Produto 3

Análise de oferta e demanda

Relatório – Diagnóstico da Horizontal Ambiente Regulatório

2017

BNDES O banco nacional do desenvolvimento

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL

Esclarecimentos sobre a delimitação da horizontal Ambiente Regulatório em Internet das Coisas no presente documento

O presente documento apresenta os principais aspectos regulatórios do país que influenciam na complexidade e no impacto do desenvolvimento de IoT. Esse registro não pretende ser exaustivo, mas sim abordará como tais aspectos regulatórios são caracterizados no país e como influenciam o ambiente IoT.

Este diagnóstico não inclui questões específicas de aprofundamento técnico ou regulatório, tampouco propostas de soluções. Tais pontos serão abordados na Fase III do estudo. [1]

As informações contidas neste documento foram levantadas a partir das análises do Consórcio e baseadas em pesquisas e estudos bibliográficos. Portanto, não representam a opinião ou juízo de valor do Ministério da Ciência, Tecnologia, Inovações e Comunicações ou do Banco Nacional de Desenvolvimento Econômico e Social.

[1] Isso inclui análises sobre questões regulatórias setoriais, como saúde (ANVISA) e drones (ANAC).

Índice

1. Contexto

O presente documento "*Análise de Oferta e Demanda – horizontal Ambiente Regulatório*" é um dos capítulos do Produto 3 do estudo "Internet das Coisas: um plano de ação para o Brasil", liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O estudo, que tem por objetivo propor um plano de ação estratégico para o país em Internet das coisas (em inglês, Internet of Things - *IoT*), está dividido em quatro grandes fases:

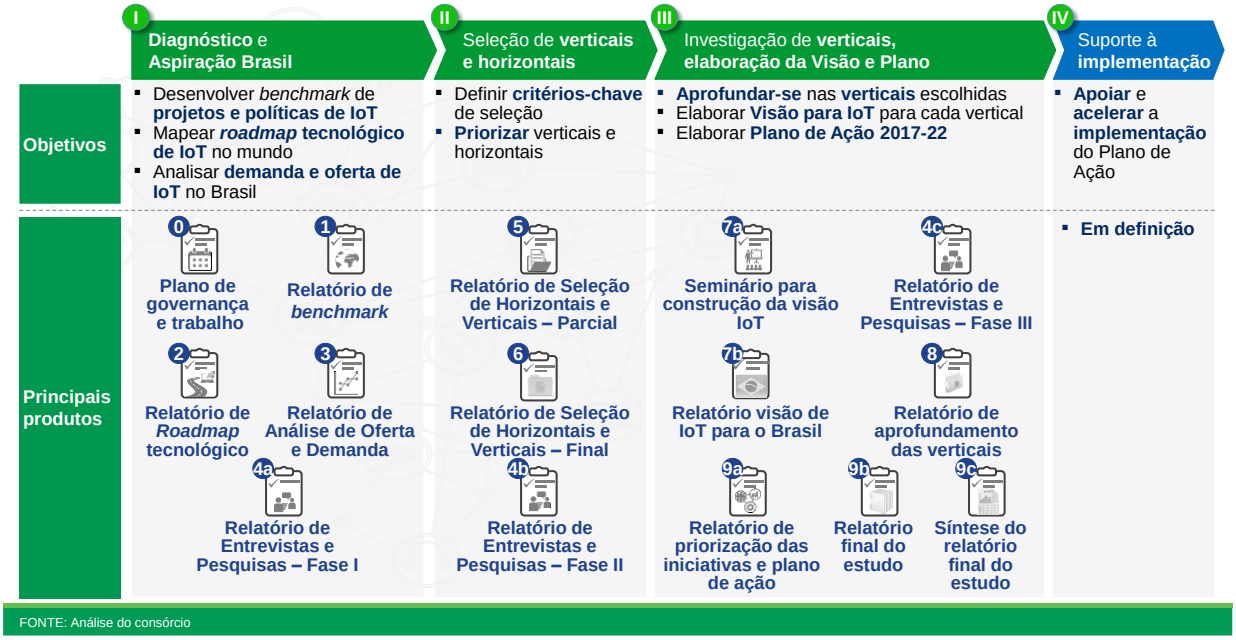
- **Diagnóstico Geral e Aspiração para o Brasil:** Obtenção de visão geral do impacto de IoT no Brasil, entendimento das competências de TIC do País e definição de aspirações iniciais para IoT no Brasil**;**
- **Seleção de verticais e horizontais:** Definição de critérios-chaves para seleção e priorização de verticais e horizontais;
- **Aprofundamento e elaboração de plano de ação (2017 - 2022):** Aprofundamento nas verticais escolhidas, elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2017-22;
- **Suporte à implementação:** Apoio à execução do Plano de Ação 2017-22**.**

As 3 primeiras fases são compostas de 9 produtos principais. O presente documento representa um dos capítulos do produto 3, inserido na Fase 1 do estudo, como descrito no Quadro 1 a seguir:

QUADRO 1

NÃO EXAUSTIVO

Fases e principais produtos do estudo "Internet das Coisas: um plano de ação para o Brasil"



FONTE: Análise do consórcio

2. Introdução

A Internet das Coisas representará uma grande oportunidade para o mundo, incluindo os países em desenvolvimento, nos próximos anos. No entanto, a forma pela qual cada país irá aproveitar esta oportunidade dependerá de suas aspirações e estratégias específicas. Essa reflexão deve considerar o contexto econômico, social, político e legal mais amplo do país bem como o contexto mais próximo de TIC e IoT.

Neste documento estão os principais aspectos regulatórios que poderiam servir de catalisadores ou barreiras para o desenvolvimento de *IoT* no Brasil.

Esses aspectos regulatórios são transversais aos ambientes onde IoT pode se desenvolver, como saúde, cidades, rural, indústria de base e fábricas, logística, entre outros. Compreendemos cada um desses ambientes como verticais. Os desafios descritos neste documento atravessam essas verticais porque são pautas relevantes para quase todas elas. Por isso, o tema é considerado como uma horizontal, assim como os demais temas relevantes para *IoT* que perpassam todas as verticais sob óticas diferentes:

- **Ambiente de negócios:** é composto pelas dimensões empresarial e de empreendedorismo relevantes para que o ecossistema brasileiro favoreça o surgimento de soluções de IoT em empresas de maior porte e também start-ups relacionadas à Internet das Coisas
- **Capital humano:** inclui os aspectos de formação básica e formação para o trabalho da mão-de-obra brasileira para atuar nos diversos setores relacionados a soluções de comunicação M2M e IoT
- **Governança de IoT:** representa o conjunto de estruturas e instituições relacionadas ao desenvolvimento de IoT no Brasil e os demais atores relevantes responsáveis pela coordenação de temas relacionados a IoT
- **Infraestrutura de conectividade:** oferece uma perspectiva da oferta de serviços de telecomunicações relevantes para atender os diferentes casos de uso de IoT no Brasil, abrangendo as principais redes de acesso, bem como a infraestrutura de suporte aos serviços e alocação de espectro
- **Investimento, Financiamento e Fomento:** compreende fontes de investimento, canais de financiamento e iniciativas de fomento, existentes e que poderiam ser estruturadas, com o propósito de incentivar o desenvolvimento da Internet das Coisas no Brasil
- **Ambiente Regulatório:** fornece um diagnóstico do quadro regulatório geral que se relaciona com o desenvolvimento do ecossistema de IoT no Brasil, com destaque para os debates envolvendo a regulação do setor de telecomunicações e as normas que regem a privacidade e a proteção de dados pessoais hoje no país.

É importante destacar que este é um diagnóstico não-exaustivo das principais questões regulatórias que impactam o desenvolvimento de IoT no Brasil. Esse diagnóstico servirá, na fase 3 do estudo, para elaborar um plano de ação mais detalhado para IoT no país.

Ressalte-se que este capítulo trata exclusivamente da horizontal "Ambiente Regulatório" e que as demais horizontais são tratadas em outro capítulo: "Relatório – Diagnóstico das horizontais" do produto 3.

3. Ambiente regulatório

A parte regulatória envolve detalhes técnicos fundamentais para que soluções em IoT se desenvolvam com segurança jurídica. As questões regulatórias relativas a IoT são abordadas do seguinte modo: (i) regulação de setor de telecomunicações; (ii) neutralidade da rede; (iii) privacidade e proteção de dados pessoais; (iv) segurança da informação; (v) questões tributárias; (vi) benefícios fiscais; (vii) burocracia no processo de importação e desembaraço aduaneiro; e (viii) padronização e entidades normalizadoras.

3.1 Desafios no setor de telecomunicações

Tendo em vista que as aplicações de IoT possuem algum tipo de conectividade e, portanto, interface direta com o setor de telecomunicações, é preciso desde logo identificar potenciais obstáculos que poderão surgir desta intersecção.

Do ponto de vista da regulamentação setorial de telecomunicações, a conectividade assume especial relevância. Isso porque a conectividade - conexão entre pessoas, entre dispositivos e pessoas, e entre dispositivos - é característica essencial de qualquer serviço de telecomunicações.

No caso de aplicações de IoT, a conectividade provida por um serviço de telecomunicações pode ser contratada: (i) diretamente pelo usuário da aplicação de IoT (v.g. junto a uma operadora de Serviço Móvel Pessoal – "SMP"), sendo que este passará a ser um usuário do serviço de telecomunicações; (ii) diretamente de um provedor de telecomunicações parceiro, como um insumo ao provimento da aplicação de IoT, na qual a oferta de telecomunicações é embarcada; ou (iii) oferecida diretamente pelo próprio provedor de IoT com base em uma rede própria de telecomunicações.

No primeiro caso, não há grandes desafios regulatórios a serem superados, haja vista que a conectividade será provida por uma operadora de telecomunicações contratada diretamente pelo usuário, em uma relação comum de prestação de serviço – no que talvez seja o arranjo mais comum para aplicações IoT. Nos dois últimos casos, entretanto, a conectividade estaria presente na própria aplicação de IoT oferecida ao cliente, o que pode suscitar algumas discussões regulatórias:

a. no segundo caso – i.e. conectividade contratada pelo provedor da solução de IoT de um operador de telecomunicações – podem surgir questionamentos sobre uma possível revenda não autorizada de serviços de telecomunicações ao usuário de IoT;

b. no terceiro caso – i.e. conectividade oferecida pelo próprio provedor de IoT – a oferta dependerá, no atual regime regulatório, da obtenção de uma outorga específica para a operação do serviço de telecomunicações, mesmo que essa rede de telecomunicação seja destinada ao uso do próprio provedor de IoT.

Como se sabe, a caracterização de uma atividade como serviço de telecomunicações atrai uma série de obrigações regulatórias que vão desde a necessidade de prévia obtenção de outorga para a prestação do serviço, eventual autorização para o uso de radiofrequência, licenciamento de estações, certificação e a homologação de equipamentos, pagamento de encargos setoriais e cumprimento de obrigações de qualidade, entre outras.

É verdade que a própria regulamentação estabelece, para certas circunstâncias, isenções ou simplificações de um ou mais dessas obrigações regulatórias. No entanto, essas isenções ou assimetria regulatória podem se mostrar insuficientes para abarcar a miríade de aplicações de IoT e fomentar o seu desenvolvimento no País.

Isso se explica, em parte, pelo modo como foram desenhadas a Lei Geral de Telecomunicações ("LGT"), Lei nº 9.472/1997, e a regulamentação da Agência Nacional de Telecomunicações ("Anatel"), isto é, com base em um modelo de prestação de serviço de telecomunicações por uma prestadora a um usuário (pessoa física ou jurídica), a partir, portanto, de uma relação direta com o prestador do serviço de telecomunicações (i.e. conectividade).

Aplicações de IoT, no entanto, podem depender de uma série de modelos que se afastam das relações de serviço mais usuais. Por exemplo, a preponderância de ausência de interação humana direta que permeia grande parte das aplicações de IoT poderia tornar inadequados certos deveres impostos pela regulamentação setorial que são próprios dos serviços tradicionais de telecomunicação prestados diretamente ao usuário (e.g., obrigações de qualidade), e não de uma comunicação máquina a máquina ("M2M").

Tais questões são relevantes mesmo nas situações em que a IoT dependa apenas de uma conexão já disponível ao usuário (e.g. conexão residencial para uma aplicação de segurança), inclusive por gargalos gerais do setor (e.g., deficiências de infraestrutura e acesso não massificado a serviços de banda larga). Isso também pode dificultar a criação de um ambiente propício para o desenvolvimento de IoT no Brasil.

Essas e outras preocupações passarão a ser detalhadas a seguir, com o fim de identificar os principais óbices que o atual estado da regulamentação do setor de telecomunicações pode vir a representar para o adequado desenvolvimento do mercado de IoT no País.

3.1.1. Acesso à internet no Brasil

Como mencionado acima, muitas soluções de IoT dependerão da conexão à internet por meio da rede pública, através dos serviços prestados pelas autorizatárias de Serviço de Comunicação Multimídia ("SCM") e Serviço Móvel Pessoal ("SMP"). Assim, é imprescindível refletir sobre a capacidade das redes existentes para acesso à internet disponível no país.

Apesar do crescimento no número de prestadoras de SCM no Brasil nos últimos anos, foram identificadas limitações ao desenvolvimento da banda larga fixa[2]. Como principais causas para estas limitações podem ser destacadas: (i) a dificuldade no uso dos recursos do FUST ("Fundo de Universalização dos Serviços de Telecomunicações") em redes dedicadas a dados e a ausência de incentivo para investimento nestas redes; (ii) o regime de reversibilidade de bens previsto para as concessões de Serviço de Telefonia Fixa Comutada ("STFC"), que geram insegurança jurídica e prejudicam novos investimentos no setor;[3] (iii) e as dificuldades para implantação de novas redes de telecomunicações e de competição entre infraestruturas.

O FUST é um importante fundo setorial, instituído pela Lei nº 9.998/2000, voltado ao financiamento da implantação de serviços de telecomunicações. Entretanto, os recursos originalmente destinados à massificação dos serviços de telecomunicações, recolhidos através do FUST nunca foram efetivamente aplicados, por razões que fogem ao escopo do presente estudo.[4]

Segundo dados disponibilizados pela Anatel, atualmente mais de cinco mil municípios brasileiros contam com cobertura de internet.[5] Entretanto, este número não permite a interpretação de que cobertura é sinônimo de acesso ou de acesso com qualidade, em

[2] Segundo a Anatel, em maio de 2016 havia 5.867 empresas autorizadas no Brasil para prestação de SCM. Processo Anatel nº 53500.207215/2015-70, versão pública SEI nº 0897749, p.143.

[3] PEREIRA NETO, Caio Mario da Silva; ADAMI, Mateus Piva e CARVALHO, Felipe Moreira de. *Reversibilidade de bens em concessões de telecomunicações*. In: Revista de Direito Público da Economia, Belo Horizonte: Fórum, nº 55, jul.-set./2016, pp. 73-109.

[4] PEREIRA NETO, Caio Mário da Silva; ADAMI, Mateus Piva. O desafio da universalização de telecomunicações: um balanço após 15 anos de LGT. In: GUERRA, Sergio (Org.). *Regulação no Brasil*: uma visão multidisciplinar. Rio de Janeiro: FGV, 2014. p.189 – 225;

[5] Idem.

especial no que se refere àquilo que seria necessário ao desenvolvimento, oferta e uso de aplicações IoT.

Outros dados merecem ser contabilizados, como por exemplo o fato de que somente 51% do total de residências brasileiras estão conectadas à internet, conforme dados veiculados no Relatório de pesquisa do Cetic.Br "TIC Domicílios 2015".[6]

Tendo isso em vista, temos, principalmente, duas situações que demandam tratamentos distintos: (i) localidades sem acesso às redes de telecomunicações; e (ii) potenciais usuários que, embora tecnicamente estejam em áreas atendidas, não dispõem de recursos para contratar os serviços.[7]

Atualmente, dois projetos despontam como alternativas para viabilizar maiores investimentos nesse aspecto: são os Projetos de Lei ("PL") nº 79/2016 e nº 7.406/2014.

O primeiro aborda a possibilidade de migração do regime de concessão para autorização na prestação de serviços de telecomunicações, com solução para a questão da reversibilidade de bens e conversão do saldo das concessões em investimentos para ampliação de acesso à internet; ao passo que o segundo propõe alterações das regras do FUST para que seus recursos sejam aplicados na massificação da banda larga.

Ambas propostas de alteração legislativa surgem em decorrência da inegável mudança no padrão de consumo de serviços de telecomunicações por parte da população brasileira. Como sabido, desde a década de 1990, a preocupação do Estado Brasileiro tem sido a universalização e continuidade da prestação de STFC.

Essa modalidade foi rapidamente superada pelo SMP em termos de penetração. E o SMP tornou-se a principal forma de acesso à internet no Brasil, mesmo sem o emprego de uma política pública específica para sua ampliação – para além das metas de cobertura presentes nas autorizações de direito de uso de radiofrequência. Por essa razão, a revisão do modelo de concessões e dos mecanismos de universalização tendem a avançar para viabilizar a concentração de recursos onde hoje eles são mais necessários: na massificação da banda larga, infraestrutura de suporte à disseminação de aplicações IoT.

Quanto à desoneração de impostos e contribuições setoriais, outro aspecto importante para fomentar o acesso ao serviço, o governo já instituiu medidas como o Regime Especial

6 Cetic.Br. Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros - TIC Domicílios 2015

7 Para mais informações recomenda-se a leitura: PEREIRA NETO, Caio Mário da Silva; ADAMI, Mateus Piva. A hora da mudança nas telecomunicações *Valor Econômico*, São Paulo, 08 jul. 2016. Disponível em: http://www.valor.com.br/opiniao/4628171/hora-da-mudanca-nas-telecomunicacoes. Acesso em: 29/03/17.

de Tributação do PNBL.[8] Além desses, o governo federal deve lançar ao longo de 2017 o Plano Nacional de Conectividade.

Todas essas iniciativas podem, certamente, contribuir para enfrentar os gargalos que impedem o desenvolvimento de redes e a massificação do acesso à internet no país, além de aumentar significativamente a capacidade de transmissão e processamento de dados. Com isso, o Estado brasileiro também contribuirá para o crescimento da oferta e demanda de aplicações IoT.

São diversos os benefícios sociais que decorrem da ampliação dos investimentos em rede e na oferta dos serviços de telecomunicações que suportam o acesso à banda larga. Por exemplo, as localidades remotas sem acesso às redes de telecomunicações, além de se beneficiarem da implantação de redes de telecomunicações e maior acesso à internet, poderão também desfrutar dos benefícios que aplicações de IoT irão proporcionar para a economia local.

Diante disso, recomenda-se que o Estado brasileiro adote medidas para aprofundar o debate sobre a ampliação do acesso à internet no país. Em especial, sugere-se a adoção de medidas e projetos específicos destinados a viabilizar a utilização de recursos públicos para ampliar a infraestrutura de acesso (local) e transporte (backhaul) de serviços de telecomunicações.

