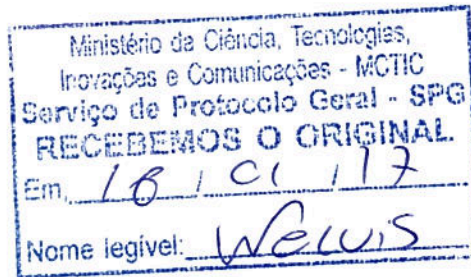




CT/Oi/GEIR/151/2017



Ao

Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC

A/C Secretário de Políticas de Informática - **Sr. Maximiliano Salvadori Martinhão**

Assunto: Contribuição à Consulta Pública sobre o Plano Nacional de IoT

Referência: Plano Nacional de IoT – CP disponível em Participa.br

Data: 16.01.2017

CÓPIA

Telemar Norte Leste S.A., Oi S.A. e OI MÓVEL S.A., doravante apenas “Oi”, vêm apresentar sua contribuição à Consulta Pública acerca do Plano Nacional de IoT, disponível pra contribuições no site Participa.br até o dia 16/01/2017 (documento anexo).

Sendo o que havia para o momento, a Oi se colocar à disposição para esclarecimentos necessários.

Atenciosamente,


Elisângela da Silva

Gerência de Competição Contencioso Administrativo


Weimar Toledo
Gerência de Universalização



Entrar na comunidade

- Blog do Portal
- Comunidade Ajuda
- Participar na mídia

POSTS DO BLOGCONFERIA AS
ULTIMAS NOVIDADES DO
PARTICIPA.BR

- 2016 (15)
 - Dezembro (3)
 - Novembro (2)
 - Abril (2)
 - Março (2)
 - Fevereiro (1)
 - Janeiro (5)
- 2015 (50)
 - Novembro (2)
 - Setembro (4)
 - Agosto (2)
 - Julho (3)
 - Junho (11)
 - Maio (7)
 - Abril (3)
 - Março (3)

Consulta Pública IoT

14 de Dezembro de 2016, 10:26, por Rafael Andrade - sem comentários ainda | 4 pessoas seguindo este artigo
Visualizado 413 vezes

- Tela cheia
- Sugerir um artigo

Voltar a Blog

0 | 0 ▼

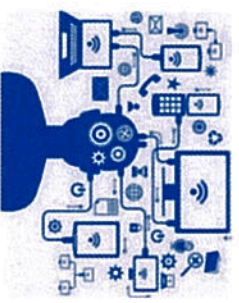


Imagem da Internet of Things

Os trabalhos da Câmara IoT do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) seguem avançando e nesta semana foi dado mais um grande passo rumo ao lançamento do Plano Nacional de Internet das Coisas: a divulgação da Consulta Pública ao Plano Nacional de IoT.

O evento de lançamento da Consulta Pública foi realizado na sede do BNDES no Rio de Janeiro, no dia de ontem, 12/12/2016, e contou com a presença do Ministro da Ciência, Tecnologia, Inovações e Comunicações, Sr. Gilberto Kassab e da Presidente do BNDES, Sra. Maria Silvia Bastos Marques.

No mesmo evento aconteceram também o lançamento do estudo contratado pelo BNDES e que será conduzido pelo consórcio formado pela consultoria McKinsey, BNDES, para juntos, conduzirem tal estudo.

A Consulta Pública fica disponível até o dia 16/01/2017 no endereço: www.participa.br/cpiot

Fonte: Rafael Andrade

SEM COMENTÁRIOS AINDA



Consulta Pública

Plano Nacional de IoT

1. PESQUISA E DESENVOLVIMENTO

Objetivo: mapear o ecossistema de comunicação M2M e IoT no que diz respeito à pesquisa e desenvolvimento, vislumbrando possíveis ações de estímulo ao seu desenvolvimento tecnológico.

1 - Quais as atuais ações e instrumentos adotados pelo Estado Brasileiro para incentivar a pesquisa, o desenvolvimento e a inovação tecnológica para os setores relacionados à comunicação M2M e IoT?

Contribuição Oi: O Brasil conta alguns programas de estímulo à Pesquisa & Desenvolvimento, como linhas de financiamento e pesquisa associadas a fontes de fomento como FINEP, órgãos estaduais (Exemplo: Faperj, no RJ) e entidades como Sebrae. De todo modo, tais programas devem ser ampliados, aumentando o número de iniciativas apoiadas, a fim de que os setores relacionados a IoT possam crescer.

2 - Existem ações não adotadas ainda pelo Estado Brasileiro, mas que poderiam impulsionar ainda mais PD&I nos setores relacionados à comunicação M2M e IoT?

Contribuição Oi: A Oi entende que a criação de linhas mais abrangentes ligadas ao incentivo direto a *startups* através de programas privados e públicos pode ser um excelente caminho para que as inovações aconteçam de forma mais próxima do mercado consumidor.

O Brasil deve adotar políticas públicas claras, de longo prazo e eficientes nas áreas de saúde, segurança, educação, infraestrutura e fiscal, a exemplo do que vem ocorrendo pelo mundo.

Como exemplo, pode-se citar o anúncio do governo britânico acerca de investimento de mais de 1 bilhão de libras esterlinas para incentivar a implantação de uma rede completa de "Fiber to the Premises" (FTTP) e para ser um "líder mundial" em 5G.

O objetivo dessa ação é catalisar o rápido investimento privado no setor para fomentar mais avaliações do 5G, IoT e implantar a banda larga para todas as casas e empresas em todo o Reino Unido. Para incentivar ainda mais o investimento da indústria em conectividade, o governo também eliminará impostos para a nova infraestrutura de fibra por um período de cinco anos.

Outra linha de ação seria a identificação dos nossos talentos (seja nas universidades, seja no mercado profissional) e providenciar a capacitação dos mesmos junto aos profissionais de excelência técnica com garantias de retorno desses talentos após o período de aprendizado (com garantia de retorno financeiro aqui no Brasil) por prazo mínimo a ser definido. Dessa forma, desenvolveríamos mão de obra local, garantiríamos a aplicação dessa mão de obra no próprio país e teríamos as manufaturas dos produtos para a melhoria do bem-estar da nossa sociedade. Deixaríamos de ser um país de commodities.

Entretanto, quaisquer que sejam as ações a serem adotadas, em primeiro lugar é preciso que se construa a visão de longo prazo para o posicionamento do Brasil nos segmentos econômico e tecnológico de seu interesse, utilizando sempre como alicerce as suas competências essenciais e principais vocações. Apenas a partir daí será possível a definição de sua trajetória com elaboração de programa sistemático para minimização de barreiras, catalisação de iniciativas, etc.

3 - O Brasil aparece no Relatório do Índice Global de Inovação 2015 (Cornell University, INSEAD, e WIPO) na posição 70 de 141 países. O estudo aponta um cenário preocupante com relação ao percentual de graduações em ciência e engenharia em relação ao total de graduações, ocupando a posição 94. Os impactos do conhecimento e das tecnologias geradas (que incluem patentes, papers e citações) posicionam o país em 72º lugar. Já Índice Global de Talento Competitivo 2015-2016 (INSEAD, ADECCO and HCLI) coloca o Brasil em 67º lugar entre 109 países, com o subíndice de quantidade equivalente de



Consulta Pública

Plano Nacional de IoT

pesquisadores em tempo integral por milhões de habitantes na posição 53. Quais os principais motivos para a atual atratividade dos cursos nas áreas de ciência e engenharia? Que iniciativas poderiam melhorar este cenário?

Contribuição Oi: A Oi entende que o país possui questão a ser resolvida na educação de base: os jovens tem fraco desempenho acadêmico e buscam cursos de menor carga analítica nas universidades. Aliado a isso, há um fenômeno de proliferação de cursos, inclusive à distância, com qualidade de ensino e avaliação de aprendizado questionáveis.

Isso posto, entendemos necessária uma mudança curricular, que insira na grade dos alunos do ensino médio e fundamental cursos técnicos de linguagem de programação e física aplicada a desafios reais. Essa ação poderia despertar maior interesse nos jovens. Aproximá-los de um ecossistema de inovação, com ementas de empreendedorismo também poderá ajudar. Desse modo, haveria a chance de mais estudantes serem atraídos para áreas de ciência e engenharia a partir da desmistificação da dificuldade percebida pela maior parte da população sobre as disciplinas técnicas.

Uma medida eficaz para a melhoria da questão seria o impulso dos benefícios da Lei do Bem através da criação de produção científica nas faculdades voltadas a estudos de IoT:

- Incentivar a pesquisa de novas redes, sempre dentro de padrões abertos ou de fato, como IEEE (*Institute of Electrical and Electronic Engineers*), 3GPP (*3rd Generation Partnership Project*), GSMA (*Global System for Mobile Communications Association*), ISO/OSI (*International Organization for Standardization/Open Systems Interconnection*).
- Incentivar e impulsionar o *Low Power Wide Area* - LPWA em frequência licenciada.
- Incentivar o investimento na produção científica por parte das empresas por intermédio de incentivos fiscais.
- Incentivar a utilização de padrões de *software* aberto.

No campo das empresas, incentivar as empresas a investir em inovação de base, com redução dos impostos para atividades atreladas à pesquisa & inovação, é outro ponto importante para garantir o desenvolvimento do capital intelectual nacional. Atualmente, para diversas atividades, a pesquisa no Brasil é muito cara, sendo mais vantajoso o desenvolvimento através de redes de parceiros no exterior. A aquisição de equipamentos de ponta, em especial, é impactada pela alta carga tributária.

4 - Quais as oportunidades e barreiras existentes nas políticas públicas atuais de incentivo à PD&I, no âmbito do ecossistema de IoT?

Contribuição Oi: A Oi entende, que apesar de diversas Instituições de Pesquisa Científica e Tecnológica (ICT) e empresas, as *startups* ainda são pouco incentivadas no país, ficando restritas a poucos centros urbanos e incentivadas por poucas aceleradoras. Nesse âmbito, programas de incentivos como o CRIATEC, financiado pelo BNDES, são importantes e deveriam ser incentivados de forma mais descentralizada.

Dentre outros fatores, é possível identificar como barreiras que comprometem PD&I em IoT, ainda, a alta carga tributária, a falta de recursos dos fundos setoriais e a escassez de linhas de financiamento.

Na prática, as maiores inovações de alto impacto vem de *startups* e o incentivo ao desenvolvimento de novas redes de incentivo é fundamental para evolução da ambiente de P&D no país. As *startups* são mais objetivas quanto ao *time to Market*, mais propensas a entregarem produtos ao mercado do que os ICT e a comunidade acadêmica, além de contarem com alguns dos melhores profissionais do mercado em suas áreas. Cidades como Rio de Janeiro, Recife, Porto Alegre e Belo Horizonte ainda não contam com um ecossistema adequado. Neste ponto, São Paulo se destaca.

Sendo assim, além de criar novas formas de incentivo, é preciso explorar as oportunidades existentes nas políticas públicas atuais, tais como as linhas especiais de financiamento, os projetos de cooperação com instituições de ensino e o direcionamento de recursos de fomento para a área de tecnologia.



Consulta Pública

Plano Nacional de IoT

5 - Existem problemas para a formação de redes de pesquisa e o fortalecimento dos vínculos entre os atores da produção de conhecimentos técnicos e científicos (universidades, institutos de pesquisa, parques tecnológicos, etc.), considerando-se as distintas camadas da arquitetura de IoT?

Contribuição Oi: Conforme mencionado na questão anterior, percebe-se que os atores citados são, em sua maioria, voltados para produção de conhecimento científico, e não necessariamente a tangibilização da inovação em produtos e serviços de mercado. A Oi entende que as *startups* podem suprir este *gap*.

Um dos maiores problemas para a formação das redes é a burocracia para acesso aos financiamentos e efetivo gasto dos valores obtidos. Passa-se muito tempo focado na discussão burocrática de formas de gasto e propriedade de patentes, quando o foco deveria ser a entrega. A desburocratização é fundamental. Isso pode ocorrer através de incentivos à criação de arranjos locais de redes de *startups* e do movimento *maker (fablabs)*.

6 - Existem problemas na relação entre indústrias e provedores incumbentes de soluções e serviços de TICs, no que tange suas relações com o ecossistema de *startups* no Brasil? Que medidas devem ser consideradas para aproximar esses atores, aproveitando-se suas principais forças, isto é, capacidade de inovação das *Startups* em setores dinâmicos como IoT e capacidade de atuar em escala da indústria e provedores de serviços incumbentes?

Contribuição Oi: Em geral, o grande desafio para as *startups* é o acesso a redes licenciadas, o que gera uma situação de desequilíbrio. Por outro lado, os provedores de serviços incumbentes são extremamente regulados, o que os impede de investir como deveriam em inovação. O cenário ideal é o envolvimento das indústrias e provedoras de soluções e serviços TIC nos ecossistemas de inovação, inclusive como investidoras de empresas promissoras, de forma que o *corporate venture* seja utilizado como ferramenta formal de incentivo ao ecossistema de *startups* focadas em soluções IoT.

Entre os grandes ingredientes fundamentais para o novo momento da indústria estão: transformação digital, economia de compartilhamento e desenvolvimento colaborativo. O desenvolvimento colaborativo será decisivo para a consolidação e crescimento do mercado de IoT, criando não só oportunidades para novas empresas do segmento, *startups*, mas principalmente uma base de conhecimento e competências.

Neste sentido, a Oi e a Nokia disponibilizaram ao mercado o primeiro laboratório de referência na América Latina para desenvolvimento de projetos, em regime colaborativo com as *startups*, para Internet das Coisas (IoT), no Rio de Janeiro.

Esta iniciativa viabiliza o desenvolvimento conjunto do ecossistema para os serviços da Internet das Coisas e de comunicação entre máquinas (M2M). O laboratório permite o uso de recursos profissionais, infraestrutura do laboratório e tecnológicos, entre outros, para viabilizar projetos para o IoT através de desenvolvimento próprio ou de parcerias, principalmente no modelo de *crowdsourcing*.

O laboratório oferece infraestrutura e suporte de profissionais para o desenvolvimento, a validação e a certificação para viabilizar projetos de IoT, através de desenvolvimento da Oi e da Nokia ou de parcerias, permitindo que as soluções se adaptem a futuras tecnologias já previstas. A Oi aposta na Inovação aberta como uma grande fonte geradora de oportunidades. O Laboratório IoT vem para ser mais uma ferramenta que nos permitirá nos relacionar com o mercado, gerando novos negócios.

7 - Há demanda para linhas de financiamento de pesquisa para P&D de produtos e aplicações para soluções de comunicação M2M e Internet das Coisas? Em que áreas? Cite necessidades e oportunidades de P&D.

Contribuição Oi: Sim. Algumas linhas de pesquisa poderiam impactar diretamente o desenvolvimento de soluções IoT, tais como:



Consulta Pública

Plano Nacional de IoT

- Soluções de monitoramento e segurança para casas e empresas
- Cidades Inteligentes (sensores para medição águas, poluição, deslizamentos, deslocamentos de pessoas, etc)
- Saúde (monitoramento proativo remoto de pacientes)
- Automotivo (monitoramento proativo de problemas estruturais)
- Agricultura (monitoramento e captação de informações para aumento da produtividade)
- Industrial (otimização de processos industrial e aumento da produtividade)
- Educação Inteligente (sistema de controle automatizado de presença e frequência do aluno, sistemas de integração ao ensino de forma digital, etc.);
- *Smart Grid* (sistema de controle e reutilização de energia);
- Transportes (controle inteligente de vias, carro autônomo, sistema integrado de serviços aos veículos, etc.);
- Soluções de “*vending*” (supermercados inteligentes e controlados, máquinas de refrigeração monitoradas, etc.)

8 - Quais as instituições de pesquisa nacionais que possuem estudos relacionados ao ecossistema de Internet das Coisas de forma relevante?

Sem contribuição.

9 - Como poderia ser realizado o incentivo à criação de um ecossistema de empresas nascentes (*startups*) com elevado grau de inovação em IoT, através de apoio estatal (p.ex., o financiamento dos projetos ou simplificação das obrigações sobre tais empresas), reduzindo o risco à inovação?

