comércio e outras instituições representando categorias de controladores[45].

A Diretiva de Proteção de Dados da União Europeia também traz a previsão de que os Estados-membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da diretiva e que deverão especificar as sanções que serão aplicadas em caso de violação das disposições adotadas. Como é possível observar, entretanto, há discricionariedade por partes das autoridades em determinar quais sanções e sua abrangência.

Sanções pecuniárias aplicadas pelas autoridades são presentes na maioria das autoridades. A tabela abaixo mostra que as sanções aplicadas por autoridades de proteção de dados na União

[44] De acordo com o Art. 2 (d) da (EC) No 45/2001, o *controller* é uma instituição ou órgão, uma diretoria-geral, uma unidade ou qualquer outra entidade organizacional que sozinha ou em conjunto determina os propósitos e formas de processamento de dados pessoais.

[45] Ireland Data Protection Act (1988-2003), Section 13. Disponível em http://www.dataprotection.ie/viewdoc.asp?DocID=796#13.

Europeia têm valores distintos, mas que podem ultrapassar um milhão de reais, como no caso de Espanha, Reino Unido e República Tcheca. Há também valores mínimos estabelecidos por algumas das autoridades, como no caso de Portugal, que pode aplicar uma sanção no valor de menos de mil reais.

Tabela 1: Mínimo e Máximo de sanções que podem ser aplicadas por autoridades de proteção de dados em selecionados países da União Europeia

País	Mínimo R$	Máximo R$
Alemanha	160.500	963.000
Espanha	2.889	1.926.000
França		481.500
Grécia		468.660
Holanda		802.500
Hungria		115.560
Itália	19.260	385.200
Polônia		866.700
Portugal	803	96.300
Reino Unido		1.340.679
República Tcheca	654.840	1.309.680
Suíça	25.359	

Fonte: Autores adaptado de Mind Your Privacy 2014 - Conversão utilizada: 3.21 Reais para 1 Euro.

A grande maioria dos Estados-membros da União Europeia permitem que as suas agências de proteção de dados monitorem o cumprimento da legislação de proteção de dados por parte dos operadores públicos e privados envolvidos no processamento de dados. Ademais, as autoridades dispoem de um poder de iniciativa a fim de exercitar esses poderes ou podem ser solicitadas por um titular de dados pessoais que alegue violações de seus direitos.

A tabela abaixo mostra boas práticas no que se refere às características institucionais das Autoridades de dados na União Europeia, conforme o demonstrado acima.

Tabela 2: Boas práticas das autoridades nacionais de proteção de dados na União Europeia

	Boas práticas para as autoridades nacionais de proteção de dados
Independência	- A atribuição de personalidade jurídica independente à autoridade de supervisão de proteção de dados e natureza jurídica de direito público (e.g.

	Portugal e Espanha); - A codificação constitucional dos poderes e da independência das autoridades (e.g. Portugal);
Poderes	- O poder de aconselhar as autoridades legislativas ou administrativas no processo de elaboração da legislação e regulamentação relativa à proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais; - O poder de investigação, de intervenção e de envolvimento em processos judiciais; - O poder de ouvir reclamações apresentadas por qualquer pessoa; - O poder de participar ativamente na formulação de códigos de conduta relacionados à proteção de dados (e.g. Irlanda); - O poder de iniciar recurso constitucional (e.g. Eslovênia)

Fonte: Autores, com base em FRA, 2010 e pesquisa primária.

ORÇAMENTO

A maioria das autoridades europeias recebe recursos públicos para desempenhar suas funções e muitas vezes os referidos recursos são canalizados por meio dos respectivos ministérios da justiça. Em alguns casos, o referido orçamento é complementado pela cobrança de valores por notificações e sanções administrativas. Em Portugal, o orçamento da autoridade provem da dotação inscrita no Orçamento da Assembleia da República e da receita própria, proveniente de multas e da cobrança de taxas de notificação.

A tabela abaixo mostra deficiências, suas razões e possíveis soluções no que se refere às características institucionais das autoridades de proteção de dados de dados na União Europeia.

Tabela 2: Deficiências, razões e possíveis soluções - autoridades nacionais de proteção de dados na União Europeia

Deficiências	Principais razões	Possíveis soluções
Falta de independência (e.g. Lituânia, Letônia, Estônia, Irlanda, Reino Unido)	- A indicação ou nomeação de agentes é feita somente pelo Governo;	- Promoção de uma reforma do processo de nomeação/indicação dos agentes; - Uma alteração na diretiva de Proteção de Dados para dar mais detalhes e especificidades sobre o que se espera no tocante à independência das autoridades.
Limitações orçamentárias (e.g. Áustria, Bulgária, Romênia, Chipre, França, Grécia, Itália, Letônia, Holanda, Portugal e Eslováquia)	- inexistência de previsão orçamentária, ou previsão orçamentária subestimando a necessidade das autoridades	- Reformas legislativas promovendo o orçamento e a contratação de pessoas para a gestão das autoridades de proteção de dados

Limitações nos poderes das autoridades (tipos de limitação variam de acordo com país)	**- Arcabouço legislativo em âmbito nacional não segue as regras estabelecidas pela União Europeia**	**- Alterações legislativas devem ser promovidas no sentido de alinhar o que já esta estabelecido em âmbito das regras da União Europeia**

Fonte: Autores, com base em FRA, 2010 e pesquisa primária.

Com base no exposto acima, podemos concluir que as autoridades de proteção de dados analisadas (i) têm natureza jurídica de direito público; (ii) são independentes, muito embora tal característica tenha diferentes formas dependendo da autoridade; e (iii) exercem diversos poderes, inclusive poderes de polícia.[46] Estas serão, portanto, as referências que usaremos abaixo na busca por um modelo aplicável à realidade brasileira.

Contexto Brasileiro

O modelo de autoridades especificas para a proteção de dados, assim como as existentes na Europa, não é utilizado no Brasil até o momento. O Anteprojeto de Lei para a Proteção de Dados Pessoais se refere a um "órgão competente", sem especificar qual seria e de que forma estaria estruturado. Ao mesmo tempo, o texto do debate público acerca do anteprojeto levanta a possibilidade de criação de uma estrutura administrativa responsável pela garantia da correta aplicação da lei de proteção de dados.

Não obstante a inexistência de uma autoridade específica, há jurisprudência relacionada ao tratamento de dados pessoais, e alguns destes casos chegaram ao Supremo Tribunal Federal assim como ao Superior Tribunal de Justiça. Uma busca na jurisprudência do Supremo Tribunal Federal, indica a existência de 25 acórdãos relacionados com a proteção de dados[47]. A mesma busca realizada no sítio eletrônico do Superior Tribunal de Justiça (STJ) indica a existência de três acórdãos[48].