3.1.2. Prestação de serviços de telecomunicações depende de prévia outorga

A IoT pode ser explorada de diversas formas junto aos usuários finais, conforme já mencionado. Em relação ao modelo que integra uma solução tecnológica a um serviço de telecomunicações, do próprio ofertante de IoT ou de terceiros, pode haver discussões quanto à necessidade de obtenção de prévia autorização para a prestação de serviço de telecomunicações junto à Anatel, sob pena de classificação da atividade como exploração clandestina de serviço de telecomunicação.

De início, destaque-se que a definição regulamentar existente para "sistemas de comunicação máquina a máquina" não afasta, de qualquer modo, esse regime jurídico.[9] O critério para a necessidade ou não de outorga continua sendo o da caracterização da prestação de serviço de telecomunicações (que demanda outorga) ou de serviço de valor adicionado ("SVA", que dispensa outorga).

[8] Ministério da Ciência, Tecnologia, Inovações e Comunicações. Regime Especial de Tributação do Programa Nacional de Banda Larga (REPNBL).

[9] Decreto 8.234/2014, artigo 1º.

Como antecipado, vislumbramos as seguintes principais implicações dessa característica da legislação brasileira para as atividades de IoT: (i) por vezes, a diferenciação possível entre SVA e serviço de telecomunicações não é clara; e (ii) não é possível a utilização de aplicações IoT em que esteja presente exploração de serviços de telecomunicações mediante o emprego de soluções de "roaming permanente".

Nos subtópicos a seguir, trataremos das duas hipóteses.

- **Fronteira nebulosa entre serviço de telecomunicações e SVA: possibilidade de caracterização de "revenda" de serviço de telecomunicações**

A distinção entre serviços de telecomunicações e SVA pode não ficar clara quando analisados os diferentes modelos de negócio adotados para o provimento de soluções de IoT, sobretudo nas situações em que há oferta integrada de ambos os serviços.

No atual marco regulatório, tem-se, a princípio, que sempre que o provedor de aplicações de IoT ofertar, juntamente com as facilidades que caracterizam SVA, algo que caracterize prestação de serviço de telecomunicações, será necessária a obtenção de prévia outorga com o órgão regulador.

Pode-se afastar a necessidade de obtenção de prévia outorga apenas nas hipóteses legais, todas restritivas e pouco sensíveis à inovação tecnológica. Para as demais hipóteses, faz-se necessária a autorização para prestação do serviço, sob pena de se configurar crime de desenvolvimento clandestino de atividades de telecomunicação.[10]

Vale ressaltar que mesmo na hipótese em que o provedor de aplicações de IoT contrata um serviço de telecomunicações de terceiro, é necessário que a sua relação com os usuários não se confunda com prestação de serviço de telecomunicações por meio da oferta de facilidade que possa direcionar para uma "revenda" de serviço de telecomunicações. No caso da contratação de SMP de terceiro, por exemplo, a revenda poderia estar configurada pela oferta de conexão por voz ou envio de mensagens SMS pelo provedor de IoT.[11]

Um exemplo que pode ser usado para facilitar a compreensão do tema é o caso dos serviços de Tecnologia de Rastreamento e Monitoramento Veicular. Estes são compostos por: (i) um serviço de telecomunicações que dá suporte à conexão entre os equipamentos embarcados nos veículos, a rede da operadora de SMP e a central de monitoramento da empresa provedora de serviço de monitoramento; e (ii) um SVA correspondente ao

10 LGT, art. 183.

11 Como mencionado na análise feita pela Anatel no Ofício Anatel nº 399/2010/PVCPR/PVCP

serviço de rastreamento propriamente dito para análise dos dados gerados pelos equipamentos embarcados nos veículos. Nesse caso, pode-se afirmar que o usuário do serviço de telecomunicações é, em última instância, o próprio provedor dos serviços de Tecnologia de Rastreamento e Monitoramento Veicular.[12]

As dúvidas surgem quando a comunicação não fica restrita a um SVA, permitindo adicionalmente o uso de serviços (ou funcionalidades típicas) de telecomunicações pelos proprietários das "coisas" (e.g. veículos).

Partindo do exemplo anterior, seria o caso de um sistema de rastreamento que aproveitasse a conexão e também disponibilizasse a conexão à internet para comunicação do usuário do veículo com outros usuários da aplicação IoT ou a central de atendimento do provedor, ou, até mesmo, para navegação em geral. Nesse caso, a empresa de Tecnologia de Rastreamento e Monitoramento poderia eventualmente ser considerada prestadora de serviço de telecomunicações, pois atuaria como uma "revendedora" deste serviço, o que demandaria a obtenção das autorizações necessárias junto aos órgãos competentes.

Essa foi uma preocupação aventada pela própria Anatel em resposta à consulta formulada pela Associação Brasileira das Empresas de Gerenciamento de Risco e de Tecnologia de Rastreamento e Monitoramento ("Gristec"), por meio do Ofício Anatel nº 399/2010/PVCPR/PVCP, a respeito do uso de serviços de telecomunicações prestados por terceiros para estabelecer a comunicação entre veículos e empresas de tecnologia de informação veicular.[13]

Embora não se trate de uma norma do órgão regulador, mas sim de resposta à uma consulta específica formulada por uma Associação, não se pode ignorar que o posicionamento da Agência neste caso pode suscitar dúvidas interpretativas sobre o alcance da regulamentação setorial. Para ilustrar o ponto, pode-se questionar o que se entende por "*outra facilidade que possa direcionar para uma revenda de Serviços de Telecomunicações*".

12 Anatel, Ofício nº 399/2010/PVCPR/PVCP, de 25 de agosto de 2010

13 Idem. Confira-se o trecho pertinente do referido Ofício: "[N]o modelo imaginado, o Usuário do SMP, com contrato de prestação de SMP firmado com Prestadora do Serviço, é a empresa TIV, que contratará Planos de Serviço do SMP específicos para a operacionalização do projeto de instalação de equipamento obrigatório antifurto, devendo esses Planos se ater estritamente ao objeto do projeto, não sendo permitido que a relação das TIV's com seus usuários se confunda com prestação de Serviço de Telecomunicações, como, por exemplo, a oferta de conexão por voz ou outra facilidade que possa direcionar para uma revenda de Serviços de Telecomunicações"

Neste contexto, qualquer funcionalidade típica de serviço de telecomunicação (e.g. comunicação por voz) é suficiente para atrair a regulamentação setorial? A contratação, pelo provedor de SVA (leia-se: IoT), de um serviço de telecomunicação como insumo, com a posterior oferta de outro serviço (e.g. rastreamento e monitoramento de veículos ou cargas) ao usuário final, seria suficiente para afastar a caracterização de prestação de serviços de telecomunicações por este provedor? Seria necessária a celebração de um contrato diretamente entre o usuário da aplicação IoT e a operadora do serviço de telecomunicações – ou mesmo um contrato envolvendo, adicionalmente, a própria provedora de aplicação IoT? Esses questionamentos tendem a inibir certas soluções de IoT e até mesmo prejudica o surgimento de modelos de negócios mais eficientes.

Assim, considerando a regulamentação atual e o entendimento externado pela Anatel, para evitar a caracterização de revenda indevida ou exploração clandestina do serviço, entende-se necessário (i) posicionamento específico da Agência reguladora quanto a essa questão ou (ii) a adoção de modelos de negócio em que, por exemplo, o usuário mantenha relação contratual direta com o prestador de telecomunicações.

De outro modo, apenas a obtenção da outorga do serviço de telecomunicações ofertado ao usuário poderá elidi-la, gerando diversas outras consequências indesejadas e até mesmo a inviabilização da solução de IoT.

Não obstante, vale ressaltar que a regulamentação setorial prevê hipótese específica de revenda legitimamente autorizada. No caso específico do SMP, verifica-se a opção de que o provedor de IoT obtenha credenciamento ou autorização para exploração do serviço por meio de rede virtual – e.g., tornando-se uma Mobile Virtual Network Operator ("MVNO").

Existem duas modelagens distintas para a exploração de SMP por meio de Rede Virtual no Brasil: (i) MVNOs Autorizadas ("Autorizada de Rede Virtual", no termo utilizado pelo regulamento) e (ii) MVNOs Credenciadas ("Credenciado", no termo empregado pelo regulamento).

As principais diferenças entre as duas modelagens podem ser analisadas no quadro comparativo abaixo:

	MVNO Autorizada	MVNO Credenciada
Natureza	Consideradas em condição análoga a dos provedores de serviços de telecomunicações para a maioria dos efeitos regulatórios.	Não são consideradas como provedoras de serviço de telecomunicações e, por isso, não podem realizar quaisquer das atividades inerentes aos agentes titulares de uma licença de serviço emitida pela Anatel. As restrições às suas atividades incluem a impossibilidade de executar contratos em atacado, operar redes e obter recursos de numeração.[14]
Atividades	Possibilidade de prover diretamente o SMP para usuários, obter licença para a operação de estações móveis de telecomunicações e executar contratos em atacado – tais como a interconexão e acordos de compartilhamento de rede – com outros provedores.	A principal atividade reservada aos titulares de licenças e que pode ser realizada por MVNOs credenciadas é a revenda de serviços de telecomunicações, nos planos de serviço comercializados pela Prestadora Origem.[15] No entanto, essa possibilidade é restrita aos serviços operados pela Prestadora Origem e nas condições dos contratos celebrados entre esta e outros provedores de SMP (isto é, contratos de roaming, acordos de interconexão, acordos de compartilhamento de rede, etc.).
Autorização	A autorização deve ser requerida junto à Anatel mediante a demonstração de uma série de condições (habilitação jurídica, qualificação técnica, qualificação econômico-financeira e regularidade fiscal) e a apresentação de contrato de compartilhamento de uso de rede com Prestadora Origem.	Não possuem autorização de serviço expedida pela Anatel. O contrato de representação deve ser submetido para homologação da Anatel.

14 Resolução Anatel nº 550/2010, Art. 11.

15 Resolução Anatel nº 550/2010, Art. 13.

Responsabilidade	Aplicam-se à Autorizada de Rede Virtual os direitos e obrigações decorrentes da regulamentação que recaem sobre as prestadoras de SMP. Assim, será responsável por licenciar as estações móveis que utilizar, recolher os tributos setoriais e, ainda, cumprir com as obrigações de qualidade do serviço previstas em regulamentos da Anatel.	A Prestadora Origem é integralmente responsável perante a Anatel e os usuários. Isso significa que os ônus regulatórios de uma prestadora de serviços de telecomunicações (e.g., outorga, licenciamento e o recolhimento de tributos setoriais) ficariam totalmente ao encargo da Prestadora Origem, e não do Credenciado.

Ressalva-se, apenas, que o Credenciado possui limitações (e.g., impossibilidade de celebrar contratos de atacado, operar rede, obter recursos de numeração e deter contrato para representação com mais de uma Prestadora Origem em uma determinada área de registro) e que o Autorizado, embora não seja limitado por tais restrições, responde por todas as obrigações aplicáveis a prestadoras de SMP.

A utilização de modelos de revenda legitimamente reconhecidos e autorizados pela Anatel pode ser um tipo de solução para o desenvolvimento de negócios de IoT. Para esse fim, pode ser recomendado avaliar alterações na regulamentação setorial, sobretudo àquela aplicável ao modelo de MVNO, para refletir o desenvolvimento tecnológico.

- ***Roaming* internacional permanente: impossibilidade e risco de caracterização de prestação irregular.**

Outra consequência da necessidade de outorga para a prestação de serviço de telecomunicações no Brasil está na impossibilidade de adoção de soluções conhecidas como de "*roaming* permanente".

Trata-se do oferecimento de aplicações de IoT que estejam conectadas a serviço de telecomunicações provido por empresa que não seja prestadora de serviço de telecomunicações no País, em base permanente a usuário brasileiro (ou seja, não por período limitado em que este usuário ou terminal encontra-se em trânsito pelo Brasil).

Essa restrição resulta na impossibilidade de uso de dispositivos com conexões permanentemente providas por operadoras estrangeiras, dado que não possuem autorização para operar no Brasil. Por outro lado, caso permitida essa hipótese, seria criada uma assimetria de tratamento em relação às prestadoras de serviços de telecomunicações presentes no país, sujeitas às obrigações regulatórias aqui estabelecidas.

O assunto foi abordado pela Agência no Ofício Circular nº 43/2012/PVCPR/PVCP, de 28 de junho de 2012, em resposta aos questionamentos sobre a regularidade de utilização de terminais móveis com Simcard e recurso de numeração de prestadoras estrangeiras, com o intuito de oferecer SVA de forma permanente para usuários residentes no Brasil.

De acordo com a Anatel, o usuário do Simcard de prestadora estrangeira estaria usufruindo do serviço como usuário visitante no território nacional, conforme definido pelo art. 3º, XXXI, do Regulamento do SMP, e, enquanto tal, poderia manter-se fora de sua área de prestação original apenas de forma temporária, devendo retornar ao país de origem ao fim de "determinado prazo".

A exigência legal de que a operação realizada pelo usuário visitante se dê apenas de modo temporário é justificada, de acordo com o entendimento da Agência, como uma proteção ao usuário do serviço de telecomunicações brasileiro. Isso porque os órgãos governamentais locais teriam maiores dificuldades de atuar sobre os agentes estrangeiros caso houvesse algum conflito entre o usuário e esse prestador de serviços, ainda que a atividade ocorra por intermédio de uma operadora brasileira.

A Agência ainda ressaltou que a prestação do serviço de telecomunicações deve ser devidamente autorizada pela Anatel, conforme estabelecido no art. 131 da LGT. Isso demonstra a possibilidade de que o uso de dispositivos conectados por provedoras estrangerias seja visto, pela Agência, como prestação de serviço de telecomunicações sem outorga e, portanto, como o desenvolvimento de atividade de telecomunicação clandestina, hipótese tipificada como crime pela LGT (art. 183).

Ademais, a Agência defendeu a vedação ao *roaming* internacional permanente em razão do impacto regulatório que poderia ser causado, em especial pelo fato de operações dessa natureza implicarem, também, o descumprimento de obrigações regulatórias, tais como, o pagamento dos encargos setoriais, o atendimento de obrigações de qualidade, uso de recurso de numeração nacional, dentre outros.

O entendimento da Anatel pela impossibilidade de que se admita o *roaming* internacional permanente no País chegou a ser externado, ainda, na Reunião da Comissão de Políticas Econômicas (SG3) da União Internacional de Telecomunicações ("UIT"), ocasião na qual se afirmou que "o *roaming* permanente poderia provocar o desbalanceamento na competição, já que acabaria sendo criada uma operadora de telecomunicações em escala global, que não pagaria os impostos das empresas locais".[16]

16 Disponível em: http://www.telesintese.com.br/brasil-diz-nao-ao-roaming-permanente/. Acesso em: 16.01.2017

Assim, mantida a atual regulamentação, soluções de IoT no Brasil que se utilizem de tecnologias e dispositivos vindos do exterior não poderão funcionar, por tempo indeterminado, a partir de conexões permanentemente providas por operadoras estrangeiras[17].

Em face desse óbice, será necessário, a fim de viabilizar a utilização de tecnologias e dispositivos vindos do exterior, a contratação de serviços de telecomunicação para dar suporte à tecnologia IoT diretamente junto a uma prestadora constituída segundo as leis brasileiras, com sede e administração no País, e autorizada pela Anatel a prestar o serviço.

É importante destacar a manifestação recente da Agência, no Processo nº 53508.007497/2016-18, segundo a qual a temática do roaming internacional permanente está sendo analisada com prioridade pela Anatel, constando inclusive da proposta de Agenda Regulatória 2017-2018, sob o item 43 intitulado "Reavaliação da regulamentação visando diminuir barreiras regulatórias à expansão das aplicações de internet das coisas e comunicações maquina-a-maquina".

Segundo a manifestação, este item está com data prevista para entrega do relatório de Análise de Impacto Regulatório (AIR) para o segundo semestre de 2018.

Neste contexto, cumpre destacar o desenvolvimento de uma nova tecnologia que merece ser avaliada quando da discussão sobre *roaming* internacional, o *embedded* SIM ("e-SIM").[18] Trata-se de um novo tipo de chip, a ser inserido nos dispositivos inteligentes, que permite sua configuração remota, afastando, portanto, as limitações inerentes à utilização de SIM *cards* vinculados a recursos de numeração de uma única prestadora.

Em virtude do avanço da IoT, foi identificado que os chips disponíveis atualmente no mercado não seriam suficientes para atender as necessidades dos clientes de IoT. Isso porque os SIM *cards* atuais não permitem que as informações nele inicialmente armazenadas sejam alteradas, por isso, quando um indivíduo opta por mudar de operadora de serviço de telecomunicações, ele é obrigado a trocar o SIM *card* de seu dispositivo por um novo.

17 "Proibição de roaming permanente - Para garantir uma maior cobertura no rastreamento de objetos para aplicações de logística e transporte é necessário utilizar a rede de mais de uma operadora móvel. - Um exemplo desta situação são equipamentos vindo do exterior com "chip" de operadora internacional e que passa a operar em roaming no Brasil. A Anatel não permite que isto ocorra de forma permanente". (Relatório do Projeto IoT Brasil. Documento preparado por solicitação da FEBRATEL, julho de 2016, Teleco, disponível em: http://www.telebrasil.org.br/component/docman/doc_download/1569-apresentacao-do-projeto-Iot-brasil?Itemid. Acesso em: 29.03.2017)

18 Disponível em: https://www.gsma.com/iot/embedded-sim/

Diante deste quadro, desenvolveu-se o e-SIM, que permite que as informações armazenadas sejam modificadas remotamente. Nesta nova tecnologia o chip vem integrado ao dispositivo, sendo necessário a alteração da configuração do dispositivo por meio do envio remoto de novas informações ao chip. Assim, o e-SIM, além de eliminar a necessidade de troca física do chip, traz como facilidades: (i) flexibilidade em relação à sua fabricação, à existência de restrições globais e a contratos de conectividade local; (ii) redução de custos logísticos quando comparado ao uso de chips SIM; e (iii) aumento do nível de disponibilidade de solução para os dispositivos que possuam ciclo de vida estendida. [19]

Dessa forma, já é possível afirmar que existem no mercado soluções que podem ser utilizadas para transpor limites tecnológicos hoje existentes no debate sobre *roaming* internacional – o que tende a reduzir sua importância para o cenário de IoT.

Evidente que, caso seja adotado este novo tipo de chip, será necessário não impor formatos de fabricação, mas apenas uma regulamentação por parte do órgão regulador para orientar a adoção deste novo padrão.

3.1.3. Limites à celebração de contratos de atacado e interconexão por usuários e por prestadoras de serviços de telecomunicações de interesse restrito e debates sobre o acesso à internet no caso dos serviços de interesse restrito.

Com relação à forma pela qual pode se dar a conexão entre o ecossistema formado pelos dispositivos IoT e a rede pública, é importante considerar, em um primeiro momento, que o modelo de exploração das aplicações de IoT pode se dar, sem maiores complicações, a partir da perspectiva de que todas as aplicações e sistemas relacionados às aplicações sejam conectadas à rede pública na qualidade de usuários.

Nesse modelo, todos os dispositivos interconectados, bem como o servidor responsável pela compilação dos dados provenientes desses dispositivos, se conectariam à internet na qualidade de usuários, isto é, mediante a contratação de um serviço de telecomunicações de interesse coletivo (e.g., SMP, SCM) prestado por terceiro, sem qualquer obstáculo à conexão com a rede pública.