Contribuição Oi: Existem diversas formas. Entre elas destacam-se:

- Apoio financeiro a criação de incubadoras
- Aumento dos programas de financiamento como o CRIATEC
- Facilitação da criação formal de *startups*, com redução da burocracia e da carga tributária, desde que comprovadamente as empresas possam ser enquadradas como *startups*
- Linhas de financiamento exclusivas e com condições competitivas para que *startups* possam competir contra empresas de maior porte em soluções IoT
- Criação de programas de modernização dos parques tecnológicos
- Garantia de acesso de *startups* aos recursos dos fundos setoriais

10 - Considerando iniciativas e o ambiente de pesquisa e desenvolvimento, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Contribuição Oi: Alguns fatores são chaves para o completo diagnóstico:

- Acesso às redes licenciadas e não licenciadas.
- Definição de padrão de comunicação e interoperabilidade das redes
- Definição do padrão de API (*Application Protocol Interface*), para que soluções distintas possam se comunicar, dando chance a todas as empresas.

2. RECURSOS HUMANOS



Consulta Pública

Plano Nacional de IoT

Objetivo: mapear a capacidade técnica e as principais lacunas na mão-de-obra brasileira, para atuar nos diversos setores que envolvem soluções de comunicação M2M e IoT.

1 - A Comunicação M2M e a Internet das Coisas afetarão a educação em sentido amplo. As aplicações dessas tecnologias em diversas áreas dependerão de habilidades profissionais variadas e nos obriga a revisitar os processos educacionais de maneira holística e questioná-los do ponto de vista da melhoria que essas tecnologias podem representar. Considerando este contexto:

- Aponte qual(is) o(s) perfil(is) de profissional que será(ão) mais demandado(s) para o desenvolvimento do ecossistema de IoT;

Contribuição Oi: Engenheiros eletrônicos, mecânicos, programadores, profissionais de informática, designers industriais, estatísticos (*data scientists*), profissionais com visão de negócios (administradores, economistas, analista de investimentos de risco, profissionais especializados na captação de financiamentos e desenvolvimento de planos de negócio, engenheiros de produção), profissionais com experiência técnica em sociologia, com competências inovadoras e disruptivas para atuar nos seguintes elos da cadeia:

- Identificação de melhorias para o bem-estar da sociedade;
- Fabricantes de *hardware* (dispositivos e sensores);
- Comunicações (telecomunicações);
- Desenvolvedores de *softwares* / aplicações;
- Plataformas;
- *Datacenters*;
- Gestão e operação de serviços;
- Suporte;
- Implantação.

O desafio está em ter uma mão de obra técnica disponível sem, no entanto, formar uma legião de acadêmicos e cientistas, mas sim profissionais *hands on* com visão de mercado. Por isso, a junção das competências técnicas com a visão de modelos de negócios é fundamental.

- Quais são as principais barreiras do nosso atual processo educacional para a formação de novos profissionais para o mercado de IoT.

Contribuição Oi: A Oi entende, que há carência de disciplinas voltadas ao empreendedorismo e ao conhecimento tecnológico nas grades curriculares. O processo educacional atual é ultrapassado, focado em um aprendizado acadêmico e pouco prático. Países com educação de base mais avançada como Austrália e Dinamarca já iniciaram a substituição de matérias humanas, como Geografia e História, por disciplinas práticas como programação e empreendedorismo, para turmas do ensino fundamental.

Pensando no ensino técnico, a capacitação de *web designers*, técnicos mecânicos e mão de obra para *fablabs* poderia auxiliar.

2 - Qual o impacto (positivo ou negativo) que a IoT pode provocar na força de trabalho?

Contribuição Oi: Um impacto positivo seria a conformação de uma nova indústria, trazendo oportunidades e/ou necessidades de novas competências e profissionais. Além disso, novas formas de pensamento e organização processual, permitindo a antecipação e ação imediata para solução de problemas. Isso gera oportunidades para profissionais com capacidade analítica para entender e tratar dados.

Pelo lado negativo, algumas profissões poderão ficar obsoletas, como operações de campo, que poderão ser feitas remotamente.

3 - Quais os potenciais benefícios da IoT para empregados e/ou empregadores?



Consulta Pública

Plano Nacional de IoT

Contribuição Oi: O principal benefício à criação de oportunidades e postos de trabalho, que, por se tratar de uma indústria não substitutiva, serão incrementais em toda economia.

Para empregadores, aumento da eficiência e produtividade, com consequente redução de custos.

4 - Considerando aspectos relacionados a força de trabalho dedicada ao ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

5 - O atual arranjo entre governo, universidade e empresas é adequado para a capacitação e formação de mão de obra aplicável à IoT?

Contribuição Oi: A Oi entende que o atual arranjo deve ser aprimorado. Em longo prazo, é preciso incrementar a oferta de cursos na área de tecnologia, principalmente através de instituições públicas de ensino superior e técnico.

Entretanto, reiteramos, que é necessário impulsionar os benefícios da Lei do Bem, através da criação de produção científica nas Faculdades voltadas a estudos de IoT: dessa forma, acreditamos que haverá incentivo ao investimento na produção científica por parte das empresas, por intermédio de incentivos fiscais. Tal medida criaria canais para o desenvolvimento do IoT no Brasil.

3. OFERTA TECNOLÓGICA E COMPOSIÇÃO DE ECOSISTEMAS

Objetivo: identificar qual o contexto atual da indústria brasileira de TIC, mapeando suas competências e oportunidades para o desenvolvimento do setor aplicado a IoT no Brasil.

1 - Considerando o setor de TICs no Brasil, que empresas apresentam produtos ou serviços que podem ser utilizados no desenvolvimento ou formação de um ecossistema local de IoT?

Contribuição Oi: Os grandes provedores de serviços de telecomunicações, com suas subsidiárias ou em parceria com empresas especializadas, são as que apresentam melhor infraestrutura e portfólio de produtos ou serviços para o desenvolvimento e/ou formação de um ecossistema local de IoT. Além deles, podemos citar as distribuidoras e transmissoras de energia elétrica e as concessionárias de água.

2 - Que instituições de pesquisa, no Brasil, desenvolvem tecnologias ou soluções que poderão ser relevantes na constituição do ecossistema de IoT no Brasil?

Contribuição Oi: As Instituições de Pesquisa Científica e Tecnológica (ICT) estão atuando no Brasil, mas de forma mais restrita. As grandes prestadoras de serviços de telecomunicações tem tido maior atuação, dando espaço para atuação conjunta de pequenas empresas. Ainda sobre o tema, entendemos que as universidades poderiam ter maior participação na constituição do ecossistema de IoT no Brasil.

3 - Avaliando o potencial das entidades brasileiras de suprir às futuras demandas de IoT, quais são as ofertas de tecnologias, produtos e serviços que poderão contribuir para disseminação de IoT nos diversos segmentos econômicos brasileiros?

Contribuição Oi: Laboratórios de IoT, como o da Oi/Nokia, e *fablabs*, como os do SENAI, são fundamentais para criação do ecossistema.



Consulta Pública

Plano Nacional de IoT

4 - Que alianças internacionais, no contexto da IoT, são relevantes para o desenvolvimento da IoT no Brasil?

5 - Identifique quais são os subsetores da cadeia de TIC mais relevantes para o desenvolvimento de IoT.

6 - Que nichos de mercado apresentam potencial para desenvolvimento de players locais?

Contribuição Oi: Soluções para indústria, agroindústria, cidades inteligentes (*smart metering*) e setor automotivo (*telemetria e tracking*).

7 - Em quais aplicações o Brasil pode ser competitivo em semicondutores?

8 - Em quais nichos de equipamentos eletrônicos o Brasil pode desenvolver tecnologia local em hardware/software embarcada?

Contribuição Oi: Setor automotivo.

9 - Em que área o Brasil pode desenvolver softwares de maior valor agregado, como software-ferramentas e/ou com elevado potencial de exportação?

Contribuição Oi: Agroindústria, pecuária leiteira e de corte e Cidades inteligentes.

10 - Considerando a oferta tecnológica e a composição do ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Sem contribuição.

4. INVESTIMENTO, FINANCIAMENTO E FOMENTO

Objetivo: mapear fontes de investimento, canais de financiamento e iniciativas de fomento, existentes ou a serem estruturadas, com o propósito de incentivar o desenvolvimento do setor aplicado a IoT no Brasil.

1 - O acesso a crédito ainda é muito oneroso para as empresas brasileiras, com taxas de juros elevadas. Além disso, a quantidade e o valor de investimentos de capital de risco ainda são baixos – no Brasil este tipo de investimento representa apenas 0,01% do PIB, enquanto outros países têm volumes muito superiores em termos relativos como os EUA que investe 0,18%, a Índia 0,12%, e a China 0,07% do PIB. Quais as fontes e modelos de financiamento disponíveis hoje no país, que atendem ao ecossistema de IoT?

Contribuição Oi: As fontes são insuficientes e o atual modelo de financiamento é ineficaz. Existem, basicamente, editais públicos, que contam com excesso de burocracia; e autofinanciamento das empresas, geralmente limitados por conta dos custos de capital do país.

2 - Como você avalia a eficácia dessas fontes e modelos de financiamento no estímulo à inovação do País, bem como na introdução de novos serviços e produtos no mercado nacional? O que poderia ser melhorado?

Consulta Pública

Plano Nacional de IoT

Contribuição Oi: Como dito anteriormente, o atual modelo de financiamento é ineficaz e excessivamente burocrático. O acesso e o estímulo ao crédito poderiam ser facilitados para empresas envolvidas na cadeia de inovação, reduzindo taxas e burocracia e subsidiando as pesquisas para *startups* e pequenas empresas.

A isenção de impostos sobre importação de insumos técnicos, destinação à pesquisa e inovação também poderia acontecer.

3 - Considerando fontes de investimento, financiamento e fomento, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Contribuição Oi: Programas relativos a fundos para IoT (ex: Programa “Minha Cidade Inteligente”, Portaria nº 2.111/2016 do Ministério das Comunicações) devem ser construídos com apoio técnico de empresas fornecedoras do setor (como está sendo feito nesta Consulta Pública), para garantir qualidade na definição das regras de prestação dos serviços. Os projetos devem prever não somente infraestrutura, mas também orçamento para todos os elos da cadeia, como:

- Identificação de melhorias para o bem-estar da sociedade;
- Fabricantes de *hardware* (dispositivos e sensores);
- Comunicações (telecomunicações);
- Desenvolvedores de *softwares* / aplicações;
- Plataformas;
- *Datacenters*;
- Gestão e operação de serviços;
- Suporte;
- Implantação.

4 - As estruturas de *Venture Capital* e *Seed Capital* existentes no Brasil são adequadas quando se considera a dinâmica de ecossistemas de inovação presentes em outros países?

5. DEMANDA

Objetivo: identificar os desafios e oportunidades nacionais nos quais a Internet das Coisas pode ter impacto significativo, tanto na esfera pública, quanto na privada. Adicionalmente, entender o potencial econômico que a Internet das Coisas pode trazer para nossa sociedade, por meio do mapeamento dos principais casos de uso.

a) Demanda pública

1 - Quais são as possíveis aplicações de IoT no Brasil na esfera pública, analisando todos os possíveis setores e ambientes de aplicação?

Contribuição Oi: Entendemos que a IoT pode proporcionar a adoção de infraestrutura, plataformas e serviços inteligentes, contribuindo com a sustentabilidade econômica, social e ambiental. Além disso, cria condições para tornar os serviços urbanos mais eficientes, melhorando o bem-estar social.

No âmbito da esfera pública, a IoT deve abranger soluções integradas, dentro de diferentes verticais – com uma gestão global e sustentável dos serviços. As aplicações podem ser distribuídas em 7 verticais (padrão da União Europeia), para as quais é possível citar exemplos:

1 – Segurança



Consulta Pública

Plano Nacional de IoT

- Agilidade no atendimento de emergências;
- Proteção de pessoas vulneráveis;
- Vídeo vigilância;
- Segurança no transporte (sistemas de localização por GPS);
- Segurança *online*.

2 – Saúde

- Programas de Saúde: Autocuidado e Pacientes Crônicos;
- Histórico clínico digital;
- Gestão de demanda assistencial – Otimização de recursos e serviços administrativos;
- Gestão da Informação;
- Prevenção e alertas sanitários;
- Suporte tecnológico para agentes de saúde;
- Gestão de emergências;
- Assistência e monitoramento remoto de pacientes.
- Aprimorar a relação entre hospital, laboratórios e planos de saúde, otimizando o envio de informações;
- Maior controle de entrada e saída de pessoas dentro de hospitais;
- Controle de localização de recém-nascidos;
- Controle de acesso por setores;
- Maior controle e segurança no armazenamento e uso de medicamentos;
- Monitoramento de equipamentos e material médico;
- Gestão de higienização de equipamentos, enxoval, uniformes, ambientes, etc;
- Gestão do lixo hospitalar;
- Redução de incidência de infecção hospitalar;
- Monitoramento de pacientes;
- Monitoramento da ingestão de medicamentos pelo paciente;
- Monitorização de ensaios clínicos;
- Monitoramento de temperatura e acondicionamento de materiais críticos;
- Monitoramento de temperatura de ambiente controlado.

3 – Educação

- Tecnologia nos Centros como Conectividade, Dispositivos, Soluções Multitáteis (Ex: Lousa Digital), Programas Interativos;
- Monitoramento pelos pais (desempenho, frequência, comunicação com a escola);
- Educação Aberta - Uso de ferramentas digitais em sala de aula – através de equipamentos como computadores e *tablets*. Cursos *online* massivos e abertos em plataformas educativas;
- Matrículas (consulta sobre disponibilidade de vagas em escolas e creches);
- Gestão escolar.



Consulta Pública

Plano Nacional de IoT

4 – Meio Ambiente

- Gestão eletrônica do processo de gestão ambiental
- Gestão da perda de água e gestão do ciclo integrado da água;
- Iluminação pública eficiente;
- Gestão de desastres ambientais;
- *Smart Metering* - medição inteligente de consumos de energia, gás e água;
- Irrigação inteligente;
- Salinidade do solo;
- Eficiência energética em edifícios públicos;
- Redes de sensores ambientais inteligentes - Redes inteligentes para fornecimento de energia, monitoramento e controle de poluição, chuvas, aplicações para reuso e reciclagem de recursos;
- Lixeiras inteligentes que sinalizam a sua capacidade de armazenamento;
- Bueiros inteligentes que sinalizam sua carga de resíduos.

5 – Mobilidade

- Transporte Público inteligente e integrado: Sistemas de transporte sustentáveis, seguros e interconectados – que integram ônibus, trens, metrô, bicicletas – com informações em tempo real para os usuários e empresas de transporte. Avaliar a capacidade de cada transporte para realocação de veículos, conforme a demanda em tempo real;
- Bicicletas compartilhadas;
- Gestão do Trânsito;
- Carro elétrico;
- Gestão de frotas;
- Estacionamentos Inteligentes;
- Monitoramento de emissão de gases e consumo energético dos veículos públicos;
- Pagamentos eletrônicos;
- Semaforização Inteligente.

6 – Economia

- Rede Avançada de Comunicações;
- Social Wifi - Disponibilização de acesso à Internet em estabelecimentos e locais públicos;
- Suporte à microfinanças e microcrédito;
- Gestão do Turismo;
- Apoio ao desenvolvimento de empresas de Tecnologia;
- Comércio Digital;
- Fluxo de deslocamento de cidadãos por localidade – Possibilitando ofertas comerciais nas proximidades dos cidadãos em tempo real;
- Aplicações que permitam ofertas personalizadas, *Big Data* para que empresas possam melhorar seus modelos de negócio;
- Painéis digitais que ofereçam informações ou ofertas em tempo real;
- Oportunidade de Renda para cidadãos: Pessoas podem vender energia não consumida gerada em suas casas através de energia eólica ou solar;
- Agricultura;
- Pecuária de leite e de corte;
- Mineração.

7 – Governo (e-Gov) - transversal

- Atenção e Comunicação com o cidadão;
- Integração das informações do cidadão;
- Novas formas de participação;
- Captação de informações de deslocamento dos cidadãos através de apps;

Consulta Pública

Plano Nacional de IoT

- Plataforma de digitalização de processos, aumentando a eficiência e reduzindo custos da gestão pública em todas as secretarias e pontos de contato entre governo e cidadão;
- *Open Data* - Disponibilização de Dados (em tempo real) aos cidadãos e empresas (Transparência);
- Aplicações que contribuam na conservação e valorização do Patrimônio;
- Plataforma Integradora.

