CONTRIBUIÇÕES À CONSULTA PÚBLICA
DO MINISTÉRIO DA JUSTIÇA
SOBRE O PROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

A Cisco, maior empresa do mundo de equipamentos de rede e TI, não só desenvolve a tecnologia para as redes de banda larga do mundo, mas também as tecnologias para a sua construção e que permitem a entrega dos serviços de rede e aplicações de ponta.

Para contribuir com o presente debate, gostaríamos de compartilhar algumas preocupações relacionadas com a abordagem do projeto de lei de proteção de dados pessoais que, quando relacionada com alguns campos específicos da tecnologia em desenvolvimento, pode impedir o desenvolvimento e o acesso dos cidadãos brasileiros a valiosas tecnologias.

Entendemos os objetivos do governo Brasileiro para estabelecer mecanismos de proteção ao tratamento e uso de dados pessoais. Contudo, as implicações dessas regras devem ser cuidadosamente avaliadas, principalmente com o intuito de evitar barreiras à inovação e a adoção de tecnologias de ponta e aplicações o que é essencial para garantir que essas regras não se transformem em uma barreira para o desenvolvimento dos ecossistemas de nuvem e TIC no Brasil.

A Internet se desenvolveu nos últimos anos se tornando uma plataforma aberta a inovação e com poucas barreiras de acesso aos usuários finais, aos fornecedores de conteúdo e aplicações. Certamente a Internet e a economia digital tem desempenhando um papel importante no crescimento e inovação da economia brasileira.

No Brasil, o número de pessoas conectadas cresceu 2.095% entre 2000 e 2013. A entrada de novos usuários em um mundo conectado só tem a trazer benefícios em termos do ecossistema como um todo, criando uma demanda para a expansão da rede, investimentos em infraestrutura e inovação.

A estrutura regulatória existente visa promover a capacidade, pelos usuários finais, de acesso e distribuição de informações bem como de executar aplicações e serviços de sua escolha e acreditamos que esse deve ser mesmo o caminho a ser seguido.

Nesse sentido, compartilhamos através deste documento algumas considerações a respeito do anteprojeto de lei e informações importantes a respeito da Internet das Coisas e as devidas implicações da lei neste e em contextos que surgirão no futuro.

Sobre a Internet das Coisas

A discussão em torno do Internet das Coisas ("IoT"), ou “Internet of Everything”, está em seus estágios iniciais. Muito se tem discutido sobre os princípios que podem ser adotados para regular este tipo de atividade, tendo em conta que, devido à sua natureza, certos tipos de controle poderiam cercear sua funcionalidade e desenvolvimento.

A Internet das Coisas é a primeira grande revolução da Internet, que está em constantes desenvolvimento e aperfeiçoamento, mas basicamente possui as mesmas funções para as quais foi projetada no início. A Internet é padronizada em IP, embora hoje em dia existam várias outras formas de protocolo de comunicação, como o Apple Talk and Token Ring, por exemplo[1].

Sendo assim, a Internet das Coisas é considerada como a primeira evolução real da Internet, conduzindo o desenvolvimento de ferramentas revolucionárias, com o poder de beneficiar nosso estilo de vida, a forma como realizamos negócios, desenvolvemos a educação e o entretenimento.

A Internet das Coisas abrange diferentes tipos de funcionalidade que, atribuídas aos objetos do cotidiano conectados à Internet, lhes permite desempenhar uma séria de novas funções. Podemos exemplificar com dispositivos automotivos, residenciais e para uso pessoal, que controlam o nível de sono e de exercícios diários, além de dispositivos para a área de saúde que podem monitorar dados médicos, como em pacientes portadores de diabetes, por exemplo.

Estamos à beira de uma era em que tudo, desde carros, árvores, iluminação pública e até mesmo vacas[2] pode ser dado um endereço de Internet e conectado a uma rede em constante expansão. Isto é o que nós descrevemos como a "Internet of Everything", e que se baseia na ideia de que quando você traz pessoas, processos, dados e coisas juntos, oportunidades sem paralelo podem ser criadas.

