Ministério da Ciência, Tecnologia, Inovações e Comunicações

Câmara IoT

Consulta Pública

"Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil"

Dezembro de 2016

Divisão das análises dos temas

TEMAS	ATA Abinee	
1. Assuntos regulatórios	(CISCO, QUALCOMM, IBM)	RESPONDER #1
2. Papel do estado	(QUALCOMM, ERICSSON, FLEX)	RESPONDER #1
3. Pesquisa & Desenvolvimento	(FLEX , SAMSUNG, ERICSSON, QUALCOMM)	RESPONDER #2
4. Recursos humanos	(FLEX , SAMSUNG, QUALCOMM)	RESPONDER #2
5. Oferta tecnológica e composição de ecossistemas	(TODOS COMISSÃO IoT)	RESPONDER #1
6. Investimento, Financiamento e Fomento	(FLEX)	RESPONDER #2
7. Demanda	(IBM, NOVUS, ERICSSON, CISCO)	RESPONDER #1
8. Aspirações	(CISCO, ERICSSON, QUALCOMM)	RESPONDER #1
9. Segurança e Privacidade	(CISCO, IBM)	RESPONDER #3
10. Gerenciamento da Infraestrutura	(TODOS COMISSÃO IoT)	RESPONDER #3
11. Suporte a aplicações e serviços	(TODOS COMISSÃO IoT)	RESPONDER #3
12. Redes e transporte de dados	(ERICSSON, NOKIA, CISCO)	RESPONDER #1
13. Gateways e dispositivos	(QUALCOMM, SAMSUNG, NOVUS)	RESPONDER #1

I. Introdução

A Internet das Coisas (em inglês, Internet of Things – IoT) já é uma realidade. A cada dia mais "coisas" (máquinas, cidades, elementos de infraestrutura, veículos e residências) se conectam à internet para informar sua situação, receber instruções e até mesmo praticar ações com base nas informações recebidas.

A possibilidade de ligar o mundo físico à Internet e a outras redes de dados tem profundas implicações para a sociedade e a economia. A Internet das Coisas torna possível monitorar e gerenciar operações a centenas de quilômetros de distância, rastrear bens que cruzam o oceano ou detectar mudanças na pressão sanguínea de um diabético, que poderia ser sinal de um ataque cardíaco. Mais que a próxima evolução da tecnologia da informação, a Internet das Coisas redefine a maneira como interagimos com o mundo físico e viabiliza formas mediadas por computação – até então impossíveis – de produzir, fazer negócios, gerenciar infraestrutura pública, prover segurança e organizar a vida das pessoas.

Estima-se que já existam mais de quinze bilhões de dispositivos conectados em todo o mundo, incluindo smartphones e computadores. Prevê-se que na próxima década esse valor aumentará drasticamente, atingindo 35 bilhões de dispositivos em 2025, ou 5 vezes a população mundial.

O crescente número de aparelhos conectados a sistemas inteligentes que podem compartilhar, processar, armazenar e analisar dados entre si terá como resultado a conexão de bilhões de máquinas e outros dispositivos a redes e a criação de ainda mais dados. Dessa forma, serão necessárias técnicas inteligentes de gestão e análise de dados para extrair *insights* significativos. Dessa forma, é fundamental o desenvolvimento de diversos setores associados à tecnologia, tais como telecomunicações, serviços de Computação em Nuvem (*Cloud Computing*) e Análise de Dados (*Analytics*).

Neste cenário, dada a relevância do tema no contexto mundial e brasileiro nos próximos anos, o Governo Brasileiro instituiu a Câmara de IoT em 2014.

A Câmara IoT tem como objetivos subsidiar a formulação de políticas públicas, promover e acompanhar o desenvolvimento de soluções de Comunicação Máquina a Máquina (M2M) e de Internet das Coisas (IoT) para o mercado brasileiro. É um fórum multissetorial com representantes do Governo, Iniciativa Privada, Academia e Centros de Pesquisa. A partir da Câmara, discussões como privacidade de dados, segurança das informações, tributação, regulação, fomento ao desenvolvimento de soluções e formação de capital humano devem ser discutidas para que o Brasil possa tirar o maior proveito possível dos benefícios desse novo mercado.

Para tanto é fundamental que sejam estabelecidos estímulos (de governo e de estado) que, com o apoio da iniciativa privada, fomentem um ecossistema favorável ao desenvolvimento e a utilização de soluções de IoT. Isso poderá incluir desde estímulos à

pesquisa e desenvolvimento de soluções inovadoras locais, à formação de mão de obra qualificada e à exportação de produtos e serviços.

Como resultado direto desses estímulos, teríamos uma melhora da qualidade de vida da população, um aumento da eficiência produtiva e a melhora da situação da balança comercial de produtos e serviços do país.

Neste sentido, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e o Banco Nacional para o Desenvolvimento (BNDES) estabeleceram um convênio para apoiar a realização de um estudo de IoT, através do Fundo de Estruturação de Projetos (FEP). Tal estudo tem como objetivo realizar um diagnóstico e propor políticas públicas no tema Internet das Coisas, estimulando a cooperação e articulação entre empresas, poder público, universidades e centros de pesquisa.

É no âmbito do estudo acima mencionado que a Câmara IoT propõe a presente consulta pública. Ela busca identificar tópicos chave para a viabilização de IoT no Brasil, que devem ser considerados e avaliados na fase de diagnóstico do estudo. Em um segundo momento, será lançada uma consulta pública adicional com foco na priorização de segmentos de aplicações (verticais) e na construção de planos de ação.

Este documento apresenta, em primeiro lugar, um alinhamento conceitual dos principais elementos relevantes ao entendimento da Internet das Coisas seguido das questões a serem tratadas na Consulta Pública. Essas questões estão segmentadas em tópicos e buscam obter a opinião dos diversos agentes envolvidos a fim de construir-se um diagnóstico abrangente dos desafios e oportunidades de IoT no Brasil.

Os resultados dessa consulta pública serão disponibilizados de maneira consolidada e discutidos no âmbito da Câmara IoT.

II. Alinhamento conceitual

A Internet das Coisas consiste na rede de todos os objetos que se comunicam e interagem de forma autônoma via internet, permitindo o monitoramento e gerenciamento desses dispositivos via software para aumentar a eficiência de sistemas e processos, habilitar novos serviços e melhorar a qualidade de vida das pessoas. Do monitoramento de máquinas no chão de fábrica até o rastreamento do deslocamento de navios no oceano e o uso de dispositivos pessoais conectados, a Internet das Coisas tem o potencial de mudar profundamente a forma como interagimos com o ambiente.

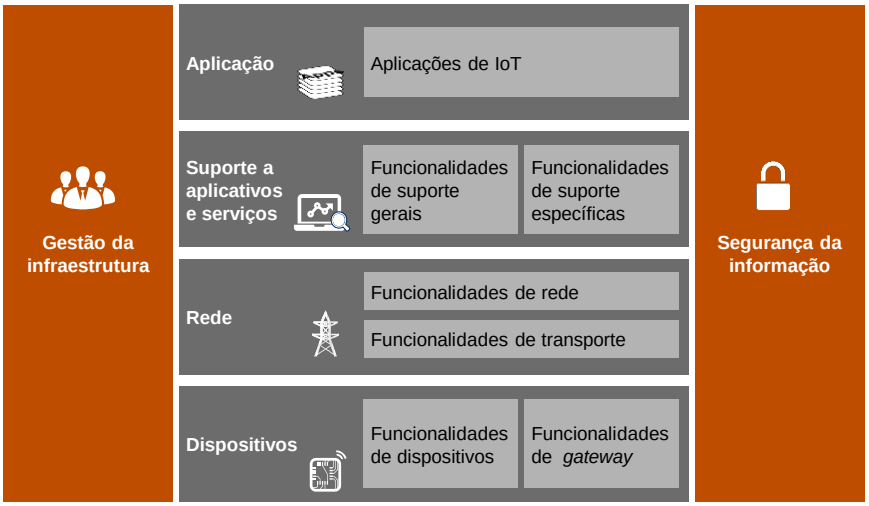
Em sua definição mais ampla a Internet das Coisas engloba todos os objetos que transmitem informações através da internet, como computadores, *tablets* e smartphones. A definição mais estrita, e comumente aceita, considera apenas os objetos capazes de detectar (através de sensores), transmitir informações e atuar sem a presença constante de intervenção humana.

No entanto, quando analisamos a Internet das Coisas, devemos nos atentar ao fato de que ela está inserida em um ecossistema, do qual as "coisas" são apenas uma pequena parte dele. Fazem parte deste ecossistema os atores que contribuição para a viabilização da internet das coisas, tais como: empresas, startups, universidades, ICTs, órgãos e esferas governamentais, etc.

Ou seja, tal qual a internet comum, a Internet das Coisas é evidentemente (e nem poderia deixar de ser) dependente dos serviços de telecomunicação e informação que a suportam. Trata-se de constatação importante, uma vez que não é possível repensar o ambiente da Internet das Coisas sem levar em consideração as características do setor de TIC.

Neste contexto, a arquitetura de referência de IoT criada pela *International Telecommunication Union* (ITU) e utilizada por diversos países no desenvolvimento de padrões e normas para IoT, pode ser adotada inicialmente para representar os principais elementos tecnológicos pertinentes à IoT, conforme indicado na figura a seguir.