Destacamos o Recurso Especial - Resp 1.419.697-RS, decisão do STJ de novembro de 2014, referente ao uso de dados pessoais pelo sistema de "credit scoring". Trata-se um método desenvolvido para avaliação do risco de concessão de crédito, e o recurso proposto junto ao STJ abordou temas como o da proteção de dados. No âmbito do recurso ora citado, o Ministro Paulo de Tarso Sanseverino, Relator do Recurso Especial, afirma que foi "um daqueles processos em cujo julgamento parte-se praticamente do zero, pois não tinha uma noção clara acerca do que seria o chamado credit scoring", embora o Núcleo de Recursos Repetitivos e Repercussão Geral do Tribunal de Justiça do Rio Grande do Sul o tenha informado da existência de cerca de oitenta

[46] O poder de polícia é atividade da administração pública que, limita ou disciplina direito, interesse ou liberdade, de acordo com o artigo 78 do Código Tributário Nacional: "Art. 78. Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos.

[47] Busca feita em fevereiro de 2015, utilizando as palavras "privacidade e dados" de forma combinada, na mesma ementa.

[48] Id.

mil recursos a respeito desse tema. O Ministro Relator citou o sistema Europeu e a Diretiva 46/95 e tratou de conceitos como consentimento e dados sensíveis.

A decisão deixa nítida a necessidade de conhecimento aprofundado acerca do tema, inclusive sobre questões específicas, como *credit scoring*, e que exigem conhecimento técnico. Essa expertise se torna essencial para o julgamento do mérito das ações. Questões conceituais poderão ser aclaradas por um arcabouço jurídico mais sólido e por uma autoridade dedicada à proteção de dados, que poderia ajudar a padronizar o entendimento de tais conceitos, contribuindo para a resolução dos mais de oitenta mil recursos a respeito do tema.

Analisando a possibilidade da criação de uma estrutura administrativa específica para a proteção de dados, assim como seus possíveis poderes e limites, e tendo em conta as experiências internacionais tomadas como referência neste documento, podemos concluir que devemos buscar uma autoridade para o Brasil que (i) tenha natureza jurídica de direito público; (ii) tenha a independência e autonomia como uma de suas principais características; e (iii) possa exercer diferentes poderes, entre eles o poder de polícia.

Considerando as características apontadas acima, podemos concluir que a autoridade de dados pessoais seria parte da administração pública descentralizada ou indireta, e não de entes da administração direta, uma vez que estes não possuem a independência necessária.

De acordo com o art. 4, II, do Decreto-Lei n.200/67, as seguintes instituições fazem parte da administração indireta: (i) autarquias, (ii) fundações públicas, (iii) empresas públicas; e (v) sociedades de economia mista. As empresas públicas e as sociedades de economia mista têm natureza jurídica de direito privado e exploram atividade econômica, o que não é função de uma autoridade de proteção de dados e portanto não serão analisadas abaixo. Fundações públicas, por sua vez, têm personalidade jurídica de direito privado. Além disso, as Fundações são criadas para o exercício de atividades em áreas que não exigem o uso do poder de polícia do Estado. Há também as paraestatais, que realizam obras, serviços ou atividades de interesse coletivo, mas não integram a administração direta ou indireta. Conforme podemos notar, resta analisar apenas as características da autarquia.

AUTARQUIA

A Autarquia é uma das formas de descentralização administrativa, prevista no art. 37, XIX da Constituição Federal. De acordo com o Decreto-Lei n. 200/67, art. 5º, inc. I, é um "serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receita próprios, para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada."

Existem autarquias que exercem a função de polícia administrativa, tais como o Instituto Brasileiro do Meio Ambiente (IBAMA), que executa (i) o poder de polícia ambiental; (ii) ações das politicas nacionais de meio ambiente; assim como (iii) ações supletivas de competência da União, de conformidade com a legislação ambiental vigente, de acordo com o que estabelece a Lei 7.735/89.

Há também as autarquias de serviço público, tais como o Instituto Nacional do Seguro Social (INSS), que é vinculado ao Ministério da Previdência Social e tem por finalidade (i) promover a

arrecadação, a fiscalização e a cobrança das contribuições sociais incidentes sobre as folhas de salários e demais receitas a elas vinculadas, na forma da legislação em vigor; (ii) gerir os recursos do Fundo da Previdência e Assistência Social; e (iii) conceder e manter os benefícios e serviços previdenciários, de acordo com o Decreto n. 569/92.

Ademais, há também as que intervêm no domínio econômico, como o Conselho Administrativo de Defesa Economia (CADE), que é uma autarquia federal, vinculada ao Ministério da Justiça, e que tem como missão zelar pela livre concorrência no mercado, sendo a entidade responsável, no âmbito do Poder Executivo, não só por investigar e decidir, em última instância, sobre a matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência, assim como o estabelecido pela Lei nº 12.529/2011. Ademais, o CADE exerce o seu poder de polícia na defesa da preservação do ambiente concorrencial.

Além disso, também há autarquias de fomento, como a Superintendência do Desenvolvimento do Nordeste (SUDENE), que é uma autarquia especial, administrativa e financeiramente autônoma, integrante do Sistema de Planejamento e de Orçamento Federal, criada pela Lei Complementar nº 125, de 03/01/2007. A SUDENE tem como objetivo fomentar a cooperação das forças sociais representativas para promover o desenvolvimento inclusivo e sustentável do Nordeste.

As agências reguladoras, por sua vez, são autarquias de caráter especial, uma vez que possuem algumas características como autonomia reforçada em relação às demais autarquias. De acordo com o art. 8º, par. 2º da Lei n. 9.472/97, que criou a ANATEL, "a natureza de autarquia especial conferida à Agência é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira".

As autarquias não têm poder coercitivo em relação a órgãos que compõem a administração pública direta ou indireta. Esta possibilidade já foi questionada no passado, por exemplo no âmbito dos limites dos poderes do Conselho Administrativo de Defesa Econômica (CADE). As regras de concorrência são aplicáveis às pessoas jurídica de direito público. Contudo, é o judiciário apenas que pode fazer este controle, e não quaisquer outros órgãos da administração pública. Entender algo diferente seria "estabelecer (ao arrepio da Constituição) uma nova hipótese de controle de constitucionalidade concentrado, e no segundo, prejudicar a autonomia das entidades reguladoras independentes, cujos atos não são revisáveis no âmbito do Poder Executivo".