Alguns exemplos de aplicações já existentes no Brasil:

Segurança:

1. Vitória/ES: Dispositivo de Segurança Preventiva (botão de pânico) permite que as mulheres que se sintam ameaçadas por parceiros avisem autoridades através de geolocalização e gravem áudio.
2. Rio de Janeiro/RJ e Santos/SP possuem Centro de Operações para Ação em Emergências, referências nacionais. Permitem ação coordenada para acidentes, tragédias e crimes.

Saúde:

1. Presidente Prudente/SP: Georeferenciamento de Doenças (como dengue) – contribuem com identificação de áreas de risco. Oferecem soluções que mapeiam e organizam informações epidemiológicas.
2. Curitiba/PR: Médicos de diferentes unidades de saúde podem consultar laudos e trocar informações de paciente.
3. Campinas/SP: Aplicativo disponibiliza informações sobre disposição de remédios em centros de saúde. Evita deslocamentos desnecessários e permite transparência.

Educação:

1. Águas de São Pedro/SP: *software* de gestão de conteúdo e utilização do mesmo através de *tablets* pelos alunos.
2. Vitória/ES: boletim *online* escolar para acompanhamento de notas pelos pais.
3. SP – Sistema de biometria para acompanhamento de frequência dos alunos.

Meio Ambiente:

1. Campinas/ SP: licenciamento ambiental *online* – sistema que permite emissão de requerimento, análise, pagamento de taxas e acompanhamento de solicitações de obras de impacto ambiental.
2. Mais de 100 PPP de Iluminação em formatação.
3. Nova Friburgo/RJ: Meio Ambiente Digital – sistema que permite todo o controle, emissão de requerimento, análise, pagamento de taxas e acompanhamento de solicitações através de sistema *online*, além de ser *database* oficial para fornecimento de centenas de camadas de informações públicas de forma estruturada.


Mobilidade:

1. Curitiba/PR: Sistema BRT – semaforização inteligente, dando prioridade ao transporte coletivo.
2. São Paulo/SP: pagamento eletrônico de passagens – considerando integração de transportes públicos (Ex: Bilhete Único).

Economia:

1. Recife/PE: Porto Digital: Revitalização de área degradada da cidade, com incentivos às TIC e de empresas de economia criativa (para se instalarem lá).
2. Juazeiro/BA: projeto geração de renda e energia: Instalação de sistemas de energia solar e eólica no telhado de casas de beneficiários do “Minha Casa, Minha Vida”. Estes podem vender energia não utilizada para Caixa Econômica Federal.

Governo:



Consulta Pública

Plano Nacional de IoT

1. Florianópolis/SC: sistema de gestão de processos eletrônicos – permite solicitação e acompanhamento de processos.
2. Rio de Janeiro/RJ: *big data* - análise de deslocamentos feitos no *réveillon* 2013 de Copacabana, baseado no uso de informação dos celulares. De onde partiram as pessoas, onde aglomeraram-se. Tais informações serviram de base para planejamento e transporte dos anos seguintes.
3. Cadastro Único: 20 milhões de famílias carentes cadastradas para programas sociais.



Consulta Pública

Plano Nacional de IoT

2 - Qual o impacto potencial estimado de IoT na economia, considerando os principais usos para o setor público no Brasil?

3 - Quais barreiras na esfera pública existentes atualmente nas diferentes áreas de aplicação de IoT que poderiam ser superadas com seu uso?

Contribuição Oi: Em diversos setores, há oportunidade de adoção de soluções inteligentes, que simplifiquem processos e otimizem custos, sem prejuízo à qualidade dos serviços. Alguns exemplos práticos de implantação podem ser vistos na resposta à questão 1.

A capacitação da mão de obra no setor público é crítica. Além das políticas de fomento de adoção de tecnologia, devem ser consideradas em paralelo o incentivo ao treinamento para operação das novas ferramentas e tecnologias pelas próprias prefeituras. Sem a capacitação associada à implantação das soluções IoT, o modelo operacional acabará sendo baseado sempre em terceirização, encarecendo o valor total das soluções para os entes públicos.

Ressalta-se que é justamente essa capacitação que permitirá aos órgãos públicos a correta elaboração de editais e a gestão posterior dos serviços a serem implantados, garantindo a continuidade e, de fato, a criação de cidades inteligentes.

Entretanto, independente do setor a ser atendido, consideramos ser imprescindível que a elaboração de editais (de PPP ou de outros modelos de contratação) não busquem especificar tecnologias, mas sim níveis de serviço. Ao restringir o desenho das soluções para determinadas tecnologias, haverá risco para o poder público em não escolher a melhor solução (tecnicamente e economicamente) para a sociedade.

4 - Considerando o mapeamento e geração da demanda por soluções de IoT, existem outras questões relevantes no setor público que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Contribuição Oi: A Oi acredita ser importante entender que a abordagem não deve se limitar à adoção de tecnologias e soluções IoT sem a devida modernização dos entes públicos, em especial as prefeituras. Logo, estabelecer um patamar mínimo de e-gov, definindo soluções básicas, que permitam fundamentalmente o desenvolvimento eficiente de soluções.

Outro ponto relevante é atrelar boas práticas de gestão eletrônica e eficiência as linhas de financiamento que serão criadas no futuro, garantindo que a adoção das soluções esteja atrelada a uma mudança de patamar de governança dos entes da federação, em particular, os municípios.


Ressalta-se também a necessidade de conexão entre empresas, centros de pesquisa e inovação e órgãos públicos, de forma que as soluções sejam elaboradas a partir de problemas reais e com a participação direta dos gestores municipais, para que haja aderência entre as soluções e as possibilidades reais de contratação e governança do setor público.

Por fim, fomentar a discussão popular para adoção das soluções através das revisões dos planos diretores parece ser uma excelente oportunidade para incentivo à participação popular.

b) Demanda privada

5 - Considerando as verticais de aplicação de IoT mapeadas e listadas abaixo, dê exemplos de casos de uso em cada uma delas.

Saúde



Consulta Pública

Plano Nacional de IoT

Contribuição Oi: Gestão de pacientes crônicos e/ou de risco, através da coleta remota de informações via gadgets, informando diretamente médicos e sistema de saúde. Redução de custos de gestão da saúde pública e privada.

Agricultura

Contribuição Oi: Monitoramento remoto de rebanhos, equipamentos e indicadores produtivos nas fazendas de qualquer natureza.

Uso consciente e inteligente dos recursos naturais.

Mapeamento de áreas para verificação de necessidade de adubação, irrigação na medida certa, correção do grau de salinidade da terra, identificação de possíveis pragas.

Monitoramento dos produtos em toda a cadeia logística entre produtor, indústria e consumidor.

Infraestrutura

Petróleo e gás

Automotivo

Contribuição Oi: Gestão proativa dos veículos (telemetria), fornecimento de serviços de entretenimento (música, auxílio a estabelecimentos), controle de emergência e localização do veículo, controle de comunicação remota do veículo, avaliação dos sensores dos itens de segurança, etc.

Bens de consumo e varejo

Energia

Contribuição Oi: Monitoramento remoto das linhas de transmissão e distribuição, em particular, dos transformadores, de forma que a gestão remota possa ser implantada com eficiência e atendendo aos padrões de segurança. Esta prática eliminará a necessidade de operações físicas remotas 24/7h, reduzindo custos e aumentando a eficiência.

Logística

Aeroespacial

Eletrônicos avançados

Mineração

Telecomunicações e mídia

Serviços bancários

Cidades inteligentes

Contribuição Oi:

- Gestão de áreas de risco de deslizamento de terra em tempo real através de sensores;
- Medições pluviométricas, indicando momentos críticos para a população envolvida (chuvas);

Consulta Pública

Plano Nacional de IoT

- Monitoramento dos níveis e da qualidade das águas, antecipando potenciais alagamentos e áreas de risco para população (rios e mares);
- Iluminação pública, tornando menos custoso e mais eficiente a gestão;
- *Movement analytics* em tempo real, utilizando dados de deslocamento de massas para planejamento de serviços urbanos;
- Mapeamento de vagas de estacionamento públicas, impactando positivamente o trânsito;
- Monitoramento e gestão do transporte público por parte de usuários e gestores do transporte, avaliando em tempo real a capacidade, tempo, distância e trajeto dos veículos;
- Lixeiras inteligentes que informam em tempo real a capacidade armazenada e necessidade de esvaziamento;
- Bueiros inteligentes que informam em tempo real a sua capacidade armazenada de resíduos e necessidade de esvaziamento evitando enchentes e alagamentos.

Indústria 4.0

Escritórios e residências inteligentes

Contribuição Oi:

- Controle de fluxo de pessoas;
- Controle do sistema de luminosidade e refrigeração;
- Controle de portas.

Pequenas e médias empresas

6 - Existe alguma vertical adicional relevante de aplicação de IoT além das previamente mapeadas?

Contribuição Oi: Extrativismo, Pecuária de Leite e de Corte, Meteorologia etc.

7 - No âmbito global, quais as principais lacunas de atuação ("white-spaces") onde o IoT poderia proporcionar importantes mudanças?

Sem contribuição.

8 - Qual o impacto potencial estimado de IoT na economia, considerando os principais usos para o setor privado no Brasil?

Contribuição Oi: O desenvolvimento do ecossistema de IoT representará um grande impacto na economia brasileira, através da redução do custo Brasil; aumento da assertividade nas atividades do setor privado, mitigando, por conseguinte, o reprocesso em bens manufaturados e em serviços; tendência ao "Zero Defeito"; incremento no PIB e o crescimento de diversos setores da economia, levando o país a altos índices de crescimento econômico; ganho de eficiência, alcançado por meio do ganho de escala e produtividade.

Consulta Pública

Plano Nacional de IoT

9 - Quais barreiras na esfera privada existentes atualmente nas diferentes áreas de aplicação de IoT que poderiam ser superadas com seu uso?

Contribuição Oi: Ao menos custos de deslocamentos e otimização de recursos materiais.

10 - Considerando o mapeamento e geração da demanda por soluções de IoT, existem outras questões relevantes no setor privado que devem ser observadas para um completo diagnóstico da IoT no Brasil?

6. ASPIRAÇÕES

Objetivo: Obter uma visão sobre quais deveriam ser as aspirações iniciais para o desenvolvimento de IoT no Brasil.

1 - Considerando a situação atual de IoT no Brasil, quais deveriam ser as aspirações para o país a médio e longo prazo?

Contribuição Oi: Em curto prazo, o Brasil deveria voltar-se para aplicação em setores onde é referência mundial, como, por exemplo, o agronegócio. Paralelamente, dever-se-ia fomentar o desenvolvimento de *startups* para o mercado de IoT, fomentando-se incubadoras com esse foco. A aspiração do Brasil deveria ser o desenvolvimento de redes aptas ao desenvolvimento de soluções IoT em todas as áreas urbanas do país, incluindo pequenos municípios.

2 - Quais países possuem aspirações para IoT que podem ser usadas como referência pelo Brasil?

Contribuição Oi: A Coreia do Sul, com o lançamento de sua rede 5G, já está se preparando para ter uma cobertura nacional que permitirá o lançamento de diversas soluções IoT na economia local. Outros países que podem ser usados como referência: Dinamarca, Suíça, Estados Unidos, Holanda, Alemanha e Suécia.

7. GERENCIAMENTO DE INFRAESTRUTURA

Objetivo: mapear as questões críticas para o gerenciamento da infraestrutura de IoT, em todas as suas camadas, com o objetivo de garantir a confiabilidade dessa estrutura através do comissionamento, monitoramento, provisionamento e configuração dos dispositivos sensores e atuadores, elementos de rede e infraestrutura computacional, suportando toda a operação.

1 - Na sua visão, quais aspectos devem ser desenvolvidos no que diz respeito à gestão de inventário, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.



Consulta Pública

Plano Nacional de IoT

2 - Que questões relacionadas a instalação de dispositivos precisam ser consideradas no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

3 - Quais os aspectos que necessitam de desenvolvimento no que diz respeito à gestão de configuração, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

4 - Quais os aspectos que necessitam de desenvolvimento no que diz respeito à faturamento, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

5 - Na sua visão, o que ainda precisa ser equacionado no que diz respeito à tratamento de falhas, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

6 - Que questões carecem de tratamento no que diz respeito à qualidade de serviço, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

7 - No que diz respeito à qualidade da experiência, no ecossistema IoT, que aspectos precisam ser desenvolvidos? Justifique sua contribuição com casos de uso.

Sem contribuição.

8 - Na sua opinião, quais as principais questões que ainda devem ser equacionadas no que diz respeito à analytics, no ecossistema IoT? Justifique sua contribuição com casos de uso.

Sem contribuição.

9 - Considerando as funcionalidades relacionadas nas questões anteriores, há necessidade de desenvolvimentos adicionais nos sistemas de gerenciamento para a implantação em larga escala da IoT? Neste aspecto, existe alguma especificidade para o caso do Brasil?

Sem contribuição.

10 - Considerando aspectos de gerenciamento da infraestrutura, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

8. SUPORTE A APLICAÇÃO E SERVIÇOS

Objetivo: mapear as questões relevantes nesta camada que provê abstrações de alto nível para uma ampla gama de dispositivos de internet das coisas, acelerando o desenvolvimento de aplicações de alto valor agregado através de serviços que contemplam: Gerenciamento de dispositivos; Padronização de API para monitoramento e atuação em dispositivos; Configuração de dispositivos virtuais (dispositivos cujo estado atual é o resultado da agregação ou transformação de estado de múltiplos dispositivos físicos); Geração de



Consulta Pública

Plano Nacional de IoT

eventos e alertas de valor agregado; Gerenciamento de histórico de eventos e comandos, entre outros. Além de propiciar a interoperabilidade entre aplicações.

1 - A interoperabilidade é a capacidade de um sistema ou aplicação de se comunicar de forma transparente (ou o mais próximo disso) com outro sistema ou aplicação (semelhante ou não). Pode-se dizer que a interoperabilidade pressupõe a comunicação entre sistemas e, conseqüentemente, troca de dados. No contexto do desenvolvimento e implantação da tecnologia IoT, qual é a importância de haver ou não interoperabilidade entre as aplicações? Justifique e dê exemplos, se possível.

Contribuição Oi: A interoperabilidade é fundamental para a sustentabilidade de qualquer sistema de comunicação e determinante para o IoT, no sentido de dar a escala ao serviço e permitir a sua evolução.

A título de exemplo, no sistema de comunicação móvel existem de um lado os fornecedores de equipamentos e de outra parte as prestadoras que utilizam esses fabricantes, conforme sua estratégia. Contudo, o serviço final ao cliente é definido por regras de negócio e de ordem regulatória, ou seja, não são as tecnologias dos fabricantes que definem o serviço a ser prestado. Esse ambiente traz consigo os benefícios da economia de escala que são fundamentais para um menor custo da cadeia de valor. Adicionalmente, esse ecossistema oferece uma maior segurança para os clientes finais que sabem que estão amparados por um sistema que se renova constantemente.

Dentro de uma vertical IoT, no aspecto de dispositivos e infraestrutura de redes, a importância da interoperabilidade fica clara. O serviço pode funcionar num contexto (elementos de rede e dispositivo de um mesmo fornecedor) e em outro não (elementos de rede e/ou dispositivos pertencentes a fornecedores distintos).


Entretanto, para a combinação de duas verticais ou mais no âmbito das aplicações, a ausência de interoperabilidade pode significar a perda de evolução e sinergia na utilização de capacidades e serviços.

Por exemplo, para casa conectada/inteligente, pode-se desenvolver um serviço de segurança combinado com câmeras (provisto pela rede 3G) e telemetria/cadeado (provisto por uma rede LoRa). Muito embora as tecnologias sejam distintas, eventualmente em duas verticais e serviços, a sua combinação cria uma outra proposição de valor e um novo serviço de segurança. A garantia que este serviço funcione está no controle através do gerenciamento de API abertas nas duas infraestruturas e aplicações desenvolvidas.