Arquitetura de referência de IoT



FONTE: ITU

Os elementos dessa arquitetura são descritos a seguir:

- ***Aplicação*** – camada que contém as aplicações de IoT, (p.ex., monitoramento de saúde; controle de automação industrial);
- ***Suporte a aplicações e serviços*** – camada que contempla o suporte ao desenvolvimento de aplicações e serviços através do provimento de funções que utilizam infraestrutura computacional em nuvem, como armazenamento de dados e processamento, propiciando interoperabilidade entre aplicações através de Interfaces de Programação de Aplicações (APIs) bem definidas e intermediando a comunicação com as camadas de rede e dispositivos;
- ***Rede*** – o foco desta camada é endereçar os protocolos e tecnologias de comunicação associados à IoT;
- ***Gateways e Dispositivos*** – camada na qual encontram-se os dispositivos e gateways contemplando os seus elementos como processadores, memórias, firmware, sensores, atuadores, captação de energia e comunicação;
- ***Gestão da Infraestrutura*** – gerenciamento da infraestrutura de IoT, em todas as suas camadas, com o objetivo de garantir a confiabilidade dessa estrutura através do comissionamento, monitoramento, aprovisionamento e configuração dos dispositivos sensores e atuadores, elementos de rede e infraestrutura computacional, suportando toda a operação;
- ***Segurança da Informação*** – esta camada, assim como a de gestão de infraestrutura, apresenta tecnologias que permearão todas as demais camadas. Nela, são mapeadas as principais tecnologias utilizadas para atender os requisitos de segurança da informação como privacidade, integridade e disponibilidade.

De igual importância para o completo entendimento e avaliação de Internet das Coisas é o conceito de ambientes de aplicação. Quando analisamos o escopo de aplicação de Internet das Coisas, verificamos que ele dificilmente está restrito a uma indústria específica, estendendo-se horizontalmente por diferentes setores.

O uso de tecnologias de Internet das Coisas geralmente ocorre em quaisquer espaços físicos, como residências, campos, cidades e fábricas. Dessa forma, para capturar de forma ampla o impacto de IoT, é necessário partir de uma perspectiva de ambiente, analisando os diferentes contextos em que IoT está presente, incluindo, por exemplo, aparelhos médicos inteligentes, sistemas autônomos, veículos conectados, tecnologia vestível e automação industrial.

III. Questões a serem tratadas

Com objetivo de facilitar o entendimento e organizar as questões, estas foram agrupadas em treze tópicos prioritários. São eles: Assuntos regulatórios e legislação; Papel do Estado; Pesquisa e Desenvolvimento; Recursos Humanos; Oferta tecnológica e composição de ecossistemas; Investimento, Financiamento e Fomento; Demanda; Aspirações; Segurança e Privacidade; Gerenciamento da infraestrutura; Suporte a aplicações e serviços; Redes e transporte de dados; e Gateways e Dispositivos.

1. 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.

1.1 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 (Regulação estatal, Auto regulação privada, Regulação baseada em incentivos do mercado, entre outros) para a rápida adoção e massificação da tecnologia IoT no Brasil.

1.2 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 tanto 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)

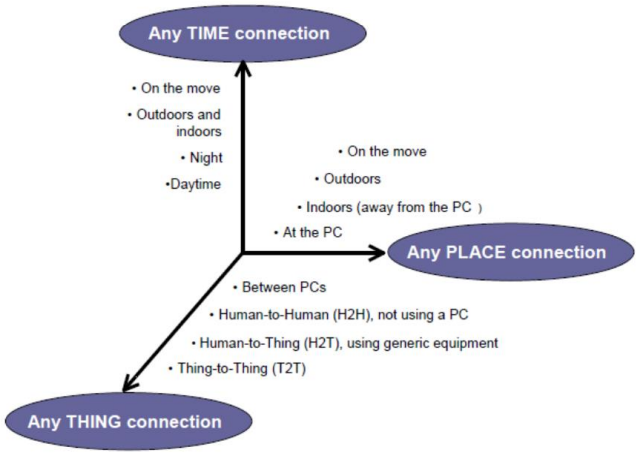
Por exemplo, os serviços de Tecnologia de Rastreamento e Monitoramento veicular, são compostos por: (i) um serviço de telecomunicações que dá suporte à conexão entre os equipamentos embarcados nos veículos; e (ii) um serviço de valor adicionado correspondente ao rastreamento propriamente dito e análise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

- Esse enquadramento regulatório é adequado? Ele traz problemas ou limitações para os sistemas IoT?
  É inerente ao mundo de IoT a conectividade, mas esta conectividade não tem como objetivo primordial o estabelecimento de comunicação da forma como conhecemos hoje (exclusivamente entre pessoas), mas sim a comunicação entre objetos conectados. Todavia a regulamentação pátria foi feita em um outro contexto e cenário, onde não existia o potencial de conexão máquina-a-máquina como passamos a conhecer a partir do desenvolvimento da tecnologia da IoT.
  Neste sentido, a avaliação do Ministério está correta em relação ao desafio do enquadramento dos dispositivos de IoT como revenda de telecomunicações, pois não se trata de oferta de conectividade como objeto da comunicação entre pessoas, mas sim oferta de conectividade para comunicação entre dispositivos conectados.
  Portanto, é fundamental que sejam feitos ajustes no ambiente regulatório das telecomunicações de modo a garantir a oferta de produtos, equipamentos e serviços baseados na oferta de conectividade máquina-a-máquina, para que esta oferta não seja configurada como uma revenda de telecomunicações.
  Ou seja, defendemos a revisão da regulamentação de telecomunicações por parte da Agência Nacional de Telecomunicações – ANATEL não para que seja criada uma outorga específica para IoT, mas sim para que seja revisto o entendimento da Agência no tocante à conectividade atrelada à IoT, deixando de ser caracterizada como revenda de serviços de telecomunicações através de uma flexibilização da regulamentação para oferta de IoT. Com a adoção desta medida, possíveis barreiras que impeçam o desenvolvimento de IoT no Brasil são afastadas.

- 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.
  O enquadramento atual está adequado para regulamentar a prestação de serviços que envolvem transmissão de dados, pois oferece proteção ao usuário final. No cenário de IoT, a prestação de qualquer serviço deverá ser devidamente protegida e regulamentada, atendendo questões de qualidade de serviço (sempre conforme definições contratuais), e com previsão de fiscalização.

- A definição de IoT presente no Decreto n. 8.234/2014 é suficiente e adequada ou ela impede o desenvolvimento de alguma atividade?
  A definição de "sistemas de comunicação máquina a máquina" disposta no Decreto 8234/2014 é dedicada a sistemas de comunicação M2M, tendo como principal escopo a comunicação sem intervenção humana, traçando objetivos referentes a medição e controle.
  Tendo em vista a evolução das tecnologias e considerando a arquitetura do International Telecommunication Union conforme figura abaixo (disponível em http://www.itu.int/en/ITU-T/techwatch/Documents/1010-B_Jamoussi_IoT.pdf), verifica-se a necessidade de buscar uma definição formal para o termo "Internet das Coisas", em termos regulatórios, para contemplar toda a gama de funcionalidades embutidas no conceito de IoT representado por esta arquitetura. Como exemplo, englobar equipamentos, produtos, prestação de serviços e o tratamento de dados que será necessário.



- Há a necessidade de se estabelecer um enquadramento regulatório de acordo com o nível de interação humana nos dispositivos M2M/IoT?
  Acreditamos que não haja necessidade de se estabelecer o enquadramento regulatório de acordo com o nível de interação humana, pois esta nos parece ser uma premissa incorreta para o estabelecimento de um arcabouço específico para dispositivos M2M/IoT. O nível de interação humana não é por si só um problema, mas deve-se existir um cuidado para não se criar níveis diferentes de regulamentação em virtude da interação. Isto porque, estas limitações em virtude

da interação podem acabar representando uma inibição ao processo de inovação e desenvolvimento tecnológico.

- A figura do Mobile Virtual Network Operator ("**MVNO**"), prevista atualmente na regulamentação da Anatel (Resolução nº 550, de 22 de novembro de 2010) é suficiente para cobrir eventuais lacunas na atuação dos agentes nos sistemas IoT?
  Entende-se que o advento de IoT pode ser um excelente indutor do crescimento de redes MVNO no Brasil. A legislação atual, no entanto, possui alguns detalhes que devem ser avaliados, para adequar a prestação de novos serviços, a saber:
  1) Atualmente é focada em usuário com pacotes de serviços e não em dispositivos M2M/IoT (que tipicamente trafegam poucos dados, e que devem ser focados em garantia de recepção de informações de sensores/dispositivos).
  2) Um MVNO credenciado somente poderá ter contrato de prestação com uma operadora por região. Isto poderia impactar no preço de prestação de serviço.
  3) A lei indica que a candidata ao credenciamento deve ser empresa brasileira com funcionários e engenheiros com CREA, caracterizando protecionismo, o que não oferece atualmente oportunidade de entrada de empresas grandes internacionais. Uma empresa grande por exemplo, não poderia comprar MVNO no Brasil. No exterior, as empresas estão comercializando MVNOs para ter pacotes de serviços globais, e no Brasil, no entanto, deve se associar com empresa local.
  4) Uma operadora celular não pode ser autorizada de MVNO, ou seja, somente poderá ser prestadora de serviço SMP. Entende-se que MVNOs serão um novo mercado de negócios, e por esse motivo não deveria haver restrição de participação das mesmas operadoras. Como exemplo, em outro país, se uma MVNO tiver um crescimento satisfatório, oferecendo serviço IoT atrativo, poderia ser comprado por uma operadora. Isso não ocorreria no Brasil, dentro do cenário atual, o que poderia impactar negativamente, afetando a inovação nos negócios.

- Faz sentido ter um arcabouço regulatório especifico para IoT/M2M?
  As tecnologias IoT/M2M estão evoluindo rapidamente, por isso, não é recomendado que o Estado crie regulamento específico para a indústria IoT/M2M, uma vez que este pode tornar-se obsoleto muito rapidamente, restritivo e inflexível, podendo ainda prejudicar os investimentos em IoT/M2M e a inovação em serviços.
  Na maioria dos casos, o Estado deve se basear nos regulamentos já existentes e guiados pelo próprio mercado, fundamentados na tecnologia e na padronização, para continuar incentivando investimentos e o crescimento da IoT/M2M para beneficiar toda a sociedade.
  Além disso, o Estado deve evitar a duplicação de regulamentações em diferentes indústrias ou setores. O que se sugere, e esperamos que o Estado apoie, é a harmonização dos regulamentos específicos já existentes nos tradicionais setores da economia ao ecossistema de IoT, para que eles auxiliem o seu desenvolvimento e promovam a inovação dentro de suas respectivas indústrias utilizando estas novas tecnologias como ferramentas.