Imagine como será o futuro daqui a 5, 10 ou 25 anos. As pessoas, processos, informações, estarão todos conectados e, em 2020, um colosso de 50 bilhões de dispositivos estarão compartilhando o que conhecemos hoje como a Internet, com tecnologia móvel pessoal, em constante mudança, fácil de usar, muitos observaram que estamos vivendo agora em um mundo hiperconectado. Mas apesar de todas essas conexões, estimamos que mais de 99% de todos os objetos físicos que podem um dia se juntar a rede atualmente ainda não estão conectados. Apenas começamos a conectar os “desconectados”

1 Mais informações disponíveis em: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

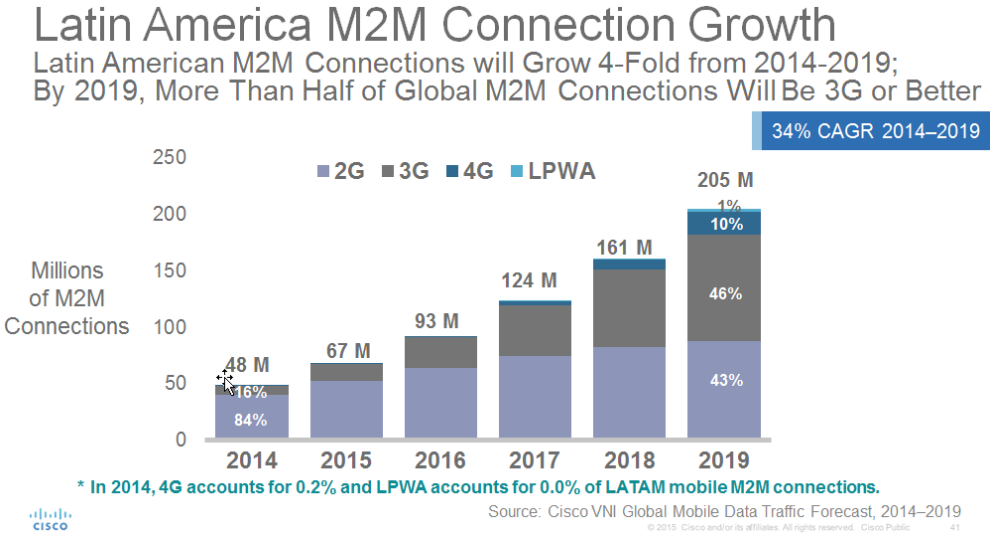
2 A Dutch start-up company, implant sensors in the ears of cattle, allowing farmers to monitor cows health and track their movements, ensuring a healthier supply of food to consume

Estamos construindo a próxima geração da via super conectada que irá fornecer a plataforma de inovação que vai gerar e nutrir a próxima geração de inovação disruptiva e criativa, gerando empregos e crescimento econômico. A Internet de todas as Coisas eleva o campo entre as grandes organizações e empresas de pequeno porte - não se trata de tamanho, é sobre a engenhosidade e ousadia da própria ideia. Como a tecnologia continua a se desenvolver em torno de nós, como conexões de se tornar mais inteligente e mais rápido, só veremos aplicativos mais criativos e inovadores da Internet das Coisas, e eles vão literalmente mudar o mundo.

Na prática, trata-se de histórias, como varejistas transformando a experiência na loja com os dados dos clientes mais perspicazes e relevantes, bem como otimizar suas cadeias de abastecimento e de valor. Trata-se de concessionárias de serviços públicos que entregam maior clareza e controle através da aplicação de medidores inteligentes. Da mesma forma, trata-se de um paciente conectado que monitoram a si mesmos e fornecem uma visão real para os clínicos e médicos de seu estado de saúde.

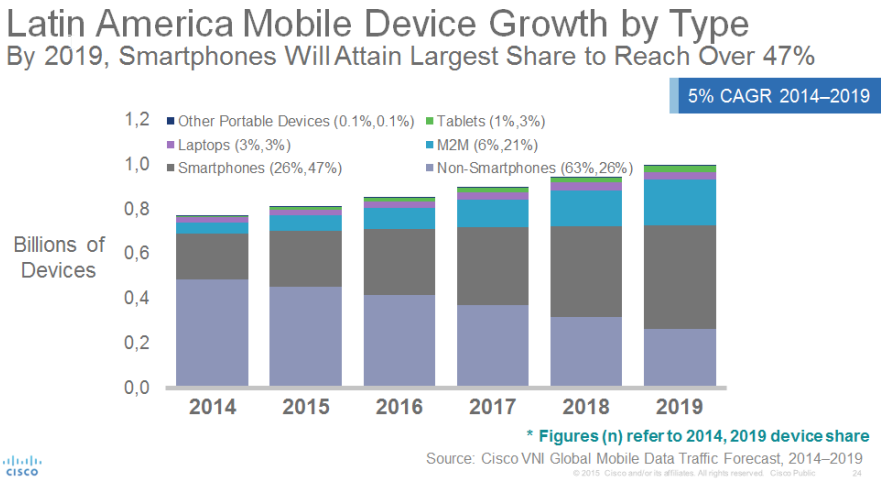
Já existem dispositivos portáteis concebidos para pessoas idosas que permitem o monitoramento de sinais vitais. As informações podem ser disponibilizadas em tempo real a um profissional de saúde que pode prestar socorro em casos urgentes como, por exemplo, nos casos de quedas em que o idoso não consegue se levantar, as informações são disponibilizadas como um alerta para atendimento imediato.