No entanto, o modelo de negócios das operadoras que exploram soluções em IoT pode ser estruturado também a partir de um serviço de telecomunicações de interesse restrito. Ou seja, quem proverá a conexão entre os dispositivos, e entre esses dispositivos e o servidor

[19] Conforme informações disponibilizadas no Produto 2: *Roadmap* de tecnologias habilitadoras. Relatório Final. 2017. p. 139

responsável pela concentração e processamento de seus dados, será o provedor de aplicações IoT na qualidade de prestador de serviço de telecomunicações de interesse restrito.

Nesse caso, a comunicação dos dados trocados entre os dispositivos e entre estes e o servidor com a rede pública encontraria obstáculo regulatório na medida em que a interconexão dos serviços de telecomunicação de interesse restrito à rede pública é vedada pelo Regulamento dos Serviços de Telecomunicações.[20] Apesar de ser possível a interligação ocorrer em caráter de acesso de usuário, esse tipo de conexão acarretaria um aumento de custos para o provedor de IoT.

Portanto, na hipótese em que o ecossistema dos dispositivos de IoT, ofertado com base em um serviço de telecomunicações de interesse restrito, necessite se conectar à rede pública, faz-se necessário que a operadora responsável pela exploração das soluções de IoT (i) se torne uma operadora de serviço de telecomunicações de interesse coletivo ou (ii) na qualidade de usuário, contrate o serviço de uma operadora de telecomunicações de interesse coletivo.

Vale notar, ainda, que o Regulamento do Serviço Limitado Privado ("SLP") pode ser interpretado de forma a restringir o acesso dos equipamentos IoT à internet, uma vez que: (i) o objeto do serviço está voltado a possibilitar a comunicação dentro de um determinado grupo de usuários;[21] e (ii) a única menção ao serviço de conexão à internet é feita em caráter excepcional, o que pode evidenciar existência de uma restrição.[22] Essa situação pode gerar insegurança jurídica e prejudicar a implantação de alguns modelos de negócio IoT, merecendo, portanto, atenção.

3.1.4. Uso do espectro de radiofrequência diante do surgimento de novas tecnologias: possíveis alternativas e suas limitações

A abordagem do uso de espectro de radiofrequência é particularmente importante diante do fato de que grande parte das aplicações de IoT detêm mobilidade e necessitarão desse insumo para operar. Além disso, cumpre-se desde logo destacar que estas aplicações poderão usufruir de dois tipos de espectro: o licenciado (i.e. que depende de autorização específica da Anatel para sua utilização) e o não licenciado (i.e. aquele que independe de

20 Resolução Anatel nº 73, de 25 de novembro de 1998, art. 72.

21 Resolução Anatel nº 617/2014, art. 3º.

22 Resolução Anatel nº 617/2014, art. 18.

prévia autorização, como é o caso do Wi-Fi, por exemplo). As particularidades destas questões serão abaixo endereçadas.

- ***Aproveitamento do espectro subutilizado***

Em princípio, é possível o aproveitamento do espectro já outorgado nos casos em que houver a subutilização de faixas de radiofrequência ou não houver demanda suficiente por determinado serviço.

Para tanto, uma solução cabível seria possibilitar a transferência da autorização de uso de radiofrequência entre prestadores de serviços de telecomunicações.

Atualmente, esse tipo de transferência só é permitido mediante a correspondente transferência da concessão, permissão ou autorização da prestação de serviço a elas vinculadas, segundo expressa disposição da LGT.[23] No entanto, o PLC nº 79/2016 propõe a alteração da legislação de modo a permitir, mediante anuência prévia da Anatel, a transferência autônoma da autorização de uso de radiofrequência – o denominado "mercado secundário" de radiofrequência –, ressalvada a competência da Agência para estabelecer condicionamentos de caráter concorrencial à sua aprovação.[24]

Outra alternativa para o aproveitamento de faixas ociosas estaria na exploração industrial de radiofrequências (*ran sharing* ou *swap* de faixas). Também nesse caso faz-se necessária a anuência prévia da Anatel (art. 14, ressalvadas as exceções previstas no §6º do artigo 41, ambos da Resolução Anatel nº 671/2016),[25] além da observância do procedimento previsto no artigo 41 da Resolução Anatel nº 671/2016.

- ***Espectro não licenciado: radiação restrita***

Ainda, considerando que grande parte das soluções de IoT poderia ser provida por equipamentos de radiocomunicação de radiação restrita,[26] caberia cogitar da alocação de

23 LGT, art. 168.

24 De acordo com o artigo 8º do PLC 79/2016, o artigo 163 da LGT seria acrescido dos seguintes parágrafos: *"Art. 163. [...] § 4º A transferência da autorização de uso de radiofrequência entre prestadores de serviços de telecomunicações dependerá de anuência da Agência, nos termos da regulamentação. § 5º Na anuência prevista no § 4º, a Agência poderá estabelecer condicionamentos de caráter concorrencial para sua aprovação, tais como limitações à quantidade de radiofrequências transferidas." (NR)"*

25 Resolução Anatel nº 671/2016, art. 41, § 6º: "*§ 6º Fica dispensada de anuência prévia a exploração industrial: I - nos casos em que houver previsão em editais ou regulamentos específicos; II - nos casos de exploração de serviço por meio de rede virtual; III - quando confinada a municípios com menos de 30 mil habitantes; ou, IV - quando limitada exclusivamente a áreas rurais, sem cobertura de redes de telecomunicações do Serviço Móvel Terrestre".*

26 Segundo dados trazidos na Consulta Pública para o Plano Nacional de IoT, redes baseadas no uso de faixas de radiofrequência de radiação restrita podem compartilhar eficientemente o espectro com outros sistemas na mesma banda, sendo ideais para aplicações de baixo débito, alto alcance (distância), baixo consumo de energia e de baixo custo. Tais requisitos, segundo contribuições à Consulta Pública, estão presentes em aplicações que representam cerca de 60-70% das aplicações de IoT.

maior quantidade de espectro para tais dispositivos. Por expressa previsão legal contida no artigo 163, §2º, inciso I da LGT, o uso desses equipamentos independe de outorga de uso de radiofrequência.

Os equipamentos de radiação restrita estão regulamentados atualmente pela Resolução Anatel nº 506/2008 e a partir de 28 de agosto de 2017 será regulado pela Resolução Anatel nº 680/2017. A utilização desses equipamentos independe da emissão de autorização prévia pela Anatel para uso de radiofrequência, bem como de licenciamento para instalação e funcionamento.[27]

De acordo com a Resolução Anatel nº 506/2008, quando (1) a atividade de telecomunicações desenvolvida pela estação de radiocomunicação extrapolar os limites de uma mesma edificação ou propriedade móvel ou imóvel; e (2) as estações de radiocomunicações fizerem uso de equipamentos que utilizam tecnologia de espelhamento espectral ou outras tecnologias de modulação digital e de sistemas de acesso sem fio em banda larga para redes locais, o regulamento determina condições específicas, conforme elencadas a seguir:

> a. Se a atividade de telecomunicação estiver associada à exploração do serviço de telecomunicações de interesse coletivo, será necessária a correspondente autorização do serviço, bem como o licenciamento das estações que se destinem à: (a.i) interligação às redes das prestadoras de serviços de telecomunicações; ou (a.ii) a interligação a outras estações da própria rede por meio de equipamentos que não sejam de radiação restrita.[28]
>
> b. Se o funcionamento dessas estações servir de suporte à rede de telecomunicações destinada a uso próprio ou a grupos determinados de usuários, não se faz necessária a autorização do serviço, exigindo-se apenas o cadastramento no banco de dados da Agência na hipótese das destinações previstas nos itens (a.i) e (a.ii).[29]

Isso significa que nos termos da Resolução Anatel nº 506/2008 a autorização do serviço para utilização de equipamentos de radiação restrita só se faz necessária, no caso dos equipamentos específicos mencionados, quando a atividade de telecomunicação

27 Resolução Anatel nº 506/2008, art. 3º e Resolução Anatel nº 680/2017, art. 3º

28 Resolução Anatel nº 506/2008, art. 3, I.

29 Resolução Anatel nº 506/2008, art. 3, II

associada à exploração de telecomunicações for de interesse coletivo. Portanto, a autorização não será necessária quando a utilização destes equipamentos servir de suporte à rede de telecomunicações de interesse restrito, para o que se exigirá apenas o registro no banco de dados da Agência.

Contudo, com a entrada em vigor da Resolução Anatel nº 680/2017, esses pontos sofrerão alterações. Pela Resolução Anatel nº 680/2017, que altera os Regulamentos dos Serviços de Telecomunicações[30], de Serviço de Comunicação Multimídia[31] e de Serviço Limitado Privado[32-33], não haverá mais necessidade de

(i) **licenciar** estações de telecomunicações das redes de suporte à prestação de serviços, tanto de interesse coletivo quanto de interesse restrito, que utilizarem exclusivamente equipamentos de radiocomunicação de radiação restrita e/ou meios confinados;

(ii) **obter** autorização para a prestação do SCM com até 5 (cinco) mil acessos em serviço, nos casos em que as redes de telecomunicações de suporte à exploração do serviço utilizarem exclusivamente meios confinados e/ou equipamentos de radiocomunicação de radiação restrita;

(iii) **obter** autorização para a prestação de SLP nos casos em que as redes de telecomunicações de suporte à exploração do serviço utilizarem exclusivamente meios confinados e/ou equipamentos de radiocomunicação de radiação restrita.

Além disso, pelo novo Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita, aprovado pela Resolução Anatel nº 680/2017, não haverá mais as restrições sobre tecnologias específicas.

Mesmo diante dessas possibilidades, o uso de equipamentos de radiação restrita está sujeito a algumas limitações.

30 Aprovado pela Resolução Anatel nº 73/1998

31 Aprovado pela Resolução Anatel nº 614/2013

32 Aprovado pela Resolução Anatel nº 617/2013

33 A Resolução Anatel nº 680/2017 também altera o Regulamento de Gestão da Qualidade do Serviço de Comunicação Multimídia.

Em primeiro lugar, deve ser considerado que a operação desses equipamentos se dá em caráter secundário, ou seja, não há direito à proteção contra interferências prejudicais, devendo, inclusive, haver inscrição, no próprio equipamento, que contenha a informação da operação em caráter secundário.[34]

Na hipótese de esses equipamentos causarem interferência prejudicial em qualquer sistema que opere em caráter primário, o funcionamento do equipamento de radiação restrita que causou a interferência deve ser cessado imediatamente.[35]

Além dessas limitações, há também limites de faixas de radiofrequências que podem ser utilizadas por esses equipamentos.[36] Ademais, deve-se recordar que os equipamentos de radiação restrita não estão isentos de possuir certificação emitida ou aceita pela Anatel,[37] e que a receita decorrente do serviço prestado mediante o uso de tais equipamentos, caso seja proveniente da prestação de serviço de telecomunicações, tampouco está isenta dos tributos setoriais incidentes sobre receita (e.g., contribuições ao FUST e ao Fundo para o Desenvolvimento Tecnológico das Telecomunicações – "FUNTEL").

É importante que seja considerado que os limites de emissão para a caracterização de um equipamento como de radiação restrita são, regra geral, mais rigorosos. Limites alternativos menos restritivos são previstos apenas de forma excepcional.[38]

Por fim, é necessário avaliar os aspectos técnicos relacionados ao aumento da disponibilidade de espectro para essa categoria de equipamentos.

Tal alocação de mais espectro para radiação restrita, porém, deve ser objeto de coordenação internacional, sob pena de gerar equipamentos incompatíveis com os padrões existentes nos demais países, o que prejudica a sua importação/exportação. Ou seja, esse desalinhamento é altamente prejudicial independentemente da postura adotada pelo País em relação aos equipamentos.

Ademais, deve-se ponderar que a alocação de mais espectro para utilização sem autorização pode ocasionar a "poluição" desse bem público, e gerar dificuldades operacionais para a prestação dos serviços que explorem essas faixas de radiofrequência.[39]

34 Resolução Anatel nº 506/2008, art. 4 e 6; Resolução 680/2017, Anexo, Artigo 3º

35 Resolução Anatel nº 506/2008, art. 4, parágrafo único; Resolução 680/2017, Anexo, Artigo 3º, parágrafo único

36 Resolução Anatel nº 506/2008, art. 8; Resolução 680/2017, Anexo, Artigo 7º

37 Resolução Anatel nº 506/2008, art. 5; Resolução 680/2017, Anexo, Artigo 4º

38 Resolução Anatel nº 506/2008, art. 9; Resolução 608/2017, Anexo, Artigo 10

39 Veja nesse sentido: "*O uso do espectro também é relevante no cenário de IoT massivo, considerando o uso de frequência licenciada e não licenciada. No caso de frequência não licenciada, tem-se a preocupação com o uso massivo de dispositivos compartilhando um*

Ainda, há limitações para o uso de equipamentos de radiação restrita, os quais serão tratados posteriormente em item próprio.

De todo modo, não pode ser ignorado que a utilização de espectro de radiofrequência não licenciada tende a ser uma opção viável para o desenvolvimento do mercado de IoT, já que eliminaria a necessidade de obtenção de autorização de uso de radiofrequência e do licenciamento da estação.[40] Contudo, a ampliação do espectro destinado a essa utilização deve ser feita com cautela e coordenada com padrões internacionais.

Portanto, concluímos que as isenções regulatórias previstas para os equipamentos de radiação restrita podem constituir um incentivo para difusão de soluções de IoT de forma menos onerosa a seus provedores.

No entanto, as restrições impostas pelo regulamento ao enquadramento dos equipamentos como de radiação restrita (i.e., limites gerais e específicos de emissão) e ao seu uso (i.e., de caráter secundário) podem limitar o alcance das suas desonerações a uma parte de aplicações de IoT que demandam maiores níveis de emissão e/ou a ausência de interferências.

3.1.5. Necessidade de considerar o procedimento de certificação e homologação de equipamentos e a discussão sobre critérios de segurança

A Anatel prevê atualmente que os equipamentos voltados à prestação de serviços de telecomunicações deverão passar por procedimento de certificação e homologação, ressalvadas as exceções estipuladas pela regulamentação.

Como um dos objetivos deste procedimento, a Agência busca assegurar que os produtos utilizados estejam em conformidade com os regulamentos e normas por ela editados. Dentre os temas endereçados nestas normas, a Anatel estabelece os requisitos técnicos para a avaliação do produto de acordo com suas características técnicas, tais como limites para as emissões de radiofrequências, tolerâncias para a potência, desvio de frequência, etc.

mesmo espectro. Por outro lado, o uso de frequências licenciadas garante a segregação da rede de sensores para determinado detentor da faixa de frequência" (Produto 2: *Roadmap* de tecnologias habilitadoras. Relatório Final. 2017. p. 133).

40 Como exemplo, recentemente a empresa brasileira WND-Brasil, anunciou que iniciará em agosto a operação de uma rede nacional de Sigfox utilizando radiação restrita. Disponível em: http://www.telesintese.com.br/primeira-rede-de-iot-do-pais-entra-em-operacao-em-agosto/

Recentemente, foi proposta a revogação das resoluções que tratam de tais aspectos técnicos, de modo que a aprovação dos respectivos requisitos passe a ser feita por meio de ato do Superintendente de Outorgas e Recursos à Prestação.[41]

Tendo sido feita esta introdução, destaca-se que a certificação e a homologação de equipamentos enfrentam alguns entraves burocráticos, esquematizados na tabela abaixo, que podem dificultar o desenvolvimento do mercado de IoT no Brasil:

Oportunidade de melhoria	Entraves	Consequências
• Processo longo e demorado[42]	Procedimento para certificação e homologação de equipamentos é complexo, e envolve múltiplas análises de diferentes agentes	• Maiores custos e menor competitividade para os fabricantes e comerciantes de produtos relacionados a IoT;[43] • Burocracia para importação de produtos estrangeiros e exportação de produtos nacionais envolvendo IoT;
• Ausência de um ARM ou outro mecanismo que possibilite a validação, pela Anatel, da certificação obtida junto a organismos de outras jurisdições;[44] • Ausência de internalização de critérios para certificação	a) *Ausência de capacitação necessária*.[45] b) *Ausência de interesse político*. Apesar da previsão legal para a realização de acordos entre diferentes jurisdições para a certificação de equipamentos, isso demandaria uma reciprocidade que hoje não existe – países desenvolvidos não aceitam a certificação brasileira; c) *Preocupações de segurança nacional.* No caso de dispositivos utilizados pelo governo brasileiro, a dispensa de um controle nacional mais rigoroso pode tornar o país mais vulnerável a riscos	

41 Anatel, Consulta Pública nº 34/2016, Processo nº 53500.009149/2016-55, encerrada em 04.01.2017.

42 Como agravante a este problema, as contribuições da Consulta Pública para o Plano Nacional de IoT apontam para os desafios e gargalos que surgiriam a partir da avalanche de produtos a serem testados e avaliados em razão do desenvolvimento dos mercados de IoT.

43 Segundo o Instituto Nacional de Metrologia, Qualidade e Tecnologia ("Inmetro"), as diferentes exigências de mercados estrangeiros constituem uma forma de barreira técnica, uma vez que os exportadores incidem em "*elevados custos extras, associados a múltiplos ensaios e múltiplas certificações, que reduzem suas margens de competitividade*". Reiterando a afirmação, o órgão cita dados da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que apontam que "*a adaptação de produtos, realização de ensaios e a obtenção de certificados para os diferentes países oneram a produção das empresas exportadoras numa faixa entre 2 e 10% de seus custos totais*". Disponível em http://www.inmetro.gov.br/barreirastecnicas/recmutuo.asp. Acesso em 23.02.2017.

44 Comentários da Consulta Pública para o Plano Nacional de IoT apontaram a necessidade de um maior alinhamento do País às práticas internacionais e a implementação de ARM como forma de tornar menos oneroso trazer soluções ao Brasil e reduzir o tempo de chegada.

45 Para países em desenvolvimento, reputa-se necessária "*a promoção de programas de cooperação técnica que viabilizem a transferência de tecnologia e a experiência dos países desenvolvidos*", de forma a capacitar a infraestrutura de acreditação dos países em desenvolvimento para nível de confiança necessário à busca de reconhecimento internacional. Disponível em http://www.inmetro.gov.br/barreirastecnicas/recmutuo.asp. Acesso em 23.02.2017.

Oportunidade de melhoria	Entraves	Consequências
utilizados em outros cantos do globo como forma de padronização dos procedimentos; • Necessidade de repetições e reanálises.	envolvendo hackeamento e tratamento de dados; d) *Risco de parcialidade*. A implementação de uma certificação "por similaridade" poderia envolver alto grau de subjetivismo.	• Atraso na entrada da tecnologia no mercado / defasagem.

Outro impasse burocrático está na dinâmica de estabelecimento dos requisitos técnicos que embasam a avaliação do produto feita pelos laboratórios e Organismos Certificadores Designados ("OCDs") por meio de atos normativos da Anatel.