- 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?
  Acreditamos que o conjunto de dispositivos que requeiram conectividade não requerem um arcabouço regulatório próprio, até mesmo porque as necessidades são distintas. Em IoT não faz sentido falar em obrigações de cobertura, disponibilidade, velocidade e etc. como verificado nos serviços de telecomunicações outorgados, em especial na forma como tais critérios são atualmente incorporados na regulamentação dos serviços de telecomunicações. O importante é que o serviço seja prestado com padrão de qualidade objetivo, previamente estabelecido e acordado.

- 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?
  O roaming internacional permanente é um fator chave para certos modelos de negócio baseados no ecossistema de IoT. Isto porque, estas aplicações estão baseadas na utilização dos serviços de forma transnacional, dependendo do roaming internacional permanente através das redes de serviço móvel ao redor do mundo para sua plena operacionalização.
  Uma das vantagens da utilização do roaming internacional permanente é simplificar o processo da cadeia de suprimentos de aplicações de M2M/IoT ao ofertar conectividade sem a necessidade de um SIM Card local para cada um dos territórios onde esta aplicação seja utilizada.
  Contudo, a legislação brasileira nunca se mostrou clara a este tema de grande relevância para promover as comunicações tanto entre dispositivos M2M quanto de IoT, qual seja, o roaming internacional permanente.
  No Brasil não existe norma específica da Agência Brasileira de Telecomunicações (ANATEL) que proíba o roaming internacional permanente no país. Entretanto, é público o entendimento da Agência de que esta prática se configura como prestação ilegal de serviços de telecomunicações no país, visto que a empresa estaria prestando o serviço sem deter a devida autorização no Brasil para exploração de serviços de telecomunicações.
  Seguindo este posicionamento, em encontro da Comissão de Estudos 3 (SG-3) da União Internacional de Telecomunicações (UIT), no final de fevereiro de 2016, para discutir parâmetros de regulamentação entre diferentes países, a ANATEL posicionou-se contra a edição de norma internacional que permita o roaming internacional permanente para dispositivos M2M como, por exemplo, carros conectados que poderão ser fabricados em outros países e chegarão ao Brasil com SIM Card embarcado de sua operadora de origem, uma operadora estrangeira (ver notícia no link: http://convergecom.com.br/teletime/10/03/2016/uit-nao-consegue-chegar-consenso-sobre-regulamentacao-de-servicos-ott/).
  A ANATEL entende que o roaming internacional permanente pode provocar o desbalanceamento na competição, pois acabaria sendo criada uma operadora de telecomunicações em escala global, que não pagaria os impostos das empresas

locais (ver notícia no link: http://www.telesintese.com.br/brasil-diz-nao-ao-roaming-permanente/).

É fundamental recordar que a capacidade de oferecer serviços globalmente é questão crítica para apoiar o desenvolvimento do ecossistema de IoT em diferentes setores da economia. Como já exposto, o roaming internacional permanente apresenta-se como a melhor forma para atender dispositivos M2M de clientes multinacionais que, em sua grande maioria, querem lidar com um único fornecedor (leia-se, operadora de origem), sem que seja necessário embarcar diferentes SIM Cards em seus dispositivos de acordo com a localização geográfica.

Por tais razões demonstra-se necessário o debate desta questão no Brasil e a reavaliação, por parte da ANATEL, de seu entendimento para garantir não só a inclusão do país como mercado consumidor de produtos e serviços M2M/IoT que utilizem roaming internacional permanente, como também propiciar que o mercado brasileiro se torne um exportador destes mesmos produtos e serviços, ampliando o campo de atuação das operadoras que atuam no Brasil através da expansão do potencial mercado consumidor.

- A permissão de utilização comercial das faixas de radiofrequência dos "espaços brancos" (*White spaces)* seria uma alternativa para a comunicação entre dispositivos M2M/IoT?

  Apesar de tecnicamente possível, entende-se que não é necessário e nem recomendado conceder o uso de "Espaços brancos" para utilizar em serviços M2M / IoT, na maioria dos casos.

  "Espaços brancos" referem-se aos espectros não utilizados que podem estar disponíveis para utilização no tempo, frequência, domínio geográfico e de código Em termos mais específicos, "Espaços brancos" na faixa de TV e radiodifusão referem-se, tipicamente, ao uso não licenciado de espectro nas bandas de radiodifusão UHF a 470 - 862 MHz (com variações nacionais).

  Muitas aplicações IoT/M2M exigem comunicações seguras e ultra confiáveis com baixa latência e qualidade de serviço que podem não ser possíveis de alcançar com o uso do espectro de "Espaços brancos".

  Além disso, a utilização do "Espaço branco" abaixo de 1 GHz poderia simplesmente poluir a utilização do espectro e pode impedir usos mais eficazes no futuro. De acordo com a UIT (Grupo Conjunto ITU-R / ITU-D), todas as bandas de frequência inferiores a 1 GHz oferecem uma oportunidade única de cobertura, mas têm capacidade limitada, uma vez que as suas excelentes características de propagação tornam difícil a reutilização de frequências sem uma abordagem bem coordenada [1].

  Em geral, as redes multi-serviços - baseadas em tecnologias sem fio, como redes celulares, RLANs, satélites e similares, bem como, tecnologias fixas e outros - podem transportar de forma segura e rentável a maioria das necessidades de serviço dos serviços IoT/M2M. Além disso, as redes sem fio utilizam soluções comerciais padronizadas usando bandas de espectro harmonizadas para garantir uma interoperabilidade de serviços adequada e evitar riscos de interferência.

Para as comunicações M2M menos rigorosas já existem bandas ISM designadas disponíveis e o uso isento de licença de determinadas faixas de serviços móveis, utilizando tecnologias RLAN.
Considerando que o uso dinâmico dos "Espaços brancos" não oferece condição adequada para serviço com os requisitos de qualidade mencionados, entende-se que o uso compartilhado do espectro através de licenciamento, tal como a arquitetura do LSA (Licensed Spectrum Access) em desenvolvimento na Europa e EUA, oferece mais segurança aos usuários, tanto o incumbente quanto o licenciado, no tocante à questão de interferência, à entrada e saída de espectro através de mecanismo de controle, e principalmente quanto ao aspecto comercial estabelecido em contrato, com autorização da Anatel. Além disso, os acordos previamente estabelecidos, com base em análises técnicas das faixas, promovem a otimização de uso do espectro.
Ref. [1] ITU-R / ITU-D Joint Group on WTDC Resolution 9

- Em relação a utilização das faixas de radiofrequência de radiação restrita pelo ecossistema de M2M/IoT, há necessidade de alteração da Resolução n. 506/2008 da Anatel?
  A regulamentação está adequada para o uso não licenciado das faixas, estabelecendo as condições de uso. Entende-se que não há necessidade de alteração da Resolução 506/2008. Um aspecto a ser observado é tornar mais ágeis os processos de aceitação de certificação/homologação de equipamentos oriundos de outros países, já certificados por FCC, ETSI, e Industry Canada, como exemplo, assim como de certificação de alianças (p. ex. Wi-Fi, Bluetooth), visando a redução de tempos e custos.

1.3 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;
  Com a chegada do conceito IoT, diversos dispositivos que antes não executavam transmissão, passam a fazê-lo, sendo transformados em dispositivos de comunicação sem-fio com tráfego de dados. Neste cenário, a homologação de dispositivos IoT deve ter conformidade não somente com requisitos regulamentados de comunicação, mas considerando também novos requisitos em aspectos de segurança [1], que são principalmente de alerta/logging, autenticação, criptografia, segurança física e segurança de plataforma. As vulnerabilidades mais comuns tem sido [2]: privacidade nos dados do consumidor; autorização insuficiente (pouca complexidade de senha), falta de encriptação para transporte na rede local, internet ou nuvem; interface web insegura; proteção inadequada de software.
  Nesse sentido, verifica-se na referência internacional dos EUA o processo do órgão certificador FCC no tocante aos dispositivos de radiofrequência [3]. Os dispositivos RF devem ser certificados conforme documento 47 CFR Part 2,

visando atender os requisitos de comunicação do regulamento FCC Part 15, "Radio Frequency Devices" [4]. A certificação pode ser dividida em duas partes: testes de Emissões Gerais e de Radiação Intencional (para conformidade com FCC Part 15 Subpart A e FCC Part 15 Subpart C respectivamente). Dentro do novo cenário de IoT, sendo desenvolvidos diversos novos produtos, verifica-se que o tempo de certificação de Radiação Intencional pode ser minimizado quando se usam módulos RF já certificados, ao invés de empregar módulos novos ou recém desenvolvidos. Outro aspecto a ressaltar é que a utilização de tecnologias consolidadas como Wi-Fi ou Bluetooth no produto IoT exige certificação adicional desses organismos, além da certificação do FCC. Em particular, tecnologias wearables ainda necessitam de testes de absorção de RF pelo corpo humano, ou SAR (specific absortion rate).

Para certificar requisitos de segurança, além da certificação de comunicação citada acima, verifica-se nos EUA a prática dos laboratórios acreditados oferecerem homologação de produtos IoT a partir de "pacote de testes" baseado em orientações emergentes de projetos de segurança e de alianças voltadas para IoT, compondo assim um pacote de requisitos oferecido e testado pelo laboratório acreditado. Como exemplo, cita-se o laboratório ICSA Lab [1] que se baseia em três diretrizes, a saber: do OWASP Open Web Application Security Project, do IIC Reference Architeture e da arquitetura do Online Trust Alliance. Todas essas diretrizes apresentam requisitos e testes considerados necessários para segurança em IoT.