As autarquias estão sujeitas ao controle externo, exercido pelo Tribunal de Contas da União (TCU), competente, de acordo com artigos 49, inciso X e 71 da Constituição Federal, para julgar as contas e fiscalizar e controlar os atos do Poder Executivo, inclusive de autoridades da administração indireta. Além disso, os dirigentes das autarquias estão sujeitos ao art. 327 do Código Penal, assim como à Lei de Improbidade Lei 8.429/92, e também podem ser responsabilizados através de ação popular e ação civil pública. Em alguns casos, o mandato de seus dirigentes está sujeito à aprovação do Senado Federal, caso a lei determine, de acordo com o que estabelece o art. 52, III, f da Constituição Federal.

Autarquias têm autonomia administrativa, são independentes e têm personalidade de direito público. Por fazerem parte da Administração Federal indireta, estão sujeitas à supervisão do

Ministro de Estado, que essencialmente aprova a proposta anual de orçamento-programa e da programação financeira da entidade, de acordo com os artigos 19, 20 e 26 do Decreto-Lei n. 200/67.

No caso das autarquias especiais – natureza das agências reguladoras - uma característica que lhes confere ainda mais independência é o mandado fixo dos dirigentes, ou seja, sua estabilidade provisória. Tal estabilidade do mandato foi considerada imprescindível para o modelo de Estado regulatório assumido no Brasil, que preza pela imunização política dos dirigentes das agências (Ver ADIN 1.949/RS). Sua independência técnico decisional também é uma característica que foi discutida no âmbito do Parecer 51/2006 da Advocacia Geral da União (AGU), segundo o qual, havendo disputa entre os Ministérios e as agências reguladoras quanto à fixação de suas competências, ou mesmo divergência de atribuições entre uma agência reguladora e outra entidade da Administração indireta, a questão deve ser submetida à AGU. Ademais, as decisões das agencias reguladoras não se sujeitam a recurso hierárquico impróprio. Assim, suas decisões não podem ser revistas pelos Ministérios ou quaisquer outras instancias do poder executivo.

Ademais, o artigo 5º da Constituição Federal, inciso XXXV determina que qualquer lesão ou ameaça de lesão a direito esta sujeita à apreciação pelo Poder Judiciário. Assim, é garantido o controle sobre os atos normativos ou concretos expedidos pela autoridade de proteção de dados, mas tal controle poderá ser exercido apenas pelo judiciário.

O orçamento das autarquias segue o indicado no art. 165, § 5º, da Constituição Federal, assim como nos artigos 107 a 110 da Lei 4.320/64. O orçamento se vincula ao orçamento da União e é aprovado por decreto do Poder Executivo, salvo se disposição legal expressa determinar que o Poder Legislativo também deve estar envolvido. As autarquias, portanto, embora possuam autonomia financeira e patrimonial, não podem complementar seu orçamento por meio de tributos ou serviços.

Já as autarquias especiais, por sua vez, podem estabelecer tributos que estejam vinculados a uma contraprestação específica, e assim aumentar seu orçamento disponível. Tal possibilidade decorre do art. 145, inciso II da Constituição Federal, e é vinculada ao exercício do poder de polícia ou pela utilização, efetiva ou potencial, de serviços públicos específicos e divisíveis, prestados ao contribuinte ou postos a sua disposição. Tal possibilidade, no entanto, é usufruída apenas pelas agências reguladoras, que possuem natureza de autarquias especiais, por conta das funções coercitivas que exercem.

O órgão competente previsto no APL de proteção de dados pessoais

Na a ausência de um marco regulatório unificado para o tratamento da proteção de dados pessoais, o Brasil não conta atualmente com autoridades específicas para este fim. O texto atual do APL faz referência mais de trinta vezes a um "órgão competente", inclusive designando algumas de suas atribuições, o que parece indicar que a compreensão da importância de uma entidade garantidora para a efetivação dos objetivos do anteprojeto.

Nota-se, entretanto, o uso do termo órgão competente com diferentes sentidos na redação atual: ora sugerindo referir-se a uma autoridade de proteção de dados pessoais, ora a um órgão qualquer que tenha competência para atuar em determinada situação.

Além disso, as atribuições dadas ao órgão em questão no decorrer do texto, traz desafios em termos de uma organização institucional, principalmente considerando que a lei, como está, se aplica tanto aos agentes públicos, quanto privados. Conforme demonstramos neste documento, geralmente os poderes de um órgão não são oponíveis a ambos.

Identificamos no texto do anteprojeto as diversas menções a um órgão competente (ou conjunto de órgãos competentes) e resumimos a seguir algumas obrigações e atribuições que ao nosso ver, deveriam ser sistematizadas e complementadas em um capítulo específico dedicado à criação da autoridade de proteção de dados. A sugestão busca alinhar o anteprojeto brasileiro com as melhores práticas internacionais na área. Além disso, é importante evitar diferentes interpretações acerca das disposições já existentes, de forma que seja garantida a proteção aos dados pessoais por meio de uma estrutura eficaz e eficiente.

O texto atual do APL menciona em diversas partes do texto a existência de um "órgão competente" que teria poderes normativos. Além disso, também são previstos poderes de polícia para tal órgão. Ademais, embora em variadas partes do texto a criação de uma autoridade específica parece ser o objetivo almejado, tal posicionamento não é claro. Ademais, tais poderes seriam oponíveis a agentes públicos e privados.

O Art. 5º do APL menciona um órgão competente no inciso XVIII, afirmando que haverá comunicação entre ele e o titular dos dados. Em seguida, o Art. 10 menciona um órgão competente, atribuindo-lhe as funções de (i) recebimento de denúncias de descumprimento da lei (inciso VII, c) e (ii) definição dos termos para a comunicação de tratamento de dados do operador ao titular (inciso VII, c, § 4).

> **Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos: [...]**
> **VII – direitos do titular, com menção explícita a:**
> **a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;**
> **b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e**
> **c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.**
> **§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.**
> **§ 2º Em caso de alteração de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.**
> **§ 3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.**
> **§ 4º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.**

O Art. 13 determina, por sua vez, que o órgão competente terá poderes para estabelecer medidas de segurança e proteção de dados sensíveis que deverão ser adotadas pelos agentes de tratamento - o que parece implicar a existência de uma autoridade específica que teria, inclusive, competência para autorizar ou não certos tipos de usos e disciplinar o tratamento de dados biométricos.

> **Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.**
> **§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.**
> **§ 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.**

O Art. 14 novamente prevê que um órgão competente terá autoridade sobre o responsável pelo tratamento de dados pessoais no que diz respeito à violação das normas aplicáveis, podendo determinar o término do tratamento de dados. Além disso, tem a responsabilidade de estabelecer prazos máximos para o tratamento. Por outro lado, o Art. 15 prevê a possibilidade de que tal órgão determine sobre a conservação dos dados em casos específicos, o que permite se supor que tal entidade terá autoridade sobre a manutenção e cancelamento dos dados.