No Brasil, estima-se que haverá 645,0 milhões de dispositivos em rede em 2018, contra 418,5 milhões em 2013, e 3,1 dispositivos em rede por habitante em 2018, acima dos 2,1 per capita em 2013. E em relação à IoE, módulos M2M serão responsáveis por 29% (187,5 milhões) de todos os dispositivos de rede em 2018, em comparação com 16% (65,4 milhões) em 2013, (23,5% CAGR).

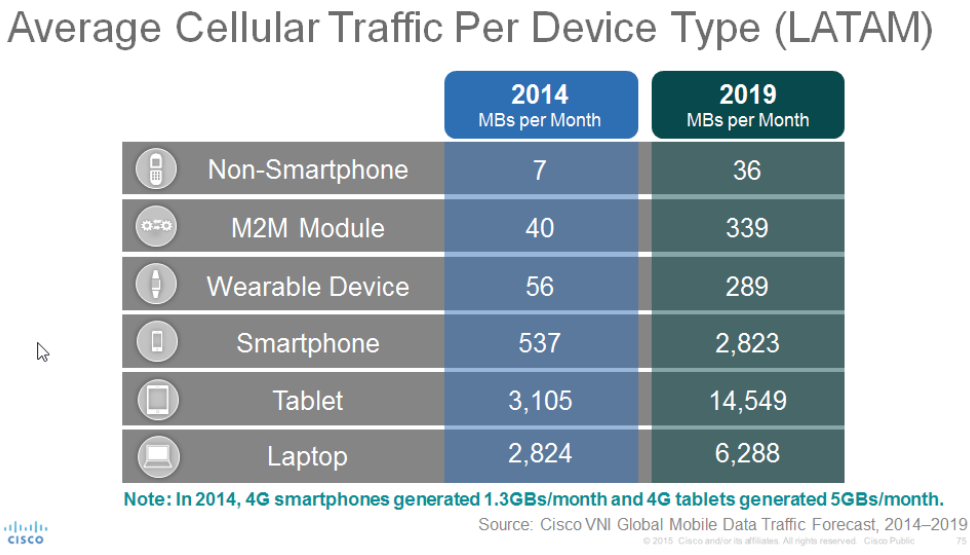


Dispositivos M2M irão aumentar de 6% em 2014 para 21% em 2019, o maior

crescimento será em Tablets (CAGR de 38%) e M2M (CAGR de 34%). Mundialmente, em 2014, um dispositivo inteligente gerará 22 vezes mais tráfego do que um dispositivo não-inteligente.



Globalmente, M2M em média gerará 366 megabytes de tráfego de dados móveis por mês em 2019, acima de 70 megabytes por mês em 2014. Excluindo LPWA, irá gerar 515 megabytes de tráfego de dados móveis por mês em 2019, acima de 70 megabytes por mês em 2014. Considerando dispositivos 'wearable' ou seja, aqueles que usamos em nossos corpos irão gerar 479 megabytes de tráfego de dados móveis por mês em 2019, acima dos 141 megabytes por mês em 2014. Estes números são impressionantes e só podemos imaginar a demanda eles vão trazer a rede de telecomunicações existente para transportar tais dados.



Estamos apenas arranhando a superfície do que é possível. Não sabemos quais aplicações e serviços serão moldados na Internet no futuro. Para continuar inovando é necessário garantir o acesso a todas as funcionalidades desenvolvidas, atendendo as necessidades dos usuários e as sugestões de melhorias.

Dessa forma, regras que buscam, por exemplo, a limitação do processamento de dados a um "mínimo" podem afetar o desenvolvimento da tecnologia e da economia, tendo em vista que novas funcionalidades e benefícios podem ser encontrados após a coleta de dados.

Igualmente, o consentimento expresso prévio sugerido pelo anteprojeto de lei seria impraticável em uma série de aplicativos e dispositivos disponíveis para o uso em automóveis e residências, que controlam desde a rota de navegação até o horário de acendimento de luzes, por exemplo. Ou, no caso dos pacientes que utilizam os monitores de saúde descritos anteriormente, certamente não seria possível a coleta de consentimento expresso todas as vezes que os dados fossem coletados e tratados[3]. Além disso, estamos apenas no início da revolução da Internet e a maior parte das aplicações e seus diferentes usos ainda estão para serem desenvolvidos.

De acordo com o projeto de lei, no que diz respeito ao "consentimento" dos usuários para o tratamento de dados e trazendo sua aplicação para o cenário da Internet das Coisas, acreditamos que os consumidores poderão ser sobrecarregados com pedidos de consentimento, impossibilitados de distinguir suas próprias prioridades. Tudo isso, certamente, quando tal consentimento expresso for possível, quando, na verdade, a maior parte dos mecanismos envolvendo a Internet das Coisas está relacionada com operação maquina a maquina ("M2M").