2 - As aplicações IoT podem ser desenvolvidas sem necessariamente utilizar a camada de suporte a aplicações e serviços. Na sua visão essa camada será comum na maioria dos casos de uso ou será considerada como um overhead desnecessário? Se sim, quais as principais facilidades que tal camada deveria ter? Quais oferecem oportunidades para desenvolvimento local? Justifique e dê exemplos.

3 - Já existem diversas ofertas comerciais de soluções para a camada de suporte a serviços e aplicações de IoT de código fechado e algumas iniciativas de código aberto. Na sua visão, qual destes dois modelos terá maior adoção?

Contribuição Oi: No âmbito das aplicações, é importante que haja ao menos um nível de transparência para garantir que as interfaces através de API (*Application Program Interface*) com a rede e infraestrutura sejam acessíveis para o desenvolvimento dos serviços em múltiplas plataformas e operações. E ainda, como acontece hoje, há uma tendência de que esta arquitetura e API sejam de *software* aberto (*Open Source*), sem a necessidade de políticas especiais, para viabilização de ambiente colaborativo necessário para a consolidação desta indústria no primeiro momento.



Consulta Pública

Plano Nacional de IoT

4 - Na sua visão, todas as funcionalidades desejáveis para a camada de suporte a aplicações e serviços deveriam ser providas por uma única solução? Caso contrário, como você vê a interoperabilidade entre soluções?

Contribuição Oi: Não, porém a padronização é necessária, pois se traduz num ordenamento tecnológico para que agentes econômicos da indústria tenham visibilidade dos esforços de desenvolvimento e investimentos. Para os dispositivos e rede, a padronização traz escala e custos compatíveis com os modelos para exploração do negócio. Estima-se que o custo dos dispositivos para algumas verticais será abaixo de 5 dólares para viabilização do seu modelo. Nesse sentido, escala é importante e só é atingida através de padronização aberta para uma ampla oferta de múltiplos fornecedores na indústria e a garantia de interfuncionamento para empresas e consumidores.

5 - Em geral essa camada se vale de infraestrutura computacional em nuvem. Na sua visão, essa nuvem seria pública, privada ou mista? O quanto IoT será significativa no crescimento deste mercado? Existem oportunidades de oferta nacional de IaaS / PaaS / SaaS para atender as demandas de IoT?

Contribuição Oi: Certamente o desenvolvimento das soluções de IoT será muito importante para o crescimento do mercado de infraestrutura computacional em nuvem, com grande potencial de crescimento e ofertas globais de IaaS/PaaS/SaaS. Entretanto, é importante que os modelos de negócios sejam desenvolvidos livremente, sem restrições ou predefinições sobre nuvem privada ou pública, por exemplo.

6 - Uma das áreas da computação que mais tem evoluído nos últimos 5 anos é *Machine Learning*. Na sua visão que facilidades a camada de suporte a serviços e aplicações deve prover, neste contexto, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.

Sem contribuição.

7 - Qual o impacto do *Machine Learning* para IoT e quais oportunidades existem para o desenvolvimento local?

Sem contribuição.

8 - Além do *Machine Learning*, que outras áreas da computação oferecem oportunidades para desenvolvimento local, no ecossistema de IoT? Que dificuldades devem ser superadas para tal?

Sem contribuição.

9 - No contexto de *analytics*, que facilidades a camada de suporte a serviços e aplicações deve prover, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.

Sem contribuição.

10 - No contexto de manipulação de dados espaço-temporal, onde os dispositivos informam o local e o tempo da informação, que facilidades a camada de suporte a serviços e aplicações deve prover, para viabilizar o desenvolvimento das aplicações? Dê exemplos com base em casos de uso.

Sem contribuição.

11 - Considerando aspectos de suporte a aplicações e serviços, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?



Consulta Pública

Plano Nacional de IoT

Sem contribuição.

9. REDES E TRANSPORTE DE DADOS

Objetivo: Identificar as tecnologias de comunicação para IoT, as soluções com maior potencial para atender os diferentes casos de uso, o melhor uso do espectro de frequência para a conectividade dos dispositivos e questões de adoção de padrões e interoperabilidade.

1 - Uma forma de facilitar a interoperabilidade é o desenvolvimento de soluções em padrões de acesso já consolidados no mercado, como, por exemplo: ethernet, WiFi, Bluetooth, entre outros. Qual a necessidade de desenvolvimento de novos padrões de acesso para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que as tecnologias de acesso já consolidadas apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).



Consulta Pública

Plano Nacional de IoT

Contribuição Oi: Utilizar protocolos consolidados. Para a IoT é necessário que se tenha escala global para ter custos compatíveis com os modelos de negócio.

Alternativamente, para garantir o desenvolvimento da indústria de IoT no Brasil há de se criar um ambiente para a viabilização de investimentos e outras oportunidades. Além dos financiamentos subjacentes às empresas parceiras, há a oportunidade de criação da exploração de novos serviços através do modelo de *crowdsourcing*, conformando novos mercados e economias.

Novos protocolos de comunicação com características específicas voltadas aplicações de IoT já estão sendo desenvolvidos. Tais protocolos priorizam o menor consumo de bateria, a maior cobertura de sinal e barateamento dos custos de *hardware*. O desenvolvimento de soluções deve se focar em aplicações que utilizem os padrões que possuam maior probabilidade de sucesso, tais como aqueles que já utilizam a infraestrutura existente, sob o risco das aplicações desenvolvidas se tornarem rapidamente obsoletas.

2 - Em que pese as tecnologias de acesso que podem ser adotadas na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à prova de futuro e por quê?

Contribuição Oi: Depende da aplicação, mas certamente as tecnologias que usam a solução de captação de energia do ambiente onde estão implantados os dispositivos de IoT merecem destaque.

Com relação ao uso do espectro, a viabilização do 4G em baixas frequências (no que concerne às possibilidades de *refarming*, *phase-out* de serviços obsoletos e estabelecimento de ecossistema completo – inclusive terminais) pode ampliar o alcance do acesso móvel em alta velocidade com menores custos de cobertura, ampliando as possibilidades de aplicações IoT.

Cada vez que surgem novas aplicações para IoT, novos desafios são identificados, haja vista que os dados coletados/providos pelos objetos podem apresentar não conformidades ou inconsistências ou, ainda, serem de diferentes tipos. Desse modo, as aplicações e os algoritmos devem conviver com esses desafios, visando levar o nível de confiança sobre os dados obtidos dos dispositivos da IoT ao máximo.

Novas tecnologias de acesso são necessárias para endereçar a demanda de IoT. Diferente dos serviços tradicionais, IoT apresenta requisitos específicos tais como baixo consumo de energia, ampla cobertura de rede, número elevado de dispositivos conectados simultaneamente, escalabilidade e baixa taxa de dados.

3 - Considerando a questão de interoperabilidade, com respeito a tecnologias do core da rede qual a necessidade de desenvolvimento de novos padrões para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que as tecnologias de core já consolidadas apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).

Contribuição Oi: O core pode ser de qualquer tecnologia de tratamento dos dados, contanto que haja *gateways* de baixo custo para interfacear com as diversas tecnologias de acesso. Não há necessidade de desenvolvimento de novos padrões.

4 - Em que pese as tecnologias de core da rede que podem ser adotadas na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à prova de futuro e por quê?

Contribuição Oi: A virtualização do core pode ser um caminho para suportar o crescimento da capacidade da rede.



Consulta Pública

Plano Nacional de IoT

5 - Considerando a questão de interoperabilidade, com respeito a protocolos qual a necessidade de desenvolvimento de novos padrões para atender as necessidades específicas da IoT? Considere em sua resposta eventuais limitações que os protocolos já consolidados apresentam no contexto de IoT, em função dos diversos casos de uso (IoT para missão crítica e IoT massivo).

Sem contribuição.

6 - Em que pese a multiplicidade de protocolos que podem ser adotados na implantação de um ecossistema de IoT, em sua opinião, quais se mostram mais interessantes ou à “prova do futuro” e por quê?

Sem contribuição.

7 - Na sua visão a IoT irá impactar o core da rede, ou a evolução destas tecnologias atualmente focadas no aumento de *throughput* para suportar serviços como vídeo em alta definição irá também acomodar naturalmente as demandas da IoT? A IoT deverá impactar ou ser impactada por novas tecnologias de core de rede como o SDN (*Software Defined Network*), convergência IP e óptica, dentre outras?

Contribuição Oi: O core da rede pode ser impactado devido ao aumento no volume de sinalização. O core é mais sensível ao aumento de sinalização e à quantidade de clientes conectados simultaneamente do que às altas taxas de transmissão.

8 - Hoje as tecnologias para o acesso de dispositivos IoT (*Wi-Fi HaLow, ZigBee, ZWave, Bluetooth LE, GSM, HSPA, LTE, LoRa, SigFox, LTE-M, NB-IoT, EC-GSM*) se encontram padronizadas ou em vias de. Em sua opinião, quais os principais desafios a serem vencidos no que diz respeito à especificação dessas tecnologias para o desenvolvimento do ecossistema de IoT? Há necessidade de desenvolvimento de aspectos tecnológicos específicos para o Brasil? Há espaço para a indústria nacional desenvolver ofertas no que diz respeito à equipamentos de rede para IoT?

Contribuição Oi: Acreditamos que, para desenvolver uma indústria local com peso relevante, devemos considerar como estratégicos os fabricantes locais de módulos de comunicação e semicondutores para comunicação (3G, 4G, NB-IoT, LTE-M, dentre outros). Estes fornecedores acabam por formar a base para a indústria de Telecom e para a cadeia de valor em M2M e IoT, como um todo. Vale ressaltar, contudo, que não há necessidade de se desenvolver um mercado customizado para o Brasil, com aspectos tecnológicos específicos para o mercado brasileiro.

Nesse sentido, cada uma das aplicações tem uma das tecnologias que melhor a suporta e nesse sentido, faz com que interfaces padrão sejam necessárias. Sem a utilização de interfaces padrão, a implantação de *gateways* é requerida e, geralmente, é muito complexa, fazendo com que tenhamos gargalos para IoT.

Esses gargalos podem ser caracterizados de duas formas: (i) toda informação trocada entre a rede e os objetos inteligentes transita através do *gateway* e (ii) a lógica da Internet remete para que a inteligência do sistema fique nas pontas. Com a implantação de *gateways*, a inteligência da IoT fica no meio da rede, o que vai de encontro aos princípios da arquitetura da Internet.

Temos que em nível mundial a *Internet Engineering Task Force* (IETF) criou dois grupos cujos objetivos é gerenciar, padronizar e levantar os requisitos para as redes de baixa potência (*Low-Power and Lossy Networks - LLN*), o primeiro é o IPv6 in *Low-Power Wireless Personal Area Networks Working Group* (6LoWPAN) cuja competência é padronizar o IPv6 para redes que fazem uso de rádios sobre o padrão IEEE 802.15.4, que, por sua vez, especifica as regras das camadas de enlace e física para redes sem fio pessoais de baixa potência de transmissão e o segundo é o *Routing over Low-Power and Lossy Links Working Group* (RoLL), que padronizará o protocolo de roteamento, que utilizará o IPv6 nos dispositivos com limitações de recursos, sendo que o protocolo

Consulta Pública

Plano Nacional de IoT

IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) já foi definido para esse fim. Este protocolo é o estado-da-arte em roteamento para IoT, o qual constrói uma topologia robusta com mínimo de estados necessários.

9 - Para soluções de conectividade IoT em área ampla (ex. LoRa, UNB, NB-IoT, EC-GSM), as que se baseiam em espectro não licenciado possuem mais ou menos potencial para a ampla adoção em comparação às soluções de espectro licenciado? Considerando-se fatores técnicos, a atual composição das faixas de frequência no Brasil é favorável para o desenvolvimento da IoT? Quais são as alterações sugeridas para fomentar o uso da IoT?

Contribuição Oi: Atualmente as soluções de conectividade são das mais diversas, no que tange a cobertura, bandas de radiofrequências utilizadas, algoritmos, quantidade de bits, etc. Por isso, quando do desenvolvimento, deve-se levar em consideração o que necessitamos e o que queremos e só assim, saberemos qual é a faixa de radiofrequências que oferecerá o melhor desempenho, seja ele técnico, seja ele econômico-financeiro. O espectro não licenciado tem como desvantagem a não proteção contra interferências e, em contrapartida, o espectro licenciado tem como desvantagem o valor e a burocracia para obtenção da outorga e para o licenciamento das estações.

10 - Qual o impacto que o desenvolvimento e implantação do 5G trará para IoT? Em que medida o desenvolvimento da IoT depende do 5G?

Contribuição Oi: O 5G trará uma maior banda por acesso, abrindo caminho para desenvolvimento e adoção de aplicações mais complexas.

11 - Qual a necessidade do conjunto de protocolos TCP/IP, em especial o IP na versão 6 (mesmo com adaptações como o 6LoWPAN), serem suportados nativamente em todos os dispositivos finais? Justifique a sua resposta baseando-se em casos de uso.

Contribuição Oi: O protocolo IPv6 é essencial para o desenvolvimento da IoT, em função do aumento no número de dispositivos.

12 - Considerando aspectos relacionados a redes e comunicação de dados, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Sem contribuições.

10. GATEWAYS E DISPOSITIVOS

Objetivo: mapear as questões relevantes às capacidades e funcionalidades dos dispositivos e gateways, o que inclui entender os elementos que o compõe, como modem, processador, *firmware*, memória, sensores e atuadores, considerando restrições como custo, consumo energético, e largura de banda.

1 - Em sua opinião, quais os principais desafios a serem vencidos no que diz respeito as tecnologias para o desenvolvimento de dispositivos e *gateways* no ecossistema de IoT? Qual o espaço para empresas nacionais atuarem neste segmento?

Contribuição Oi: É preciso incentivar as *design-houses* que demandam especialização e alto grau de conhecimento tecnológico (ex: engenheiros eletrônicos, telecomunicações e computacionais). Além disto, há que se considerar ajustes nos aspectos tributários, que atualmente oneram em demasia toda a cadeia de valor e produção local de equipamentos, além de custos regulatórios, inclusive relacionados à segurança da informação.



Consulta Pública

Plano Nacional de IoT

2 - No que diz respeito a microcontroladores de pequena capacidade e baixo consumo (ex.: ARM Cortex-M, Quark Intel), que arquiteturas se mostram mais interessantes ou à prova de futuro e por quê? Há espaço para desenvolvimento de novas arquiteturas de processadores em âmbito nacional?

3 - No que diz respeito a baterias de longa duração e elementos de captação energia, que tendências tecnológicas são vislumbradas para o curto e médio prazos, e quais seus potenciais impactos no ecossistema de IoT? Há espaço para desenvolvimento de novas tecnologias de sistemas de geração, armazenamento e captação de energia em âmbito nacional?

Contribuição Oi: Elementos de captação de energia do ambiente onde estão implantados os dispositivos de IoT das mais diversas formas são a aposta para o futuro.

Sempre há espaço para o desenvolvimento de novas tecnologias em âmbito nacional, basta haver estímulo e condições apropriadas.

4 - Levando em consideração a multiplicidade de aplicações que podem ser implantadas, quais famílias de sensores (MEMS, PFOE, Ópticos, etc) apresentam maiores oportunidades de desenvolvimento local? Justifique com exemplos.

Sem contribuição.

5 - Os sistemas operacionais embarcados de código livre e demais bibliotecas já se encontram em maturidade suficiente para atenderem os casos de uso de IoT ou ainda há gaps? Considere na sua resposta questões como suporte a novos protocolos de rede e mecanismos de segurança, assim como sua aderência à estratégia de uso/adoção

Contribuição Oi: Sempre há necessidade de uma maior maturidade. A cada *step* superado, serão identificados *gaps* que precisarão ser ultrapassados, requerendo esforços de pesquisa adicionais, como: (i) construção de infraestruturas mais robustas e mais tolerantes a falhas para gerenciar e processar dados provenientes dos vários dispositivos integrados; (ii) maior gerenciamento de incertezas e resolução de conflitos, e; (iii) maior suporte à adaptação de aplicações sob condições dinâmicas do ambiente.

6 - O papel dos Gateways é relevante na maioria dos casos de uso de IoT ou a tendência mais proeminente é os dispositivos terem acesso direto a Internet? Considere em sua resposta aspectos tais como a capacidade de processamento, processamento distribuído, interação entre dispositivos e autonomia para a tomada de decisão.