Para o contexto brasileiro, considera-se que os requisitos, normas e boas práticas internacionais devem ser seguidos. Idealmente, em uma estrutura dinâmica capaz de acompanhar as constantes evoluções dos requisitos internacionais, de forma que sejam rapidamente vistos e incorporados no Brasil (p. ex., em um site do órgão que coordena essas informações). Além disso, entende-se que é necessário que a Anatel acelere os processos de homologação de dispositivos, para que seja possível absorver o grande número que é esperado. Nesse sentido, a implementação de acordos de reconhecimento mútuo de certificação poderá agilizar os processos internos.

[1] https://www.icsalabs.com/technology-program/iot-testing
[2] http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WFrIJ1MrLIW
[3] https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization
[4] https://www.fcc.gov/general/rules-regulations-title-47

- 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;

  Como referência internacional para padrões de qualidade/confiabilidade destaca-se o trabalho do órgão de padronização europeia ETSI para Internet das Coisas [1]. Oferece extenso mapeamento dos padrões existentes, que são específicos para os diferentes aspectos ou "Áreas de Conhecimento" (como

definidas no AIOTI WG03) dentro da arquitetura. Para a área dedicada a "Comunicação e Conectividade", o relatório técnico ETSI TR 103 375 v1.1.1 (2016-10) indica especificações de protocolos em todas as camadas. No tocante às métricas de desempenho, verifica-se que são itens em desenvolvimento, conforme relatório técnico ETSI TR 103 376 v1.1.1 (2016-10), pois ainda estão em desenvolvimento, sendo considerados lacunas potenciais a serem desenvolvidas.
[1] http://www.etsi.org/technologies-clusters/technologies/internet-of-things

- 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;
  A destinação de radiofrequências para serviços de telecomunicações para sistemas IoT deve estar alinhada com evolução da tecnologia com potencial para oferecer serviços e aplicações com qualidade e confiabilidade, livre de interferências prejudiciais. Atualmente, verifica-se na expansão das redes de serviços móveis celulares e no desenvolvimento de redes 5G, que ocorrerão em novas faixas de frequência, o atendimento a esses requisitos de qualidade. Assim, para que o desenvolvimento de IoT ocorra em ambiente regulatório com barreiras minimizadas, entende-se que não se deve dedicar faixas de espectro específicas para sistemas IoT, deixando-se livre o desenvolvimento do mercado. Em análise com a indústria será possível avaliar quanto espectro licenciado e não licenciado será necessário.
  Cita-se algumas atividades internacionais sobre espectro: 1) CCP.II, Radiocomunicações, com avaliação das prioridades regionais em preparação para CMR-19, aprovação de recomendações regionais e verificação para não criar fragmentação na utilização do espectro; 2) UIT-R GT 5D, Sistemas IMT, com Questão 9.1.8 da CMR-19 (relatórios e recomendações sobre MTC e IoT) e com início de trabalho em um novo relatório com informações de diferentes verticais da indústria; 3) UIT-R TG 5/1, com item de agenda 1.13 da CMR-19 (novas faixas de espectro para IMT, para banda larga móvel 5G).

- Outras assimetrias regulatórias e tributárias entre os serviços de telecomunicações destinados a IoT e aos usuários em geral;
  Ao permitir a conexão dos mais diversos dispositivos hoje existentes e muitos que estão por vir, a Internet das Coisas possibilitará o monitoramento, medição e controle de quase tudo que nos cerca, permitindo uma verdadeira revolução dos processos que conhecemos e abrindo caminho para o desenvolvimento de muitos outros, ainda inimagináveis, que trarão maior bem estar à sociedade, produtividade, qualidade e gestão de recursos.
  Apesar de reconhecermos que o grande avanço da Internet das Coisas será perceptível através das aplicações que serão desenvolvidas, estas só terão efetividade se for possível a implementação de redes de comunicação de alta velocidade, com a mais ampla cobertura, assim como a instalação de dispositivos em tudo que se possa imaginar.
  O cenário que acabamos de descrever pode ser resumido por uma palavra: "Inovação". É impossível prever tudo o que está por ser desenvolvido, sendo,

portanto, um risco à inovação qualquer iniciativa de se prever e regular o que estar por vir. Neste cenário é fundamental:

- Que haja flexibilidade regulatória, que não bloqueie a inovação e a oferta de novos serviços, permitindo inclusive a existência de assimetrias se estas forem necessárias para as diferentes aplicações.
- É importante reconhecer que diferentes aplicações requerem diferentes graus de qualidade e confiabilidade. Aplicações de condução autônoma de veículos e controle de tráfego ou ainda de medicina à distância, que permita a realização de cirurgias remotamente, requerem elevadíssimos parâmetros de qualidade, robustez e confiabilidade, comparadas a aplicações de medição de consumo de água e energia.
- No novo cenário de TICs que se avizinha, é recomendável a adoção de um modelo regulatório "ex-post", para a eventual necessidade de corrigir assimetrias de mercado.
- Que haja redução ou isenção tributária que permita o florescimento de modelos de negócios inovadores.
- A proliferação de novos dispositivos conectados e o desenvolvimento de novos modelos de negócios só serão possíveis se os encargos tributários não inviabilizarem sua existência. A recente redução tributária sobre dispositivos M2M comprova a necessidade dessa nova postura.

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

  A partir de levantamento da consultoria Machina Research em 2014 [1], entre 68 países consultados, 11 permitem, 52 não possuem regulamentação (provavelmente permitem), em 3 não há regulamentação (provavelmente proíbem) e apenas em 2 países, sendo um deles o Brasil, não aceitam o roaming internacional permanente.

  Os prós e contras podem ser elencados em função da experiência dos países. Em países que não permitem, os argumentos contra o Roaming Permanente são:

  1) Esses países possuem tipicamente mais atuação regulatória sobre o mercado, regulando a competição. Não se deseja, por exemplo, que uma única empresa venha a dominar o mercado. As empresas estrangeiras não possuem licença direta para operar no mercado nacional e há sempre discussões se o acesso ao mercado deve ser feito através de acordo de roaming negociado comercialmente.
  2) Esgotamento da faixa de numeração quando os dispositivos IoT usarem numeração extraterritorial. O atendimento a escala global pode esgotar rapidamente as faixas de numeração. Essa situação depende dos recursos disponíveis. Também há desafio logístico na criação de novas faixas
  3) Proteção ao consumidor pode não ter segurança legal suficiente quando o contrato é feito com firma estrangeira, se comparado quando é feito com firmas nacionais. No entanto considera-se que poucos serviços IoT serão de venda de serviço B2C. No caso de o provedor de serviço contratar operadora internacional de comunicação, não há implicação direta para o consumidor.

4) Interceptação legal de operação de comunicação eletrônica, por exemplo sobre cartões SIM, seria mais complexa de ser implementada.
5) Taxas de licenciamento pagas pelo operador a órgão regulador sobre numeração E.164 doméstica que não seriam pagas no uso de SIM cards em roaming.

Os argumentos a favor do roaming permanente são os seguintes:

1) Ainda não foi detectado problema significativo nos países onde foi permitido, pois o impacto de SIMs em roaming permanente tem sido pouco notado. Entretanto pode haver crescimento de escala no mercado, pois a consultoria Machina Research previu que entre 2013 e 2023 as conexões M2M celulares em todo o mundo crescerão de 3% para todos os SIMs para 21%.
2) Manter as implementações existentes para não haver interrupção massiva. Como exemplo, na Europa aproximadamente 25% dos SIMs M2M operam em roaming. Se fosse proibido, a grande maioria desses SIMs deveriam ser desativados, impactando fortemente os custos dos serviços.
3) Consideração que o roaming permanente é ferramenta temporária, pois as conexões M2M serão apenas de dados e não necessariamente precisam ser endereçadas por número E.164. Entretanto o uso de IPV6 no futuro e o processo de substituição do E.164 ainda não está claro. A principal razão para ser considerado temporário é o uso de gerência de subscrição, que com o aumento de MNOs (e provedores de serviços M2M) permitirá a localização de um cartão SIM dentro de rede nacional.

[1] https://machinaresearch.com/what-we-do/advisory-service/m2m-iot-regulation/

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

A realidade da Internet das Coisas obrigará que uma infinidade de produtos, que em sua essência não são "inteligentes" e nem wireless, passem a ter circuitos de RF integrados.

Atualmente a certificação de produtos com circuitos de RF faz parte do escopo da Anatel, e a imensa maioria dos dispositivos aprovados pela Agência ainda está circunscrita aos limites dos produtos tradicionalmente vistos como de telecomunicações (ex: telefones celulares, antenas, cabos, etc).

Com o desenvolvimento dos mercados de IoT e suas verticais no Brasil haveria uma avalanche de produtos a serem testados e avaliados e, consequentemente, uma enorme demanda pela certificação destes, o que acabaria por impor muito mais desafios e gargalos aos já escassos recursos da Anatel.