O objetivo do projeto de lei não é minar a capacidade dos consumidores de exercerem suas habilidades de suas informações pessoais. E sim proporcionar meios para que o consumidor realize escolhas significativas com base na necessidade real do seu consentimento para coleta e tratamento de dados. A redução das hipóteses em que esse mecanismo se faz necessário dará um caráter mais significativo ao consentimento.

Dentro do contexto de Internet das Coisas e análise de "big data", o consentimento expresso e específico sugerido no projeto de lei não poderá sempre ser obtido de maneira prática. Todavia, outras formas legítimas de processamento deveriam ser consideradas, com o intuito de facilitar o uso responsável de dados que são benéficos para os indivíduos e para sociedade e que permitem práticas legítimas de negócios e inovação, evitando danos e respeitando a privacidade dos indivíduos.

Neste sentido, uma determinação rígida de requisição de consentimento do usuário, conforme previsto no projeto de lei é impraticável e resultaria em um consentimento ilusório e desinformado e poderia minar as proteções efetivas de privacidade.

Assim como apontado pela autoridade norte-americana responsável pelas normas de proteção de dados (FTC) no relatório "Privacy and Security in a Connected World"[4], a indústria

3 https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things

4 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

da Internet das Coisas está relativamente em seu estado inicial e não há necessidade de abarcar privacidade e riscos à segurança através de uma legislação específica para o tema no momento.

Nesse sentido, destacamos, como exemplo, o "legítimo interesse", tido como base nas operações de processamento de dados no âmbito da Diretiva de Proteção de Dados da União Europeia e do Regulamento de Proteção de Dados em discussão atualmente na UE, e que entendemos deva ser utilizado de referencia na construção da legislação brasileira, principalmente porque permite que um controlador processe dados na existência de um interesse legítimo seu ou de um terceiro envolvido no processo, desde que não ultrapasse direitos ou liberdades fundamentais garantidos aos indivíduos[5].

Conforme dito até aqui, o fornecimento do consentimento para coleta e uso de dados deve ser obrigatório nos casos em que as alterações na tecnologia, sejam de fato relevantes. Considerando o constante desenvolvimento da Internet das Coisas, pequenas alterações e correções não podem ser determinantes para a obrigatoriedade de um novo consentimento por parte do usuário para continuidade da utilização do produto ou serviço, pois acaba por criar confusão e distração do usuário para as alterações realmente significativas e para as quais ele deve efetivamente prestar atenção.

Igualmente, o anteprojeto, da forma como proposto, apresenta um desafio sobre a óptica da Internet das Coisas na medida em que permite que a autoridade competente determine um tempo máximo para o tratamento de dados, exigindo o cancelamento do tratamento depois de decorrido esse período máximo a ser estipulado. Acreditamos que seria extremamente prejudicial para a inovação e o desenvolvimento econômico como um todo que tal limitação faça parte do escopo da legislação, especialmente dentro do contexto da Internet das Coisas.

Conforme exposto, a Internet das Coisas pode fornecer uma gama de mecanismos inovadores para melhorar e facilitar a vida humana, e, mesmo com o desenvolvimento de todos os produtos já existentes, sabemos que muito mais está por vir e colocar estes mecanismos sob o controle de proteção de dados neste momento pode retardar o desenvolvimento dessas tecnologias em um período de crise financeira, quando eles poderiam ser mais necessários.

---

5 No que consiste a preocupação com a regulamentação da UE, a abordagem recomendada pelos reguladores de proteção de dados é abordagem da "privacidade desde a concepção". O atual projeto de regulamentação Privacidade na UE estabelece que: A proteção dos direitos e liberdades dos titulares dos dados relativamente ao tratamento dos seus dados pessoais exige a tomada de medidas técnicas e organizacionais adequadas, tanto no momento da conceção como no momento da execução do tratamento, para assegurar o cumprimento dos requisitos do presente regulamento. A fim de assegurar e comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deve adotar regras internas e aplicar medidas apropriadas que devem respeitar, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. ***O princípio da proteção de dados desde a conceção obriga a que a proteção de dados seja inserida em todo o ciclo de vida da tecnologia, desde a fase inicial de conceção, até à sua instalação, utilização e eliminação finais. Isto deve abarcar também a responsabilidade pelos produtos e serviços utilizados pelo responsável ou pelo subcontratante. O princípio da proteção de dados por defeito obriga a que as definições de privacidade aplicáveis a serviços e a produtos cumpram, por defeito, os princípios gerais da proteção de dados, tais como a minimização dos dados e a limitação das finalidades.*** http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//PT

Assim como aconteceu com outras tecnologias, os cidadãos certamente se preocupam com sua privacidade e precisam entender exatamente como suas informações serão utilizadas. Portanto, acreditamos fortemente que, como já é na prática[6], a transparência e o livre acesso à informação sobre os mecanismos envolvidos nas funcionalidades das tecnologias da Internet das Coisas são essenciais para apoiar a sua implementação junto aos cidadãos.