Contribuição Oi: Depende do desenho de topologia do projeto, porém ambas as situações possuem aplicabilidade e merecem atenção.

7 - Na sua visão, qual tendência é prevalente: dispositivos/gateways dotados de menor capacidade de processamento ou dispositivos/gateways com maior potencial para tomada de decisão de forma autônoma? Justifique com exemplos.

Contribuição Oi: Se a utilização de *gateways* for imprescindível, estes devem ser dotados de menor capacidade de processamento, visando não onerar o meio de rede, deixando para o *core* tomar a decisão, que por vezes será comum a diversos dispositivos.



Consulta Pública

Plano Nacional de IoT

8 - Em relação aos protocolos de comunicação entre dispositivos, quais dos protocolos disponíveis são à prova de futuro? Neste contexto, qual é o nível de maturidade necessária à um padrão aberto para que ele alcance a adoção mundial no cenário IoT?

Sem contribuição.

9 - Considerando o volume de dados e os protocolos existentes, quais são os avanços tecnológicos necessários para memórias de Gateways e dispositivos, para que estas atendam as questões de segurança e autonomia demandadas pelas aplicações em IoT?

Sem contribuição.

10 - Qual o potencial dos Smartphones atuarem como Gateways para os dispositivos IoT? Esse cenário será comum? Se sim, em quais casos de uso?

Sem contribuição.

11 - Considerando aspectos relacionados a dispositivos e gateways, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Sem contribuição.

11. SEGURANÇA E PRIVACIDADE

Objetivo: abordar como lidar com as questões relacionadas à segurança geral do ecossistema de IoT, bem como das informações e privacidade dos dados em um ambiente que, a cada dia, estará mais conectado utilizando mais informações potencialmente relacionadas com indivíduos, em nome da melhoria das prestações de serviços, pertinentes as suas liberdades individuais – v.g. localização, saúde, bens adquiridos.

1 - A partir do momento que um dispositivo se conecta à Internet com dados do seu usuário e transmite informações/se comunica com outros dispositivos, várias ameaças surgem:

a) Violação de privacidade: a violação de privacidade é a primeira, mais óbvia. Como o ambiente M2M/IoT pode coletar informações sobre um usuário, alguma outra parte pode se aproveitar disso para prejudicá-lo. É uma ameaça horizontal, ou seja, afeta todas as áreas.

b) Segurança física: segurança física do usuário também entra em risco, uma vez que não é mais preciso ter proximidade física para causar lesões à indivíduos. Para citar uma ameaça possível na área residencial, por exemplo, seria possível provocar um vazamento de gás e explodir uma casa remotamente. Outro exemplo de ameaça possível é provocar acidentes remotamente em carros conectados ou em indústrias automatizadas. Trata-se de uma ameaça horizontal.

c) Ataques distribuídos: a perspectiva é ter bilhões de dispositivos IoT e se pegarmos uma grande parcela deles é possível realizar ataques distribuídos, como por exemplo, um ataque de negação de serviço a uma rede de transmissão e de distribuição de energia. Novamente é uma ameaça horizontal.

d) Perdas financeiras: perdas financeiras podem acontecer através de fraudes em dispositivos IoT. Para citar uma ameaça possível nas áreas residencial e elétrico, seria possível alterar o consumo de uma casa,



Consulta Pública

Plano Nacional de IoT

por exemplo, registrar 100 kW no medidor de energia quando o consumo real foi 1 MW. Trata-se de uma ameaça horizontal.

Nesse aspecto, o trabalho do OWASP (*Open Web Application Security Project*) ilustra perfeitamente a complexidade e a imaturidade do mercado no que se refere à segurança em ambientes M2M/IoT, haja vista as seguintes falhas de segurança:

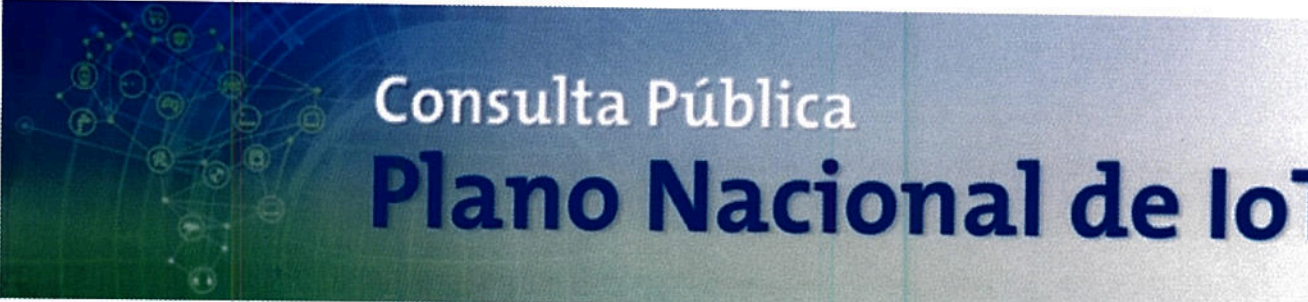
1. Interface *web* insegura
2. Autenticação e autorização insuficientes
3. Serviços de rede inseguros
4. Ausência de transporte seguro
5. Preocupações com a privacidade
6. Interface com a nuvem insegura
7. Interface móvel insegura
8. Configurações de segurança insuficientes
9. Software e firmware inseguros
10. Segurança física deficiente

Essas falhas típicas do mundo pré-IoT serão fonte de ameaças ainda maiores no ambiente M2M/IoT, uma vez que esse novo ambiente é caracterizado por:

1. Grande quantidade de fornecedores de dispositivos, muitos dos quais sem qualquer experiência em segurança.
2. Há dispositivos IoT feitos para serem descartáveis.
3. Existem dificuldades em se realizar atualizações.
4. Controles tradicionais necessitam de adaptação ou não funcionam no escopo de IoT.
5. Há maior superfície de ataque.

Desse modo, fica claro que a segurança e a privacidade devem ser blocos essenciais de qualquer modelo de referência para IoT, sendo necessário uma implementação adequada em todas as camadas, do hardware ao software, das aplicações de negócio e de controle. Portanto, é importante que a segurança e a privacidade sejam tratadas em todas as etapas de desenvolvimento de um produto ou serviço comercializado no mercado, incluindo avaliações sobre a segurança do dispositivo, o software, a gestão de identidades e controle de acesso, a comunicação entre dispositivos e sistemas e o monitoramento e tratamento de incidentes de segurança.

Em linhas gerais, partindo do modelo preconizado pelo ITU, o qual estabelece camadas de Aplicação, Suporte a serviços de aplicações, Rede, Dispositivos e Gestão, há uma camada de capacidade de Segurança que deve ser responsável por:



Consulta Pública

Plano Nacional de IoT

- a) Na camada de aplicação: autorização, autenticação, proteção à integridade e confidencialidade de dados, proteção à privacidade, auditoria de segurança e antivírus;
- b) Na camada de rede: autorização, autenticação, confidencialidade de dados de uso e de sinalização, e proteção de integridade de sinalização;
- c) Na camada de dispositivos: autenticação, autorização, validação de integridade do dispositivo, confidencialidade de acesso, controle e dados e proteção de integridade.

Com base nesse contexto, quais os desafios para a implementação dessas camadas de capacidade de segurança em dispositivos M2M/IoT? Em sua opinião, existe no contexto de M2M/IoT a necessidade de novos mecanismos de segurança, devido a particularidades desses novos ambientes? Se sim, existe oportunidade para desenvolvimento local? Poderia citá-los juntamente com os cenários de uso?

Contribuição Oi: As questões atinentes à segurança das informações e privacidade dos dados dos indivíduos são tratadas de acordo com os processos padrão para gestão e mitigação de riscos da indústria. É importante ressaltar que esses processos ocorrem de forma preventiva e não são estanques.

Os processos para gestão de risco difundidos no mercado atualmente não aguardam a materialização de risco para que sejam tomadas ações. Pelo contrário, uma postura preventiva é essencial para que quaisquer prejuízos, seja ao cliente ou à empresa, não ocorram. Além do caráter preventivo é importante que ações para mitigação de riscos sejam eficientes e ágeis, para que os impactos causados por quaisquer ameaças sejam os menores possíveis.

As práticas de gestão de riscos empregadas no mercado evoluem naturalmente de acordo com as necessidades impostas pelo ecossistema em que o serviço/produto está inserido. Definir padrões de antemão, sem compreender o comportamento e dinâmica das ameaças de segurança pode significar limitar a inovação e evolução dos serviços e produtos em questão e até mesmo dos padrões de segurança a serem utilizados para assegurar a adequada proteção de seus usuários.

A Internet das Coisas pode levar, progressivamente, ao surgimento de um ecossistema distinto daquele que observamos atualmente. Todas as relações que derivam desse ecossistema, por consequência também estão sendo modificados, incluindo a relação das empresas entre si e com seus usuários. Nesse contexto, é natural que o comportamento das empresas, envolvidas com o universo de IoT, para lidar com as ameaças derivadas dessa nova dinâmica, também sejam readaptados. Muitas empresas, principalmente aquelas intensivamente envolvidas com o ecossistema digital, vêm realizando transformações profundas em seus processos de negócio (dentre eles o de gestão de riscos), para se adequar à nova dinâmica, com o mínimo de prejuízo possível.

Em suma, existem desafios para lidar com as ameaças advindas de um novo ecossistema. Os atores de mercado, contudo, estão cada vez mais preparados em termos de conhecimento, tecnologias e ferramentas para implantação e manutenção de medidas de segurança que visem proteger seus usuários e, consequentemente, a sustentabilidade dos negócios.

2 - Quanto a criptografia, embora ela seja técnica fundamental para se manter a segurança e a privacidade em dispositivos M2M/IoT, a grande maioria dos dispositivos possui limitações técnicas e de capacidade de processamento que dificultam a utilização de soluções de criptografia robustas. Desse modo, quais algoritmos e soluções de criptografia devem ser incentivados em dispositivos M2M/IoT para garantir eficiência e segurança no ecossistema?

Contribuição Oi: A criptografia é realmente fundamental e imprescindível para a privacidade dos dados enviados pelos dispositivos IoT. Muitos desses dispositivos são construídos visando baixo consumo de energia a fim de aumentar a vida útil das baterias que os mantêm e, com isso, acabam ficando "enxutos" demais a ponto de dificultar a utilização de soluções criptográficas robustas. Entendemos, que durante a fase de desenho da solução, o poder computacional necessário para suportar protocolos de criptografia seguros e atuais deva ser garantido, assim como a capacidade de atualização e principalmente de randomização dessas chaves.



Consulta Pública

Plano Nacional de IoT

3 - Conceitualmente, o ecossistema de IoT exige a cooperação e compartilhamento de informações entre seus agentes, em especial para se ter uma rápida divulgação de vulnerabilidades de *software* que possam comprometer a segurança de toda a rede. Como desenvolver um ambiente de cooperação entre os agentes do ecossistema de M2M/IoT? Em especial, como prevenir os riscos de ataques de negação de serviço massivos implementados através de redes de dispositivos M2M/IoT?

Contribuição Oi: Toda vez que pensamos em interatividade ou praticidade pensamos em um peso a ser contrabalanceado com a segurança, ou seja, quanto mais interativo menos seguro. A Internet começou exatamente com este conceito, facilitar a comunicação, e hoje é fácil verificar um sem número de ameaças à segurança ali existentes.

Nesse sentido, o desenvolvimento de qualquer solução deve ser feito de forma consciente e focado inicialmente na garantia da confiabilidade e privacidade dos indivíduos. Incansáveis *pentests* e aplicação de *baseline* durante as fases de homologação e desenvolvimento reduzem drasticamente vulnerabilidades e, junto com a educação do usuário quanto à correta utilização destes IoT, se tornam peças chaves para garantir tanto a segurança dos indivíduos que os utilizam quanto dos próprios dispositivos e da Internet como um todo.

4 - No que tange a privacidade e proteção de dados pessoais, além das vulnerabilidades já mencionadas é importante ter em mente que o ecossistema de M2M/IoT poderá potencializar os negócios com *big data*, em especial com empresas interessadas em monetizar bases de dados, seja para fins publicitários ou outras destinações. Essas bases de dados podem possuir dados pessoais individualizados ou dados agregados/anonimizados sobre indivíduos. Nesse cenário, ciente da coleta e comunicação de dados potencializada pelo desenvolvimento do ecossistema de M2M/IoT, qual a abordagem legal, existente ou a ser implementada, necessária para proteger a privacidade e os dados pessoais dos indivíduos? Como deve ser tratada a coleta de dados de sensores IoT? Existem experiências estrangeiras que lidam com o binômio desenvolvimento e proteção à privacidade dos indivíduos no ecossistema M2M/IoT? Os projetos de lei em trâmite no Congresso Nacional referentes a proteção de dados pessoais (PL 4060/2012 da Câmara dos Deputados, PL 330/2013 do Senado e PL 5276/2016 de Autoria do Executivo) possuem regras adequadas para lidar com esse cenário e ao mesmo tempo possibilitar o desenvolvimento do ecossistema de M2M/IoT? É possível desenvolver dispositivos M2M/IoT com “políticas de privacidade” embarcadas, de modo a possibilitar a comunicação entre dispositivos com políticas compatíveis?

Na sua contribuição, considere os seguintes perfis de indivíduos:

- Que admitem o uso de dados dos dispositivos associados à sua identidade;
- Que só admitem o uso de dados do dispositivo se desassociados de sua identidade;
- Que não admitem o uso de dados do dispositivo associados e desassociados de sua identidade.

Contribuição Oi: Para proteger a intimidade do usuário, seja em qualquer um dos perfis citados, deve-se utilizar o ordenamento jurídico vigente, o qual protege o indivíduo de todas as formas, inclusive no que se refere à intimidade, privacidade, segurança.

Deve-se ter claro que as normas já vigentes, principalmente a Constituição Federal trazem princípios e garantias fundamentais, que protegem o indivíduo nas questões atinentes à segurança, intimidade, privacidade, de modo que o indivíduo estará amplamente amparado nas mais diversas situações.

Consulta Pública

Plano Nacional de IoT

Portanto, o arcabouço normativo existente atualmente já contempla dispositivos que asseguram de maneira equilibrada e eficiente a segurança dos cidadãos em ambientes digitais. A existência de um número excessivo de normas e regras que regem as relações nesse ecossistema pode representar uma limitação do processo evolutivo da economia digital e das inovações que podem trazer benefícios para toda a sociedade, ao mesmo tempo em que não significam melhor proteção ao direito dos indivíduos.

No mais, os usuários receberão toda a informação necessária para o uso das ferramentas e soluções, até mesmo porque o próprio mercado possui o interesse de garantir aos seus usuários a segurança adequada, bem como adquirir e manter a sua confiabilidade. Assim, eventual uso abusivo da IoT será eliminado naturalmente, seja pelos usuários, seja pelo Judiciário ou pelas próprias empresas, com a auto-regulamentação.

Assim, entendemos que o arcabouço normativo atual atende a necessidade individual de segurança, ao mesmo tempo em que assegura a possibilidade de inovação e desenvolvimento de novos negócios e produtos. Qualquer lei ou regulamentação adicional que vier a surgir deve ter em vista que a criação de normas limitadoras pode ferir um dos principais valores fomentados pela economia digital que é a liberdade, e por isso deve adotar um caráter mais principiológico.

5 - Para se criar um ambiente de inovação disruptivo, algumas premissas devem ser atendidas, como o não confinamento de recursos e a liberdade de aplicação de dados, por exemplo. Estas tratam, respectivamente, do uso de um mesmo dispositivo e de informações para fins diferentes dos originalmente previstos. Dentre elas pousam questões de segurança sobre as duas primeiras premissas.

Vamos explicar seus significados:

Os recursos não podem estar confinados. Não confinar recursos significa utilizar um mesmo dispositivo para aplicações diversas. Por exemplo, a mesma câmera que monitore a segurança nas ruas também pode medir iluminação, otimizar tempo de semáforo por contagem de carros em uma via, pode estar acessível ao cidadão para monitorar seu carro estacionado, existência de vaga de estacionamento, presença de taxi livre ou mesmo para verificar se um ônibus se aproxima do ponto para o qual alguém se desloca.