O problema foi identificado pela Agência, que, em recente consulta pública, propôs a revogação das normas pertinentes e a sua substituição por atos administrativos da superintendência responsável.[46]

Oportunidade de melhoria	Consequência	Proposta da ANATEL	Objetivo
Estabelecimento dos requisitos técnicos para certificação por meio de atos normativos da Anatel	Latência indesejada e barreira de entrada a novos produtos, afetando usuários, fabricantes e prestadores dos serviços de telecomunicações	Revogar 36 normas e regulamentos que tratam da certificação e homologação de produtos de telecomunicações, e a sua substituição por requisitos formulados pela superintendência responsável, por ato administrativo, sem necessidade da intervenção do Conselho Diretor.	Tornar mais eficiente e atualizar as "*referências técnicas de forma a acompanhar a evolução tecnológica e evitando o bloqueio do uso de produtos que possuam novas tecnologias no País*"

46 Anatel, Consulta Pública nº 34/2016, Análise de Impacto Regulatório, Junho/2016, Processo nº 53500.009149/2016-55.

Para além desses entraves, deve-se considerar que a certificação e a homologação de equipamentos realizadas hoje não consideram os riscos de segurança atrelados à disseminação de IoT no País e à expansão no número de dispositivos conectados suscetíveis a falhas e ataques.

A exigência de um padrão mínimo de segurança como requisito para a certificação e homologação de equipamentos poderia se apresentar como uma forma de evitar, ou, ao menos, mitigar tais riscos. No entanto, é preciso enfrentar algumas discussões:

a) *Conflito com o princípio da neutralidade tecnológica*. A depender das condições exigidas, a opção regulatória poderia implicar a exclusão de determinadas tecnologias e modelos de negócio do mercado, em prejuízo à inovação e à liberdade de contratar.

b) *Diversidade de aplicações*. São inúmeras as formas de os dispositivos serem aplicados para a composição de soluções de IoT – além de tantas outras que podem vir a ser criadas no futuro. Isso dificulta a formulação de um único padrão, extensível a todas as possíveis aplicações.

c) *Diferentes graus de criticidade.* O emprego dos diversos equipamentos pode se dar de forma mais ou menos crítica, para as quais uma exigência de segurança pode se mostrar também mais ou menos necessária. Enquanto para aplicações de usos menos sensíveis, a exigência de padrões mais rigorosos possa se mostrar dispensável, o mesmo não valeria para aplicações de maior criticidade (e.g., sensores de incêndio, dispositivos empregados em ambientes hospitalares, etc.).[47]

d) *Limitações técnicas*. Por exemplo, dispositivos extremamente restritos (e.g., sensores) não são capazes de criptografia, nem mesmo criptografia leve.[48]

e) *Evolução tecnológica*. Pode tornar critérios de segurança que, hoje, são suficientes para a devida proteção dos usuários e da rede, obsoletos e, assim, inadequados para o seu propósito. Da mesma forma, tecnologias mais modernas de segurança podem ser criadas no futuro.

f) *Expertise*. É necessária uma expertise própria para o assunto. Hoje, o órgão mais preparado para a avaliação desses critérios seria a Anatel, mas mesmo a Agência teria limitações para lidar com uma infinidade de novos pedidos de

47 Veja-se nesse sentido: "[a] *segurança nos dispositivos da Internet das Coisas não deve ser tida de forma binaria, como sendo apenas seguro ou não seguro, mas sim como um espectro, que varia desde dispositivos que não apresentam segurança alguma até dispositivos com várias camadas de mecanismos para prover segurança"* (Produto 2: *Roadmap* de tecnologias habilitadoras. Relatório Final. 2017. p. 97).

48 Sobre criptografia para dispositivos restritos ver Produto 2: *Roadmap* de tecnologias habilitadoras. Relatório Final. 2017. p. 100

homologação/certificação de dispositivos de IoT. De fato, os temas trabalhados pela Anatel estão mais relacionados a questões de radiofrequência e segurança física do usuário, e não chegam a envolver outros aspectos de segurança como a criptografia, por exemplo.

Além disso, vale destacar que mesmo a criação de padrões distintos para aplicações, ou grupo de aplicações, diversas encontraria dificuldades. Isso porque não seria possível identificar, *a priori*, as funções que os dispositivos fabricados assumiriam depois de sua comercialização.

Por fim, é importante mencionar que algumas novas tecnologias podem demandar revisões nos requisitos para certificação de dispositivos. Como exemplo, temos os equipamentos para operar a rede LoRa,[49] os quais tem enfrentado dificuldade de certificação diante de uma regra específica constante da Resolução nº 506 e do Ato nº 1135/2013 da ANATEL, acerca do pico da densidade espectral de potência. Com a entrada em vigor da Resolução nº 680/2017 no dia 28 de agosto, essa barreira poderá ser endereçada.

3.1.6. Discussões sobre licenciamento de estações: a experiência das desonerações M2M

A discussão sobre a instituição – ou não – de tratamento diferenciado para o ambiente dos serviços que envolvem IoT, já foi iniciada, sendo relevante uma reflexão sobre a tentativa de reduzir os custos relacionados às taxas de fiscalização. Esse movimento ilustra uma experiência brasileira e as dificuldades de aplicar a assimetria regulatória de forma efetiva para aplicações IoT.

Uma das obrigações financeiras que recai sobre as prestadoras de serviços de telecomunicações corresponde ao recolhimento do Fundo de Fiscalização das Telecomunicações ("FISTEL"). E para as prestadoras que atuam no âmbito da IoT não é diferente.[50]

Como sabido, todas as estações utilizadas para a prestação de serviços de telecomunicações geram o dever de recolhimento de taxas do FISTEL. Assim, as aplicações de IoT que envolvam o uso de estações deverão contabilizar este custo.

[49] LoRa é uma tecnologia *Low Power Wide Area Network (LPWAN).* Para maiores informações sobre a tecnologia LoRa, conferir em seu site oficial: http://www.semtech.com/wireless-rf/internet-of-things/what-is-lora/

[50] A questão especificadamente do FISTEL será tratada posteriormente por este documento, no tópico "IV Dos Obstáculos Tributários ao Desenvolvimento da IoT".

Com o intuito de reduzir os valores referentes a esta taxa, a Lei nº 12.715/2012, em seu art. 38, autorizou a desoneração para os equipamentos que se classificam como sendo de comunicação máquina a máquina ("M2M"), ficando estes produtos vinculados ao recolhimento da taxa de fiscalização por chip no valor de R$ 5,86 (cinco reais e oitenta e seis reais).[51]

Por ser o valor da desoneração significativo, passando de R$ 26,83 (vinte e seis reais e oitenta e três centavos) para os citados R$ 5,86 (cinco reais e oitenta e seis centavos), instituiu-se a discussão sobre quais seriam as estações elegíveis para usufruir deste benefício.

A Lei estabeleceu como requisito a observância de comunicação M2M, tendo o Decreto nº 8.234/2014 definido que: "*serão considerados sistemas de comunicação máquina a máquina os dispositivos que, sem intervenção humana, utilizem redes de telecomunicações para transmitir dados a aplicações remotas [...]*".[52]

Ocorre que não está normatizado o que seria entendido como ausência de intervenção humana que possa qualificar uma comunicação como M2M. Esta dúvida foi inclusive abordada por contribuições feitas à Consulta Pública destinada à coleta de subsídios sobre o desenvolvimento da IoT no Brasil.[53]

No geral, as contribuições neste sentido apontaram que seria necessária uma maior reflexão sobre a desoneração voltada às comunicações M2M e o conceito adotado no Decreto nº 8.234/2014, já que não seria justificável um tratamento tributário distinto para as aplicações ao ser avaliado o nível de intervenção humana envolvida. Assim, defendeu-se que este tratamento benéfico deveria ser aplicado a aplicações semelhantes.

Como parte da justificativa apresentada nas contribuições, foi destacado que os produtos envolvidos no universo da IoT são em muito similares, não havendo uma resposta exata para determinar quais seriam os produtos contemplados pela desoneração.

Portanto, a questão a ser resolvida reside no conceito de intervenção humana, não incluído no Decreto nº 8.234/2014. E esta é essencial, já que ao ser estudada a possibilidade de inaugurar um tratamento diferenciado para a IoT, ou seja, quando falamos da

51 Lei nº 12.715/2012

52 Art. 1º do Decreto nº 8.234/2014.

53 Consulta Pública Plano Nacional de IoT.

possibilidade de instituir uma assimetria regulatória, é essencial poder delimitar com clareza quem será impactado por esta medida.

Destacamos ainda, que a Anatel, desde 2014 reconhece que os terminais do SMP desonerados graças à previsão da Lei nº 12.715/2012 seriam denominadas como terminais "M2M Especial" – sendo assim considerados apenas aqueles nos quais não há qualquer tipo de interação humana.[54]

A inciativa trazida pela Lei nº 12.715/2012 é louvável, entretanto, o fato de seu critério de aplicabilidade residir na ausência total de intervenção humana não parece razoável, conforme indicado nas contribuições da Consulta Pública de Internet das Coisas.

Isso porque existem diversas aplicações que possuem um contato mínimo humano, sem deixarem de ser afetas ao ecossistema IoT, mas acabam não se beneficiando do referido tratamento assimétrico.

Aqui, relevante considerar as ponderações apresentadas na Consulta Pública acima mencionada. Em uma das contribuições é defendido que o conceito de intervenção humana seja flexibilizado de forma a permitir que outros serviços de IoT sejam contemplados com desonerações fiscais concedidas aos serviços que envolvem comunicação M2M.[55]

Apontamos também que em algumas das contribuições foi postulada a necessidade de suprimir a expressão "sem intervenção humana" do Decreto nº 8.237/2014, a fim de viabilizar uma diminuição dos ônus fiscais de forma mais abrangente.

Como argumento, as contribuições apontaram que o universo da IoT é complexo e que nem sempre a ausência completa do elemento humano será passível de identificação. A presença de mínimas intervenções não deveria, assim, afastar a classificação do serviço como um serviço de IoT que é viabilizado por meio de uma comunicação M2M.[56]

No geral, as contribuições apontaram a necessidade de esclarecer o conceito de intervenção humana, destacando que, no estágio atual do ordenamento jurídico brasileiro, ainda seria necessária uma maior precisão conceitual.

54 Anatel. Comunicação Máquina a Máquina. Disponível em http://www.anatel.gov.br/dados/destaque-1/282-comunicacao-maquina-a-maquina. Acesso em 30.03.2017.

55 Contribuições feitas à Consulta Pública do Plano Nacional de IoT

56 Idem.

Este ponto já está sendo enfrentado em outras jurisdições e as soluções adotadas podem servir como referência para o quadro brasileiro. Na Alemanha, por exemplo, optou-se em definir comunicações M2M como aquelas que são *predominantemente* automatizadas. A intervenção humana não seria usual, mas a sua presença, de forma limitada, seria admitida e não afastaria a classificação de comunicação M2M.[57]

Dessa forma, seria necessário reavaliar (i) o conceito da IoT e/ou M2M, de modo a reduzir a assimetria de tratamento entre aplicações com diferentes níveis de intervenção humana e (ii) os valores das taxas setoriais, buscando chegar a um valor de cobrança que seja proporcional ao serviço prestado, evitando sua oneração excessiva.[58]

Pelo exposto, fica claro que não há consenso sobre a terminologia utilizada para identificar as aplicações (ou serviços prestados por meio destas) que seriam beneficiados com uma desoneração quanto ao FISTEL. Importante ter em mente que para muitas funcionalidades no âmbito da IoT não será sempre possível excluir completamente a presença da interação humana, sendo necessária uma maior reflexão quanto a este ponto. Dessa forma, é essencial que os conceitos envolvidos na desoneração de comunicações M2M sejam debatidos e, na sequência, esclarecidos, evitando assim a oneração excessiva das funcionalidades da IoT.

3.1.7. Qualidade dos serviços de telecomunicações que suportam aplicações de IoT: tratamento igualitário e a reflexão sobre assimetria regulatória

Outra discussão muito relevante para o desenvolvimento de IoT no país diz respeito ao ônus regulatório imposto ao setor das telecomunicações e da atual impossibilidade de conceder um tratamento diferenciado em função da aplicação que será suportada pelo serviço de telecomunicações, em especial nos serviços de interesse coletivo que podem servir de suporte para aplicações IoT.

Trata-se da condição de igualdade imposta pelos RGQs, os quais trazem metas de qualidade a serem observadas pelas prestadoras de SMP e SCM. Nestes regulamentos, a redação dos respectivos arts. 1º, §3º estabelecem que as metas, relacionadas à rede e aos usuários, deverão ser igualmente cumpridas por todas as prestadoras – ressalvadas apenas aquelas que se enquadram como sendo de pequeno porte. [59]

57 Alemanha. Definição de comunicação M2M adotada pelas autoridades alemãs.

58 Contribuições feitas à Consulta Pública do Plano Nacional de IoT.

59 Resolução Anatel nº 575/2011.

Isso significa que há obrigatoriedade de que toda a conexão contratada siga os parâmetros mínimos de qualidade fixados nos RGQs. Dos elementos de qualidade definidos nos regulamentos, apenas a velocidade é efetivamente sujeita às condições comerciais das operadoras – que podem ofertar planos com maior ou menor velocidade, garantindo, apenas, que ela esteja efetivamente disponível em uma parcela do tempo.

No entanto, elementos como índice mínimo de tentativas bem-sucedidas de conexão com a rede de dados (art. 20 do RGQ/SMP), ou latência bidirecional mínima de 80 milissegundos em 95% dos casos (art. 18 do RGQ/SCM), correspondem a indicadores de qualidade que incidem sob qualquer conexão.

Nesse sentido, tendo em mente que a maior liberdade para as operadoras ofertarem planos adequados às aplicações IoT – e.g. com maior latência bidirecional – pode ser uma forma de baratear o custo do serviço, os RGQs podem representar um óbice a esse objetivo. Ou seja, o tratamento das aplicações IoT como usuários comuns pode resultar em um custo proibitivo para a sua disseminação.

Ainda que haja uma predisposição da Anatel em excluir do cômputo das metas e parâmetros mínimos de qualidade dos respectivos serviços os indicadores associados a dispositivos M2M conectados, é preciso regulamentar exceções visando garantir alguma segurança jurídica para o setor. Esta assimetria de tratamento seria plenamente justificável, na medida em que parâmetros mínimos de qualidade concebidos para comunicação humana não são necessariamente adequados para níveis de serviço destinados a comunicação entre máquinas.

De qualquer modo toda assimetria deve ser introduzida com cautela, para não gerar distorções no mercado, ainda que a intenção seja a mais legítima possível. Por exemplo, tendo em vista que ao ser disponibilizado ao mercado um nicho com ônus regulatório reduzido a tendência é que os players busquem a inclusão do maior número possível de serviços neste ambiente.

Por isso, caso seja compreendida como acertada a opção de inaugurar uma assimetria regulatória para o âmbito do IoT, o primeiro passo seria instituir conceitos adequados, tanto de IoT em si, quanto avaliar como utilizar a "intervenção humana" (ou não) como critério.

3.2. Neutralidade da rede

Seguindo o diagnóstico, uma das grandes preocupações indicadas na Consulta Pública de Internet das Coisas, versou sobre o papel da neutralidade da rede para o desenvolvimento do ecossistema de IoT no Brasil.

No Brasil, o MCI estabeleceu regra geral de neutralidade da rede, determinando a obrigação de tratamento isonômico de pacotes de dados aos intermediários que operacionalizam a transmissão de dados na rede.[60] A regra diz respeito ao tráfego de dados em nível de infraestrutura da rede.

Objetivamente, o que se veda com a regra de neutralidade da rede no MCI é a discriminação técnica de tráfego de dados quanto ao conteúdo, origem, destino, terminal ou aplicativo.

Note-se que, embora o MCI dedique a obrigação geralmente ao "responsável pela transmissão, comutação ou roteamento", o Relatório Final da Comissão Especial do Senado ilustra os destinatários da obrigação como os "provedores de conexão, empresas de telecomunicação, backbones, prestadores de serviços de comutação, de roteamento de pacotes e demais agentes que trabalham na operacionalização da internet."[61]

Não obstante a implementação da regra de neutralidade da rede, o MCI admite duas exceções, listadas em rol exaustivo. Primeiro, admite-se a priorização de tráfego a serviços de emergência. Segundo, a priorização de pacotes de dados em decorrência de requisitos técnicos indispensáveis à prestação e fruição adequada de serviços e aplicações.

Para enquadramento nas exceções, há três condicionantes necessárias: abstenção de causar prejuízos injustificados ao usuário, respeito à livre concorrência e transparência.

Para além disso, a regra da neutralidade da rede foi regulamentada pelo Decreto nº 8.771/2016. O Decreto nº 8.771/2016 se dedica primordialmente a delimitar os critérios que permitem as exceções ao dever de tratar o tráfego de dados de forma isonômica; e estabelecer as condições em que se permite arranjos entre o responsável pela transmissão, comutação e roteamento de dados e os provedores de aplicação, tais como zero-rating e acesso patrocinado.

60 Lei nº 12.965/2014, art. 9.

61 Parecer final da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 5.403, de 2001, p. 40, disponível em www.camara.leg.br/internet/agencia/pdf/PL5403ParecerFinal.doc .

Em relação às exceções ao dever de tratamento isonômico, o Decreto nº 8.771/2016 deixa claro tratar-se de medida excepcional, permissível somente nas duas hipóteses listadas no MCI: requisitos técnicos indispensáveis para a prestação adequada de serviços e aplicações e priorização de serviços emergenciais.

Em ambas as hipóteses, resta claro que devem ser cumpridas as condições listadas pelo MCI cumulativamente. Aos requisitos técnicos indispensáveis para a prestação adequada de serviços, o Decreto nº 8.771/2016 é claro ao estabelecer que somente podem ser considerados como tal o tratamento de questões de segurança da rede ou o gerenciamento de rede em situações excepcionais de congestionamento.

Note-se que a abordagem admite a possibilidade de gerenciamento de rede por parte dos responsáveis pelo tráfego de dados, desde que a prática tenha como objetivo preservar a estabilidade, segurança e funcionalidade da rede, dentro ainda dos limites estabelecidos pela Anatel e as diretrizes do CGI.br.

Já aos serviços de emergência, o decreto regulamentar é igualmente claro ao estipular hipóteses exaustivas para a discriminação ou a degradação de tráfego. São essas o risco de desastre, emergência ou estado de calamidade pública, e ainda a comunicação entre provedores de comunicação dos serviços de emergência.

Em relação à celebração de arranjos comerciais entre o responsável pelo tráfego e o provedor de aplicação, o Decreto nº 8.771/2016 efetivamente procura estender a tutela da neutralidade da rede a planos conhecidos como zero-rating, nos quais provedores de conexão isentam o tráfego decorrente de determinado conteúdo da franquia de dado de usuários, e acesso patrocinado, nos quais o provedor de aplicação arca com o custo referente ao tráfego de dados pelo usuário.

Observe-se, contudo, que o Decreto nº 8.771/2016 não extrapola os limites da lei ao banir planos zero-rating ou acesso patrocinado, na medida em que não haja discriminação no tráfego de dados. Assim, caso a oferta respeite a isonomia no tráfego de pacote de dados, não haveria violação à norma.