Dessa forma, enfatizamos que a tecnologia da Internet das Coisas, por suas características específicas e funcionalidades, não deveria ser discutida no âmbito desse projeto de proteção de dados pessoais ou, alternativamente, no mínimo, deveria estar enquadrada dentro das exceções específicas ao consentimento expresso.

COMENTÁRIOS ESPECÍFICOS – APL

Tendo em vista as informações apresentadas anteriormente, e para que possamos melhor esclarecer nosso entendimento, apresentamos também algumas observações específicas para alguns itens do projeto de lei, para os quais entendemos que uma abordagem alternativa e discussões mais profundas devem ser consideradas.

Disposições Preliminares

> **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.
>
> **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.
> **§1º** - Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> **§ 2º** - Esta Lei não se aplica aos tratamentos de dados:
> I – realizados por pessoa natural para fins exclusivamente pessoais; ou
> II – realizados para fins exclusivamente jornalísticos.
> **§ 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

6 Na cidade de Aurora, Estados Unidos, onde foi implementado um novo sistema de controle por câmera nas vias públicas, os cidadãos temiam a vigilância e um efeito de "big brother". Para melhor resolver essas preocupações a cidade autorizou os cidadãos a rever os vídeos gravados para compreender melhor a prática. http://www.govtech.com/library/papers/How-the-Internet-of-Everything-Can-Unlock-New-Possibilities-for-Cities-Across-the-Globe-1409.html

> mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.
>
> **Art. 3º** - As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
>
> **Parágrafo único**. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.
>
> **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.

Como mencionado anteriormente, em muitos contextos, como a Internet Da Coisas, o consentimento expresso é impraticável. Consentimento expresso é impraticável em uma infinidade de aplicações e dispositivos concebidos para funcionar em carros, casas, *wearable*s e tantos outros usos de dispositivos conectados, bem como no contexto de *big data* ou de inovação baseada em dados.

Consideramos que a transparência é a principal medida a ser adotada perante o consumidor, especialmente no que diz respeito ao funcionamento de dispositivos IoT, estimulando o uso consciente desses mecanismos. Certamente o objetivo dessa legislação não é o de impedir o desenvolvimento, mas sim apresentar mecanismos que legitimem o uso de dados conscientemente. Dessa forma, reforçamos ao legislador brasileiro que leve em consideração considere os riscos de um regime de consentimento de uso de dados altamente restritivo e suas consequências no desenvolvimento econômico do país num futuro próximo.

Dados Pessoais, Dados Anônimos e Dados Sensíveis

> **Art. 5º** Para os fins desta Lei, considera-se:
> I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;
> II – tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou

fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;
III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;
IV – dados anônimos: 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;
V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;
VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;
VII – consentimento: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;
X – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;
XI – interconexão: transferência de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;
XII – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma;
XIII – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;
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;
XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;
XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;
XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e
XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

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.
§ 3º Nos casos de aplicação do disposto nos itens 'a' e 'b' pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do §1o do art. 6o.

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.

A definição de dados pessoais poderia ser melhor definida, indicando que dados são aquilo que está relacionado com uma pessoa, identificável através de meios utilizados pelo responsável pelo tratamento. Os dados requerem proteção quando uma pessoa responsável tem interesse em relacioná-lo com um suporte e usá-lo de alguma forma. Assim, pode-se afirmar que é desproporcional exigir medidas de proteção especiais, quando a pessoa responsável não está realmente tentando identificar o titular de algum dado, e que para isso precisaria sair do seu escopo de trabalho.

Acreditamos que o âmbito da definição de "tratamento", tal como proposto, é muito amplo e pode levar à confusão e falta de segurança jurídica quando vier a ser implementado pela autoridade competente. Portanto, gostaríamos de sugerir a revisão da definição de tratamento incluindo as atividades claramente identificáveis, suprimindo sinônimos. Por exemplo, o significado de transporte pode ser igual ao de transmissão no presente caso.

O projeto de lei deve ser construído sobre princípios e definições de conceitos claros e irrefutáveis, garantindo clareza nos direitos e deveres envolvidos. Em outras palavras, o projeto deve evitar o uso de definições que possuam um significado diferente em outro contexto legal, como o uso do termo "interconexão", que é, por definição contida na legislação específica de telecomunicações (Lei nº 9.472 / 97 -. LGT[7]), a funcionalidade de conexão que liga redes compatíveis de telecomunicações e serviços de telecomunicações, com todas as implicações legais e fiscais que tal tratamento envolve.