Deve haver liberdade na aplicação dos dados, sem que isso implique em violações a privacidade e aos dados pessoais dos indivíduos. Um equipamento monitor de pressão arterial é utilizado com frequência para verificação de doenças coronarianas. Os dados são utilizados apenas por seu médico e depois descartados. Ocorre que pode haver diversos outros indivíduos interessados no conjunto de informações cardíacas agregadas e anonimizadas da população e, por isso, dispostas a oferecer contrapartida pela informação, o mesmo sendo válido para centros de pesquisas e universidades para elaboração de estudos científicos. Entretanto, a mesma informação poderia vir a ser utilizada por seu plano de saúde, sua seguradora implicando em graves violações a privacidade e proteção de dados pessoais dos indivíduos.

Neste contexto, questiona-se:

- Quais os limites de segurança e privacidade na premissa de não confinamento de recursos para que seja fomentado o ambiente de inovação?

Contribuição Oi: Os limites de segurança e privacidade devem ter como premissa assegurar o direito individual a segurança e, portanto, evitar abusos que o firam. E para isso não há necessidade da criação de quaisquer regras que visem formatar as ações dos agentes de mercados responsáveis pela gestão dos dados dos usuários. Ressaltando a possibilidade de os usuários anuírem com a disposição de seus dados pessoais, respeitando o direito à informação.

Consulta Pública

Plano Nacional de IoT

O estabelecimento de um arcabouço normativo restritivo e invasivo, além de não assegurar o adequado nível de segurança aos indivíduos, pode rapidamente se tornar obsoleto em um mercado de rápida evolução como é o de tecnologia da informação. Além disso, tem enorme potencial de limitar o processo de inovação e de evolução natural da economia digital.

Um bom arcabouço normativo para qualquer atividade relacionada ao mundo digital é aquele que direcione os provedores de produtos/serviços a adotarem medidas para assegurar o nível adequado de segurança a seus usuários, sem, no entanto, ceifar iniciativas de inovação. São, portanto, normas baseadas em princípios mais do que em regras.

Além disso, é preciso que referido arcabouço normativo leve em consideração as características específicas dos dados a serem coletados e tratados, em especial o fato de serem dados anônimos, isto é, dissociados de seus titulares.

- Como fomentar um ambiente de compartilhamento de informações de modo a aprimorar os padrões de segurança em IoT?

Contribuição Oi: Em conformidade com os princípios e garantias constitucionais e legislação vigente. Além disso, a participação em fóruns de discussões e alianças internacionais fará com que o país acompanhe a evolução do tema nos centros de referência internacionais.

- Quais padrões e modelos de anonimização de dados devem ser implementados de modo a possibilitar o não confinamento de dados em IoT?

Contribuição Oi: Deve-se esclarecer que dados anonimizados não estão sujeitos à proteção de dados pessoais, uma vez que, após a utilização de técnicas de anonimização, o novo dado gerado não identifica individualmente uma pessoa.

E caso um agente econômico não utilize de técnicas adequadas e robustas para a anonimização dos dados pessoais dos usuários de IoT, deverá responder pelos prejuízos.

Contudo, nos casos em que exista a possibilidade de não anonimização de dados pessoais, tal informação deve ser previamente divulgada e o usuário, para a utilização da aplicação, deverá receber todas as informações e aceitar os termos de privacidade específicos.

- Até que ponto a premissa de liberdade na aplicação dos dados pode ser utilizada de maneira virtuosa para o conjunto da sociedade?

Contribuição Oi: A premissa de liberdade na aplicação dos dados pode ser utilizada de maneira virtuosa no processo de inovação e criação de soluções, sejam elas produtos ou serviços, para a resolução de problemas do dia-a-dia. Atualmente, a inovação é não apenas um processo virtuoso para efeitos comerciais, mas também para efeitos sociais. Inúmeros projetos de inovação/empreendedorismo social são desenvolvidos, com o intuito de trazer benefícios à sociedade, que não podem ser fornecidos pelo Estado – por quaisquer questões que sejam.

Obviamente, com intuito de atingir objetivos virtuosos, as iniciativas de inovação devem estar de acordo com os princípios e garantias constitucionais e com base na legislação já vigente, principalmente o princípio da isonomia entre os diversos atores da cadeia do ecossistema do M2M/IoT.

6 - Existem outros fatores de Segurança e privacidade que possam criar barreiras ao desenvolvimento do ecossistema de IoT?

Contribuição Oi: Existem inúmeros fatores que podem significar barreiras para o desenvolvimento e evolução de qualquer ecossistema digital, inclusive o do IoT. Grande parte dessas barreiras diz respeito a obstáculos de mercado que surgem ao longo da criação e aprimoramento de produtos e serviços específicos. Essas barreiras, contudo, são naturalmente superadas com a evolução do conhecimento e das tecnologias, ou seja, as forças de mercado, naturalmente, empurram os atores para o desenvolvimento de soluções aos problemas encontrados.



Consulta Pública

Plano Nacional de IoT

Há, contudo, barreiras artificialmente criadas. É possível dizer que essas barreiras significam uma ameaça maior do que as anteriores a evolução do ecossistema, pois exigem mais esforço e recursos para que sejam superadas. Esse é justamente o caso do excesso de regras (regulamentação e burocratização) de um sistema.

Esse fator nocivo é extremamente prejudicial ao processo de inovação, parte essencial a evolução de qualquer mercado, dado que colocam, de antemão, regras que limitam qualquer ação virtuosa que vise dar solução a problemas existentes.

Num mercado em constante e rápida evolução e em que "não se sabe o que surgirá de novo amanhã", criar regras que buscam formatar as ações dos agentes, sem sombra de dúvidas, é a principal barreira ao desenvolvimento.

12. PAPEL DO ESTADO

Objetivo: identificar oportunidades e desafios no papel do estado, no que diz respeito ao modelo de governança de IoT no Brasil e ao direcionamento de modelos de negócio, com o objetivo de alavancar o desenvolvimento do ecossistema de M2M/IoT.

1 - Diante de um cenário novo e ainda incerto, qual deveria ser o papel do Estado no desenvolvimento do ecossistema de M2M e IoT?

Contribuição Oi: Dado o atual estágio de maturidade dos ecossistemas de M2M e de IoT, acreditamos que o Estado precisa estar empenhado em promover incentivos, que podem materializar-se, por exemplo, na forma de:

- Racionalização da carga tributária, por meio da isenção ou da redução de tributos;
- Busca da eficiência nos processos administrativos, reduzindo burocracia na medida do possível e viabilizando maior agilidade para Pesquisa, Desenvolvimento, Produção e Comercialização;
- Constituição de linhas de financiamento às iniciativas acadêmicas e do setor privado, para desenvolvimento e produção de soluções integradas ou de tecnologia de base;
- Incentivo à Pesquisa & Desenvolvimento.

Adicionalmente, destacamos que o presente momento requer que o arcabouço regulatório favoreça a segurança jurídica e que seja capaz de atrair investimentos do setor privado; deve-se evitar, portanto, a adoção excessiva de normas e a imposição de obrigações onerosas, o que amplificaria as incertezas do cenário. Isto porque, dependendo da intervenção estabelecida neste estágio, o desenvolvimento poderia ser onerado financeiramente, barreiras potencialmente desnecessárias poderiam restringir iniciativas de Inovação e, conseqüentemente, poderia haver distanciamento entre a realidade nacional e o cenário mundial. Este descompasso pode privar o Brasil de maximizar a captura de valor e de se beneficiar das oportunidades apresentadas pelo crescimento desse ecossistema em âmbito global.

Para a expansão do ambiente IoT no Brasil, é importante atuar para garantir a isenção ou redução da Taxa de Fiscalização de Instalação (TFI) e da Taxa de Fiscalização de Funcionamento (TFF), que compõem o FISTEL, caso entenda-se que os objetos a serem conectados à Internet sejam considerados estação de telecomunicações (conjunto de equipamentos ou aparelhos, dispositivos e demais meios necessários à realização de telecomunicação, seus acessórios e periféricos, e, quando for o caso, as instalações que os abrigam e complementam, inclusive terminais portáteis)

Vale mencionar, ainda, a existência de Projetos de Lei que tratam da parceria público-privada (PPP) e que estão sendo discutidos no Congresso Nacional. Vislumbra-se, assim, uma oportunidade para se garantir que o tema IoT seja tratado nesse ambiente. Além disso, há, atualmente, 33 proposições em tramitação no Congresso Nacional sobre a proibição de oferta de planos e serviços de banda larga fixa. Nesse sentido, é preciso avaliar o impacto de eventual proibição no ambiente IoT para então se avaliar estratégias de atuação.



Consulta Pública

Plano Nacional de IoT

Em paralelo, consideramos importante acompanhar qualquer iniciativa em discussão na esfera legislativa que gere impacto, em algum nível, no ecossistema.

2 - Em que áreas ou fases o Estado deverá exercer uma coordenação das ações para desenvolvimento do ecossistema de IoT?

Contribuição Oi: O Estado deve estar atento ao desenvolvimento do ecossistema, agindo à medida que as deficiências se apresentem. Entretanto, sua atuação – seja no papel de coordenação ou não, conforme cada situação – precisa evitar interferências desnecessárias ou desproporcionais (sob os riscos já elencados na resposta à questão 1).

A coordenação, quando exigida pelas circunstâncias, deve visar ao equilíbrio de interesses sem prejuízo às iniciativas de desenvolvimento e de inovação.

3 - Seria interessante a atuação do Estado na formação de novos mercados de nicho para IOT? Por quê? Exemplifique.

Contribuição Oi: A formação dos mercados de nicho para IoT decorrerá da dinâmica inerente ao desenvolvimento do próprio ecossistema. Novas soluções e aplicações tendem a emergir à medida que a tecnologia evolui e que as pesquisas do setor (tanto no âmbito acadêmico quanto empresarial) progridem.

4 - Cabe ao Estado desenvolver ou adaptar instrumentos fiscais visando o desenvolvimento e comercialização de produtos que se encaixam nas distintas camadas da IoT, conforme arquitetura apresentada? Por quê? De que forma os instrumentos atuais podem obstruir o desenvolvimento?

Sem contribuição.

5 - Existem questões sobre como o Estado assegura a preservação dos direitos de propriedade intelectual (patentes e registros de software) que desfavorece o desenvolvimento da IoT, no Brasil?

Sem contribuição.

6 - Existem barreiras de entrada que dificultam a localização da produção de soluções tecnológicas para IoT, no Brasil? Se sim, exemplifique.

Contribuição Oi: Dentre as principais barreiras de entrada, podemos citar:

- Insegurança jurídica sobre determinados aspectos do ecossistema, inviabilizando o desenvolvimento de soluções (por exemplo, por consequente elevação da carga tributária ou por imposição de obrigações onerosas desproporcionais);
- Gaps de qualificação técnica e acadêmica da força de trabalho;
- Processos burocráticos em diversos trâmites, como certificação, licenciamento, permissões, dentre outros;
- Eventual obrigatoriedade de adoção de padrões tecnológicos incompatíveis com a experiência internacional;
- Fomento insuficiente à Pesquisa & Desenvolvimento;
- Atual estrutura tributária do setor de Telecomunicações.

7 - A Internet das Coisas vai afetar diferentes setores, de diferentes formas, em diferentes momentos. Os governos irão se beneficiar enormemente. A Cisco identifica quatro potenciais alavancas de economia no setor público: produtividade dos funcionários, redução de custos, melhoria da experiência do cidadão e aumento das receitas. A análise estima que mais de 25% de um valor estimado de US\$ 19 trilhões do valor do mercado global disponível até 2022 pode ser realizado pelo setor público. Para usufruir desses

Consulta Pública

Plano Nacional de IoT

benefícios – e ao mesmo tempo fomentar o mercado, dando escala aos fornecedores de soluções –, o Governo pode se tornar um demandante de soluções que utilizem a Internet das Coisas.

8 - Os municípios são os espaços onde os benefícios com implantação do ecossistema de M2M/IoT são descritos como os mais imediatos. Os estados, por sua vez, podem usufruir desse ambiente na melhoria da prestação dos seus serviços. Já a União tem desafios, sobretudo logísticos, em que a aplicação de tecnologia e inteligência de dados é fundamental para tornar mais eficientes setores como energia, transporte e saúde, por exemplo.

9 - Quais são as principais áreas de aplicações de IoT que podem melhorar os serviços públicos ou a gestão pública nas diferentes esferas?

Sem contribuição.

10 - Ainda nesse contexto, que problemas específicos você sugeriria que o Governo resolvesse por meio dessas novas tecnologias e quais seriam as áreas prioritárias de atuação e os meios de contratação existentes mais adequados?

Contribuição Oi: As áreas que devem ser prioritárias são:

- Modernização da frota de veículo com tecnologia embarcada de gestão de frotas;
- Programa nacional para melhoria de iluminação pública;
- Plano nacional para modernização dos medidores de energia e água;
- Modernização dos semáforos com tecnologia comunicação;
- Soluções *e-health* (prontuários integrados digitais, cirurgia remota, etc.);
- Soluções de *e-government* (integração digital das plataformas governamentais);
- Gestão de transportes (controladores de velocidade por GPS para os veículos da frota pública);
- *Smart Devices* (gestão digital de residências e prédios comerciais);
- Soluções de segurança;
- Educação Digital;
- Agricultura;
- Pecuária de leite e de corte, dentre outros.

11 - No âmbito da atual legislação, há dificuldades para a aquisição pelos Entes da Federação das soluções que utilizam as tecnologias de Comunicação M2M e Internet das Coisas? Justifique preferencialmente com detalhes e exemplos.

Contribuição Oi: Entendemos que não há dificuldade, apenas não há incentivo. Para aumentar o incentivo na contratação desses serviços, a Administração Pública deve se preocupar em especificar o produto/serviço objeto da licitação e estabelecer a qualidade pretendida. Esse ponto é muito importante para que não ocorra o *lock in*, ou seja, a determinação de uma determinada tecnologia para atender o Edital, uma vez que o mesmo deve ser e agnóstico à tecnologia.

Também poderiam ser considerados modelos de negócio que permitissem a implantação de soluções e a sua posterior remuneração a partir de ganhos de produtividade (*success fee*). Tais modelos poderiam acelerar a contratação e a implantação de soluções M2M/IoT no setor público.

12 - Na busca pelo desenvolvimento do ecossistema de IoT, qual deveria ser o papel das parcerias público-privadas (PPPs)?

Contribuição Oi: A PPP é uma forma de trazer investimentos privados em infraestrutura, uma vez que o governo não tem condições de fazê-lo sozinho.

Consulta Pública

Plano Nacional de IoT

É necessário garantir que seja desenvolvido um modelo nas PPP no qual o negócio em si traga garantias financeiras/jurídicas para que a iniciativa privada possa investir. Também poderiam ser considerados modelos de negócio que permitissem a implantação de soluções e a sua posterior remuneração a partir de ganhos de produtividade (*success fee*). Tais modelos poderiam acelerar a contratação e a implantação de soluções M2M/IoT no setor público.

Além disso, é importante que a atuação da Câmara de IoT garanta que esses processos não tenham como premissa a definição de tecnologias ou de rede de comunicação específicas nos editais (ex: somente pode RF Mesh). Há exemplos de alguns editais que seguiram o caminho de adotar uma determinada tecnologia e posteriormente foram revistos por não conseguirem atender os seus objetivos e, por consequência, não avançar como pretendido. Seria interessante a existência de Editais "referência", gerados pela Câmara IoT, que poderiam ser adotados pelo poder público, garantindo qualidade dos serviços contratados. Dessa forma, reduz-se o risco para o governo de não trazer a melhor solução (tecnicamente e economicamente) para a sociedade.

Adicionalmente, destacamos o Projeto de Lei no 4.847/2016, atualmente em tramitação no Congresso Nacional, que "dispõe sobre a instituição, no âmbito da União, de parceria público-privada visando o desenvolvimento de tecnologias de informação e comunicação para emprego na área de segurança pública e aplicação na transformação das áreas urbanas em cidades inteligentes em todo o território nacional". Trata-se de uma iniciativa positiva no sentido de promover o desenvolvimento de projetos de *Smart Cities* e de suas respectivas soluções tecnológicas, suportados por parcerias entre o Poder Público e o setor privado.

13 - De que forma a burocracia brasileira pode ser uma barreira ao desenvolvimento de IoT?