Desta forma, propomos que produtos de IoT tenham um regime de certificação voluntário, o que permitiria um acesso mais rápido dos mesmos ao mercado, menos burocracia e menos custos.
Muitos dos dispositivos IoT serão produtos simples e baratos, podendo em várias situações não se justificar financeiramente os gastos com testes para um eventual processo de certificação compulsório.
É também razoável supor que o parque laboratorial brasileiro não daria conta de atender a diversidade e a quantidade de dispositivos IoT que eventualmente teriam que ser testados e certificados.
Assim, propomos também como medida auxiliar que sejam criadas definições claras de produtos IoT (para diferenciá-los dos produtos tradicionais de telecomunicações), afim de delimitar os dispositivos passíveis dessa certificação voluntária.
Muitos dos dispositivos IoT serão de dimensões reduzidas, portanto, solicitamos que mesmo que fabricantes e distribuidores optem pela certificação estes sejam dispensados de marcações, selos ou etiquetas com logos e dizeres (como por exemplo, o que informa que o produto opera em caráter secundário). Além da questão dimensional, há que se considerarem como impeditivos destas marcações a questão da segurança (um selo colado a uma lâmpada por exemplo pode oferecer perigo ao usuário), a própria logística envolvida na colagem de um selo e os custos de confecção destas etiquetas. A fim de garantir ao consumidor a informação de que o dispositivo foi voluntariamente certificado, pode-se alternativamente haver alguma marcação na embalagem do produto.
Os aspectos de interoperabilidade estão sendo tratados nos organismos de padronização e principalmente por diversas alianças de fabricantes internacionais. Dada a vastidão do ecossistema IoT, a interoperabilidade também entre as alianças é buscada como requisito vital pelos fabricantes. Compõe-se dessa forma um cenário de multiplicidade de características de interoperabilidade sendo buscado pelos fabricantes, que naturalmente buscam essas certificações. No cenário de desenvolvimento de IoT no Brasil, sob o aspecto de produtos internacionais, a busca da certificação através de processo de reconhecimento mútuo se mostra uma abordagem facilitadora da inserção destes no mercado nacional. Outro aspecto é para que a inovação brasileira tenha campo, o acesso a essas normas e requisitos deve ser facilitado e agilizado pelos organismos brasileiros competentes, abrindo espaço para o franco desenvolvimento dos produtos e soluções nacionais.
Assim, entende-se que a certificação deve ser voluntária, com reconhecimento mútuo, estabelecendo-se também a certificação por declaração de conformidade. A Anatel deve continuar certificando apenas os aspectos já previstos atualmente, ligados principalmente à parte de RF, compatibilidade e segurança elétrica, etc. A avaliação de interoperabilidade deve ser deixada os fabricantes e alianças, pois com tantos sistemas disponíveis, será impossível “garantir que toda a solução seja interoperável”, conforme destaque na pergunta.

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

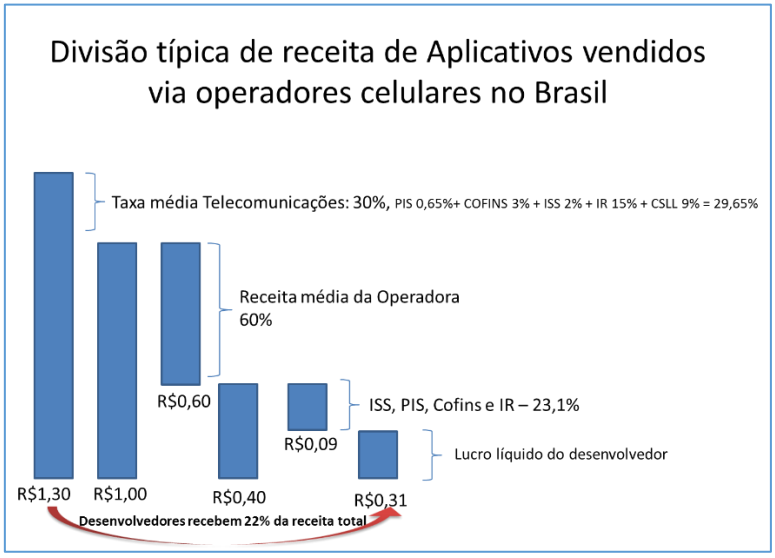
Para apoio ao diagnóstico completo de IoT no Brasil, cita-se as atividades internacionais sobre políticas para IoT, a saber:

- CITEL CCP.I "Políticas TIC", que aprovou uma Recomendação para as Américas, incluindo flexibilidade regulatória para encorajar o desenvolvimento e a adoção de IoT, promoção da neutralidade tecnológica, revisão de requisitos de certificação e elaboração de regras de proteção de dados que permitam o fluxo de dados entre fronteiras;
- *PCC.I/REC. 26 (XXVIII-16)* a Comissão Interamericana de Telecomunicações (CITEL) da OEA recomenda1 que adotem frameworks de proteção de dados que permitam fluxos de dados internacionais entre uma máquina localizada no respectivo Estado Membro e uma máquina em outro país, reconhecendo o equilíbrio entre a necessidade da coleta, do tratamento e da utilização dos dados e a necessidade dos usuários finais de dispor de um nível adequado de privacidade.
- UIT-T CE 20 "IoT", estudando estruturas e roadmaps para o desenvolvimento harmonizado e coordenado de IoT, incluindo comunicações M2M, redes de sensores onipresentes e cidades inteligentes.
- IEEE P2413 Standard for an Architectural Framework for the Internet of Things (IoT)
- ISO/IEC JTC1 WG10 "Internet of Things"
- ITU Study Group 20 "IoT and its applications including smart cities and communities".
- IEC SEG 7 – Smart Manufacturing
- IEC SyC – Smart Energy

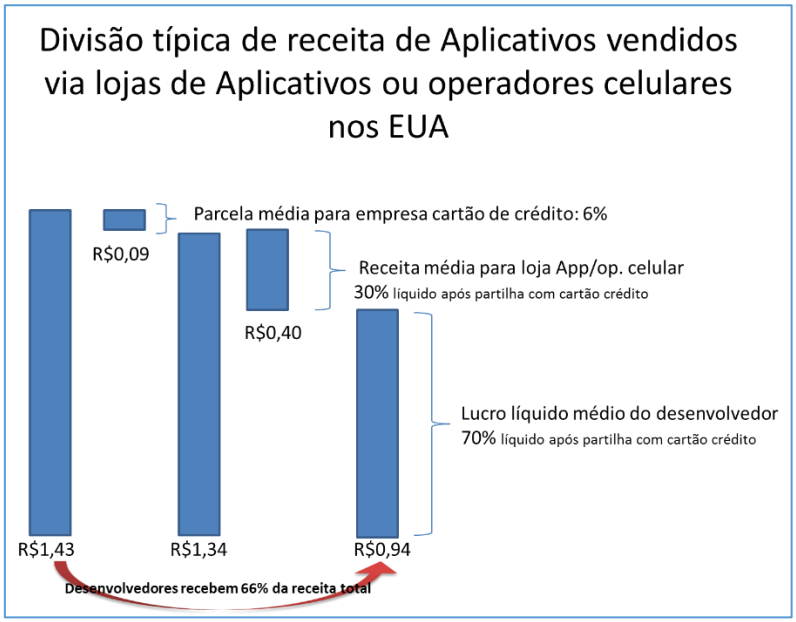
1.6 Qual impacto a carga tributária do Brasil pode ter sobre o ecossistema de Internet das Coisas?

A carga tributária no Brasil se configura excessiva, impondo obstáculos ao crescimento econômico. O ecossistema IoT, que abrange desde o processo produtivo de inúmeros dispositivos, as importações de itens, a venda de produtos e soluções, o estabelecimento de empresas, os investimentos em inovação e a geração de empregos, além de outros aspectos, será afetado pelos excessivos tributos em cada uma dessas áreas. Na venda de produtos, cerca de 50% do seu custo é oriundo de impostos federais e estaduais. A tributação em cascata encarece os custos de produção e os valores finais de produtos e a prestação de serviços, sendo necessário buscar a unificação dos impostos. Além disso, essa distorção alimenta a burocracia. Em relação ao custo de mão de obra, verifica-se que a carga trabalhista no Brasil é cerca de 2.7 vezes a carga na China, impactando fortemente manter empresas, particularmente as nascentes que precisam de tempo de maturação para se estabelecerem no mercado.

Em particular, cita-se o exemplo do custo do desenvolvimento de aplicativos para celular e o retorno para o desenvolvedor. O valor que ele receberá será cerca de 22% do custo de venda do aplicativo, configurando um percentual muito baixo, e extremamente desestimulante para esse mercado. Esse cálculo considera a primeira taxação sobre o valor da venda, de cerca de 30% (PIS 0,65%+ COFINS 3% + ISS 2% + IR 15% + CSLL 9% = 29,65%). Após esse desconto, retira-se 60% para o operador (MNO), e os demais 40% a serem pagos para o desenvolvedor, ainda são taxados novamente em 23% (ISS, PIS, Cofins e IR). Por fim, o que o desenvolvedor recebe é cerca de 22% do valor de venda. A figura abaixo ilustra as etapas dos impostos.



Nos EUA, esse mesmo estudo foi realizado, e o percentual que o desenvolvedor do aplicativo recebe pe cerca de 65% do valor de venda. A figura abaixo ilustra a parcela de 6% direcionada para o cartão de crédito, e a seguir o operador MNO fica com 30%.



1.7 Existem outros fatores fiscais ou tributários que impeçam o desenvolvimento do Ecossistema?

Para que sejam reduzidos os fatores tributários que impactam o desenvolvimento do ecossistema, sugere-se a ampliação da categoria de dispositivos que possuem Fistel reduzido. Assim, dentre os incentivos para o ecossistema IoT, tem-se que os dispositivos classificados pela Anatel como "Terminais M2M" possuem taxa de Fistel reduzida. Entende-se que esse incentivo pode se estender aos dispositivos e também aos serviços.

Além da classificação dos terminais para fins de redução de imposto, sugere-se a criação de categorias de serviços M2M que tenham redução de imposto de serviços (ISS). Como exemplo, usar as categorias para MTC sugeridas no documento do 3GPP TS 22.3688, ("Especificações Técnicas dos Grupos de Serviços e Requisitos de Serviço para MTC"). Esse documento define que comunicações MTC diferem dos atuais serviços de comunicação de redes móveis pois envolvem diferentes cenários de mercado, comunicação de dados, baixos custos, potencial número elevado de terminais de comunicação, e em grande escala, pouco tráfego por terminal. Alguns serviços MTC e aplicações MTC podem aceitar requisitos de desempenho menos críticos. Como exemplo, podem ser classificadas aplicações MTC dentro das seguintes áreas de serviço: segurança, rastreamento, pagamento, saúde, controle de sensores (iluminação, bombas, válvulas), medição e dispositivos para o consumidor.

Outra abordagem indicada é a da NGMN Alliance, que propõe categoria com base em características técnicas das aplicações (p. ex número de nós, alcance, potência, mobilidade, taxa de dados). Nesse sentido, sugere-se aplicar categorias mais detalhadas de dispositivos/serviços como extensão do Decreto 8.234/2014. De forma geral, a categorização pode contemplar serviços por seu impacto social (p. ex Smart grid, Water metering, etc), por área de serviço (segurança, rastreamento, pagamento, saúde, controle remoto, medição e dispositivos para o consumidor) ou dispositivos/soluções por especificação técnica (p. ex número de nós, alcance, potência, mobilidade, taxa de dados).