Observamos ainda que uma série de definições são variações sobre a divulgação de dados para outra parte (ou, no caso da interconexão outra base de dados). Acreditamos ser recomendável uma compilação das definições propostas, a fim de se evitar falta de clareza na aplicação do conceito. Nesse sentido, sugerimos que haja um esclarecimento sobre a razão da obrigação de duas empresas obterem o consentimento quando a transferência de dados se dará de um 'banco de dados' para outro dentro da mesma empresa, para além que do é alcançado pelas cláusulas sobre transferência de dados internacional.

Finalmente, ainda analisando as definições propostas no projeto de lei, também gostaríamos de chamar a atenção para o conceito de dados anônimos. Embora o projeto apresente uma definição de dados anônimos, ele não consegue excluir expressamente esses dados do âmbito de aplicação da lei, o que sugerimos que seja esclarecido, ainda que mantendo a interpretação padrão, na medida em que tais dados não são, por sua própria natureza, dados pessoais.

Entendemos que essa interpretação está correta, já que os dados anônimos não são considerados dados pessoais por não permitirem uma identificação razoável e, portanto, não devem receber o mesmo grau de proteção que os dados pessoais.

Consentimento

> **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.
> **§2º** É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.
> **§3º** O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.
> **§4º** O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.

7 LGT – Art. 146 - Parágrafo único. Interconexão é a ligação entre redes de telecomunicações funcionalmente compatíveis, de modo que os usuários de serviços de uma das redes possam comunicar-se com usuários de serviços de outra ou acessar serviços nela disponíveis.

§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.
§6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.
§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.
§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.

Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.

Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:
I – finalidade específica do tratamento;
II – forma e duração do tratamento;
III – identificação do responsável;
IV – informações de contato do responsável;
V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;
VI – responsabilidades dos agentes que realizarão o tratamento; e
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.

> **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.

Em análise à redação do artigo 10 observamos que, em muitos casos não será possível prever com antecedência todos os fins específicos a que se atribuirá a justificativa para coleta e tratamento de dados. Por isso, as palavras “clara, adequada e ostensiva” podem ser demais amplas e descoladas dos objetivos da lei, criando um cenário de insegurança jurídica.

O mesmo artigo 10, inciso VII, item b, prevê a possibilidade de revogação do consentimento. No entanto, é importante deixar claro que a revogação do consentimento pode implicar no cancelamento do serviço oferecido.

Nessa esteira, o artigo prevê que o consentimento deverá ser renovado sempre que o propósito para o qual foi solicitado for modificado, ou ainda o usuário a quem se destinava. Ato contínuo, durante a coleta de dados feita pelas empresas, estas devem explicar claramente o propósito e o contexto geral em que as informações coletadas serão utilizadas, - e obter as autorizações apropriadas dos indivíduos para tanto. Todavia, em inúmeras situações, após a coleta de informações pessoais, as organizações podem descobrir usos inesperados e inovadores para essas informações e que não estavam inicialmente previstas, quer pelo indivíduo ou pela organização em si - mas que estão, no entanto, dentro do mesmo contexto informado no momento da coleta de dados.

Enquanto as empresas responsáveis se mantiverem transparentes desde o início sobre a sua intenção de usar os dados de maneiras potencialmente inovadoras, obedecendo ao

mesmo contexto do momento da coleta (por exemplo, informando os cidadãos em geral sobre sua intenção de usar as informações coletadas para melhorar ou oferecer novos produtos / serviços, melhorar a experiência do usuário, ou aumentar as medidas de segurança em determinado serviço ou produto), nenhuma nova aprovação deverá ser exigida para o uso de dados. Exigir a renovação do consentimento para qualquer novo uso, ainda que dentro do mesmo contexto, seria sufocar a inovação e, potencialmente, evitar os usos de dados de forma altamente benéfica para os indivíduos e para a sociedade em geral.

Na sequencia, quando se trata da lista de exceções ao consentimento indicadas no artigo 11, acreditamos que algumas considerações devem ser estabelecidas no que diz respeito ao interesse legítimo. O interesse legítimo[8] é uma das bases do sistema europeu de proteção de dados e, neste contexto, a introdução do interesse legítimo, entre as exceções ao consentimento, como uma hipótese de autorização expressa para o tratamento de dados pessoais deve ser objeto de um estudo mais aprofundado por parte do legislador brasileiro.