Contribuição Oi: A burocracia torna-se uma barreira a medida em que:

- Adota procedimentos complexos e demandam prazos longos para conclusão;
- Submete solicitações e projetos à aprovação de múltiplas instâncias da Administração Pública, aumentando a quantidade de interlocutores, dificultando o rastreamento dos processos e a preservação de consistência das informações;
- Estabelece restrições em demasia ao processo de Inovação;
- Não prevê flexibilidade de tratamento para novas situações, decorrentes da dinâmica de um mercado em processo de formação.

14 - Quais são atualmente os países de referência em políticas públicas de IoT?

Sem contribuição.


15 - De que forma as soluções demandadas pelo governo devem ser especificadas, buscando, na medida do possível, aproximar a demanda brasileira da que seria uma demanda em um mercado internacional, facilitando uma posterior exportação dos bens e serviços?

Contribuição Oi: A Administração Pública deve se preocupar em especificar o produto/serviço objeto da licitação e estabelecer a qualidade pretendida. Esse ponto é muito importante para que não ocorra o *lock in*, ou seja, a determinação de uma determinada tecnologia para atender o Edital, uma vez que o mesmo deve ser e agnóstico à tecnologia.

Em termos de desenho de especificações funcionais, pode-se recorrer a estudos e *benchmarks* (nacionais e internacionais), visando à captação de aprendizados.

16 - Considerando a atuação do Estado no ecossistema de IoT, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Sem comentários.



Consulta Pública

Plano Nacional de IoT

13. ASSUNTOS REGULATÓRIOS

Objetivo: Identificar as possíveis questões regulatórias (incluindo questões fiscais e tributárias) que necessitam de criação ou alteração de legislação ou regulamentos para que os negócios que envolvam comunicação M2M/IoT possam se desenvolver.

Os sistemas regulatórios vêm apresentando expressiva expansão nos últimos anos, em diferentes áreas de atuação estatal de diversos países que buscam crescimento econômico sustentável. Um Sistema de Gestão Regulatória robusto tem como foco a regulação de alta qualidade, que não distorce desnecessariamente a concorrência; é simples, proporcional, consistente, transparente e atende aos objetivos de política pública a que se destina com o menor custo possível para a sociedade e considerando as novas tecnologias, tais como a Internet das Coisas. Diante deste cenário, considere em sua contribuição os aspectos relacionados a seguir:

- Estágio atual do sistema regulatório do Brasil, no que tange à Internet das Coisas;
- As lacunas na legislação brasileira que podem constituir desafios à difusão de IoT no país;
- Disposições legais ou regulamentares que consistam em barreiras à entrada e que prejudiquem modelos de negócio IoT; e
- O nível de regulação adequado para a rápida adoção e massificação da tecnologia IoT no Brasil.

Segundo o Decreto n. 8.234/2014, são considerados “sistemas de comunicação máquina a máquina os dispositivos que, sem intervenção humana, utilizem redes de telecomunicações para transmitir dados a aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes”. As atividades inerentes a um sistema IoT, de ponta a ponta, abrangem tantos serviços de telecomunicações quanto serviços de valor adicionado (“SVA”), nos termos da Lei Geral de Telecomunicações (Lei n. 9.472/97 – LGT), assim definidos:

- Serviços de telecomunicações como o “conjunto de atividades que possibilita a oferta de telecomunicação”, entendendo-se, por telecomunicação, a “transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza” (LGT, art. 60);
- Serviços de Valor Adicionado (SVA) como a “atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações” (LGT, art. 61)

Por exemplo, os serviços de Tecnologia de Rastreamento e Monitoramento veicular, são compostos por: (i) um serviço de telecomunicações que dá suporte à conexão entre os equipamentos embarcados nos veículos; e (ii) um serviço de valor adicionado correspondente ao rastreamento propriamente dito e análise dos dados gerados pelos equipamentos embarcados nos veículos.

As dúvidas surgem quando a comunicação não fica restrita à IoT, permitindo adicionalmente o uso de serviços de telecomunicações pelos proprietários das “coisas”. Partindo do exemplo anterior, seria o caso de um sistema de rastreamento que também disponibilizasse a conexão à internet para comunicação do usuário do veículo com outros usuários dos serviços de telecomunicações. Nesse caso, a empresa de



Consulta Pública

Plano Nacional de IoT

Tecnologia de Rastreamento e Monitoramento atuaria como uma revendedora de serviço de telecomunicações, o que demandaria a obtenção das autorizações necessárias junto aos órgãos competentes.

Nesse contexto, questiona-se:

1. Esse enquadramento regulatório é adequado? Ele traz problemas ou limitações para os sistemas IoT?

Contribuição Oi: Do ponto regulatório, é essencial, para o desenvolvimento desse serviço no país, a criação de um ambiente que seja mais propício para os investimentos e as relações contratuais, onde o livre mercado seja a regra.

O nível de regulação adequado para a rápida adoção e massificação da tecnologia IoT no Brasil é a auto regulação privada, uma vez que no nosso ordenamento jurídico já existem todas as normas necessárias para as negociações que envolvam comunicação IoT. Além do mais, não há necessidade de regulamentar toda e qualquer relação e contratação para que se tenha um controle efetivo dessas situações. No mais, o excesso de regulamentação prejudica e onera não só as empresas, como também toda a cadeia de fornecimento, onerando, em última análise, o usuário final.

Dentro desse espírito e com o intuito de se estabelecer meios para o desenvolvimento desse mercado no Brasil, entendemos que existem duas frentes a serem tratadas:

A primeira refere-se a uma revisão tributária sobre a prestação do serviço. Em primeiro lugar, cabe esclarecer que na camada de rede de telecomunicações verifica-se a existência de diversas tecnologias de IoT e no aspecto tributário vemos que deve ser adotado o princípio de isonomia de tributos com objetivo de igualdade de condições entre os diferentes serviços. Assim sendo, serviços IoT, devem receber tratamentos já estendidos para os produtos M2M, ainda que verificado algum elemento mínimo de intervenção humana.

Adicionalmente, é essencial que os formadores de políticas públicas compreendam que os serviços de M2M e de IoT tem como característica básica o baixo consumo de dados, que por consequência geram uma receita por usuário, ARPU, significativamente inferior aos demais serviços prestados pelas empresas. Nesse sentido, ressalta-se que quando evoluímos para as novas tecnologias mais aderentes ao mercado de IoT, temos novas redes voltadas a atender a demanda de comunicação em banda estreita, onde os requisitos são: baixo consumo de energia; ampla cobertura de rede e alto volume de dispositivos conectados por estação rádio base; e o pouco volume de dados trafegados. Esses requisitos definem o conceito que se chama LPWA. Dentro desse conceito, a tendência é que o custo unitário da conectividade varie em função da quantidade de mensagens enviadas diariamente por dispositivo, tendo como objetivo o menor custo de conectividade. Diante disso, é fundamental que o modelo tributário relativo ao FISTEL (TFI/TFF) seja revisto, uma vez que o atual arcabouço regulatório (FISTEL M2M) deverá ter um peso excessivo na composição da conectividade nesse conceito. Um caminho que pode ser trilhado é estabelecer um percentual relativo ao serviço prestado.

A outra frente a ser tratada deve ser no campo regulatório, onde deverá haver uma garantia na isonomia tributária para os serviços de IoT independentemente da radiofrequência utilizada, uma vez que os tributos são barreiras ao desenvolvimento de novos serviços desse segmento. Alternativamente, propor a alteração da Resolução nº 506/08 (art. 3º), de modo que a ANATEL possa incluir, por intermédio de um Ato, novas estações de radiocomunicação na lista de equipamentos de radiação restrita isentas de cadastramento ou licenciamento para instalação (pagamento de TFI) e funcionamento (pagamento de TFF).

2. Seria mais adequado haver outro enquadramento regulatório – v.g. considerar todas as atividades compreendidas como serviços de telecomunicações ou SVA? Caso positivo, identificar qual seria e se haveria (ou não) necessidade de alteração regulamentar ou legislativa.

Contribuição Oi: Devido às suas características, o IoT pode ser definido como um arranjo complexo de produtos e serviços, utilizando, como subsídio, os serviços de telecomunicações.



Consulta Pública

Plano Nacional de IoT

3. A definição de IoT presente no Decreto n. 8.234/2014 é suficiente e adequada ou ela impede o desenvolvimento de alguma atividade?

Contribuição Oi: O fato do conceito de intervenção humana não estar claro no arcabouço regulatório, acaba por gerar insegurança regulatória para o setor e, por conseguinte, impede o desenvolvimento de alguns serviços essenciais para a sociedade. Deve ficar estabelecido que se um serviço é capaz de ser realizado de forma automática, entre as máquinas, mesmo que haja uma redundância manual, realizada pelo homem, como por exemplo, para relatar uma emergência, como nos casos hospitalares, de frota ou de elevadores, não há de se falar em intervenção humana, ou seja, o serviço prestado não deixa de ser IoT.

Dentro desse escopo, existem diversos serviços que tem alta demanda e que são de certa forma, cada vez mais essenciais, como aqueles que apoiam, por exemplo, pacientes com doenças crônicas e que se utilizam de um baixo volume de dados e que deixam de ser prestados ou cobrados de uma forma racional pela inviabilidade econômica resultante da alta carga tributária, uma vez que podem incorrer em algum tipo de intervenção humana, de forma pontual. Nesse contexto, existe a necessidade de se compreender que a intervenção humana é inerente ao IoT, e o que deve ser esclarecido é o uso pontual de uma situação de redundância, emergência ou mesmo crítica, onde necessariamente devem existir níveis aceitáveis de intervenção para uma ou outra situação em que fique caracterizado que o serviço não funciona de forma automática, ou seja, sem a necessidade de uma intervenção humana.

Diante de todo o exposto, é necessária a inserção de forma mais clara, o que deve ser caracterizado intervenção humana, garantindo ao mesmo tempo níveis aceitáveis dessa intervenção, principalmente nos casos de redundância.

4. Há a necessidade de se estabelecer um enquadramento regulatório de acordo com o nível de interação humana nos dispositivos M2M/IoT?

Contribuição Oi: O nível de regulamentação necessita que seja revisto para minimamente se adequar a uma ampla competição, beneficiando a sociedade.

Entre os aspectos para minimização de desequilíbrio na exploração estão as taxas de instalação (TFI) e fiscalização (TFF). Tecnologias, como LoRa e SigFox em implantação no Brasil possuem tratamento tributário vantajoso no que concerne à instalação de infraestrutura e habilitação dos dispositivos (SIM Cards). Em contrapartida, tecnologias equivalentes (LTE-MTC) e baseadas em celular (2G/3G) incidem pesadas taxas de instalação de infraestrutura e dispositivos (SIM Cards). Hoje as prestadoras de serviço que usam o LoRa e SigFox oferecem aos seus usuários valores anuais da ordem de 1 USD por objeto conectado. Impossível para as prestadoras móveis, onde cada dispositivo há pelo menos uma taxa por SIM Card ativado paga anualmente.

Outro aspecto importante é o tratamento de priorização de tráfego, sem ferir a neutralidade de rede, para algumas aplicações de missão crítica: *mHealth*, *Connected Cars*, *Driveless Cars*, etc. Estes tráfegos devem ter marcações adequadas e tratamento com priorização no transporte da rede, sob a pena de causar riscos à saúde e econômicos.

5. A figura do Mobile Virtual Network Operator ("MVNO"), prevista atualmente na regulamentação setorial, deve ser tratada para verificar a necessidade de cobrir eventuais lacunas na atuação dos agentes em sistemas IoT, levando em consideração os impactos na regulação?

Contribuição Oi: O entendimento da Oi é de que o IoT não é um serviço de telecomunicação isoladamente. Um serviço de telecomunicações necessariamente dá suporte ao IoT. Não há de se falar em transbordo de serviço de internet para usuário como revenda de telecomunicação. Ademais, não seria cabível uma autorização ou mesmo credenciamento de uma MVNO para comercializar somente um serviço de IoT, o que acabaria por fragilizar o Regulamento de MVNO e permitir a flexibilização excessiva do arcabouço regulatório, trazendo para o mercado uma insegurança jurídica.

Espera-se no 5G uma ampliação do conceito de exploração de comunicações móveis através de exploração de serviços no regime atacado, como IaaS, PaaS, SaaS, *Network Sharing* etc. Também, será permitida a exploração

Consulta Pública

Plano Nacional de IoT

de serviços através de micro-operadoras. O arcabouço regulatório apresenta limitações para explorações de serviços como estes que virão com o IoT e 5G.

6. Faz sentido ter um arcabouço regulatório específico para IoT/M2M?

Contribuição Oi: Do ponto de vista regulatório, é essencial, para o desenvolvimento desse serviço no país, a criação de um ambiente que seja mais propício para os investimentos e as relações contratuais (segurança jurídica), onde o livre mercado seja a regra. Isso só irá ocorrer com a revisão da legislação – regulatória e tributária - para o serviço.

7. O conjunto de dispositivos que requeiram conectividade deveria ter um arcabouço regulatório próprio, visto que as complexas obrigações das operadoras e os direitos e deveres dos usuários dos serviços de telecomunicações muitas vezes são inconsistentes no cenário de conectividade de máquinas?

Contribuição Oi: Consideramos que não seja possível afirmar que o processo de certificação atual atenda adequadamente à realidade de todos os dispositivos de IoT, dada a grande variedade de equipamentos envolvida (dos mais simples aos mais complexos).

De todo modo, acreditamos que a eventual criação de um arcabouço próprio para disciplinar a certificação de equipamentos de IoT:

- Dependendo do estabelecimento de padrões de mercado (dentre outros, por exemplo, os que estão atualmente em discussão no 3GPP);
- Deva assegurar o cumprimento das normas competentes vigentes, no que couber (como normas de radiação e mitigação de interferências);
- Deva buscar a conformidade com requisitos mínimos de interoperabilidade;
- Deva evitar a adoção de processos demasiadamente burocráticos e/ou desnecessários, sob a pena de retardar e onerar o desenvolvimento de soluções.

8. O eventual roaming internacional permanente (p.ex., chips de dispositivos operando no Brasil mas conectados permanentemente à operadoras de outros países) deveria passar a ser permitido?

Contribuição Oi: Não. As regras devem ser mantidas, uma vez que chips que têm numeração de outros países passam ao largo da regulamentação brasileira, abrindo espaço para possíveis práticas não aderentes ao arcabouço jurídico/ regulatório pátrio.

Assim, a liberação do *roaming* pode gerar impactos negativos para o mercado brasileiro, já que as prestadoras internacionais não responderão por pela prática de eventuais ilícitos e haverá maior dificuldade de rastreamento dos usuários.

Ademais, por definição, *roaming* é uma condição passageira e não definitiva, ou seja, *roaming* é itinerância. Itinerância é um termo com origem no latim, cujo significado está relacionado com o ato de se deslocar constantemente, de percorrer itinerários, de viajar. O termo é associado a tudo aquilo que pressupõe uma mudança constante de lugar.

9. A permissão de utilização comercial das faixas de radiofrequência dos “espaços brancos” (*White Spaces*) seria uma alternativa para a comunicação entre dispositivos M2M/IoT?

Contribuição Oi: A tecnologia de rádio que permite a utilização das faixas de radiofrequência disponíveis (*White Spaces*) ainda se encontra em desenvolvimento, mesmo no exterior. Por isso, parece prematuro se definir sobre a melhor utilização, de modo comercial, destes dispositivos na aplicação de M2M/IoT.

Entendemos que o Órgão Regulador brasileiro deve acompanhar e participar da evolução mundial desta e de outras tecnologias, mantendo a diretriz/recomendação de se utilizar tecnologia padrão, já estabelecidos no



Consulta Pública

Plano Nacional de IoT

mercado internacional, em todas as faixas de radiofrequências licenciadas, de forma que seja garantida o ganho de escala e a redução de custos na implantação de soluções para aplicação na oferta de M2M / IoT no Brasil, sem a necessidade de se desenvolver soluções de padrão fechado e específicas para o País.

Novas faixas serão necessárias para exploração dos serviços IoT e 5G. Hoje observa-se um descasamento entre a agenda internacional no rumo ao 5G com as políticas de destinação da Anatel. Em recentes consultas a Anatel destinou faixas de 60 GHz e 28 GHz para serviços de rádio ponto a ponto e Satélite na banda Ka, que seriam fundamentais ao 5G na exploração, por exemplo de serviços de *connected cars*, por exemplo.