De maneira geral, a tributação sobre serviços IoT/M2M deve ser razoável para permitir a introdução do serviço IoT/M2M. De acordo com a Comissão Interamericana de Telecomunicações (CITEL)1 da OEA, "os governos devem considerar a implementação de isenções ou incentivos fiscais para promover o investimento e a pesquisa e desenvolvimento dos serviços de IoT/M2M ".

Segundo um recente relatório da GSMA[2], a Internet móvel e novas tecnologias como a M2M têm se beneficiado de um tratamento tributário preferencial em relação à telefonia móvel básica em alguns estados brasileiros. Entre os segundos trimestres de 2014 e 2015, o número de cartões SIM M2M cresceu 1,5 milhões de ligações, um aumento de 17%.

Embora isso já tenha sido reconhecido em isenções regionais de serviços específicos de banda larga móvel do ICMS e na redução federal das taxas FISTEL para os cartões SIM M2M, mais poderia ser feito no nível federal. Os serviços móveis no Brasil ainda estão sujeitos a maiores taxas de ICMS específicas do setor,

um imposto de vendas estatal de valor agregado, que varia de 25% a 35% (O ICMS sobre bens e serviços padrão varia entre 7% e 25%).

Apesar do Brasil ser atualmente o quarto maior mercado mundial de M2M, novas reduções de impostos poderiam incentivar a contribuição do setor para o crescimento econômico e social no país. Ao reformar a tributação sobre o setor móvel e transitar para uma estrutura de tributação mais equilibrada onde o móvel é tributado de forma semelhante a outros bens e serviços, o governo do Brasil poderia avançar para uma economia competitiva inclusiva e baseada no conhecimento, além de potencialmente se beneficiar do aumento das receitas fiscais no curto prazo como resultado do crescimento adicional do PIB.

Neste sentido, também devem ser levados em conta alguns cenários adicionais para estudar o impacto da redução da tributação específica sobre o setor móvel de conectividade e serviços, especialmente no que diz respeito aos serviços IoT, que poderia melhorar ainda mais as aplicações inovadoras e abrir possibilidades para o setor aumentar seu valor econômico através de toda uma nova geração de produtos e serviços no Brasil.

Concluindo, de acordo com este relatório, alguma reforma fiscal poderia adicionalmente ser feito. Tais como: a abolição de fundos setoriais como FUST e FUNTTEL; unificação e simplificação tributária, redução de carga tributária sobre serviços, dispositivos e investimentos em infraestrutura e outros.

Ref. 1: PCC.I/REC. 26 XXVIII-16

Ref. 2: Digital Inclusion and Mobile Sector Taxation

2. 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.

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

O Estado deve tomar a liderança na adoção em grande escala da Internet das Coisas para demonstrar os benefícios que a tecnologia pode trazer para a Administração Pública e a sociedade, fomentando a sua utilização.
Investir em tecnologia inteligente para projetos de infraestrutura pública aumentará a segurança, reduzirá os custos de manutenção e melhorará as operações. Além disso, esses projetos gerarão dados valiosos que deverão ser

disponibilizados ao público e a iniciativa privada para promover a inovação e o consequente desenvolvimento de novos produtos e serviços.

Com relação as parcerias, muitos projetos de IoT poderão ser beneficiados através do estabelecimento de parcerias entre Estado e iniciativa privada. Isto permitirá que cidades com orçamentos escassos, ou sem orçamento, consigam realizar investimentos em projetos de IoT que possam auxiliar ou melhorar o desenvolvimento urbano, podendo usufruir de todos os benefícios e progresso trazidos pela IoT. Como exemplo, temos Mumbai, na Índia, que através de uma parceria entre Estado e uma empresa privada de medição inteligente conseguiu identificar uma falha na infraestrutura de saneamento (água tratada) que gerava a perda de 50% de toda água que era consumida diariamente.

Outrossim, é notório que o ecossistema de IoT no Brasil está florescendo e, por encontrar-se nesta fase inicial de desenvolvimento, entendemos ser tentadora a ideia de o Estado propor sua regulamentação buscando assim prever e abordar todos os tópicos e cenários que atualmente apresentam-se como relevantes, mas que, rapidamente, ficarão ultrapassados. Entretanto, esta abordagem gerará uma regulamentação que nascerá obsoleta, tendo em vista o constante e veloz processo de evolução da IoT, criando entraves de difícil transposição para a continuidade de seu desenvolvimento e adoção no país.

Como consequência não-intencional e prejudicial de uma eventual regulação precoce, poderemos nos deparar com a drástica limitação ou quiçá paralisação do processo de inovação do ecossistema de IoT.

Uma proposta de regulamentação específica para IoT poderá causar sua fragmentação, dificultando a interoperabilidade entre dispositivos e a agregação de dados entre distintas plataformas. Há que se entender que, apesar da tecnologia de IoT ser revolucionária em certos aspectos, ela se configura como uma extensão de uma tecnologia já existente. A harmonização da regulamentação vigente em diferentes setores da economia brasileira aos respectivos produtos e serviços de IoT por eles utilizados nos parece suficiente para guiar o desenvolvimento deste mercado no país ao longo dos próximos anos, afastando a necessidade de edição de regulamentação própria.

Cabe ressaltar que a propositura de uma regulamentação deve ser baseada em decisões e recomendações fundamentadas em rigorosa análise econômica e empírica, tendo como objetivo resolver questões específicas e persistentes que afetam e prejudicam determinado setor da economia. Outrossim, a decisão de criar uma regulamentação deve basear-se em evidências e não em especulação. Quer dizer, a intervenção do Estado deverá ocorrer apenas quando o próprio mercado não conseguir solucionar uma questão prejudicial e persistente.

Contudo, não é este o cenário que verificamos no Brasil. Pelo contrário, as aplicações de IoT são utilizadas em uma miríade de setores da economia e o seu ecossistema ainda está em desenvolvimento. Ou seja, não são identificados pressupostos que possam ensejar a necessidade de criação de uma regulamentação para este mercado.

Desta forma, entendemos que o Estado deve adotar uma posição de observador neste momento, aguardando o desenrolar da evolução da IoT no país, visto que este ainda é um mercado nascente. Outra sugestão é harmonizar as estruturas regulatórias já existentes nos diferentes setores da economia para que elas abarquem as necessidades dos respectivos produtos e serviços de IoT, respeitando-se suas especificidades técnicas.

Outro ponto relevante a ser levantado foi a criação, em 2014, da Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas (Câmara IoT). Agregando diferentes atores do ecossistema de M2M e IoT, a Câmara IoT dá suporte à definição de cenários, diagnóstico de barreiras e identificação de pontos de ação, pois sua atuação junto a outros organismos e no âmbito dos Ministérios permite um olhar transversal das necessidades e possibilidades. Entende-se que ela atuará fortemente nas áreas Horizontais, uma vez que esses temas podem vir a definir as políticas públicas necessárias para o desenvolvimento de IoT.
Por fim, o Estado também deve buscar o diálogo constante com as Associações que representam as empresas que atuam no ecossistema de IoT, para ouvir o que o mercado tem a dizer, buscando entender as dificuldades/barreiras que serão identificadas por estas Associações e atuando de forma rápida para elaborar mecanismos de saneamento destas dificuldades.

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

O Estado deve dar prioridade às áreas que demandam maior investimento tecnológico e agregam retorno estratégico e/ou financeiro para o país. Desta forma, Indústria, Agricultura, Saúde, Segurança, Meio Ambiente, Educação, Infraestrutura, Energia, Telecomunicações e Bens de Consumo devem ser indicadas como áreas estratégicas para desenvolvimento do ecossistema de IoT.

As ações para criação deste ecossistema favorável devem ocorrer desde o início, abarcando a nova onda tecnológica e seus benefícios, definindo objetivos e identificando barreiras, de forma a favorecer todos os aspectos de desenvolvimento.

Nesse sentido pode-se desenvolver uma cadeia de participação a partir do conceito das verticais, integrada por diversos órgãos, academia e setor privado. Como exemplo, a vertical Agricultura deve ter a participação do Ministério de Agricultura, Secretarias estaduais e Centros de Pesquisa de Agronomia, que deverão identificar ações a serem adotadas e objetivos comuns. Além disso, sugere-se que o Estado monitore a efetividade de políticas públicas avaliando o incremento no PIB relacionado a essa vertical.

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

Entende-se que o Estado pode vir a ser um cliente potencial (consumidor) de soluções para melhoria da máquina pública, desde oferta de serviços básicos para a sociedade, p.ex. nas áreas de saúde, educação, saúde, segurança pública e meio ambiente, até a melhoria de infraestruturas através da implantação de cidades inteligentes. Nesse caso, é crucial identificar as demandas específicas das cidades, e a partir delas delinear as soluções necessárias. Nesse contexto destaca-se a importância do Estado como consumidor de soluções, movimentando a economia, no entanto sem atuar de forma impositiva como a criação de obrigações (p. ex. de adoção de soluções técnicas obrigatórias em setores públicos) que onerem ainda mais as empresas fornecedoras de soluções. O Estado pode ser grande fomentador de iniciativas de negócios, promovendo encontros para agregar demandas e ofertantes de soluções, atraindo empresas pequenas e médias para apresentar soluções para casos ou demandas específicas.

2.4 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?

Sim, cabe ao Estado, através de desenvolvimento ou adaptações não somente dos instrumentos fiscais, mas jurídicos e alfandegários, incentivar o desenvolvimento e comercialização de produtos ligados à IOT e Indústria 4.0. Considerando ainda que uma das principais vantagens da adoção em larga escala de soluções de IoT é o ganho de eficácia e redução de custos, eventuais renunciais fiscais que alavanquem o setor podem ser compensadas pela economia gerada. É estratégico para o Brasil que a nossa Indústria esteja na vanguarda tecnológica, pois, as grandes ondas de crescimento econômico mundiais foram relacionadas às revoluções industriais.