Em suma, do ponto de vista das preocupações indicadas na Consulta Pública quanto a importância da neutralidade da rede para o desenvolvimento da Internet das Coisas, é fato que o Brasil possui uma regulação moderna e adequada ao desenvolvimento de inovações na internet, garantindo a proteção ao tratamento isonômico na internet.

3.3. Questões envolvendo privacidade e proteção de dados pessoais

O debate relacionado a privacidade e a proteção de dados pessoais no ecossistema de IoT remete tanto aos dispositivos pessoais vendidos a consumidores (ex: bonecas com conexão à internet; televisões inteligentes; wearables), considerados como titulares de dados pessoais, como quanto aos sistemas IoT/M2M em geral que possam gerar preocupações de privacidade e proteção de dados pessoais (ex: sistema de monitoramento inteligente por câmeras nos logradouros; rastreamento direto ou indireto de consumidores em ambientes físico e online).

Como pode ser identificado na Consulta Pública do Plano Nacional de Internet das Coisas e nos eventos do Estudo Nacional de Internet das Coisas, esse tema é especialmente importante em IoT, merecendo o devido destaque no presente diagnóstico. A seguir, abordaremos as principais questões jurídicas mapeadas nesse tópico.

3.3.1. Legislação aplicável a privacidade e a proteção de dados pessoais no Brasil

O Brasil é um dos poucos países entre as maiores economias do mundo que ainda não possui uma legislação geral sobre proteção de dados pessoais. Na inexistência de norma específica são aplicáveis normas esparsas, em especial a Constituição Federal e as normas do Marco Civil da Internet e do Código de Defesa do Consumidor. A seguir, apresentamos um resumo dos principais normativos potencialmente aplicáveis ao tema.[62]

- **Constituição Federal**

De início, o quadro legal brasileiro possui direitos fundamentais previstos na Constituição Federal que estabelecem proteções a privacidade dos indivíduos.

Em seu artigo 5º, inciso X, a Constituição estabelece a inviolabilidade da intimidade, vida privada, da honra e da imagem como um conjunto de direitos. De modo geral, a proteção ao direito à intimidade aplica-se aos aspectos íntimos do indivíduo, aos quais não se admite acesso de terceiros. Já o direito à vida privada diz respeito às informações comunicadas a terceiros, como nome, endereço, dentre outros dados.[63]

[62] Fazem parte desse arcabouço as proteções legais ao sigilo fiscal e ao siglo bancário (LC 105/2001) também.

[63] FERRAZ JR., Tércio Sampaio, Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, RT. Cadernos de Direito Constitucional e Ciência Política. São Paulo, ano I, out./dez. 1992, p. 79.

No âmbito digital, há incerteza se o artigo 5º, X, supriria a ausência de uma lei geral para a proteção de dados pessoais.[64] Por um lado, argumenta-se que o artigo 5º, X seria insuficiente para tutelar a coleta, tratamento e uso de dados nos moldes atualmente praticados pela indústria e, assim, não preencheria a lacuna causada pela ausência de uma lei específica sobre proteção de dados.[65-66] Por outro, sustenta-se que os direitos à inviolabilidade da intimidade e à vida privada provêm proteção suficiente para serem considerados em conjunto como um "direito fundamental à proteção de dados pessoais".

Outro direito fundamental previsto pela Constituição é o direito ao sigilo de comunicações, garantido pelo artigo 5º, XII. O sigilo protegido por este dispositivo tem por objeto, especificamente, as comunicações de indivíduos, independentemente do meio tecnológico adotado pelos interlocutores (correspondência, telegrafia, telefonia, etc.), com a ressalva, entretanto, da possibilidade de quebra de sigilo da comunicação telefônica no contexto específico de investigações criminais.

Note-se que não há relação direta entre "sigilo" e "privacidade". Mesmo que o dado seja tornado "público" pelo indivíduo a um determinado interlocutor, deve ainda assim ser considerado privado e ensejar a tutela jurídica da privacidade.[67]

No contexto da internet, o direito ao sigilo de comunicações é utilizado para consubstanciar a proteção dos interlocutores de uma possível interferência de terceiros na comunicação de dados.

É importante ressaltar a interpretação de que o artigo 5º, XII protege a 'comunicação', não os dados em si, ou seja, protege-se a transmissão de dados, seja por rede pública ou privada, de intervenção de terceiros. A partir do momento em que cessa a comunicação e os dados são armazenados em disco rígido, é interrompida também a proteção do direito ao sigilo de comunicações e passam a incidir outros direitos, como os previstos pelo artigo 5º, X.[68]

Em todos os casos, a proteção como direito da personalidade estará sempre associada ao dado ligado diretamente a uma pessoa específica e individualizada ou individualizável.

64 CASSEB, P. Fundamentos Constitucionais do Marco Civil da Internet. In: DE LUCCA, Netwon, SIMÃO FILHO, Adalberto, ROSA PEREIRA DE, Cíntia. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015

65 Ibid, p. 165.

66 Para ilustrar o descompasso, pode-se dizer que uma informação poderá ser "privada", mas não "dado pessoal", nos termos comumente utilizado no âmbito da proteção de dados, e.g., dado que identifica ou permite identificar o titular de dados.

67 LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2012, p. 65.

68 LEONARDI, Marcel, *apud* Marcarini, Augusto Tavares Rosa, Direito e Informática: uma abordagem jurídica sobre criptografia, São Paulo: Forense, 2002, p. 146.

Em ambiente em que a comunicação não envolver diretamente um indivíduo, como em comunicação máquina a máquina, a incidência da proteção constitucional apresentada acima dependerá da associação a dado pessoal de titular individualizado ou individualizável.

Por fim, é importante mencionar também o instrumento do *habeas data*, previsto no artigo 5º, LXXII da Constituição, que foi regulado pela Lei 9.507/1997 e será abordado na sequência.

- ***Código de Defesa do Consumidor***

Para além da Constituição Federal, a proteção à privacidade e a proteção de dados pessoais no país, possui outro marco chave, que é a Lei nº 8.078/1990, que instituiu o Código de Defesa do Consumidor (CDC).

O CDC foi considerado por anos como a principal norma no quadro legal brasileiro na proteção de dados pessoais, até a entrada em vigor do Marco Civil da Internet e das Leis nº 12.414 (Lei do Cadastro Positivo) e 12.527 (Lei de Acesso à Informação), ambas de 2011.[69] Mesmo com a edição do Marco Civil da Internet e das Lei do Cadastro Positivo e de Acesso à Informação, o CDC permanece diretamente aplicável, em diálogo com o Marco Civil da Internet, sempre que houver relação de consumo, até que entre em vigor uma legislação específica sobre proteção de dados pessoais em ambiente virtual.[70]

Nas hipóteses em que incidir o CDC, aplicar-se-á o regime da responsabilidade objetiva ao fornecedor de serviços. Isso implica que, nos casos de violações à segurança do serviço ou da base de dados, o prestador deverá responder pelos danos materiais e morais causados. Caso haja vazamento de dados, ainda, prestador de serviços deverá notificar o consumidor.

Note-se que, nos casos de violação à segurança dos serviços ou da base de dados, haverá responsabilização do prestador de serviços mesmo que não haja culpa. O regime estabelecido pelo Código Civil se aplica, de forma em que a excludente de

69 Lei nº 8.078/1990.

70 ESPÍNDOLA LONDONI KLEE, Antônia, MAGALHÃES MARTINS, Guilherme. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). In: NETWON DE LUCCA, ADALBERTO SIMÃO FILHO, CÍNTIA ROSA PEREIRA DE. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015, p. 358.

responsabilização dependerá de caso de força maior ou culpa exclusiva da vítima ou de terceiros.[71]

Um fator-chave para a coleta e tratamento de dados pessoais diz respeito à obtenção de consentimento do consumidor. O consentimento não será válido caso seja baseado no fornecimento de informações enganosas ao consumidor.

Essa análise levará em consideração a boa-fé objetiva do prestador de serviços, as expectativas do consumidor e os impactos e riscos do tratamento de dados. Em caso em que a coleta de dados seja considerada invasiva ou desleal, haveria violação ao princípio da boa-fé objetiva.[72] Note-se, assim, que sob o aspecto de obtenção de consentimento para coleta e tratamento de dados, o CDC propicia alto grau de proteção ao consumidor.[73]

Além disso, o CDC efetivamente garante o direito de acesso por titulares de dados às informações armazenadas em bases de dados. Esta garantia de transparência deve ocorrer antes que o dado seja efetivamente utilizado e, embora o CDC não estabeleça o momento exato da comunicação, a jurisprudência entende que deverá sê-lo antes da inscrição no banco de dados.[74]

No ambiente digital, essa tutela se mostra protetiva ao consumidor frente a provedores de conteúdo e anunciantes, por exemplo.[75] Isso porque há obrigação de notificação por escrito em caso de criação de banco de dados. O arquivista – ou, no contexto da proteção de dados, o "controlador de dados" – é ainda obrigado a conceder acesso ou retificar eventuais dados incorretos em até cinco dias úteis do requerimento do consumidor.[76]

Outro ponto de controvérsia diz respeito ao prazo máximo de armazenamento de informações do consumidor. Isso porque a norma estabelece que os cadastros ou banco de dados só poderão conter "informações negativas" a respeito de consumidor por até 5

71 Ibid., 389.

72 SCHERTEL MENDES, Laura. A Tutela da privacidade do consumidor na internet: uma análise à luz do Marco Civil da Internet e do Código de Defesa do Consumidor. In: NETWON DE LUCCA, ADALBERTO SIMÃO FILHO, CÍNTIA ROSA PEREIRA DE. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015, p. 482.

73 Ibid., p. 481.

74 DONEDA, Danilo. Princípios de proteção de dados pessoais. In: NETWON DE LUCCA, ADALBERTO SIMÃO FILHO, CÍNTIA ROSA PEREIRA DE. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015, p. 379. Segundo o autor, a Súmula 359 do STJ estabelece que, no contexto de inscrição de consumidores em bases de dados de análise de crédito, "[c]abe ao órgão mantenedor do Cadastro de Proteção ao Crédito a notificação ao devedor antes de proceder à inscrição".

75 Ibid., p. 305.

76 Essa concepção do direito à privacidade, no campo do Direito do Consumidor, faz-se presente ainda no Decreto nº 7.963/13, que introduz o Plano Nacional de Consumo e Cidadania (PNCC) e estabelece claramente a autodeterminação do consumidor como uma das diretrizes do PNCC.

(cinco) anos. Note-se que a norma só diz respeito às "informações negativas". Sobre as informações em geral, não há determinação legal no CDC.

Ressalta-se que, na ausência de legislação específica, a doutrina projeta o artigo 6º, III do CDC para obrigar ao prestador de serviços informar ao consumidor sobre quais os dados tratados; para quais finalidades; se serão transmitidos a terceiros; por qual período serão conservados; quais os mecanismos de segurança utilizados.

Na prática, tal divulgação pode se dar por meio da política de privacidade do serviço, de contrato celebrado entre as partes, ou mesmo pela prestação de informações ao consumidor antes do consentimento.[77] No caso de falha pelo prestador de serviços, há mesmo possibilidade de indenização por dano material e moral, o que apresenta um risco ao prestador de serviços em modelo de negócios que não possibilite o cumprimento do CDC nos moldes da norma, como nas hipóteses em que não há interface com o consumidor para a prestação de informações.[78]

Por fim, é importante ter em mente que a fiscalização e aplicação de sanções no ambiente do CDC é feita de maneira difusa, em especial através da atuação do Sistema Nacional de Defesa do Consumidor (SNDC), conforme regulamentação prevista no Decreto Presidencial nº 2.181, de 20 de março de 1997.

- ***Lei Geral de Telecomunicações***

No setor de telecomunicações, a Lei nº 9.472/1997 (LGT) surge como a legislação aplicável a proteção da privacidade e da proteção de dados pessoais.

A LGT garante ao usuário o direito à inviolabilidade e ao segredo de suas comunicações, salvo nas hipóteses de restrições legais. A utilização de informações pessoais só é permitida por operadoras no limite da execução de suas atividades, evitando, assim, a comercialização de informações que permitam a identificação de perfis de usuários a terceiros, salvo em caso de anuência expressa e específica do usuário.[79]

Para além das limitações no uso e compartilhamento de dados por operadoras de telecomunicações, cabe ressaltar a possibilidade de quebra do sigilo por ordem judicial.

77 SCHERTEL MENDES, Laura. A Tutela da privacidade do consumidor na internet: uma análise à luz do Marco Civil da Internet e do Código de Defesa do Consumidor. In: NETWON DE LUCCA, ADALBERTO SIMÃO FILHO, CÍNTIA ROSA PEREIRA DE. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015, p. 486.

78 Ibid.

79 Lei nº 9.472/1997, art. 72.

Conforme estabelecido pelo STF, tem-se que os dados cadastrais dos usuários de telefonia somente poderão ser compartilhados mediante decisão judicial fundamentada, em caso concreto.[80]

Entretanto, a LGT estabelece que informações agregadas sobre o uso dos serviços, no entanto, podem ser divulgadas pelas prestadoras. Nesses casos, a possibilidade de compartilhamento dependerá de agregação que impossibilite a identificação, direta ou indireta, do usuário.

Ainda, as Resoluções nº 632/2014 e nº 477/07 (Regulamento sobre SMP) da Anatel garantem ao usuário privacidade nos documentos de cobrança e na utilização de dados pessoais, aplicando-se concomitantemente o CDC.[81][82]

- ***Lei do Habeas data***

Em seguida a publicação da LGT, foi promulgada a Lei 9.507/1997, que regulamentou o instrumento do *habeas data*, previsto no artigo 5º, LXXII da Constituição Federal.

De imediato, cabe ressaltar que o *habeas data* é remédio aplicável tão somente para a obtenção de informação em bancos de dados públicos, com o objetivo de proteger a esfera íntima de indivíduos na ocasião da inserção de dados pessoais em registros públicos.

Em casos de usos abusivos de dados pessoais, como a introdução de dados sensíveis – tais como os dados que permitam identificar a origem racial, posição perante política, religião ou filosofia, filiação partidária ou sindical, orientação sexual – ou mesmo de introdução e conservação de dados falsos ou ilegais em registros públicos, o indivíduo pode invocar o remédio do *habeas data* para exigir a retificação.[83]

A eficácia do *habeas data* na tutela da privacidade do cidadão no ambiente virtual e na proteção de dados pessoais possui, assim, limitações, já que o instrumento não se aplica a registros mantidos pela iniciativa privada.[84] Pelo contrário, o instrumento é destinado aos

80 STF, AC 1.928/RS, rel. Min. Ricardo Lewandowski, publicação em 01/02/2008.

81 Resolução Anatel nº 632/2014; Regulamento do Serviço Móvel Pessoal, anexo à Resolução nº 477/2007.

82 Lei nº 8.078/1990.

83 AFONSO DA SILVA, José. Curso de direito constitucional positivo. São Paulo: Ed. Malheiros, 34ª edição, 2011, p. 454.

84 ZANATTA, Rafael A. F., A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In: NETWON DE LUCCA, ADALBERTO SIMÃO FILHO, CÍNTIA ROSA PEREIRA DE. Direito & Internet III - Tomo I. São Paulo: Quartier Latin, 2015, p. 451.

registros mantidos por "entidades governamentais" ou de "caráter público", conforme estabelecido pela Lei nº 9.507/1997.[85]

- ***Código Civil***

Outro marco legal importante da proteção à privacidade no país, está sedimentado na Lei nº 10.406/2002 (Código Civil) que dedica um capítulo específico aos direitos da personalidade, protegidos pela Constituição Federal por meio do artigo 5º, X, citado acima.[86] São protegidos, sem a pretensão de rol exaustivo, o direito à integridade psicofísica, ao nome e ao pseudônimo, à imagem e à inviolabilidade da vida privada.

Trata-se do primeiro momento em que o legislador se ocupa da proteção a direitos da personalidade.[87] Na disciplina do Código Civil, são direitos intransmissíveis e irrenunciáveis, de forma em que não podem ser renunciados ou abandonados, mas apenas voluntariamente limitados.

Em particular atenção ao direito à inviolabilidade da vida privada, o dispositivo positivado estabelece uma obrigação de não-fazer. Em caso de descumprimento, permite-se ao prejudicado pleitear medida judicial para que cesse a prática de ato abusivo ou ilegal.[88] A norma permite não apenas que o indivíduo busque interromper qualquer violação à sua vida privada, mas também a reparação por danos já cometidos, nas dimensões material e moral.

O legislador excluiu da proteção à privacidade a pessoa jurídica, considerando apenas a privacidade de pessoas naturais como inviolável.[89] Tal opção é clara pela redação do artigo 21, que condiciona a proteção à "vida privada da pessoa natural". Mesmo que o artigo 52 do Código Civil conceda às pessoas jurídicas a proteção dos direitos da personalidade "no

85 Lei nº 9.507/1997. A lei considera como registro ou banco de dados de caráter público aquele que contenha informações "que sejam ou possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações". São entidades de "caráter público" as "instituições, entidades e pessoas jurídicas privadas que prestem serviços para o público ou de serviço público", tais como concessionárias, permissionárias ou as que exercem atividades autorizadas. Um exemplo de entidade sobre a qual seria permitido obter acesso aos dados ou retificação seriam as instituições de scoring de crédito, tratadas em maior detalhe posteriormente.

86 Lei nº 10.406/2002.

87 DONEDA, Danilo. Os Direitos da Personalidade no Código Civil. Disponível em http://fdc.br/Arquivos/Mestrado/Revistas/Revista06/Docente/03.pdf.

88 GONÇALVES, Carlos Roberto. Direito Civil Brasileiro, vol. 1, 8ª edição, São Paulo: Saraiva, 2010, p. 205.

89 DONEDA, Danilo. Os Direitos da Personalidade no Código Civil. Disponível em http://fdc.br/Arquivos/Mestrado/Revistas/Revista06/Docente/03.pdf, p. 91.

que couber", pode-se dizer que a redação do artigo 21 é taxativa, limitando a incidência da proteção às pessoas naturais.

- ***Lei 12.414/2011 - Lei do Cadastro Positivo***

A Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011 – "Lei nº 12.414/2011"), que disciplina a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito, por sua vez, requer, para a abertura de cadastro, autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada, e o limite temporal das informações de quinze anos.

Essa lei impõe ao fornecedor do serviço, além disso: (i) o dever de veracidade; (ii) o dever de clareza; (iii) o dever de objetividade; (iv) a vedação de informações excessivas; e (v) a vedação de informações sensíveis.[90] Chama a atenção a previsão de informações proibidas, isto é, as qualificadas como excessivas ou sensíveis. Por excessivas, entende-se aquelas "que não estiverem vinculadas à análise de risco de crédito ao consumidor".[91] Já as informações sensíveis são definidas como "*aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas*". A vedação desses dados busca evitar a utilização discriminatória da informação – a distinção é muito comum no Direito Europeu como se verá adiante.