Para as faixas de sub 1 GHz, além das faixas do IMT, a OFCOM já identificou faixas em VHF especialmente úteis para o IoT

Consulta Pública

Plano Nacional de IoT

10. Em relação a utilização das faixas de radiofrequência de radiação restrita pelo ecossistema de M2M/IoT, há necessidade de avaliar alterações regulatórias, considerando seus impactos setoriais?

Contribuição Oi: O arcabouço regulatório deverá garantir isonomia tributária para os serviços de IoT independentemente da radiofrequência utilizada, uma vez que os tributos são barreiras ao desenvolvimento de novos serviços desse segmento. Alternativamente, propor a alteração da Resolução nº 506/08 (art. 3º), de modo que a ANATEL possa incluir, por intermédio de Ato, novas estações de radiocomunicação na lista de equipamentos de radiação restrita isentas de cadastramento ou licenciamento para instalação (pagamento de TFI) e funcionamento (pagamento de TFF).

Em função de múltiplos sistemas nas faixas não licenciadas há de se implantar a utilização deste espectro de maneira justa, como a funcionalidade de *Listen Before Talking*.

11. Quais referências internacionais comparáveis podem ser utilizadas do ponto de vista de regulação/legislação? Em especial, discorrer como a legislação estrangeira de referência trata dos seguintes temas:

- Definição de padrões de segurança e/ou requisitos específicos para a homologação de equipamentos IoT pelos órgãos competentes;
- Definição de padrões de qualidade/confiabilidade para serviços de telecomunicação que servem de suporte à IoT e eventual existência de assimetrias em relação aos serviços de telecomunicações destinados aos usuários em geral;
- Destinação de radiofrequências aos serviços de telecomunicações que servem de suporte a sistemas IoT e regras de utilização, inclusive em relação à interferência com outros serviços;
- Outras assimetrias regulatórias e tributárias entre os serviços de telecomunicações destinados a IoT e aos usuários em geral;

12. Quais os prós e contras de se permitir o roaming permanente internacional? Quais foram os efeitos da permissão nos mercados locais de outros países?

Contribuição Oi: A liberação de *roaming* permanente para prestadoras internacionais gera riscos para o desenvolvimento de serviços e de tecnologias nacional, pois essas poderiam explorar o mercado brasileiro sem nenhum controle dos órgãos nacionais, o que gera concorrência direta às prestadoras e possíveis práticas não aderentes ao arcabouço jurídico/ regulatório pátrio. Como não estarão sob a nossa jurisdição, as prestadoras internacionais não responderão por possíveis práticas ilícitas, ou seja, não haverá punição cabível por tais práticas. Ressalta-se ainda que, sob a guarda do *roaming* internacional, a rastreabilidade dos usuários destas prestadoras torna-se muito difícil.

A liberação do *roaming* junto com a liberação das faixas de frequência poderia ter impactos negativos importantes no mercado nacional, ainda mais sabendo-se que, atualmente, já é possível tecnologicamente realizar a troca de um código de acesso estrangeiro para um código de acesso nacional, o que reforça o argumento de que não deve ser permitido o *roaming* permanente.

13. A questão de interoperabilidade está intimamente ligada à forma de sua validação ou certificação. O modelo de certificação para IoT deve garantir que toda a solução seja interoperável garantindo ao usuário final a fruição do serviço/aplicação que escolheu. Dentre as formas de certificação, compulsória



Consulta Pública

Plano Nacional de IoT

ou voluntária, em sua opinião, qual se mostra mais adequada ao desenvolvimento do ecossistema de IoT no Brasil? Justifique.

Contribuição Oi: Considerando que a interoperabilidade é fundamental para a sustentabilidade de qualquer sistema de comunicação e que esses padrões são definidos por regras de negócio e regulatórias, ou seja, a padronização não fica refém das empresas de tecnologia, o nosso entendimento é de que deve haver uma certificação compulsória. O ambiente aqui proposto traz consigo os benefícios da economia de escala que são fundamentais para um menor custo da cadeia de valor. Adicionalmente, esse ecossistema oferece uma maior segurança e menores custos para os clientes finais que sabem que estão amparados por um sistema que se renova constantemente e que segue os padrões internacionais.

14. Considerando aspectos regulatórios e de legislação, existem outras questões relevantes que devem ser observadas para um completo diagnóstico da IoT no Brasil?

Contribuição Oi: O nível de regulamentação necessita que seja revisto para minimamente adequar a uma ampla competição, beneficiando os usuários e a sociedade.

Entre os aspectos para minimização de desequilíbrio na exploração estão as taxas de instalação (TFI) e fiscalização (TFF). Tecnologias, como LoRa e SigFox em implantação no Brasil possuem tratamento tributário vantajoso no que concerne à instalação de infraestrutura e habilitação dos dispositivos (SIM Cards). Em contrapartida, tecnologias equivalentes (LTE-MTC) e baseadas em celular (2G/3G) incidem pesadas taxas de instalação de infraestrutura e dispositivos (SIM Cards). Hoje as prestadoras de serviço que usam o LoRa e SigFox oferecem aos seus usuários valores anuais da ordem de 1 USD por objeto conectado. Impossível para as operadoras móveis, onde cada dispositivo há pelo menos uma taxa por SIM Card ativado paga anualmente.

Outro aspecto importante é o tratamento de priorização de tráfego para algumas aplicações de missão crítica: *mHealth*, *Connected Cars*, *Driveless Cars*, etc. Estes tráfegos devem ter marcações adequadas e tratamento com priorização no transporte da rede sob pena de causar riscos à saúde e econômicos, marcações de prioridade estas impedidas pelo Marco Civil da Internet (neutralidade de rede).

15. Qual impacto a carga tributária do Brasil pode ter sobre o ecossistema de Internet das Coisas?

Contribuição Oi: Segundo estimativas, a carga tributária da prestação de serviços de telecomunicações é da ordem ou superior a 60%. Por se tratar de uma indústria de aplicação massiva de dispositivos ativos e serviços, onde o custo é o principal atributo, a carga tributária tem relevância determinante para futuro desta indústria no Brasil.

De fato, a carga tributária é um dos principais fatores para o desenvolvimento (ou não) do IoT no Brasil. Isso porque a IoT tem como característica básica o baixo consumo de dados e por consequência uma receita por usuário, ARPU, significativamente inferior aos demais serviços prestados pelas prestadoras de serviços de telecomunicações.

Diante disso, o patamar das taxas de TFF/TFI, dentre outros tributos, impede a viabilidade econômica do serviço. A racionalização tributária pode revolucionar a prestação dos serviços e até mesmo potencializar outras formas de cobranças, as quais deverão ser mais aderentes ao modelo de IoT, incentivando e massificando esses serviços no Brasil.

Cabe esclarecer que, na camada de rede de telecomunicações, verifica-se a existência de diversas tecnologias de IoT e no aspecto tributário vemos que deve ser adotado o princípio de isonomia de tributos com objetivo de igualdade de condições entre os diferentes serviços. Assim sendo, serviços IoT, devem receber tratamentos já estendidos para os produtos M2M, ainda que verificado algum elemento mínimo de intervenção humana.

No que tange as especificidades de cada tributo, é de nosso entendimento que devam ser considerados os seguintes requisitos:



Consulta Pública

Plano Nacional de IoT

ICMS - Redução de Carga Tributária (Alíquota Efetiva) – Há várias operações em que houve a redução da carga tributária de modo que a alíquota efetiva para o cliente é reduzida, tal como ocorre para o serviço de TV por assinatura, que é beneficiada com alíquotas reduzidas em até 10%.

ICMS - Redução de Carga Tributária (Alíquota Efetiva) – Tal como ocorre para TV por assinatura o benefício da aplicação de uma carga tributária de ICMS reduzida em até 10%, tem o condão de reduzir o impacto da tributação no preço para o cliente.

FISTEL – Necessidade de revisão do modelo, pois a incidência da taxa de instalação a cada equipamento implantado (TFI) e taxa de fiscalização anual (TFF) são extremamente onerosas. Assim, o que se propõe é a avaliação de uma desoneração do M2M e IoT com relação a estas taxas. Destacando que, sobre a receita do serviço de comunicação relativa ao M2M/IoT sofrem também a incidência do FUST (1%) e FUNTTEL (0,5%).

Por fim, ressalta-se que, quando evoluímos para as novas tecnologias mais aderentes ao mercado de IoT, temos novas redes voltadas a atender a demanda de comunicação em banda estreita, onde os requisitos são: baixo consumo de energia; ampla cobertura de rede e alto volume de dispositivos conectados por estação rádio base; e o pouco volume de dados trafegados. Esses requisitos definem o conceito que se chama LPWA. Dentro deste conceito, a tendência é que o custo unitário da conectividade varie em função da quantidade de mensagens enviadas diariamente por dispositivo, tendo como objetivo o menor custo de conectividade. Diante disso, é fundamental que o modelo tributário relativo a FISTEL (TFI/TFF) seja revisto, uma vez que o atual arcabouço regulatório (FISTEL M2M) deverá ter um peso excessivo na composição da conectividade nesse conceito. Um caminho que pode ser trilhado é estabelecer um percentual relativo ao serviço prestado. Por outro lado, é necessário avaliar as mesmas condições de tributos para redes LPWA em frequência não licenciada, pois hoje são enquadradas como serviço de radiação restrita onde não caiba FISTEL.

Consulta Pública

Plano Nacional de IoT

16. Existem outros fatores fiscais ou tributários que impeçam o desenvolvimento do Ecosistema?

Contribuição Oi: Sim, dentre as quais se destacam:

1) Revisão da Política Fiscal - Há uma premente necessidade de revisão da política fiscal tributária, neste ponto deveria ser discutida a adoção de um Imposto sobre o Valor Agregado (sobre o Consumo), como ocorre em outros países, além da simplificação da tributação inclusive considerando o PIS e COFINS que incidem sobre a receita.

Um dos principais pontos de insegurança jurídica no âmbito tributário é a incerteza sobre o campo de incidência do ISS e/ou ICMS sobre determinadas atividades, tais como *software*, disponibilização de conteúdo, publicidade, *video on demand*, etc. O cenário que se avizinha com o desenvolvimento da IoT implicará inúmeras discussões sobre qual dos impostos ICMS e/ou ISS incidirá sobre as atividades desenvolvidas e sobre as respectivas soluções de IoT. Isto porque, para os Estados tudo o que envolve o serviço de comunicação ainda que como insumo, deve ser enquadrado como tal e deve sofrer a incidência do ICMS, enquanto os municípios almejam a sua fatia de receita tributária pelos serviços que serão prestados.

2) ICMS

a. Seletividade x Essencialidade – Discussão sobre a essencialidade dos serviços de comunicação e energia elétrica para fins de tributação e consequente redução das alíquotas de ICMS (25% a 35), pois hoje estas atividades são tributadas pelas mesmas alíquotas de produtos/bens supérfluos (bebidas alcoólicas, armas e munição, perfumes, fogos de artifício dentre outros), assim, considerando este novo cenário de IoT que representará uma grande mudança na vida das pessoas (trabalho e lazer), fica mais evidente que os serviços de comunicação e energia elétrica são essenciais, e não podem ser tratados como operações com itens supérfluos.

As alíquotas do ICMS sobre o serviço de comunicação são no patamar de 25% a 35%, isto ocorre pois o serviço de comunicação apesar de ser essencial para o desenvolvimento de quaisquer operações atualmente, desde os primórdios é enquadrado pelas legislações estaduais no mesmo critério aplicado para bens supérfluos tais como: bebidas alcoólicas, armas e munição, perfumes, fogos de artifício dentre outros. O mesmo acontece para energia elétrica a qual é essencial para todos os processos envolvendo M2M e IoT. Este tema está no Supremo Tribunal Federal para avaliação de ofensa aos princípios da isonomia tributária e da seletividade previstos na Constituição Federal, em sede de repercussão geral no âmbito do Recurso Extraordinário 714139.

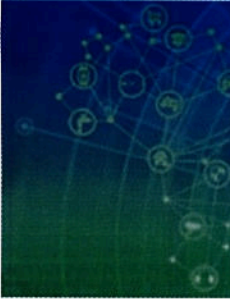
b. Definição/distinção entre Serviços de Comunicação e outros serviços conexos e SVA – Necessidade de distinção legislativa dos serviços que sofrem a incidência de ICMS e ISS. Por exemplo: serviço de comunicação x *Cloud*.

Há uma grande insegurança jurídica no setor privado, pois não é possível identificar com clareza a incidência do ICMS e ISS sobre determinadas operações. Como exemplo, podemos destacar a atual discussão sobre a incidência do ICMS ou ISS sobre operações com *software*, programas, aplicativos, disponibilização de conteúdo, por qualquer meio, ante a publicação do Convênio CONFAZ ICMS nº 181/15, em concomitância com o Projeto de Lei nº 386, convertido no dia 30/12/16 na Lei Complementar nº 157, incluindo na Lista do ISS atividades tais como disponibilização de conteúdo.

3) Substituição Tributária – Necessidade de desburocratização e padronização do mecanismo de substituição tributária do ICMS sobre mercadorias, facilitando e reduzindo o ônus das empresas.

O ICMS é um imposto não cumulativo, o que implica na possibilidade de aproveitamento de créditos no decorrer da cadeia de comercialização. Ocorre que na sistemática de substituição tributária um dos atores da cadeia é responsável por recolher todo o ICMS que seria devido na cadeia. Contudo, em algumas situações, a cadeia de comercialização não se realiza implicando no direito ao crédito do ICMS, mas os procedimentos para reaver os créditos são extremamente morosos e complexos, acarretando um grande ônus para as empresas para tal recuperação, assim, é necessário discutir a flexibilização dessas regras de modo a facilitar e desburocratizar o aproveitamento de créditos do ICMS.

4) Revisão do FISTEL: O atual arcabouço impede de aplicação de modelos mais flexíveis, como por exemplo, pagamento por uso, cobrança por evento. Com as condições atuais, isto é, obrigação do pagamento da taxa em função da instalação ou da manutenção dos equipamentos, o mercado adotou como forma padrão de cobrança, planos mensais. Esses planos são os mecanismos para garantir o equilíbrio econômico-financeiro das



Consulta Pública

Plano Nacional de IoT

Prestadoras, custos fixos e investimentos. Uma nova visão sobre a cobrança do FISTEL pode potencializar outras formas de cobranças, as quais deverão ser mais aderentes ao modelo de IoT, que tem como característica básica o baixo consumo de dados e por consequência um ARPU reduzido.

Há de se rever as taxas de instalação (TFI) e fiscalização (TFF) para infraestrutura e dispositivos objetivando uma competição justa entre tecnologias e operações. Como exposto, tecnologias, como LoRa e SigFox em implantação no Brasil possuem tratamento tributário vantajoso no que concerne à instalação de infraestrutura e habilitação dos dispositivos (SIM Cards). Em contrapartida, tecnologias equivalentes (LTE-MTC) e baseadas em celular (2G/3G) incidem pesadas taxas de instalação de infraestrutura e dispositivos (SIM Cards). Hoje as prestadoras de serviço que usam o LoRa e SigFox oferecem aos seus usuários valores anuais da ordem de 1 USD por objeto conectado. Impossível para as operadoras móveis, onde cada dispositivo há pelo menos uma taxa por SIM Card ativado paga anualmente.

5) Criação do REPNIoT - Regime Especial de Tributação do Programa Nacional de Internet das Coisas: Assim como acontece na Banda Larga, seria importante para o IoT a criação de um regime especial de Tributação para acelerar o desenvolvimento desse serviço no Brasil. A título de exemplo pode-se citar a tecnologia do NB-IoT, *Narrow Band IoT*, que está sendo desenhada para aplicações IoT que possuem características de baixo tráfego e baixo consumo de bateria. Para esses casos, REPNIoT fomentaria a implementação dessas redes nas prestadoras.

Por fim, é importante adequação do arcabouço regulatório para tratar dos recursos futuros do FUST, de modo que possam ser utilizados nas iniciativas de expansão da banda larga fixa e móvel, que é a infraestrutura-base para o desenvolvimento das IoTs, no país.