É fato que os incentivos fiscais existentes, tais como a Lei do Bem, a Lei de Informática, PADIS e PADTV de apoio a P&D nas empresas, atuam de forma ampla para atender fabricantes nas áreas ali destacadas.

Caso o Estado não desenvolva ou adapte, os instrumentos fiscais atuais continuarão desatualizados e não compatíveis com o cenário tecnológico e dinâmico existente hoje no mundo. Se não houver agilidade na adaptação de legislação e procedimentos do Estado e uso estratégico das regras comerciais internacionais não há como desenvolver e, posteriormente, entregar produtos e serviços desenvolvidos no país para a comunidade internacional.

Além disto, a obstrução ao desenvolvimento pode ocorrer quando a regulamentação é muito complexa e detalhista, dificultando a aplicação. Por esse motivo, deve-se atentar para o foco dos incentivos, de forma a não ficarem restritos à tecnologias de IoT.

Deve ser aprovada também legislação afastando a incidência das taxas do setor de telecomunicações (Fust, Fistel e Funtel) das soluções de IoT. Bem como é

interessante desenvolver ou adaptar instrumentos fiscais para apoiar o avanço das tecnologias de comunicação, em particular as comunicações celulares com foco em IoT (4G e 5G)

2.5 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?

O desenvolvimento de novas soluções de IoT no Brasil e a mais rápida aplicação no País de tecnologias desenvolvidas em ouras partes, assim como a participação de desenvolvedores brasileiros em projetos e iniciativas internacionais de P&D colaborativo são amplamente dependentes da segurança percebida na proteção dos direitos de propriedade intelectual para esse tipo de invenções no Brasil.

Há duas questões fundamentais a serem tratadas no campo do papel do Estado na garantia dos direitos de propriedade intelectual, que se entrelaçam e conjuntamente desfavorecem o desenvolvimento da IoT no Brasil: o atraso no exame e concessão de patentes, particularmente insustentável no campo das TICs, e a incerteza quanto ao alinhamento do posicionamento do INPI (e do judiciário brasileiro) às melhores práticas internacionais de avaliação dos requisitos para concessão de patentes no campo dos inventos baseados em programas de computador.

O atraso gera imensa insegurança e incerteza jurídica. Efetivamente, se não se reduzir o tempo de exame para algo internacionalmente aceitável, dificilmente se poderá eleger o Brasil como hospedeiro de iniciativas de P&D no campo da IoT. A patente concedida é condição necessária para o investimento, e este tem data de validade: ele não espera, é feito em outro lugar.

Quanto a qualidade do exame, deve-se dizer que o INPI tem tido, em geral, um posicionamento equilibrado, garantindo a concessão de patentes importantes nesse campo, como foram as dos sistemas de compressão de dados e outras. Contudo, o imenso atraso no exame de patentes nas áreas de TI e telecomunicações impede uma avaliação mais consistente do nível de harmonização entre as decisões do INPI e as dos principais escritórios de patentes no que tange aos avanços recentes da técnica. A incerteza se agrava devido ao fato de que apenas muito recentemente foram publicadas diretrizes para exame de patentes de invenções baseadas em programas de computador, e assim sendo, sua interpretação não está ainda sedimentada. A Lei 9279/96 é considerada pouco clara no que tange à proteção desse tipo de invenções, o que torna imprescindível a rápida consolidação de um entendimento do INPI acerca do assunto alinhado às melhore práticas internacionais, o que é possível à luz das novas diretrizes, mas ainda não está assegurado. Da clareza do entendimento do INPI se seguirá a pacificação da jurisprudência – desde que se resolva o problema do atraso.

Outro problema é a falta de informação dos depositantes que não apontam corretamente o título ressaltando serem patentes relacionadas a IoT, pois isso aumenta problemas entre requerentes de mesma patente (p.ex. problema na

busca de patentes, justamente porque o requerente da patente com IoT não menciona no título).

Mais uma questão a ser avaliada é a falta de proteção para softwares que, embora previsto na lei, é facultativo e por isso muitas empresas não efetuam esta proteção. Entende-se que a P&D&I só avança se houver proteção devida do que é inventado, e para IoT patentes e softwares.

O problema é mais a parte prática: além do sistema de proteção patentário no Brasil ser lento (INPI ainda demora muito para processar pedidos), as pessoas são pouco informadas e não depositam patentes por não saberem, não terem um bom aconselhamento técnico e jurídico, bom monitoramento para controlar prazos, pagamento de taxas, etc. Além disso, o software no Brasil, apesar da lei estar bem feita, não garante proteção efetiva pois não há busca de software quando um requerente tem interesse em proteger. O INPI (diferente de patente e marca) simplesmente confere a titularidade e se houver algum problema de conflito, será resolvido na Justiça, que notoriamente é lenta. Deveria haver maior proteção, controle, efetividade numa busca e não simplesmente conceder titularidade de um software para quem busca o título no INPI. Claro que este título pode ser depois anulado, mas com base na decisão judicial. No Brasil não há uma prática em proteger softwares no INPI, até porque este tipo de registro é facultativo (o sw é considerado direito autoral).

Entende-se que o fato do Estado assegurar a PI não afeta a IoT no Brasil, até porque o número de patentes depositadas sobre este assunto é extremamente baixo. Comparando-se com países no exterior, a representação do Brasil nesta questão está em baixa e isto não é devido à existência da lei (reconhece-se que é muito bem estruturada). O problema reside na falta de colocá-la em prática.

Torna-se importante a preocupação com um retorno significativo para os agentes envolvidos no processo de P&D e com a garantia dos direitos de propriedade intelectual de possíveis patentes adquiridas, pois os elevados investimentos em P&D para o desenvolvimento de novos projetos com base na IoT de perspectiva multidisciplinar pode ser um fator determinante para evolução dessa tecnologia, como também, para o alcance de uma escala de produção comercial aceitável pelos investidores e desenvolvedores de aplicações.

Há pesquisas e projetos que estão avançando, principalmente na China e Estados Unidos, países que mais investem em PD&I para IoT. A maioria dos pedidos de patentes recuperados nas bases de dados consultadas, principalmente os contemporâneos, pertencem a esses dois países. Isto reflete o fato de suas economias continuarem crescendo. Observou-se também que a China ocupa a primeira posição em número de pedidos de patentes de IoT, e os Estados Unidos ocupam a segunda posição.

No Brasil, apesar da quase ausência de patentes como dito acima, existem projetos que utilizam essa tecnologia. Entende-se que estejam faltando os recursos financeiros para investimento em P&D que proporcionem estudos de maior complexidade para aplicações mais ousadas com IoT, e assim justificar pedidos de patentes para proteção de novas tecnologias desenvolvidas por brasileiros com a Internet das Coisas.

Ressalta-se a revisão da Lei de Patentes para incentivar a iniciativa privada a investir mais no Brasil e ter tranquilidade em relação à exploração das patentes.
Por outro lado, há uma visão mais específica sobre redução da interferência do Estado, na qual entende-se que a forma de atuação do Estado em PI desfavorece o desenvolvimento de IoT no Brasil, e, por isso, o Estado deve deixar que o assunto seja definido entre as partes, sem interferência.
Ao Estado somente deveriam ser asseguradas as licenças compulsórias nos casos de emergência nacional ou interesse público, declarados em ato do Poder Executivo Federal, desde que os titulares dos direitos de propriedade intelectual e ou seus licenciados não atendam a essas necessidades. (Texto adaptado do Art. 71 da Lei 9.279, de 14 de maio de 1996, que regula direitos e obrigações relativos à propriedade industrial, mas que poderia ser utilizado para qualquer direito de propriedade intelectual)
Com isso, o Estado, através dos seus órgãos que eventualmente podem estar envolvidos no desenvolvimento de propriedade intelectual com outros atores da sociedade em geral, ficaria isento de custos de gerenciamento e registro de propriedade intelectual nos países onde existe mercado efetivo para uso dessa propriedade e da sua respectiva manutenção nesses países, podendo utilizar seus recursos para aquilo que efetivamente é seu foco, ou seja educação, saúde pública, segurança pública e meio ambiente.
Assim sendo, se mantidos os processos legais de registro de propriedade intelectual nos órgãos competentes e sem a interferência do Estado na preservação de direitos de propriedade intelectual, não só o desenvolvimento de IoT seria estimulado no Brasil – também o seria o desenvolvimento de outras tecnologias e a introdução das inovações daí advindas no mercado seria mais rápida.
Com relação ao INPI, para garantir os direitos de propriedade intelectual aos atores da sociedade, o Estado deve agir com celeridade de forma que tais atores sintam-se protegidos na administração dos seus negócios. Uma forma de garantir isso, no curto e médio prazo é a de estender o PPH para TIC e IoT/M2M.

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

Em primeiro lugar, para identificação das barreiras para produção no Brasil, cita-se a Sondagem Industrial feita pela CNI com pequenas, médias e grandes indústrias em dezembro de 2015. Os principais problemas citados na pesquisa indicam, em ordem decrescente: 1) carga tributária elevada, que equivale a 36% do PIB; 2) demanda interna insuficiente, reflexo do cenário político, provocou redução na produção, nos investimentos (queda de 13,4%) e famílias reduziram as compras (queda de 2,3% em relação a 2014), enfraquecendo a economia; 3) falta ou alto custo da energia (alta de 12,4% no segundo trimestre); 4) taxa de câmbio com forte variação, prejudicando planejamento de importações e exportações, formação de preços e previsão de investimentos das industrias; 5) taxa de juros elevada, afetando custos e dificultando acesso ao crédito para empresas que precisam de financiamento para investir ou operar.