Como forma de assegurar o cumprimento de tais deveres e preservar a *autodeterminação* do usuário, a lei ainda garante ao cadastrado os direitos de (i) obter o cancelamento do cadastro quando solicitado; (ii) acessar gratuitamente as informações sobre ele existentes no banco de dados; (iii) solicitar a impugnação de qualquer informação sobre ele erroneamente anotada; (iv) conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; (v) ser informado previamente

90 Lei 12.414/2011, artigo 3º.

91 *"A Lei 12.414/2011 veda o tratamento de informações excessivas. Se pode ser verdadeiro que, sob a ótica econômica, quanto mais informações melhor é a avaliação de crédito (more is better), para o direito, para proteção jurídica da privacidade, é fundamental restringir, tanto no tempo, como na qualidade e quantidade, as informações que circulam pelos bancos de dados de proteção ao crédito. A primeira forma de limitar a qualidade da informação que circula em arquivos de consumo é exigir que ela esteja vinculada ao propósito específico do banco de dados. Os dados coletados devem ser visivelmente úteis para os objetivos específicos do arquivo. Se não atenderem a esse pressuposto, a coleta e o tratamento da informação devem ser considerados ilegais, ilegítimos e ofensivos à privacidade (art. 5º, X, da CF). A redação do inc. I do §3º atende justamente a essa preocupação, pois consideram-se informações excessivas "aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor". Antes mesmo da edição da Lei 12.414/2011, era possível sustentar, em razão do núcleo essencial do direito à privacidade (art, 5º, X, da CF), que o tratamento de informações excessivas ou desvinculadas das finalidades específicas dos arquivos de consumo seria inconstitucional. O dispositivo comentado positiva tal entendimento. De fato, para conferir significado mínimo à inviolabilidade da privacidade, prevista tanto na Constituição Federal (art. 5º, X) como no Código Civil (art. 21), há que ser estabelecidas restrições positivas. Não se cuida de desconsiderar a possibilidade de restrição ou conformação de direito fundamental, mas do cuidado em preservar o núcleo essencial do direito. É imprescindível, no âmbito da moderna concepção de proteção de dados, limitar tanto o conteúdo como a quantidade de informação que é tratada pelas entidades de proteção ao crédito*". Cadastro Positivo: comentários à Lei 12.414/2011. São Paulo: Editora Revista dos Tribunais, 2011, pp. 93-94)

sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; e (vi) solicitar àquele que acesse informações no banco de dados a revisão de decisão realizada exclusivamente por meios automatizados.[92]

- ***Lei 12.527/2011 – Lei de Acesso a Informação***

Já a Lei de Acesso a Informação (LAI), também trouxe importantes elementos para o debate de proteção de dados pessoais no país.

A LAI modificou a presunção de sigilo sobre informações de interesse público, atribuindo a órgãos públicos a obrigação de fornecer informações independente de solicitação (transparência ativa) ou após demanda apresentada por cidadão (transparência passiva). Nesse sentido, a Legislação determina que informações produzidas ou custodiadas por órgãos públicos se submetem à obrigação de publicidade e transparência, salvo se a informação for sigilosa ou resultar em violação à intimidade, à vida privada, à honra e à imagem dos indivíduos.

Informações serão consideradas sigilosas quando imprescindíveis à segurança da sociedade ou do Estado e serão classificadas como tal pelo órgão competente mediante justificativa que deverá ser disponibilizada ao público. Da classificação decorre a indisponibilização da informação pelo máximo de 25 anos, quando se tratar de informação ultrassecreta.

Já as informações pessoais são classificadas pela LAI como aquelas relacionadas à pessoa natural identificada ou identificável e que terão acesso restrito, independente de classificação de sigilo, pelo prazo máximo de 100 anos da data de sua produção, salvo quando houver determinação legal ou consentimento expresso das partes.

Há a possibilidade de dispensa de consentimento para a disponibilização de informações pessoais quando elas se mostrarem necessárias, dentre outros, para (a) a realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei; (b) ao cumprimento de decisão judicial; (c) à defesa de direitos humanos; e (d) à proteção do interesse público e geral.

- ***Lei nº 12.965/2014 – Marco Civil da Internet (MCI)***

[92] Lei 12.414/2011, artigo 5º.

O marco mais moderno no que tange a proteção da privacidade e da proteção dos dados pessoais no Brasil atualmente está consignado na Lei nº 12.965/2014, o Marco Civil da Internet (MCI).[93] O MCI introduziu no ordenamento brasileiro um microssistema de proteção de dados pessoais na internet.

Em complemento às normas já tratadas, o MCI estabelece rol de direitos dos usuários quanto a proteção dos seus dados pessoais, garantindo, no acesso à internet, dentre outros, a tutela dos direitos à inviolabilidade da intimidade e vida privada, inviolabilidade e sigilo do fluxo de comunicações, inviolabilidade e sigilo de comunicações privadas armazenadas.

Em relação especificamente à proteção de dados pessoais, a norma garante que a coleta de dados pessoais somente pode ocorrer mediante o fornecimento ao usuário de informações claras e completas, seguidas pela obtenção de consentimento livre e expresso do titular de dados. O consentimento deve ocorrer ainda destacado das demais cláusulas contratuais.[94-95] Isso implica dizer que deve haver uma manifestação de vontade clara e específica do usuário, não bastando inferências ou manifestações implícitas, ou mesmo uma manifestação de vontade única para a relação contratual.

Para não possibilitar tratamento ilimitado de dados, o Artigo 7º, inciso VIII do MCI complementa a proteção aos usuários indicando que os dados pessoais somente poderão ser utilizados para finalidades que a) justifiquem sua coleta, b) não sejam vedadas pela legislação e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. Essa disposição complementa a indicação anterior em relação às informações claras e completas, na medida em que os dados pessoais dos usuários somente poderão ser usados se houver a previsão do seu uso na política de privacidade ou termos de uso do serviço e houver uma justificativa para referida utilização.

No que tange ao tratamento dos dados pessoais, o MCI implica responsabilidades ao controlador de dados. Este deve assegurar que os dados permaneçam confidenciais, deve documentar a lógica de tratamento de dados e fiscalizar a transferência a terceiros. O controlador deve ainda ser acionado para acesso aos dados pelo titular dos dados ou por

93 Lei 12.965/2014.

94 Lei nº 12.965/2014, artigo 7º, inciso VIII.

95 *Ibid*., artigo 7º, inciso IX.

autoridades e, em caso de violações e falhas de segurança, informar tanto o titular quanto as autoridades competentes.[96]

Além disso, quanto à prática comum de transferência de dados a terceiros, a norma estabelece restrição com o fim de somente permiti-la caso haja consentimento livre, expresso e informado do titular de dados ou nas hipóteses previstas especificamente em lei.[97]

Por fim, garante-se ao titular de dados o direito de requerer a exclusão dos dados pessoais que tenha fornecido a alguma aplicação de internet quando terminada a relação entre as partes, ressalvadas as hipóteses previstas no próprio MCI quanto aos logs de acesso.

Embora o MCI tenha estabelecido esse microssistema de proteção de dados pessoais, ele não estabelece uma definição do que seja "dados pessoais" e "tratamento de dados pessoais". Foi a partir do Decreto nº 8.771/2016 que regulamentou o MCI, que referidas definições passaram a integrar o ordenamento jurídico pátrio, como se verá abaixo.

- ***O Decreto nº 8.771/2016 – Regulamento do Marco Civil da Internet***

De imediato, o decreto introduz definição a conceitos-chave à proteção de dados pessoais, como "dado pessoal" e "tratamento de dados pessoais".

Como "dado pessoal", o Decreto nº 8.771/2016 define o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".[98] Já como "tratamento de dados pessoais", tem-se "toda operação realizada com dados pessoais", o que inclui, de forma exemplificativa, a "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".[99]

Uma crítica de fundamento jurídico feita pela doutrina ao Decreto nº 8.771/2016 é que, como instrumento regulamentador, este deveria se ater aos limites da lei da qual se deriva.

96 Centro de Tecnologia e Sociedade da Faculdade Getúlio Vargas/RJ (CTS/FGV/RJ), Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO sobre a definição de termos relativos à proteção de dados presentes no Marco Civil, disponível em http://marcocivil.cgi.br/contribution/contribuicao-do-centro-de-tecnologia-e-sociedade-da-fgv-direito-rio-sobre-a-definicao-de-termos-relativos-a-protecao-de-dados-presentes-no-marco-civil/160, acesso em 26 de janeiro de 2017.

97 Lei nº 12.965/2014, artigo 7º, inciso VII.

98 Ibid., artigo 14, I.

99 Ibid., artigo 14, II.

Esse limite decorre da própria previsão da figura do poder regulamentar na Constituição Federal, que estabelece que o Presidente da República deve expedir decretos para a fiel execução da legislação.[100] Assim, não caberia ao Decreto nº 8.771/2016 estabelecer a definição de dados pessoais ou de tratamento de dados pessoais, como mencionado acima, além das balizas para a obtenção de consentimento de titulares de dados e transferência de dados entre empresas.[101] De todo modo, é necessário ressaltar que, afora as manifestações doutrinárias de inconstitucionalidade do Decreto nº 8.771/2016 no que toca à proteção de dados pessoais, a norma continua em vigor e aplicável a todos, não tendo havido uma decisão definitiva do Poder Judiciário confirmando ou negando sua validade até o momento.

Outro ponto de controvérsia diz respeito à abordagem do decreto regulamentador sobre a definição de padrões de segurança. Por um lado, foi ventilado que a definição de padrões de segurança por meio de um decreto não seria tecnicamente adequada, já que a norma poderia engessar a indústria aos parâmetros escolhidos. Por outro, um número de organizações civis defendeu que o decreto deveria estabelecer ao menos padrões mínimos de segurança, envolvendo, por exemplo, a encriptação obrigatória de banco de dados compostos por dados pessoais.[102]

De fato, o Decreto nº 8.771/2016 optou pela última opção. A norma estabelece as diretrizes de segurança que devem ser observadas por provedores de conexão e aplicação, envolvendo (i) controle estrito dos responsáveis autorizados a acessar os bancos de dados, (ii) a criação de inventário detalhado do histórico de acessos, incluindo sistemas de autenticação dupla, (iii) o uso de soluções como encriptação, a fim de garantir a segurança dos dados.[103] Note-se que não há previsão obrigatória de uso de criptografia em si, mas apenas a sugestão de adoção de criptografia como uma das medidas de segurança possíveis.

Por fim, o Decreto define a Anatel, SENACON e o Conselho Administrativo de Defesa Econômica (CADE) como autoridades responsáveis para a fiscalização e apuração de infrações dentro de suas respectivas atribuições estabelecidas em lei. Assim, a Anatel como autoridade responsável pela fiscalização e apuração de infrações por prestadoras de

100 Constituição Federal, artigo 84, IV.

101 Grupo de Ensino e Pesquisa em Inovação (GEPI) – FGV Direito SP. Contribuição para regulamentação do Marco Civil da Internet (2015). Disponível em http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/Contribuição-GEPI-Regulamentacao-MCI1.pdf, acesso em 27 de janeiro de 2017.

102 Ibid., p; 38.

103 Decreto nº 8.771/2016, art. 13.

serviços de telecomunicações em relação ao cumprimento de obrigações do MCI e, em paralelo, a SENACON como autoridade responsável pela fiscalização do cumprimento do CDC. Já o CADE é responsável para a apuração de infrações à ordem econômica.

Tabela – Resumo Quadro Legal – Privacidade e Segurança	
Constituição Federal	
Garantias ao cidadão	– Art. 5º, X: Direito à inviolabilidade da intimidade e da vida privada; – Art. 5º, LXXII: Habeas Data; – Art. 5º, XII: Direito ao sigilo de comunicações.
Código de Defesa do Consumidor	
Regime de responsabilidade civil	– Em relações de consumo aplica-se o regime de responsabilidade objetiva ao fornecedor de serviços;
Direitos do consumidor	– Art. 4º, III: Regime da boa-fé objetiva; – Art. 6º, III: Dever de informação; – Art. 42, § 2°: Notificação por escrito em caso de criação de bancos de dados; – Art. 43, § 3°: Direito de acesso e retificação a informações armazenadas em bancos de dados; – Art. 43, § 1°: Limite de armazenamento de "informações negativas" por até 5 (cinco) anos em base de dados.
Lei Geral de Telecomunicações	
Direitos do usuário	– Art. 3º, V: Direito à inviolabilidade e ao segredo de suas comunicações, salvo restrições legais; – Art. 3º, IX: Compartilhamento de dados cadastrais por operadoras de telefonia pode ocorrer mediante decisão judicial fundamentada; – Art. 72, § 2°: Informações agregadas, que não permitam a identificação do usuário, podem ser divulgadas por expressa autorização legal;
Lei do Habeas Data	

Direitos do usuário	– Art. 2º: direito de acesso a informações relativas à pessoa do requerente, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; Art. 3º e seguintes: Ação de Habeas Data
Código Civil	
Proteção aos direitos da personalidade	– Arts. 11 a 21. Rol ilustrativo: proteção ao direito à integridade psicofísica, ao nome e ao pseudônimo, à imagem e à inviolabilidade da vida privada à pessoa natural.
Lei do Cadastro Positivo	
Direitos do consumidor	– Art. 3º, § 3º: Proibição de anotação de informações excessivas ou sensíveis; – Art. 4º: Necessidade de autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada; – Art. 5º e 6º: Dever de informação e transparência com o cadastrado; – Art. 7º: Restrição a utilização das informações constantes dos bancos de dados positivos, as quais somente pode servir para análise de risco de crédito ou para subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.
Lei de Acesso a Informação	
Direitos do indivíduo referenciado	– Art. 31: Dever de tratar informações pessoais de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. – Art. 31, § 1º, I: restrição de acesso pelo prazo máximo de 100 anos.

	– Art. 31, § 2º: Responsabilização pelo uso indevido de informações pessoais.
Marco Civil da Internet	
Direitos do usuário	– Art. 3º: Proteção da privacidade e dos dados pessoais, dentre outros, como princípios do uso da internet no Brasil; – Art. 7º, I e II: Garantia à inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de comunicações pela internet (salvo por ordem judicial).
Proteção de dados pessoais	– Art. 7º, VIII a X: Estabelece princípios na proteção de dados pessoais. o O fornecimento de dados pessoais e registros de conexão e de acesso a aplicações de internet a terceiros deverá ser precedido da obtenção de consentimento; o Obrigação de prestar informações claras; o A coleta deverá observar a obtenção de consentimento expresso, livre, informado e destacado; o Obrigação de exclusão de dados pessoais, caso requerido pelo titular de dados.
Obrigação de retenção de dados de conexão e de acesso a aplicações	– Art. 10 a 17: Obrigações na guarda de registros e dados pessoais. o A guarda e disponibilização de registro de conexão e de acesso a aplicações deve atender à preservação da intimidade, vida privada, honra e imagem; o Armazenamento de registros de acesso por aplicações de internet pelo período de 6 (seis) meses; o Armazenamento de registro de provisão de conexão de conexão à internet pelo período de 1 (um) ano; o Para acesso aos dados de registro, o interessado deverá obter autorização judicial prévia. o Dados cadastrais que informem qualificação pessoal, filiação e endereço podem ser acessados por

	autoridade administrativa com competência legal para a requisição.
Decreto nº 8.771/2016	
Proteção de dados pessoais	– Art. 14: Definição de "dados pessoais" e "tratamento de dados pessoais"; – Art. 13: Obrigação de exclusão de dados tão logo atingida a finalidade ou se encerrado o prazo determinado por obrigação legal.
Segurança	– Art. 13: Diretrizes de segurança a provedores de conexão e aplicações: (i) mecanismos para autenticação de acesso aos registros; (ii) criação de inventário de histórico de acesso; (iii) sugestão de adoção de criptografia ou meio equivalente para segurança dos dados.

Esse conjunto de normas, é definido pelo seu caráter setorial (ex. relações consumeristas; prestação de serviços de telecomunicação; utilização da internet), sendo aplicado cada qual em contextos específicos. Desse modo, o primeiro grande desafio para um cenário de desenvolvimento do ecossistema de IoT, está na adequação desse quadro legal para lidar com as novas perspectivas e desafios trazidos por esse novo mundo de dados.[104]

3.3.2. Insegurança jurídica na proteção de dados pessoais

A fragmentação relatada acima acaba por gerar uma insegurança jurídica em decorrência das interpretações distintas aplicáveis a proteção de dados pessoais atualmente no país.

Esses conflitos interpretativos podem gerar questionamentos no ambiente de IoT, não apenas diante dos modelos de negócio e soluções inovadoras, que poderão não ser compreendidos adequadamente pelas autoridades e pelo judiciário, quanto pelos riscos de práticas abusivas quanto aos dados pessoais de usuários.

[104] Faz-se referência aqui a expressão cunhada e utilizada pelo Grupo de Ensino e Pesquisa em Inovação da FGV Direito SP. Disponível em: http://direitosp.fgv.br/grupos/pesquisa-inovacao-gepi

Tais conflitos podem surgir especialmente nas relações de consumo e em aplicações que envolvam a utilização da Internet, diante da aplicação do Código de Defesa do Consumidor e do Marco Civil da Internet.

3.3.3. A importância da aprovação de uma lei geral de proteção de dados pessoais

Em decorrência desse cenário de fragmentação normativa e insegurança jurídica, a maior parte da sociedade, academia, setor público e privado, considera como a melhor solução a aprovação de uma lei geral de proteção de dados pessoais, que passaria a reger de maneira uniforme e coerente o ambiente legal para o tratamento de dados pessoais, bem como prever as situações em que a legislação não se aplicaria (ex. anonimização de dados pessoais). Em nossa análise, esse seria o cenário mais adequado lidar com as questões de proteção de dados pessoais no ambiente de IoT.

Nesse sentido, já tramitam no Congresso Nacional três projetos de lei com o fim de regular especificamente a proteção de dados pessoais: no Senado, o projeto de lei nº 330/2013, além de dois projetos que tramitam em conjunto na Câmara de Deputados, quais sejam o PL 4060/2012 e o PL 5276/2016, apensado ao anterior, derivado do anteprojeto de lei sobre proteção de dados pessoais elaborado pelo Ministério da Justiça.

Em nossa análise, alguns pontos importantes que precisarão ser abarcados na futura legislação, de modo a assegurar o desenvolvimento adequado do ecossistema de IoT, sem colocar em risco os direitos individuais, são:

- Definição clara sobre o que são "dados pessoais" e "dados pessoais sensíveis", estabelecendo os requisitos para os respectivos tratamentos;
- Definição de regras tanto para o setor privado quanto para o setor público;
- Estabelecimento de limites para a coleta e tratamento de dados pessoais;
- Definição acerca do regime para o tratamento de dados pessoais de crianças e adolescentes;
- Estabelecimento de direitos claros para os indivíduos cujos dados pessoais estejam sendo tratados;
- Incorporação do conceito de anonimização;
- Definição da responsabilidade dos atores na cadeia de tratamento de dados pessoais;

- Estabelecimento de um regime claro acerca das possibilidades de transferência internacional de dados pessoais, que incorpore mecanismos modernos de regulação; e
- Criação ou desginação de uma autoridade de proteção de dados pessoais.

3.4. Segurança da informação

A temática de segurança informação assume um caráter primordial no ambiente de IoT, com o desafio de estruturar o país para lidar com o tema de forma satisfatória. O tema foi enfatizado ao longo dos fóruns do Estudo de Internet das Coisas e da Consulta Pública realizada, com consenso dentre os particiantes acerca de necessidade de explorar articulações e estratégias amplas de governança público e privada para o tema.