> **Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:**
> **[...]**
> **IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.**
> **Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.**

> **Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a**
> **conservação para as seguintes finalidades:**
> **[...]**
> **Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.**

O Art. 18 afirma que o órgão competente pode dispor sobre os formatos para a disponibilização dos dados pessoais quando da solicitação do titular.

> **Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:**
> **[...]**
> **§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.**

§ 2º As informações e dados poderão ser fornecidos, a critério do titular:
I – por meio eletrônico, seguro e idôneo para tal fim; ou
II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.
§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que
permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.
§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

O inciso III do artigo Art. 24 parece afirmar que o órgão competente teria autoridade sobre outros órgãos e entidades públicas no que diz respeito à comunicação e interconexão.

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:
[...]
III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.
Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:
I – à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;
II – ao oferecimento aos titulares de opção de cancelamento de seus dados; ou
III – ao cumprimento de obrigações complementares determinadas por órgão competente.

A leitura do Art. 26 reforça a ideia presente no parágrafo único do artigo 24 de que o órgão competente teria autoridade sobre outros órgãos e entidades públicas no que diz respeito à comunicação e interconexão.

Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.

O Art. 28 traz um problema, pois dá margem para uma interpretação que fragilizaria a proteção do titular no caso da transferência internacional, ao sugerir que qualquer órgão competente - não necessariamente uma autoridade de proteção de dados - poderia autorizar a transferência para países que não possuem um nível de proteção equiparável ao da lei brasileira. Outra leitura do inciso III sugere que tal órgão possuirá um regulamento próprio, e que este regulamento poderia delimitar exceções à lei. O parágrafo único, por sua vez, também sugere a existência de um órgão

específico para a proteção de dados, que - entre outras funções - seria responsável por avaliar o nível de proteção dos países de destino dos dados.

> **Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:**
> **[...]**
> **III – quando órgão competente autorizar a transferência, nos termos de regulamento;**
> **[...]**
> **Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:**
> **[...]**

O Art. 30 faz referência à possibilidade do órgão competente elaborar cláusulas padrão para reger a transferência internacional de dados pessoais e ao fato de que as empresas de um mesmo grupo econômico ou conglomerado multinacional poderão solicitar a permissão de tal órgão para realizar a transferência entre suas afiliadas. Já o parágrafo 3º permite se inferir que o órgão competente poderá solicitar informações às empresas e realizar verificações das operações.

> **Art. 30. A autorização referida no inciso III do caput do art. 28 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.**
> **§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.**
> **§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.**
> **§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.**

O Art. 33 parece importante ao determinar ao órgão competente a autoridade para interpretar a legislação, na medida em que lhe caberia desenvolver normas que ajudariam a identificar que tipo de tratamentos se configurariam como transferência internacional.

> **Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.**

Já o artigo 39, determina que o órgão competente pode solicitar relatórios de impacto à privacidade aos responsáveis pelo tratamento de dados pessoais.

> **Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.**
> **[...]**
> **§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.**

O Art. 41, que trata das atribuições do encarregado do tratamento de dados pessoais, reforça a atribuição do órgão competente de estabelecer normas complementares à lei. O mesmo faz o Art. 47, que trata do estabelecimento de critérios de segurança para a proteçao de dados pessoais, e o Art. 49, sobre a adoção de padrões técnicos que facilitem a gestão dos dados por parte dos titulares. Também o Art. 51, quando trata do estabelecimento de normas para a adequação dos bancos de dados existentes antes da aprovação da lei às suas exigências.

> **Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.**
> **[...]**
> **§ 2º As atividades do encarregado consistem em:**
> **I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;**
> **II – receber comunicações do órgão competente e adotar providências;**
> **III – orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e**
> **IV – demais atribuições estabelecidas em normas complementares ou determinadas pelo responsável.**
> **§ 3º Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.**

> **Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.**

Segundo o Art. 45, o órgão competente também teria a responsabilidade de determinar quais providências devem ser tomadas em caso de incidentes de segurança com dados pessoais, inclusive medidas para amenizar seus efeitos.

> **Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:**
> **I – pronta comunicação aos titulares;**

> **II – ampla divulgação do fato em meios de comunicação; ou**
> **III – medidas para reverter ou mitigar os efeitos de prejuízo.**
> **§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.**
> **§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.**

Finalmente, o Art. 50 estabelece que o órgão competente é responsável por aplicar sanções administrativas em caso de infrações por parte de pessoas jurídicas de direito privado e de entidades e órgãos públicos no caso de algumas medidas específicas relacionadas ao tratamento (dissociação ou bloqueio de dados pessoais, suspensão da operação de tratamento, cancelamento dos dados pessoais, proibição do tratamento de dados sensíveis).

> **Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:**
> **I – multa simples ou diária;**
> **II – publicização da infração;**
> **III – dissociação dos dados pessoais;**
> **IV – bloqueio dos dados pessoais;**
> **V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;**
> **VI – cancelamento dos dados pessoais;**
> **VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e**
> **VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.**
> **§ 1º As sanções poderão ser aplicadas cumulativamente.**
> **§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.**
> **§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.**
> **§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.**
> **§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.**

Como é possível entender por meio da análise do texto do APL, para que sejam protegidos os direitos que dão origem a uma lei de proteção de dados, é necessário que exista um sólido aparato jurídico-administrativo. Assim como o demonstrado por meio da experiência de proteção

de dados dos países da União Européia, parece recomendável que seja criada uma autoridade de proteção de dados, ou até mesmo um sistema de proteção de dados. Vejamos a seguir algumas possibilidades de organização desta autoridade, ou deste sistema de proteção de dados.

Proposta de criação de um sistema nacional de proteção de dados pessoais

Conforme o exposto acima, a criação de uma entidade administrativa específica para garantir a proteção de dados poderia ser benéfica uma vez que maior especialização para a garantia da proteção de dados se faz necessária. A guarda e a proteção de dados é questão complexa, ainda mais num contexto em que tais dados dão armazenados em várias plataformas, por meio de tecnologias diversas, com diferentes características. A criação de uma autoridade é, portanto, um passo fundamental para a plena efetividade de dispositivos contidos no anteprojeto de lei de proteção aos dados pessoais e também de dispositivos relacionados à privacidade presentes na Lei 12.965/14, o Marco Civil da Internet brasileira.

Ademais, tais autoridades servem como fonte de referência em questões de privacidade e ajudam a dar coerência e lógica e técnica aos diferentes leis, documentos, regras relacionados à questão da privacidade. Todas as possíveis funções de uma autoridade se fazem ainda mais necessárias dados o contexto de crescente fluxo de dados, e da presença constante de tecnologias em diferentes âmbitos de nossas vidas.

É portanto necessário pensar nas opções jurídico-administrativas para a autoridade em questão . Conforme o descrito acima, a criação de uma autarquia poderia ser um dos caminhos. Contudo, tal modelo também enfrentaria limitações. Exploraremos também, portanto, a possibilidade de um sistema que envolveria outros órgãos além de uma autarquia. Vejamos abaixo.