Essa alteração permite ao controlador processar dados à partir de um interesse legítimo, realizando um equilíbrio entre os seus interesses e os interesses e os direitos fundamentais do usuário. Isso garante a flexibilidade necessária para executar o processamento de dados nos casos em que não há impacto sobre os indivíduos e as mudanças na tecnologia não são materialmente significativas. Além disso, permite a abrangência do uso de dados nas áreas de segurança de rede e da informação, onde pode não ser viável nem desejável solicitar a usuários maliciosos ou participantes inconscientes a permissão para o tratamento de seus dados pessoais.

Reforçamos que o conceito tradicional de processamento de dados adotado pelo projeto de lei não é adequado para o processamento de dados de grande escala, como o que é realizado dentro do cenário de análise de “big data” e, em particular, pode não funcionar para os dispositivos de IoT, por não ser prático ou até mesmo possível obter o consentimento do usuário, considerando estágios prematuros da relação comercial em que não será possível celebrar um contrato com o consumidor.

O conceito de interesse legítimo traz segurança jurídica para o processamento de dados para esse possa ser feito legalmente e com segurança, sem sobrecarregar os controladores de dados ou impor ao consumidor a revisão constante das suas autorizações.

Comunicação, Interconexão e Uso Compartilhado de Dados

> **Art. 22**. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do

8 Artigo 7. Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se : 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 n " 1 do artigo 1 ". http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.
Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.

Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

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:
I – nas hipóteses de dispensa do consentimento previstas nesta Lei;
II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou
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.

Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.

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.

Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.

De acordo com os artigos propostos no anteprojeto de lei, os diversos agentes envolvidos no tratamento de dados pessoais são solidariamente responsáveis e sujeitos à regulamentação brasileira de proteção de dados, no entanto a responsabilidade solidária entre o cedente e o cessionário de dados na forma proposta poderia levar a uma responsabilidade indevida daqueles envolvidos na operação de tratamento de dados. Não é razoável, além de

impraticável trazer para toda a cadeia dos agentes econômicos a responsabilidade sobre o tratamento de dados pessoais.

O Responsável é quem decide sobre a utilização de dados e faz sentido que, em última análise, é sua a responsabilidade que é tratada pela lei. Um cessionário (ou Operador) pode ajudar a pessoa responsável com certos aspectos do tratamento dos dados, mas isso difere de um tipo de tratamento para outro. Dessa forma, qualquer responsabilidade que recaia sobre o Operador será melhor arranjada através de contrato entre Responsável e Operador.

A responsabilização solidária cria incertezas quanto ao real responsável por eventuais danos ou irregularidades, e o operador poderá ser responsabilizado por perdas e danos que não guardam relação com o tratamento que realiza. Além disso, o Responsável é a figura mais provável pela interação com o titular, o que, portanto, tornaria mais complicado para o usuário quando fosse necessário ingressar com qualquer medida judicial para reparação danos ou pleitear indenizações.

Transferência Internacional

> **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.
>
> **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.
>
> **Art. 31**. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.
>
> **Art. 32**. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.
>
> **Art. 33**. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

A economia globalmente interdependente de hoje depende de fluxos internacionais de informação, que são uma importante fonte de valor econômico e social. É uma preocupação válida de que tais transferências podem resultar em proteções mais fracas, se tratadas de forma diferente em um país estrangeiro com um enquadramento jurídico diferente, ou inexistente.

Existem diferentes abordagens para a proteção dos dados pessoais transferidos para o exterior. Na UE, a lei proíbe a transferência de informações pessoais para outra jurisdição, a menos que a Comissão Europeia determina que a proteção conferida pelas leis nesse país

terceiro é "adequada", ou mecanismos específicos, tais como regras corporativas ou cláusulas contratuais- sejam usadas, semelhante a atual proposta no Brasil.

No Canadá, por outro lado, tem se evitado a abordagem de país para país em favor de fazer as organizações que manuseiam os dados responsáveis por assegurar que os dados serão protegidos. A Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) estabelece que as organizações serão responsáveis pela proteção de transferências de dados pessoais no âmbito de cada arranjo individual de internacionalização. A vantagem dessa abordagem é de que os obstáculos administrativos e excessivos são evitados ao mesmo tempo em que a responsabilidade recairá sobre os devidos agentes. Mantendo a empresa responsável pela segurança e cumprimento das normas durante a transferência de dados garante que a organização envidará os devidos esforços para se certificar de que os dados não sejam transferidos para empresas que não cumprem normas de proteção adequadas.

Esse mecanismo permite que, ainda que o outro País mantenha regras de proteção de dados, seja possível a certificação de que o destinatário dos dados de fato cumpre com essas normas, evitando-se assim um excesso de procedimentos administrativos. Portanto, nossa recomendação é de que o Brasil possa seguir o modelo canadense, garantindo maior efetividade na proteção de dados pessoais.