Especificamente no que tange ao diagnóstico regulatório sobre o tema, percebe-se que não há modelo estruturado no Brasil. Pelo contrário, percebe-se um váculo na atribuição de lideranças e um desafio na coordenação entre diversas esferas do Poder Público, iniciativa privada, academia e sociedade civil.

Um dos grandes dilemas identificados é como lidar com os crescentes riscos sistêmicos trazidos por IoT, como os riscos decorrentes de falhas na implementação de protocolos de segurança (e.g. dispositivos mantidos com senhas padrões ou até mesmo sem a possibilidade de alteraração de senha) e os riscos derivados de vulnerabilidades. Esses desafios se tornam ainda mais latentes diante da utilização de aplicações IoT em infraestruturas críticas, vide o potencial lesivo de ataques em redes de prestação de água e energia, por exemplo.

Por ora, no que tange ao setor privado, não há um consenso em como abarcar os riscos e vulnerabilidades que se apresentam. Há, entretanto, prevalência pela organização da iniciativa privada em modelo de auto ou co-regulação, com incentivo à criação de melhores práticas e adoção de padrões "*security by design*" e "*security by default*".

No âmbito da Administração Pública Federal ("APF"), o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) tem atuado fortemente na gestão da segurança da informação, em especial por meio da edição das Normas Complementares (NC) à Instrução Normativa nº 01 GSI/PR/2008, utilizadas como parâmetro por órgãos e entidades da APF.[105]

[105] Disponíveis em: http://dsic.planalto.gov.br/legislacaodsic/53

Além disso, entre fevereiro e maio de 2017, o MCTIC instituiu Grupo de Trabalho Interministerial para a elaboração de política nacional sobre o ambiente digital, a Estratégia Brasileira para a Transformação Digital, a ser publicada ainda em 2017. No que toca à segurança da informação, a política deve analisar as possibilidades de modelos regulatórios, com a hipótese de criação de agência específica. O documento deverá lidar, ainda, com a importância do estabelecimento de mecanismos de cooperação nacional e internacional, o fomento a programas de educação e conscientização sobre segurança da informação, a elaboração de planos para a prevenção e resposta a incidentes e a elaboração de estratégias para fomentar o compartilhamento de informações pela iniciativa privada.

O debate sobre segurança da informação será aprofundado na Fase III do Estudo, acrescentando perspectivas e abordagens específicas dos ambientes priorizados, em especial sobre as alternativas possíveis para cooperação internacional, arranjo instituicional, modelos de certificação de dispositivos e segurança em infra-estruturas críticas.

3.5. Questões tributárias

O Sistema Tributário Nacional, como a seguir será demonstrado, possui desafios no que tange ao fomento de novas tecnologias, incluindo-se nesse contexto o desenvolvimento da IoT precipuamente, por haver sobreposição de atividades, que envolvem desde a importação de componentes, venda interna de dispositivos, utilização de serviços de telecomunicação,[106] realização de SVA[107] e serviços de outra natureza (licenciamentos[108] e desenvolvimento de *software*).

Diante da natureza híbrida da IoT, muitas questões podem surgir, sobretudo porque (i) há um acúmulo de tributos sobre consumo que geram cargas fiscais efetivas bastante elevadas, sofrendo a incidência múltipla de tributos sobre consumo,[109] os quais, inclusive, incidem de maneira cumulativa; (ii) há inúmeras incertezas quanto à competência para tributar determinados serviços, diante da falta de clareza do que seja serviços de comunicação (sujeito ao Imposto sobre Operações relativas à Circulação de Mercadorias e

106 LGT, art. 60.

107 LGT, art. 61.

108 Não é objeto desse estudo a discussão sobre a constitucionalidade do ISS sobre licenciamento de softwares. De fato, a matéria está sob julgamento do E. Superior Tribunal Federal, no âmbito do Recurso Extraordinário nº 688.223.

109 As atividades de IoT sofrem a incidência múltipla de tributos sobre consumo, e.g., do Imposto de Importação ("II"), Imposto sobre Produtos Industrializados ("IPI"), ICMS, Contribuição ao Programa de Integração Social ("PIS"), Contribuição para o Financiamento da Seguridade Social ("Cofins") e ISS, bem como de taxas e contribuições setoriais (contribuição ao FUST, contribuição ao FUNTTEL e taxa ao FISTEL).

Prestação de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação – "ICMS", imposto estadual) e do que estaria fora desse conceito (sujeito ao "Imposto Sobre Serviços de Qualquer Natureza" – ISS, imposto municipal); e (iii) há complexidade para aprovar qualquer mudança no sistema, de forma que o atual sistema tributário ainda encontra-se sob os contornos dados pela Constituição Federal de 1988 e ancorado em um Código Tributário Nacional de 1966.

Some-se a isso a necessidade de cumprir extensa lista de obrigações acessórias exigidas pela União, pelos 27 Estados e mais de 5,5 mil Municípios, o que consome elevado tempo e recurso dos contribuintes. Segundo o Estudo *Doing Business* do Banco Mundial (2017)[110] são necessárias 2.038[111] horas por ano para uma empresa pagar tributos e cumprir com obrigações acessórias. O Brasil figura na posição 181 de um ranking de 190 países, ficando abaixo de países como México, Colômbia e o restante de América Latina.

Toda essa situação torna o desenvolvimento da IoT pouco atrativo no Brasil. Por esse motivo, é necessário simplificar o sistema tributário, por meio do desenvolvimento de política fiscal que minimize os problemas acima elencados, além de introduzir incentivos fiscais, similares ao M2M indicado acima, que sejam capazes de fomentar o desenvolvimento tecnológico.

a. Características do ambiente IoT que afetam a tributação

As inovações tecnológicas deram origem à chamada economia digital,[112] que afeta as relações de comercialização de bens e prestação de serviços, por meio de novos modelos de negócios. Essas alterações promovidas pelas tecnologias digitais afetam diretamente o sistema tributário nacional e internacional, na medida em que rompem com os conceitos de bens e serviços tradicionalmente conhecidos. A IoT, nesse contexto, vem potencializar muitas questões já enfrentadas com o desenvolvimento tecnológico, bem como apresentar novos questionamentos, evidenciando a fragilidade do sistema tributário atualmente vigente. Os aspectos mais relevantes sob a perspectiva fiscal estão relacionados à mobilidade dos serviços prestados; ao intenso uso de sensores conectados a dispositivos,

110 Disponível em http://www.doingbusiness.org/~/media/wbg/doingbusiness/documents/profiles/country/bra.pdf. Acesso em: 16.03.2017.

111 A média de países da OCDE é de 163,4 horas. O Brasil figura em último lugar.

112 Conforme OECD (2015), *Adressing the Tax Challenges of Digital Economy, Action 1 -2015*. Final Report OECD/G20, Base Erosion and Profit Shifting Project, OECD Publishing, Paris. Disponível em: http://dx.doi.org/10.1787/9789264241046-en. Acesso em: 16.03.2017.

na medida em que gera expressiva transmissão de dados; à volatilidade e inovação; e, ainda, à diversidade de modelo de negócios; porque interferem diretamente nos parâmetros tradicionalmente utilizados para qualificação das atividades e eleição de sujeitos passivos.

b. Impacto da IoT no imposto sobre a renda

O ambiente de IoT é inconsistente com conceitos utilizados para fixação de competência tributária, de residência, estabelecimento permanente ou fonte, tanto como na legislação interna brasileira como nos Tratados celebrados segundo à Convenção Modelo da OCDE. Isso porque todos eles exigem algum tipo de presença física dos contribuintes e beneficiários, seja por meio de uma instalação ou de um representante. Essa característica de presença física, muitas vezes, pode não ser consistente com a IoT.[113]

Além disso, o sistema de IoT exige uma análise aprofundada de como deve ser tributada a riqueza produzida pelos dados e informações coletadas. Umas das características mais relevantes da IoT, conforme já destacado, é a expressiva habilidade de coletar, processar e compartilhar dados por meio de um sistema conectado a múltiplos dispositivos, sensores e componentes de nuvens.

Nesse sentido, os dados coletados no ambiente de IoT são essenciais na economia digital e sua valoração é uma tarefa complexa, já que tais dados podem ser obtidos diretamente de usuários (por meio de registros) ou a partir da análise de observações (registros de acessos, localização e data) e sua destinação pode ser variável, i.e., eles podem ser vendidos diretamente a terceiros ou ser empregados na expansão de novos produtos e serviços. E, ainda assim, qual seria o impacto desses dados nas regras de preço de transferência e atribuição de lucros do estabelecimento permanente? Por todas essas razões, valorar esses dados não é algo simples.

Ainda nesse contexto, o ambiente de IoT gera novos modelos de negócios, que podem envolver simultaneamente prestação de serviços de telecomunicação, entrega de produtos e serviços de outras naturezas. Há, dessa maneira, várias formas simultâneas de monetização, que podem impactar a tributação da renda, tais como receitas de propaganda, de aquisição ou locação de conteúdo digital, como aplicativos, venda de

113 Conforme OECD (2015), *Adressing the Tax Challenges of Digital Economy*, *Action 1 -2015*. Final Report OECD/G20, Base Erosion and Profit Shifting Project, OECD Publishing, Paris. Disponível em: http://dx.doi.org/10.1787/9789264241046-en; p. 100-101. Acesso em: 16.03.2017.

conteúdo, de associação, de venda de produtos e serviços, licenciamento de *software*, venda a dados.

Em razão dessa variedade de possibilidades, levantam-se questionamentos sobre como caracterizar essas operações e os rendimentos produzidos por elas para fins de aplicação da legislação interna e dos Tratados. Sob o aspecto fiscal, no âmbito nacional e internacional, a tributação da renda pode variar de acordo com a natureza do rendimento, e.g., os pagamentos a beneficiários no exterior sujeitam-se ao imposto na fonte à alíquota de 15% a 25%; de outro lado, alíquota de 15% para remessas em geral e de 25% no caso de serviços em geral; para *Royalties* e serviços técnicos, por outro lado, sujeitam-se à alíquota de 15% e Contribuição de intervenção no domínio econômico ("Cide") de 10%. Em decorrência disso torna-se difícil caracterizar essas operações e, consequentemente, os rendimentos produzidos para fins de tributação pelo imposto sobre a renda.

c. Impacto da IoT sobre impostos sobre consumo

Em relação ao imposto sobre consumo, é importante apontar que as atividades de IoT são desenvolvidas por meio do sistema que envolve (i) fornecimento de mercadoria (dispositivo); que se (ii) conectará a internet, por meio de redes de telecomunicações; para (iii) transmissão de dados e informações monitoradas por referidos dispositivos.

Essa amplitude de atividades envolvidas no sistema de IoT dificulta a identificação da atividade fim e, consequente, o tratamento tributário aplicável, i.e., serviço de telecomunicação sujeito ao ICMS ou SVA, sobre o qual pode incidir o ISS. Nesse contexto, o sistema de IoT pode agravar ainda mais o conflito de competência existente entre Estados e Municípios, na medida em que as atividades relacionadas à IoT apresentam relações mais complexas do que as atualmente enfrentadas. A depender da forma como as atividades de IoT serão desenvolvidas, pode-se dizer que os serviços de comunicação poderão ser utilizados apenas como meio para a realização de outras utilidades, ao passo que se for oferecida conectividade aos usuários pode-se entender que há prestação de serviço de comunicação e, por consequência, haverá incidência do ICMS.

Além disso, há problemas relativos à identificação da origem e destino da atividade desenvolvida, critérios importantes para fixação da competência tributária do ISS e ICMS. Imagine-se uma hipótese em que, um adquirente, pessoa física, possa ter acesso a serviços de dados a partir de qualquer localidade, de forma que não se pode precisar um destino pré-determinado, para qual ente da Federação deverá ser recolhido o imposto? Atualmente, considerado os liames do sistema tributário brasileiro, não se poderia afirmar

de forma precisa, para qual Estado o imposto deve ser recolhido. Insurgiria, também, dúvida quanto à importação desse tipo de serviço a partir de empresa estrangeira em abstrato, diretamente por pessoa física na qualidade de consumidor final, para fins de se definir se há fato gerador do imposto ou não, e, no caso de ser configurado, de quem seria a responsabilidade do imposto e para que Estado deveria ser recolhido.

E não é só. O mesmo tipo de problemática surge no bojo das operações de prestação de serviços que, a depender da sua natureza, ficam sujeitas à incidência do ISS. Portanto, dada as condições abstratas que os serviços de IoT por sua natureza exteriorizam, não será surpresa se o assunto desencadear discussões sobre a competência e local para fins de incidência e recolhimento do imposto.

d. Exemplo de tipos de conflitos

A título ilustrativo das questões apontadas anteriormente, veja-se uma empresa que oferece monitoramento de veículo em tempo real. Esse serviço permite que os operadores obtenham diversas informações sobre os veículos da frota, tais como localização, velocidade, funcionamento dos motores, se a mercadoria se encontra devidamente resfriada etc.. Além disso, disponibiliza ajuste automático da temperatura da câmara e bloqueio de velocidade.

No exemplo, para a atividade ser desenvolvida, é preciso utilizar um serviço de telecomunicação, a princípio, prestado por uma operadora e um serviço de valor adicionado que permite coletar os dados dos veículos. Os dados são processados sendo possível emitir comandos para controlar as condições do veículo.

Para desenvolvimento dessas facilidades, confira-se, não é preciso que o prestador esteja localizado no Brasil. O serviço pode ser fornecido no território nacional, ao passo que os servidores podem estar localizados no exterior, não se enquadrando no conceito de residência para fins tributários. Por outro lado, poder-se-ia admitir que os chips instalados nos veículos sejam compreendidos como estabelecimento permanente? Da mesma forma, é complexo identificar a localização do usuário e da prestação de serviço, uma vez que o rastreamento pode ser remoto e o veículo está em constante deslocamento. Nessa hipótese, qual Estado ou Município teria competência para tributar essa atividade?

Na verdade, qual seria a natureza desse serviço, já que a princípio seria um SVA, mas no momento em que disponibiliza comunicação via rede de telecomunicações presta efetivamente um serviço de comunicação. O que prepondera nesse caso? Quem está

consumindo os dados coletados? E, por fim, como estão sendo explorados economicamente?

Percebe-se, com base no que foi até o momento exposto, que o ambiente de IoT poderá sim ser impactado por conflitos e debates já existentes no âmbito da tributação nacional. Além disso, não deve ser ignorado que o setor de serviços propiciados pela IoT é muito recente no nosso país, o que poderá desencadear o surgimento de outras questões tributárias relevantes para o seu desenvolvimento.

3.6. Benefícios fiscais

No âmbito de facilitação do desenvolvimento de IoT importante mencionar que já há alguns benefícios fiscais atualmente vigentes que poderiam, em tese, fomentar a indústria voltada ao IoT.

É importante, todavia, esclarecer que os benefícios aqui mencionados são potenciais, porquanto algumas questões, as quais não foram definidas, podem influir na fruição desses benefícios, tais como (a.) a forma de comercialização no mercado dos produtos no ambiente de IoT; (b.) a necessidade de importação de peças e componentes, as quais podem ou não ter similares no Brasil; (c.) a produção dos produtos inteiramente no exterior ou em território nacional etc.

Essas informações são de suma importância para a definição da utilização dos benefícios atualmente vigentes e sua ausência afeta a possibilidade de confirmação se poderão ser efetivamente aplicáveis às empresas que explorarão o ambiente de IoT no Brasil. Confira-se abaixo cada um dos referidos benefícios fiscais vigentes.

a. Lucro da Exploração.

O Lucro da Exploração, benefício instituído pela Medida Provisória n.º 2.199-14, de 24.08.2001, prevê a redução de 75% no imposto sobre a renda e adicionais calculados com base no lucro da exploração[114], das pessoas jurídicas que tenham projeto aprovado até 31.12.2018 para instalação, ampliação, modernização ou diversificação enquadrado em determinados setores da economia considerados, prioritários para o desenvolvimento

114 O lucro da exploração está definido no artigo 544 do Decreto n.º 3.000, de 26.03.1999.

regional, nas áreas de atuação da Superintendência de Desenvolvimento do Nordeste ("SUDENE") e da Superintendência de Desenvolvimento da Amazônia ("SUDAM").[115]

Os empreendimentos prioritários acima referidos foram estabelecidos por meio dos Decretos n.ºs 4.212, de 26.04.2002, e 4.123, de 26.04.2002, respectivamente. No ambiente de IoT, aqueles, em tese, aplicáveis seriam os voltados para a indústria de transformação nos seguintes grupos: (a.) eletroeletrônica; (b.) mecatrônica; (c.) informática; e (d.) indústria de componentes (microeletrônica).

Note-se, contudo, que para utilização do benefício é necessário que a pessoa jurídica tenha projeto protocolizado e aprovado até 31.12.2018, podendo ser fruído, dessa forma, por dez anos, a partir do ano-calendário subsequente ao início da operação. Vale mencionar, que o início da operação deve ser atestado por laudo emitido pelo Ministério de Integração Nacional.

Além da redução anteriormente mencionada, a Medida Provisória n.º 2.199-14/2001 trouxe também a isenção do imposto sobre a renda e de seu adicional, calculados com base no lucro da exploração para pessoas jurídicas que fabricarem máquinas, equipamentos, instrumentos e dispositivos, baseados em tecnologia digital, voltados para o programa de inclusão digital.

b. Pesquisa e Desenvolvimento em Inovação Tecnológica.

As pessoas jurídicas que investirem em pesquisa e desenvolvimento de inovação tecnológica, podem aproveitar os benefícios previstos no âmbito da Lei n.º 11.196, de 21.11.2005 (a "Lei do Bem"). Veja-se, contudo, que os benefícios previstos na Lei do Bem somente podem ser usufruídos caso a inovação resulte em novo produto ou processo de fabricação, bem como a agregação de novas funcionalidades ou características ao produto ou processo que implique melhorias incrementais e efetivo ganho de qualidade ou produtividade, resultando maior competitividade no mercado.

Em síntese, os benefícios fiscais aplicáveis neste caso implicam em redução no IRPJ, IRRF, CSLL, IPI, da seguinte forma: (a.) possibilidade de dedução nas bases de cálculo do IRPJ e da CSLL, de valor 60% a 80% dos dispêndios realizados com pesquisa e no desenvolvimento de inovação tecnológica; (b.) redução de 50% do IPI incidente sobre máquinas, equipamentos, aparelhos e instrumentos destinados ao desenvolvimento

[115] As regiões da SUDENE estão estabelecidas na Lei Complementar n.º 125, de 03.01.2007. De outro lado, as regiões da SUDAM, foram estabelecidas por meio da Lei Complementar n.º 124, de 03.01.2017.

tecnológico; (c.) depreciação acelerada integral, para fins de apuração do IRPJ e da CSLL, na aquisição dos novos produtos mencionados em (b.); (d.) amortização acelerada, mediante dedução como custo ou despesa operacional, dos dispêndios relativos à aquisição de bens intangíveis classificáveis no ativo diferido; e (e.) redução a zero da alíquota do IRRF nas remessas efetuadas para o exterior destinadas ao registro e manutenção de marcas, patentes e cultivares[116].

c. Zona Franca de Manaus

A Zona Franca de Manaus é uma área de livre comércio de importação e exportação e de incentivos fiscais especiais[117], estabelecida com a finalidade de desenvolver o interior da Amazônia, sendo administrada pela Superintendência da Zona Franca de Manaus ("SUFRAMA").