CRIAÇÃO DE UMA AUTARQUIA

A criação de uma autarquia se justificaria em função de sua (i) natureza jurídica de direito público; (ii) independência e autonomia; e (iii) possibilidade de exercer poderes de polícia. De acordo com o descrito neste documento, este modelo se aproximaria do modelo de referência, o modelo usado nos países da União Europeia.

É necessário lembrar, contudo, que o poder de uma autarquia não pode ser oponível em relação aos órgãos que compõem a administração pública direta ou indireta, uma limitação de um modelo institucional baseado em uma autarquia. Assim, necessitamos pensar na em mecanismos de proteção de dados pessoais que também possam ser oponíveis a órgãos que compõem a administração pública.

Por fim, ressaltamos que caso seja criada uma autarquia, será necessária a aprovação de uma lei não apenas para a criação da autoridade em questão, mas também seria necessária uma lei caso seja necessário extingui-la.

CRIAÇÃO DE UM SISTEMA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

Sistemas nacionais de proteção, assim como o Sistema Nacional de Defesa do Consumidor (SNDC), como o Sistema Brasileiro de Defesa da Concorrência (SBDC), e o Sistema Nacional de Proteção e Defesa Civil (SINPDEC), são compostos por diferentes órgãos públicos e muitas vezes também por entidades civis. O SNDC, por exemplo, é composto pela SNDC a Secretaria Nacional do Consumidor do Ministério da Justiça e os demais órgãos federais, estaduais, do Distrito

Federal, municipais e as entidades civis de defesa do consumidor. Já o SBDC é formado pelo Conselho Administrativo de Defesa Econômica (CADE) e pela Secretaria de Acompanhamento Econômico do Ministério da Fazenda, com as atribuições previstas nesta Lei. Já o SINPDEC, é constituído pelos órgãos e entidades da administração pública federal, dos Estados, do Distrito Federal e dos Municípios e pelas entidades públicas e privada de atuação significativa na área de proteção e defesa civil.

Cada um dos órgãos e entidades que compõe os sistemas citados tem diferentes responsabilidades dentro do sistema, assim como aportam diferentes conhecimentos e exercem diferentes poderes.

A criação de um sistema nacional de proteção de dados seria uma forma de permitir que diferentes objetivos sejam cumpridos. Por exemplo, que a futura lei de proteção de dados assim como as normas dela decorrentes sejam oponíveis a entes públicos e privados. Além disso, permitiria que a elaboração de normas de forma a levar em consideração diferentes aspectos técnicos e políticos envolvidos. Assim, é possível que seja desenvolvido um sistema que conte com uma autarquia e um órgão da administração direta. Desta forma, as diferentes entidades trabalhariam de forma a coordenar a política pública e a regulação da proteção de dados. Ademais, outros atores também poderiam ser envolvidos no sistema, conforme o explicitado abaixo.

ENVOLVIMENTO DE DIFERENTES AGENTES INDEPENDENTEMENTE DO MODELO ADOTADO

Independentemente do modelo adotado para o "órgão competente" para a proteção dos dados no Brasil, tal composição institucional poderia ser complementada pela formação de um conselho - ou outra forma de colaboração - composto por membros da sociedade civil, da academia, do setor privado e do setor público. Este modelo de Conselho já é adotado por alguns sistemas nacionais. Como exemplo podemos citar o Conselho Nacional de Proteção e Defesa Civil (CONPDEC), parte do Sistema Nacional de Proteção e Defesa Civil (SINPDEC) mencionado acima e que conta com representantes da União, dos Estados, do Distrito Federal, dos Municípios e da sociedade civil organizada, incluindo representantes das comunidades atingidas por desastre, e por especialistas de notório saber. O Conselho tem diferentes atribuições, como auxiliar na formulação e propor normas, acompanhar o cumprimento das disposições legais e regulamentares de proteção e defesa civil, entre outros.

Além de trazer mais pluralidade às decisões, interesses estariam equilibrados, e capacidade técnica poderia ser aportada ao sistema. Esta forma multissetorial de atuação tem sido aplicada em outros âmbitos, como no Comitê Gestor da Internet (CGI), que conta em sua composição com representantes do setor público, privado, assim como da sociedade civil e academia. Este modelo tem sido apontado como referência de governança de políticas relacionadas à Internet. Conforme vimos acima, em alguns países da Europa, esta pluralidade de atores foi institucionalizada na proteção de dados pessoais, como no caso da França.

Conclusões

De acordo com a análise apresentada, há variadas vantagens na criação de uma autoridade específica para a proteção de dados e tal modelo já foi implementado em diversos países. Embora a criação de uma autoridade demande a alocação de recursos financeiros, humanos e políticos, esse é um passo fundamental para a plena efetividade de dispositivos contidos no

anteprojeto de lei de proteção aos dados pessoais e também de dispositivos relacionados à privacidade presentes na Lei 12.965/14, o Marco Civil da Internet brasileira. Além disso, a importância de uma autoridade aumenta com o exponencial crescimento do acesso e uso de tecnologias e consequente acesso a dados pessoais por diferentes entes públicos e privados também.

Já existe uma figura jurídico-administrativa que tem natureza similar àquelas das autoridades de proteção de dados usadas como referência. Seria necessário portanto escolher dentre as possibilidades existentes, quais sejam a de uma (i) autarquia; ou uma (ii) autarquia com regime especial. O que as diferencia é que, no caso das autarquias de regime especial, há maior autonomia, inclusive financeira, uma vez que este permite que sejam cobradas taxas administrativas.

Muito embora a criação de uma autarquia ofereça diversas vantagens, tal modelo teria limitações. Portanto, seria possível pensar num sistema nacional de proteção de dados, que incluísse não apenas uma autoridade parte da administração pública indireta - uma autarquia - mas também um órgão da administração pública direta. Assim, seria possível exercer poderes oponíveis tanto ao setor público como o privado.

Seria ainda interessante pensar em um sistema que inclua a sociedade civil, a academia e o setor privado nos debates, assim como outros érgãos da administração pública direta e indireta que tenham relação com o tema. Assim, independentemente da forma escolhida para uma autoridade de proteção de dados, é importante que sejam criadas instâncias de participação de destes diferente atores.

Estamos certos, no entanto, que a discussão a respeito do Anteprojeto de Lei simboliza um avanço do país no tocante à proteção de dados pessoais e de sua importância para o desenvolvimento econômico e social do país. Além disso, o anteprojeto sinaliza a necessidade da criação de uma autoridade específica para a proteção de dados pessoais, reforçando a possibilidade de efetivação dos direitos que se pretende proteger. Esperamos, portanto, que o documento apresentado seja um subsídio para esta importante discussão.