Responsabilidade dos Agentes – Responsável e Operador

> **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.
>
> **§ 1º** O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.
> **§ 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.
>
> **Art. 40**. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, observado o disposto no art. 15.
> **Parágrafo único**. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.

As responsabilidades aqui propostas podem conduzir à responsabilidade indevida dos agentes envolvidos no tratamento de dados, considerando a responsabilidade solidária prevista para o cessionário. Como mencionado anteriormente, é importante que se faça uma distinção clara entre as atividades envolvidas no tratamento de dados pessoais restringindo a responsabilidade de cada agente econômico de acordo com a atividade efetivamente realizada.

Segurança e Sigilo de Dados Pessoais

Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Parágrafo único. A comunicação deverá mencionar, no mínimo:

I – descrição da natureza dos dados pessoais afetados;

II – informações sobre os titulares envolvidos;

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

IV – riscos relacionados ao incidente; e

V – medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

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.

Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

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

Embora a adoção de medidas de segurança para a proteção dos dados pessoais seja de extrema importância, acreditamos que essas medidas devam ser adotadas de acordo com a escolha feita por cada agente econômico, à partir de critérios técnicos e individuas, não devendo sofrer a interferência do órgão regulador quanto à forma de melhor garantir a proteção de dados pessoais.

Além disso, acreditamos que as notificações a respeito de eventos relacionados à segurança de dados devam ser obrigatórias apenas em casos de falhas que resultem em danos significativos aos indivíduos e, nestes casos, a legislação deve proporcionar uma maior orientação para o que deve ser obrigatoriamente apresentado ao usuário.

É importante ressaltar que o prazo para envio das notificações deve variar de acordo com a proporção do incidente; com base em experiências anteriores em outros países, as notificações imediatas podem enfrentar algumas dificuldades, é necessário respeitar o tempo para que sejam tomadas as medidas necessárias para estabelecer a matriz das falhas e corrigi-las corretamente. O envio da notificação imediata e sem os devidos critérios resultará em indivíduos incapazes de distinguir entre as notificações que são de natureza grave e os que não criam um risco de dano significativo.

Por fim, notamos que nos termos do anteprojeto proposto, a análise a ser realizada pelo órgão competente devem considerar as medidas técnicas de proteção adotadas para tornar o indecifrável. Entendemos ainda que tal consideração deve se aplicar a todos os casos em que um dado tenha se tornado indecifrável ou inutilizável e em que tais medidas técnicas de proteção tenham sido adotados, de modo que nesses casos o responsável não seja obrigado a enviar qualquer tipo de notificação ao órgão competente.

Sanções Administrativas

> **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

Embora entendamos que a função das sanções como um importante incentivo para o cumprimento integral da legislação de proteção de dados pessoais, também acreditamos, fortemente, que essas sanções devem possuir critérios de razoabilidade de proporcionalidade com relação ao dano ou violações ocorridas.

Algumas das penalidades previstas na proposta de lei têm o efeito indesejado de efetivamente encerrar negócios e não acreditamos que seja esta a intenção do legislador. O objetivo deve ser o de coagir para garantir a conformidade com o dispositivo legal e não apenas para levar à cessação das atividades de negócio.

Portanto, nós recomendamos fortemente que o artigo 50, incisos V, VI, VII e VIII sejam excluídos do projeto de lei, como uma forma de implementar um sistema mais eficaz de proteção de dados, garantindo segurança jurídica para os processadores de dados de um lado, e assegurar a proteção aos direitos fundamentais dos usuários, de outro.

Autoridade Competente

O projeto de lei prevê que um "órgão competente" terá o dever de interpretar, acompanhar e fazer cumprir a lei. Melhores práticas nos regimes de proteção de dados pessoais indicam que uma autoridade de proteção de dados independente é a pedra angular em um quadro viável proteção de dados.

Nesse sentido, quase todos os países que promulgaram leis de proteção de dados pessoais também criaram um organismo nacional específico, independente e exclusivo, com o poder de interpretar, monitorar e fazer cumprir a lei, geralmente chamado de "autoridade de proteção de dados", ou DPA. Entre as principais vantagens de um modelo de autoridade

federal independente para a proteção de dados pessoais é a consistência nas interpretações, a aplicação de conhecimentos técnicos e jurídicos sobre o tema, a segurança regulamentar e a independência necessária para agir de forma eficaz e pesar todos os direitos e interesses em discussão.

Portanto, gostaríamos de sugerir que - tendo em vista referência internacional - o projeto de lei proponha a criação de tal agência, de nível federal, como um órgão técnico e independente, com o intuito de supervisionar a implementação e aplicação de um regramento tão importante para o estabelecimento dos direitos dos cidadãos brasileiros na era digital.

Atenciosamente,

Giuseppe Sidrim Marrara

Diretor de Relações Governamentais
Cisco Brasil

*****