Esta região[118] oferece incentivos fiscais proporcionados pelos governos federal, estadual e municipal, além de incentivos extrafiscais[119] oferecidos pela Suframa, para implantação de projetos industriais e agropecuários na sua área de abrangência. Os benefícios são destinados ao produto e não ao projeto, e a empresa fabricante só passa a usufruí-los a partir do início da produção.

Há diversos benefícios que podem ser concedidos às empresas que tenham interesse de operar via ZFM. Nesse sentido, inclusive, há incentivos genéricos que poderão ser utilizados ou adaptados às operações realizadas no âmbito do IoT.

Dentre o rol dos benefícios existentes, destacam-se a redução de até 88% do II sobre os insumos destinados à industrialização, isenção do IPI nas importações realizadas pela ZFM e revendas dos produtos industrializados na ZFM para todo território nacional, isenção da contribuição para o PIS/PASEP e da Cofins nas operações internas na ZFM, Crédito Estímulo do ICMS sobre o imposto devido na saída dos produtos (variando de

116 Sobre o assunto, em 18.04.2017, Gileno Barreto e Antonio Rocca publicaram artigo no jornal Valor Econômico: "Importante mencionar, inicialmente, que sob a ótica do incentivo fiscal a legislação brasileira é relativamente eficiente, comparativamente à de outros países. Dados do relatório R&D and Tax Incentives da OCDE, de 2013, demonstram que a Lei do Bem põe o Brasil na 9ª posição quanto ao volume de subsídios. Contudo, em um cenário de prejuízos – o que normalmente ocorre em períodos de crise – a legislação brasileira nos leva à 20ª posição, por não prever a possibilidade de diferimento do incentivo para outros exercícios (...) O Brasil não pode mais se dar ao proveito de desperdiçar o tempo. A Indústria 4.0 bate a nossa porta, a "Internet das Coisas" está avançando nos países desenvolvidos. Temos um bom modelo legal de incentivos à inovação que precisa de poucos mas significativos ajustes, que proporcionem ao setor privado a segurança jurídica necessária para que seus projetos saiam dos mais recônditos escaninhos e virem realidade"

117 Regulada pelo Decreto-Lei n.º 288, de 28.02.1967, recepcionado pela Constituição Federal de 1988. Os incentivos fiscais estão previstos até 2073, conforme Emenda Constitucional n.º 83/2014.

118 A região está dividida em 3 "sub-regiões", a saber: (i) Zona Franca de Manaus ("ZFM"), (ii) Amazônia Ocidental ("AMOC") e (iii) Áreas de Livre Comércio ("ALC").

119 Como por exemplo, pode-se mencionar vantagens locacionais, cf. consta em http://www.suframa.gov.br/zfm_incentivos.cfm.

55% a 100%), diferimento do ICMS em importações de matérias primas, entre tantos outros benefícios vigentes.

Ainda, para empresas que produzirem bens de informática de acordo com o Processo Produtivo Básico ("PPB")[120], investirem 5% de seu faturamento bruto em atividades de pesquisa e desenvolvimento na Amazônia, há benefícios específicos de isenção para II e IPI., .

d. Lei de Informática.

Assim como previsto no item (d.), supra, foi instituído benefício fiscal para empresas que desenvolverem ou produzirem bens e serviços de informática, ou que invistam em atividades de pesquisa e desenvolvimento em tecnologia, que se localizem fora da Zona Franca de Manaus.

A Lei n.º 8.248, de 23.10.1991 (a "Lei de Informática"), previu, assim, casos de redução do IPI sobre os bens de informática produzidos de acordo com o PPB, que poderão ser aplicáveis em todo o território nacional, bem assim nas regiões Centro-Oeste, SUDAM e SUDENE. As reduções do IPI, nesses casos podem variar entre 70% a 100%, na produção de, entre outros, de componentes eletrônicos, insumos de natureza eletrônica, máquinas, equipamentos e dispositivos baseados em técnica digital, com funções de coleta, tratamento, estruturação, armazenamento, comutação, transmissão, recuperação ou apresentação da informação, partes, peças e suporte físico para operação, programas para computadores, máquinas, equipamentos e dispositivos de tratamento da informação e respectiva documentação técnica associada (software).

Para a utilização desse benefício, igualmente ao mencionado na seção supra, é necessário que as empresas produtoras de referidos bens invistam, anualmente, 5% de seu faturamento bruto em atividades de pesquisa e desenvolvimento a serem realizadas na Amazônia.

Veja que os benefícios aqui tratados não poderão ser utilizados em conjunto com os previstos no item (c.) supra.

[120] O PPB é o conjunto mínimo de operações, no estabelecimento fabril, que caracteriza a efetiva industrialização de determinado produto, sendo estabelecidos pelos Ministros de Estado do Desenvolvimento, Indústria e Comércio Exterior e da Ciência e Tecnologia. O PPB aplicável à ZFM foi estabelecido pela Lei 8.371, de 30.12.1991 e é regulado pelo Decreto n.º 6.008, de 23.12.2006.

e. *Ex-tarifário*

Por fim, cumpre ainda indicar como incentivo passível de aproveitamento no desenvolvimento do ambiente de IoT o Ex-tarifário. Este consiste na redução temporária de até 2 anos da alíquota do Imposto de Importação de Bens de Capital, de Informática e de Telecomunicações, bem como de suas partes, peças e componentes, sem produção nacional equivalente, assim grafados na Tarifa Externa Comum do Mercosul (TEC).

Atualmente, a disciplina do regime é dada pela Resolução CAMEX n.º 66, de 14.08.2014. O interessado deve requerer o Ex-tarifário à Secretaria de Desenvolvimento da Produção do Ministério do Desenvolvimento, Indústria e Comércio Exterior ("MDIC"), acompanhado, entre outros, de catálogo e descritivos dos produtos. Após procedimento admistativo, se atendidos todos os requisitos, é criado um Ex-tarifário especial para os produtos na TEC sujeito a alíquotas reduzidas.

3.7. O processo de importação e desembaraço aduaneiro

Em seguida a essas questões faz-se importante analisar o processo de importação e desembaraço aduaneiro no Brasil, o qual tem grande importância no desenvolvimento e na expansão de soluções de IoT.

De fato, na importação devem ser seguidas inúmeras regras e os importadores devem ser credenciados em diferentes sistemas de controle, instituídos e gerenciados pela Receita Federal do Brasil ("RFB") e pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior ("MDIC"). Assim, quaisquer componentes e mercadorias que se pretenda importar e que sejam necessárias ao desenvolvimento do IoT dentro do país, também deverão obedecer aos referidos controles e regras.

Na prática, as questões mais comuns em um processo de importação costumam se exteriorizar na fase de parametrização, o que pode implicar em maior tempo para finalização do desembaraço das mercadorias e, consequentemente, atraso nas operações comerciais pretendidas pelos contribuintes e aumento de encargos alfandegários. Essa fase do processo de importação se inicia com análise preliminar dos documentos apresentados, podendo haver diferentes caminhos a se seguir em razão dessa primeira análise realizada pelos fiscais aduaneiros.

Os prazos para a efetivação de uma importação, então, dependem do canal de parametrização pelo qual foi submetida a DI. A legislação só disciplina prazos para os canais verde e cinza, nada dispondo sobre os canais amarelo e vermelho. No canal verde

a liberação para o desembaraço aduaneiro costuma ser imediata, já no caso do canal cinza, a duração pode ser de até 180 dias (onde, necessariamente, as mercadorias passam pelo procedimento denominado conferência aduaneira). Como a legislação é silente sobre os prazos dos canais de parametrização amarelo e vermelho, já existem decisões judicias que entendem como razoável um prazo médio de até 8 dias para que a RFB e os órgãos aduaneiros e intervenientes a ela subordinados analisem tudo que o que acham pertinente.

Como mencionado, a depender do canal de parametrização em que uma importação for enquadrada, surgirão preocupações relativas ao prazo efetivo para que ocorra o desembaraço aduaneiro e consequente liberação da mercadoria. Isto porque, se houver direcionamento do processo de importação para um dos canais de parametrização que se exija análise mais minuciosa, possivelmente será aberto um procedimento administrativo paralelo, pelo qual as autoridades fiscais apurarão tudo o que entenderem necessário para certificar a regularidade da importação e, só a partir de sua conclusão, permitir o regular processamento da operação.

Do ponto de vista fiscal, são exemplos clássicos de problemas vivenciados em canais de parametrização: (i) casos em que as autoridades fiscais possuem dúvida quanto à classificação fiscal ("NCM") adotada para a mercadoria objeto de importação, fato que pode, inclusive, refletir na tributação da operação. Em muitos desses casos há instauração de um processo específico para verificação das características e natureza do bem importado, com pedido de perícia e o que mais for necessário para assegurar se a NCM utilizada é a mais adequada ou não; (ii) casos em que as autoridades fiscais possuem dúvida sobre a origem e o fluxo que ensejou a importação da mercadoria ou, ainda, sobre os preços praticados nas operações (i.e., hipóteses de triangulação e interposição fraudulenta de pessoas estabelecidas em outros países, não observância de regras de transfer pricing em operações praticadas entre coligadas, fraudes em caráter antidumping afetando a competitividade nacional, etc.).

Como mencionado, há uma série de regras e controles a serem observados no âmbito das operações de COMEX, que envolvem além dos contribuintes importadores, outros tantos intervenientes necessários para que o fluxo de um processo de importação se concretize (transportador, agências reguladoras, logística portuária, despachantes, RFB, SECEX, etc.).

Nesse contexto, vale mencionar que, o Brasil aderiu recentemente ao Acordo de Facilitação de Comércio da OMC, o qual visa, entre outros objetivos, principalmente, reduzir os impactos burocráticos sobre importações e exportações, reduzir o tempo de transporte e desembaraço, custos, etc.

Mesmo antes da adesão, o Brasil já se preparava para essa nova realidade, de forma que foi criado o Portal único de Comércio Exterior, que possui como pilares a integração dos intervenientes, o redesenho dos processos e investimento em tecnologia da informação. Em linha com o referido acordo, esse portal visa harmonizar todas as normas e processos relativos no âmbito do COMEX de forma gradativa.

Ainda, como medida de desburocratização das operações de COMEX, em 2015 foi criado o Programa Brasileiro de Operador Econômico Autorizado ("OEA"), o qual de acordo com RFB, visa conceder diversos tipos de certificações às empresas interessadas. A depender do nível da certificação concedida, os interessados farão jus a uma série de benefícios no fluxo de importação, como por exemplo, percentual reduzido de canais de seleção na importação e na exportação, registro antecipado de DI no modal marítimo, resposta à consulta de classificação fiscal em até 40 dias, participação em seminários e treinamentos, entre outros tantos benefícios.

3.8. Padronização e entidades normalizadoras

O ponto de partida ao abordar a discussão sobre padronização é o debate acerca da interoperabilidade dentro do ecossistema de IoT. Entretanto esse debate sofre da ausência de contornos claros a respeito que se entende por interoperabilidade.

Pode-se falar em interoperabilidade em IoT em relação a aspectos diversos, como: interoperabilidade na camada de rede; na troca de dados entre um e outro dispositivo; no uso de um terceiro aplicativo que facilita a interoperação, por meio de interfaces de programação de aplicações; por conexão híbrida, envolvendo tanto a troca direta de dados entre aplicativos e uso de terceiro aplicativo.

Desse modo, por se tratar de uma grande quantidade de tópicos técnicos distintos e ainda em desenvolvimento no cenário de IoT, uma das grandes preocupações do mercado é evitar a definição prematura de padrões, deixando as tecnologias se desenvolverem e o mercado definir os vencedores. Essa tem sido a política desenvolvida no âmbito de IoT, possibilitando o desenvolvimento adequado de todo o ecossistema de IoT.

Com a maturação do ecossistema de IoT, a atuação das entidades normalizadoras terá um papel importante, e o país já conta com um sistema robusto e que está acompanhando os desenvolvimentos em IoT. No Brasil, o Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (SINMETRO), instituído pela Lei nº 5.966/1973, é a autoridade

responsável por padronização no âmbito nacional.[121] Dentro dos braços do SINMETRO, merecem destaque os setores normativo, exercido pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO), e executivo, pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO).

Destes, em primeiro lugar, o CONMETRO é responsável por formular políticas públicas na área de normalização. As reuniões do órgão normativo possibilitam que o governo, institutos de tecnologia e a indústria possam debater a formação de consenso nas áreas de metrologia, normalização e certificação de qualidade. É o CONMETRO, por exemplo, que irá delimitar as diretrizes da estratégia brasileira de normalização para o período de 2015 a 2020, ainda em discussão.[122]

Já o INMETRO é responsável pela atuação como órgão acreditador de organismos de avaliação de conformidade e pelo exercício de poder de polícia. Especificamente no âmbito de IoT, há previsão específica no regulamento interno do órgão para o desenvolvimento de internet das coisas. Isso porque o regimento estabelece como competência do Laboratório de informática do INMETRO desenvolver programas de avaliação de software em IoT.[123]

Ainda neste contexto, a ABNT atua como o Fórum Nacional para Normalização. Trata-se de organização privada, mantida por capital público e privado, encarregada no âmbito do SINMETRO da criação de padrões e mesmo da implementação no Brasil de padrões criados no exterior.[124] Internamente, a ABNT conta com um número de entidades técnicas setoriais, responsáveis por discutir a necessidade e o escopo da padronização. Respeitando o procedimento interno da ABNT, a adoção de um padrão deve passar não apenas por discussões internas, mas por um procedimento de consulta pública, online.[125]

A política interna da ABNT é de utilização de padrões internacionais sempre que possível, mesmo em relação aos padrões determinados como obrigatórios pelo CONMETRO.[126] Há

121 Lei nº 5.966, de 11 de dezembro de 1973, disponível em http://www.planalto.gov.br/ccivil_03/leis/L5966.htm, acesso em 18 de janeiro de 2017.

122 BRUM, Fábio. Inmetro participa da 68ª reunião do Conmetro em Brasília. Disponível em https://www.linkedin.com/pulse/inmetro-participa-da-68%C2%AA-reuni%C3%A3o-do-conmetro-em-bras%C3%ADlia-fabio-brum.

123 Portaria nº 2 de 4 de janeiro de 2017 do Ministério do Desenvolvimento, Indústria e Comércio Exterior (Regimento Interno do INMETRO), art. 84, disponível em https://www.diariodasleis.com.br/legislacao/federal/exibe_artigo.php?ifl=235081.

124 BORGES BARBOSA, Denis. Intellectual Property and Standards in Brazil, disponível em http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_072297.pdf.

125 As consultas públicas são disponibilizadas ao público pelo endereço http://www.abntonline.com.br/consultanacional/.

126 Ibid., p. 5.

interface com organizações normalizadoras no exterior, como a Associação de Normalização do Mercosul e as organizações internas dos países membros do grupo regional. Ainda, essa referência diz respeito a entidades como o Organismo Internacional de Normalização (ISO), o Instituto de Padrões de Telecomunicações Europeu (ETSI) e o Instituto Nacional Americano de Padrões (ANSI), responsáveis pela implementação de padrões como os definidos pela 3GPP ou OneM2M – alianças criadas por membros da indústria para a definição de padrões em telecomunicações.

3.9. Desafios regulatórios para o desenvolvimento de IoT

Em resumo, para o adequado desenvolvimento do ecossistema de IoT no Brasil, pode-se identificar no diagnóstico do quadro regulatório geral alguns desafios chave. Separamos os desafios nas seguintes categorias (i) Telecomunicações, (ii) Privacidade e Proteção de dados pessoais, (iii) Segurança, (iv) Tributação, (v) Benefícios fiscais, (vi) Importação e Desembaraço Aduaneiro e (vii) Padronização e entidades normalizadoras:

- Telecomunicações:
    - Como viabilizar o **investimento na expansão da internet** e garantir que a demanda das aplicações de IoT sejam **suportadas pela rede?**
    - Qual o **conceito de IoT/M2M mais** adequado para fomentar o desenvolvimento do mercado?
    - Como tratar a **insegurança jurídica** trazida pelo fato de **soluções de IoT com conectividade embarcada** poderem ser enquadradas como **revenda ou prestação irregular** de serviços de telecomunicação?
    - Há interesse em possibilitar, do ponto de vista regulatório, soluções **de IoT com *embedded* SIM Cards?** Se sim, como?
    - Os **requisitos mínimos de qualidade do serviço** de conectividade, atualmente previstos na regulação do setor, podem impactar o **custo e a viabilidade** das aplicações de IoT? Como endereçar essa questão?
    - Como reformar o processo de certificação e homologação para que seja mais **rápido e eficiente**, sem, no entanto, perder a tecnicidade necessária? Há interesse em possibilitar a **validação da certificação obtida em outros países?**
    - A **regulamentação** e os **testes de certificação** estão adaptados paras novas tecnologias de conectividade?
- Privacidade e Proteção de dados pessoais:

- **Como estruturar uma regulação de proteção de dados pessoais que traga segurança jurídica** tanto para empresas quanto para usuários?
- **Deve haver um órgão específico competente** para fiscalizar e regulamentar a proteção de dados pessoais no país?
- Deve-se prever a possibilidade de **utilização de dados anônimos ou anonimizados? Quais procedimentos devem ser adotados ou aceitos para anonimizar dados pessoais?**
- Quais procedimentos devem ser adotados em **casos de ataques ou vazamentos de dados?**
- Como controlar o **fluxo de dados pessoais em um mundo de Big Data e de criação constante de perfis comportamentais e decisões automatizadas?**
- **Quais as proteções ao uso indiscriminado de dados pessoais pelo Estado?**

- Segurança:
  - Como estabelecer **parâmetros de segurança** que, ao mesmo tempo em que **protejam os usuários**, **não onerem o desenvolvimento de aplicações IoT?**
  - **Há interesse em ceder espaço para a autorregulação? Seria a melhor abordagem?**
  - Como lidar com **riscos sistêmicos de ataques DDoS e de vulnerabilidades em massa em dispositivos IoT?**
- Tributação:
  - Como adequar um modelo tributário que foi desenhado para uma **realidade não digital**?
  - Em que medida o atual sistema tributária inviabiliza o pleno desenvolvimento de IoT? Há interesse em conceder **incentivos específicos para esse setor**?
  - Como endereçar o conflito entre a incidência de **ISS e ICMS**?
  - A **desoneração** atualmente concedida para dispositivos M2M é **suficiente para efetivamente incentivar** soluções IoT/M2M?
- Benefícios fiscais:
  - As **atuais legislações que concedem benefícios fiscais** são eficazes e/ou suficientes para o desenvolvimento do mercado de IoT?

- Importação e desembaraço aduaneiro:
    - A Política e Regulação aduaneira de **importação** interferem de forma relevante/negativa no desenvolvimento de IoT?
- Padronização e entidades normalizadoras:
    - É possível ou desejável estabelecer obrigações regulatórias nesse **momento inicial de desenvolvimento** das tecnologias?