Princípios da privacidade desde a concepção (*privacy by design*) e privacidade como padrão (*privacy by default*)

As ideias de privacidade desde a concepção (privacy by design) e privacidade como padrão (privacy by default) implicam em esforços para reforçar a esfera protetiva da regulamentação da proteção de dados e vai ao encontro da ideia de que a privacidade é benéfica não apenas para os titulares de dados, mas também para a atividade empresarial, no sentido de que construir a privacidade desde o início e contemplando todo os sistemas de gestão de dados pode gerar muitos benefícios decorrentes do reforço da confiança (Cavoukian, 2011).

O conceito do princípio de "privacidade desde a concepção" foi proposto na recomendação da Comissão Européia de 10 de outubro de 2014 (2014/724/EU) relativa ao modelo de avaliação do impacto na proteção de dados no contexto das redes inteligentes e dos sistemas de contadores inteligentes, com a seguinte definição:

> **A «proteção dos dados desde a concepção» exige a aplicação, tendo em conta o estado da arte e o custo de execução, tanto no momento da determinação dos meios de tratamento como no momento do próprio tratamento, de medidas e procedimentos técnicos e organizacionais adequados para que o tratamento satisfaça os requisitos da Diretiva 95/46/CE e assegure a proteção dos direitos das pessoas em causa;**

O tema também foi explorado pelo grupo de trabalho Article 29 na Opinião 8/2014 sobre Internet das Coisas, no qual reconhece a proteção de dados como direito fundamental e destaca a importância da proteção de dados desde a concepção e por padrão em todos os níveis da cadeia de valor da Internet das Coisas, em particular para os fabricantes de dispositivos, desenvolvedores de aplicativos e plataformas sociais.

No contexto da reforma do marco legal sobre proteção de dados pessoais europeu, o Parlamento Europeu buscaram detalhar medidas técnicas e organizacionais para a implementação deste conceito. Segundo o órgão, os responsáveis deveriam ter em conta (i) o conhecimento técnico atual, as melhores práticas internacionais e os riscos representados pelo processamento de dados e (ii) a gestão do ciclo de vida dos dados pessoais e os resultados da avaliação de impacto, se houver, ao desenvolverem tecnologias de processamento de dados pessoais. O texto também adiciona a privacidade desde a concepção como um pré-requisito para os contratos públicos, em especial para as concessionárias.

A organização European Digital Rights (EDRI) defendeu que a proposta de privacidade desde a concepção indique que se refere tanto às medidas técnicas de arquitetura de produtos ou serviços, como a medidas organizacionais e de políticas operacionais do responsável - proposta incorporada no texto mais recente do Conselho da União Europeia. A entidade também apresentou uma proposição em que traz as definições de privacidade desde a concepção e privacidade como padrão nos seguintes termos:

> **A privacidade desde a concepção é o processo pelo qual a proteção de dados e a privacidade são integrados no desenvolvimento de produtos e serviços através de medidas**

> técnicas e organizativas. A privacidade como padrão significa que os produtos e serviços são, por padrão, configurados de forma que limita o processamento e, especialmente, a divulgação de dados pessoais. Em particular, os dados pessoais não devem ser divulgados a um número ilimitado de pessoas por padrão. (Tradução nossa)

Também nos Estados Unidos o tema tem sido alvo de discussões. A Federal Trade Commission (FTC) — entidade de proteção de direitos do consumidor e defesa da concorrência —, propõe a privacidade desde a concepção como um dos três princípios a construírem um panorama de respeito à privacidade do consumidor. Segundo a agência, o princípio apresenta dois aspectos:

- **A incorporação de medidas substantivas de proteção do direito à privacidade, na prática, pelas empresas e;**
- **A adoção de procedimentos de manutenção de dados específicos ao longo do ciclo de vida de seus produtos e serviços.**

O anteprojeto brasileiro não possui qualquer previsão explícita relativa ao princípio da privacidade desde a concepção, apesar de prever alguns de seus aspectos em seu rol de princípios (art. 6º) — em especial o princípio da prevenção (inciso VIII).
O art. 6º poderia fazer menção direta à aplicação do princípio de privacidade desde a concepção, reforçando a política protetiva da lei ao adiantar a preocupação com a proteção de dados pessoais desde momento inicial da elaboração de ferramentas e medidas organizacionais que podem impactar em sua esfera.

Essa opção legislativa poderia ser acompanhada de que garantissem que o princípio seja efetivamente incorporado na prática. Algumas das medidas discutidas em âmbito internacional e que poderiam ser incorporadas seriam: (i) a necessidade de mapeamento prévio de toda a gestão do ciclo de vida dos dados pessoais e dos riscos envolvidos no processamento de dados e a adoção das melhores práticas internacionais pelos responsáveis por tratamento de dados; (ii) a adoção de política de minimização da coleta de dados; (iii) a atenção ao princípio de privacidade desde a concepção como pré-requisito para os contratos públicos, em especial para aqueles em regime de concessão ou permissão; (iv) a responsabilização de todos os agentes que atuem na cadeia de tratamento de dados pelo respeito ao princípio.

Pode ser considerada ainda a possibilidade, sugerida pelo Conselho da União Europeia naquele contexto, de se desenvolver mecanismos de certificação para se demonstrar o cumprimento dos requisitos da privacidade desde a concepção pelos responsáveis e demais agentes que realizam o tratamento de dados.

O conceito da privacidade como padrão prevê que qualquer sistema que envolva dados pessoais deve ser configurado, por padrão, da forma mais protetiva da privacidade. Isso significa que os serviços e produtos cujo uso implica a coleta e o tratamento de dados pessoais devem, por padrão, ser configurados em conformidade com os princípios gerais de proteção de dados, tais como a minimização dos dados e a limitação da finalidade.

Apesar de ser aplicável tanto no ambiente online como nos tratamentos de dados em geral, esse princípio tem especial implicação no contexto da internet, buscando impedir que, por exemplo,

as configurações de redes sociais ou plataformas similares determinem que todos os conteúdos publicados sejam compartilhados com todos por padrão, inclusive em outras páginas, mecanismos de busca, etc. A ideia é garantir a proteção do usuário que, muitas vezes, ao interagir nesses ambientes têm a expectativa de que seus dados serão visíveis apenas no âmbito em que foram compartilhados (entre amigos, dentro de uma determinada plataforma, etc.).

Tendo como base a assunção de que as funções de um determinado produto ou serviço que afetem a privacidade devem limitar o tratamento de dados ao mínimo necessário e de que a possibilidade de ampliar esse tratamento deve ser exclusivamente do sujeito detentor desses dados, defende-se a implementação da privacidade por padrão bucando promover um equilíbrio entre os dados coletados e os serviços oferecidos.

O Grupo de Trabalho Article 29, por exemplo, afirma que o princípio da privacidade como padrão deve orientar a construção de aplicativos e dispositivos de forma a contribuir para limitar o impacto e a extensão de possíveis violações de dados pessoais, desabilitando por padrão funcionalidades críticas e evitando o uso de fontes de atualização de softwares não confiáveis. De maneira geral, conclui que todas as partes interessadas devem aplicar estes princípios e adotar um política de minimização dos dados de forma que a quantidade de dados coletados seja limitada apenas ao que é exigido para fornecer o serviço.

Na medida em que o art. 23 da proposta de regulamentação européia não prevê expressamente que devam ser adotadas as medidas técnicas e organizacionais que garantam a implementação da proteção à privacidade como padrão, especialistas em proteção de dados têm pleiteado maior especificação no texto legal, reforçando a proposta de lei nesse sentido. Dessa maneira, sem que os usuários precisem tomar qualquer medida afirmativa, seus dados não serão acessíveis a um número indefinido de indivíduos e os próprios usuários terão controle mais robusto sobre o compartilhamento de seus dados pessoais.

As consequências do compartilhamento público de certas informações pode, em muitos casos, ser irreversível, uma vez que outros usuários podem se apropriar e compartilhar os mesmos dados de forma independente e incontrolável por quem o postou inicialmente. A garantia pleiteada tem, desse modo, destacada importância

Além disso, relatório recente publicado por pesquisadores de duas universidades belgas a respeito do monitoramento massivo realizado pelo Facebook aponta que a preocupação com as configurações de privacidade devem ocorrer não apenas na relação entre os usuários, mas também em relação à própria plataforma e seus parceiros. Os padrões utilizados pela rede social foram classificados como problemáticos, na medida em que os mecanismos de "opt out" dão uma falsa impressão de que o usuário teria o controle de seus dados, quando, perante a plataforma e terceiros associados não é permitida a administração das configurações de compartilhamento de informações.

No contexto brasileiro, a ideia do princípio da privacidade como padrão encontra-se de alguma forma refletida no rol de princípios do anteprojeto de lei de proteção de dados pessoais atualmente submetido a debate público (art. 6º), em especial os princípios da finalidade, da adequação, da necessidade, da qualidade dos dados e da segurança.

O princípio poderia ser incluído como princípio independente no rol do art. 6º e poderia apresentar a seguinte definição:

> **Art. 6º [...]**
> **princípio da privacidade por padrão, pelo qual as configurações de privacidade dos produtos ou serviços devem ser as mais protetivas possíveis, considerando os estritos fins que legitimaram a coleta de dados, tanto em aspectos técnicos como organizacionais, sendo facultado ao usuário alterá-las para padrões mais públicos.**

Essa possibilidade pode ser acompanhada da especificação de algumas garantias da privacidade como padrão de forma que contemple:

I. **a garantia que os dados dos usuários não estarão, por padrão, disponíveis a um número indefinido de indivíduos e que os próprios sujeitos de dados poderão controlar a distribuição e circulação desses dados;**
II. **a incidência sobre a própria empresa que coleta e processa dados no que diz respeito à sua política de compartilhamento de dados com parceiros, bem como a incidência no que diz respeito a publicização de dados em relação a outros usuários;**
III. **a permissão e o estímulo do uso de pseudônimos, sempre que a política de nome verdadeiro não for estritamente necessária para o oferecimento do produto ou serviço.**

Direitos do titular: a portabilidade de dados

A garantia da portabilidade visa permitir que o titular possa transferir suas informações pessoais de um responsável para outro sem impedimentos técnicos ou de outra natureza. Ela se somaria aos direitos do titular, portanto, reforçando o interesse do indivíduo, num contexto de incremento das comunicações online, de obter cópias de seus dados pessoais a fim de reutilizá-los em outras plataformas ou sistemas. Com isso, além de fortalecer a proteção do titular ao permitir que ele efetivamente goze de seu direito de escolha, a medida estimula a concorrência, uma vez que restringe a possibilidade aprisionamento (ou "lock-in") de usuários em determinados produtos ou serviços.

Decorrente do direito do titular de livre acesso aos dados, o direito à portabilidade consiste em uma ferramenta de proteção do direito humano à privacidade na medida em que garante o efetivo controle do cidadão sobre o destino e uso de seus dados pessoais ao permitir a migração entre diferentes serviços e plataformas. Modelos que prevêem o fornecimento de dados de modo interoperável garantem que o controle dos dados caiba unicamente ao titular.

Nesse sentido, o direito de mover dados de um provedor para um outro é instrumental a fim de garantir ao titular de dados pessoais a possibilidade de mudar de serviço, inclusive migrando para aqueles que protejam sua privacidade de maneira mais efetiva. Paralelamente, a portabilidade estimula o surgimento de novos serviços - que podem, inclusive, promover uma maior proteção aos dados pessoais como elemento para a atração de novos usuários - e competição entre eles.

No âmbito europeu, a preocupação com a portabilidade encontra-se refletida no artigo 18 da proposta de Regulamento geral sobre a proteção de dados pessoais da Comissão Europeia. Naquele contexto, o direito à portabilidade apresenta dois elementos: (i) o direito dos indivíduos cujos dados pessoais são processados eletronicamente e "estruturado em um formato comumente utilizado" a obter cópia desses dados para utilização posterior, e; (ii) o direito de os titulares de dados transferirem seus dados pessoais de um responsável pelo tratamento de dados para outro.

É importante observar que a previsão europeia poderia ter aplicabilidade limitada, na medida em que se referiria apenas aos dados pessoais que sejam processados em "formato comumente utilizado", ainda que não seja claro o significado prático dessa expressão. Nesse sentido, a autoridade de proteção de dados inglesa alerta para o perigo de que os responsáveis se utilizem da expressão "formatos comumente utilizados" para afastar a necessidade de oferecer o direito a portabilidade ao processar dados pessoais em formatos não comumente utilizados.

Outra questão que se discute é que impor a garantia de portabilidade pode representar um fardo a alguns responsáveis pelo tratamento de dados, porque lhes poderia gerar custos adicionais excessivos (Bapat, 2013). De fato, a determinação do direito à interoperabilidade, que inclua a disponibilização, sempre que possível em formatos abertos[49], poderia implicar em custos de

[49] Nesse sentido, a European Digital Rights (EDRi) também propõe uma emenda ao artigo 18 da reforma da diretiva europeia Proposta de emenda à reforma disponível em: http://protectmydata.eu/articles/articles-11-20/article-18/.

conversão de dados que já foram organizados num formato não-interoperavel para um formato interoperável.

Outro risco discutido no contexto europeu é de que o direito do titular de obter cópia de seus dados não deve ser aplicável quando não puder ser implementado sem revelar dados pessoais de terceiros ou dados confidenciais do responsável. Além disso, o Conselho da União Europeia afirma que a portabilidade não deve ser aplicada quando infringir a propriedade intelectual relativa ao processamento de dados. Para o órgão, a portabilidade inclui o direito do titular de "receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento dos dados, num formato estruturado, de uso corrente e de leitura automática" e "de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem se forneceram os dados o possa impedir, sempre que: [o] tratamento se baseie no consentimento [...] ou num contrato [e o] tratamento for realizado por meios automatizados."[50]

Considerando essas preocupações, chega-se a opinar que[51] seria mais adequado tratar a portabilidade em leis de direito da concorrência ou de propriedade intelectual, além d incluir o tema nas leis de proteção de dados pessoais, já que o assunto também diria respeito ao funcionamento de mercados.

O Relatório do Comitê de Liberdades Civis, Justiça e Assuntos Internos do Parlamento da União Europeia, ressalta o direito à portabilidade como um dos aspectos do direito do titular de acesso aos seus dados e também destaca a necessidade de se relacionar o direito à portabilidade com a necessidade de exclusão de dados, no sentido de que o respeito à portabilidade de dados não poderá servir como justificativa para a retenção indevida de dados que já não atendem mais a necessidade do processamento, os quais deverão ser excluídos.

O texto do APL brasileiro refletiu em seu art. 18, § 3º, a preocupação com a portabilidade, sem apresentar as limitações ao formato "comumente utilizado" ou a necessidade de um contrato entre responsável e titular, o que parece constituir um panorama mais protetivo do que o europeu. Ele afirma que:

> **Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:**
> **I – em formato simplificado, imediatamente; ou**
> **II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.**
> **§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.**
> **§ 2º As informações e dados poderão ser fornecidos, a critério do titular:**
> **I – por meio eletrônico, seguro e idôneo para tal fim; ou**

[50] Artigo 18 da Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Bruxelas , 2012/0011 (COD), 11 de junho de 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pt/pdf

[51] Portabilidade de Dados (artigo 18), comentado pelo escritório de direito internacional Olswang, especializado em tecnologia, mídia e telecomunicações. Disponível em http://www.olswang.com/eu-data-protection-reform/data-portability/.

> **II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.**
> **§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.**

No entanto, assim como no contexto europeu, parece importante estabelecer expressamente que o direito a portabilidade é estabelecido sem prejuízo da necessidade de exclusão de dados quando não mais necessários. Além disso, nos parece importante aperfeiçoar a redação do artigo de forma a estabelecer o direito a obter cópia interoperável, e que tal interoperabilidade pode ser realizada mais eficazmente através do uso de formatos abertos..

Por fim, há de se estabelecer critérios mais específicos para a garantia do direito a portabilidade, equilibrando esse direito com o correspondente ônus gerado aos diferentes responsáveis por tratamento de dados, de forma a evitar obrigações excessivas. Nos parece que uma futura autoridade garantidora independente de proteção de dados pessoais poderia incorporar essa atribuição, na medida em que terá a expertise necessária para estabelecer parâmetros que sejam compatíveis com a realidade, de acordo com o estado da arte da tecnologia.

Referências

Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. 2011.

Article 29 Data Protection Working Party. Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector. 2014.

Article 29 Data Protection Working Party. Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes. 2014.

Article 29 Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things.

BAKOS, Yannis and MAROTTA-WURGLER, Florencia and TROSSEN, David R. "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts". In: Journal of Legal Studies, Vol. 43, No. 1, 2014; CELS 2009 4th Annual Conference on Empirical Legal Studies Paper; NYU Law and Economics Research Paper No. 09-40. 2014. Disponível em http://ssrn.com/abstract=1443256 (consultado em 11/05/2015).

BAPAT, Anita. "The new right to data portability". In: Privacy & Data Protection Journal, Volume 13, Nº 03, 2013.

BRAGA NETTO, Felipe Peixoto. Manual de direito do consumidor: à luz da jurisprudência do STJ. 2014.

BRUNO, Fernanda. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

Cavoukian, Ann. "Privacy by Design: Origins, Meaning, and Prospects." Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards (2011): 170. Disponível em: https://www.privacybydesign.ca/content/uploads/2012/04/Privacy-by-Design-Origins-Meaning-and-Prospects.pdf

COHEN, Julie E., "What Privacy Is For". In: Harvard Law Review, Vol. 126, 2013.

Commission of the European Communities, v. Germany, E.C.J., No. C-518/07, 3/9/10

Diretiva 95/46/CE do Parlamento Europeu e do Conselho. 24 de Outubro de 1995. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=en

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

European Agency for Fundamental Rights (FRA). Data Protection in European Union: the role of National Data Protection Authorities. 2010. Disponível em http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

Latanya Sweeney, Uniqueness of Simple Demographics in the U.S. Population (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000).

MARQUES, Claudia Lima. "Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002". In: Revista da Esmese, Nº 07, 2004 - DOUTRINA - 17 Disponível em http://www.estig.ipbeja.pt/~ac_direito/ClaudiaLM.pdf.

MCDONALD, A. M., & CRANOR, L. F. "The cost of reading privacy policies". In: ISJLP, 4, 543. 2008.

MORAES, Paulo Valério Dal Pai. Código de Defesa do Consumidor: o Princípio da Vulnerabilidade. 3. ed. Porto Alegre: Livraria do Advogado. 2009.

Ohm, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization." UCLA Law Review 57 (2010): 1701.

Protocolo Adicional da Convenção de Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais, de 28 de Janeiro de 198. Disponível em http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

SARMENTO, Daniel. Direitos Fundamentais e Relações Privadas. Rio de Janeiro: Lumen Juris, 2004.

SOLOVE, Daniel. Introduction: Privacy self-management and the consent dilemma. In Harvard law review, 2013. Vo. 126: p. 1884. Available em: http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf. Access: em 05 de janeiro de 2014. p. 1880-1903.

Sweeney L, Abu A, Winn J (2013) Identifying Participants in the Personal Genome Project by Name (A Re-identification Experiment). ArXiv.

Centro de Tecnologia e Sociedade FGV DIREITO RIO (CTS-FGV)

Coordenação:
Luiz Fernando Marrey Moncau
Marília Maciel

Pesquisadores envolvidos no desenvolvimento desta contribuição:
Jamila Venturini
Luca Belli
Luiza Louzada
Nathalia Foditsch
Pedro Mizukami

Agradecemos aos seguintes pesquisadores que se dispuseram a discutir conosco temas relacionados à contribuição:
Bruno Bioni
Danilo Doneda
Eduardo Jordão
Katarzyna Szymielewicz
Katitza Rodriguez
Marília Monteiro
Nicolo Zingales
Renato Leite