Por outro lado, é possível analisar a posição do Brasil no cenário internacional de inovação, e como isso reflete a atratividade por investimentos internacionais aqui no País. Como referência cita-se estudo feito pela Fundação de Tecnologia da Informação e Inovação (ITIF), que analisou 56 países responsáveis por 90% da economia mundial, para saber como as políticas internas de cada um impactam o ambiente internacional de inovação. Nesse estudo, o Brasil é classificado, junto com China, India, Rússia, Tailândia, Turquia e Vietnã, como "mercantilista de inovação", cuja definição descreve países buscam o seu crescimento através de protecionismo e com políticas de comércio distorcidas visando expandir a produção tecnológica doméstica e exportação de bens tecnológicos. O Brasil ficou em 41º lugar, com pontuação de -8,3, com nota negativa que significa que as políticas públicas brasileiras, no geral, prejudicam a inovação no mundo, por possuir vastas barreiras comerciais e apresentar ambientes mais fracos de proteção de propriedade intelectual do que o exigido pela norma global. O estudo destaca algumas políticas brasileiras que têm efeito negativo na inovação global:

1) Impostos altos sobre consumo: Brasil cobra 17% de impostos sobre produtos de tecnologia da informação e comunicação. A carga tributária reduz a adoção de produtos de tecnologia no país em mais de 20%, fazendo com que o crescimento da economia brasileira seja pelo menos 1,2 ponto porcentual menor do que poderia ser;

2) Exigências de conteúdo local: problema de barreiras de localização ao comércio, como exigências de produção mínima no país. Além de comunicações e tecnologia da informação, as exigências de conteúdo local brasileiras atingem setores como energia, máquinas e equipamentos, saúde, mídia, resseguros, têxteis, vestuário e calçados. Em 2010, barreiras de localização ao comércio, como as impostas pelo Brasil, afetaram cerca de US$ 928 bilhões do comércio mundial de bens e serviços, o que representou 5% dos US$ 18,5 bilhões negociados;

3) Tarifas elevadas de importação: Países como Suíça, Cingapura e Hong Kong praticamente não impõem tarifas de importação. Na União Europeia, elas costumam ficar abaixo de 1,5% e, nos EUA, a taxa média é de 2,81%. O Brasil está num grupo de países que impõem mais de 10% de tarifa de importação. Nos produtos de comunicação e tecnologia da informação, o Brasil e Argentina cobram mais de 12%;

4) Ausência de acordos internacionais: Países como o Brasil, que decidiram não participar do Acordo de Tecnologia da Informação em 1995, viram sua participação nas cadeias globais de valor de tecnologia da informação e comunicação cair mais de 60%. A tecnologia da informação tem participação menor que 1% nas exportações do Brasil, Chile e Argentina, que não participam do acordo. Em países em desenvolvimento que decidiram participar, como Costa Rica, Vietnã, China, Malásia e Filipinas, a tecnologia tem uma fatia de mais de 20% nas vendas ao exterior.

Entende-se que os processos de importação ou exportação podem ser melhorados para tornarem-se ágeis. Além deles, a complexidade tributária que

é maior para quem produz - tanto para comercialização local quanto para exportação - do que para quem simplesmente importa, desestimulando a localização de produção no país.

É necessário que haja incentivos para produção local para estímulo à produção de soluções tecnológicas.

O fato de também existir possibilidade de greves de fiscais da Receita Federal em portos e aeroportos e que podem ficar semanas sem serem resolvidas, também faz com que players potenciais que poderiam ser fornecedores a partir do Brasil deixem de considerar o país como uma alternativa para isso, principalmente em um mercado altamente dinâmico, onde os prazos são curtos e os custos para a implantação de soluções são extremamente altos.

2.7 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 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.

Sim. Certamente um dos mais promissores campos para a utilização de soluções de IoT é o setor público. Pode-se citar como exemplo o serviço de iluminação pública. Trata-se de típica obrigação do Estado que pode ser o ponto de partida para um projeto de Cidades Inteligentes. Assim, ao se adicionar uma solução de IoT a um projeto incialmente simples de mera substituição de lâmpadas de vapor de sódio por lâmpadas de LED, o Estado pode economizar muitos recursos e melhorar de maneira significativa a qualidade dos serviços prestados à população. Explica-se. Com a sensorização dos postes de iluminação pública e a criação de uma rede de comunicação interligando estes postes será possível agregar diversos outros serviços, como por exemplo, câmeras de segurança. Com isto, será possível adequar a iluminação das vias, de acordo com a necessidade. Ou seja, locais com pouco ou nenhum tráfego de pessoas e veículos, poderiam ter a iluminação reduzida em 20, 30, 40 ou até 50%, conforme a necessidade, gerando economia. Eventuais lâmpadas queimadas, seriam identificadas de maneira precisa e trocadas imediatamente, evitando que equipes façam vistorias periódicas para tanto. Consequentemente, serão necessários menos funcionários, gerando economia com salários e deslocamentos. Câmeras de segurança acopladas poderão ser utilizadas tanto para o planejamento de ações de segurança, incrementando o efetivo policial onde houver necessidade, quanto para o controle do fluxo de pedestres e pessoas ao se interligarem ao sistema de semáforos inteligentes, que ajustará o tempo de abertura conforme a necessidade. Isto melhorará o tráfego de veículos, reduzindo o tempo das

viagens, o que aumenta a qualidade do serviço e reduz a demanda por combustíveis fósseis, trazendo, novamente, economia. O mesmo raciocínio pode ser aplicado em relação ao planejamento dos investimentos públicos. Com soluções de IoT será possível mapear de maneira precisa os locais da cidade que estão crescendo e demandam novos serviços. Logo, o Poder Público poderá fazer seus investimentos na exata medida da necessidade da população, evitando erros e desperdícios. Em última análise, isto será uma maneira de se garantir a efetivação do princípio da eficiência, previsto no artigo 37, caput, da Constituição Federal.

2.8 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.

Questões relacionadas à logística e planejamento podem ser aplicadas em todas as esferas de governo.

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

As aplicações de IoT voltadas para os serviços públicos ou gestão pública visam o desenvolvimento de cidades inteligentes, que de forma geral são caracterizadas pela otimização de operações de serviços existentes e de processos de gestão (planejamento, logística, controle e fiscalização e gestão e execução orçamentária), além do surgimento de novos serviços.
Citam-se a área de distribuição de energia elétrica (implantação da infraestrutura avançada de medição, AMI, que são redes de comunicação com pontos concentradores e com a central de distribuição, e na ponta do consumidor o uso de medidores eletrônicos para gestão de consumo); área de transporte urbano nas cidades através da otimização de tráfego, controle de semáforos, vigilância para segurança pública, e área de saúde pública, no tocante à informatização de serviços, da digitalização de itens hospitalares, melhoria de gestão de recursos, estruturação de bancos de dados e melhoria de comunicação entre organismos públicos . Destaca-se também as áreas de educação, segurança pública e meio ambiente, indústria, agricultura, energia e petróleo, Serviços e Consumo.

2.10 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?

Considerando a vertical Cidades Inteligentes, na área de energia elétrica há desafios no âmbito da distribuição de energia que podem ser atendidos, a saber: redução do tempo de downtime da rede elétrica (parâmetro DIC), redução do percentual de perdas técnicas, através da otimização e melhor

detecção de falhas, redução do percentual de perdas não técnicas (roubos e desvios de energia), também o incentivo à indústria de medidores eletrônicos para inserção de novas interfaces de comunicação, p. ex. para integração com redes celulares, fomentando parcerias de pesquisa e desenvolvimento dos fabricantes. A integração da medição da rede de águas com a rede de medição de energia, e também com a distribuição de gás, pode trazer benefícios para a sociedade, desde indústria, com o desenvolvimento de produtos e soluções, capacitação de pessoal e geração de empregos.
Citam-se os problemas específicos de planejamento, logística, controle e fiscalização e gestão e execução orçamentária, além da necessidade de se utilizar os meios atuais para endereçar as melhorias em educação, saúde pública, segurança pública e meio ambiente.
Ressalta-se a importância do fomento à renovação tecnológica do parque fabril (Manufatura Avançada) e de desenvolvimentos para agricultura.
No desenvolvimento de Cidades Inteligentes a experiência internacional tem mostrado práticas de contratação extremamente eficazes, como p.ex. no Projeto H2020 na Comunidade Europeia. É feita a ação inicial dos Governos em incentivar a adoção de soluções através de chamadas de projetos com recursos financeiros, muitas vezes a fundo perdido, considerando parcerias com empresas privadas fornecedoras de produtos e soluções, com a quais se estabelece a implantação do projeto, e posterior gestão do mesmo, oferendo manutenção da infraestrutura. Essas parcerias são necessárias para que o projeto tenha continuidade, através da gerência adequada, com previsão de melhorias técnicas que surgem a partir da evolução da tecnologia ou para atendimento a novas demandas e crescimento.
As chamadas públicas para envio de propostas técnicas usariam os órgãos de fomento e projetos de PD&I onde a tecnologia de M2M e IoT teriam aspectos com várias categorias, incluindo inovação.

2.11 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.

A adoção de tecnologias de Comunicação M2M e IoT pode ser fortemente incentivada através dos editais para licitação de infraestruturas públicas, nos quais destaca-se a necessidade de definição de critérios que pontuem o uso de soluções com tecnologias IoT, visando implementar seu uso e principalmente sua continuidade de uso e constante evolução tecnológica. Nesse sentido, a atual legislação da Lei 8666 para licitações e contratos está sendo revista para modernização, e alterações estão sendo propostas através do PLS 559/2013.
As alterações incluem incentivo de uso de soluções tecnológicas. Cita-se como exemplo o Art.30 (Critérios de Julgamento) que apresenta texto abrangente, de forma a permitir o incentivo de soluções tecnológicas como parte do texto do edital a ser elaborado em cada caso. O entendimento é que a Lei crie condições para que isso aconteça.

Para que seja incentivado um formato de edital em que seja prevista mais pontuação para soluções IoT, esta ação pode ser iniciada no âmbito do organismo que solicita o edital.

Outro exemplo a ser citado é que o texto da Lei 8666 não havia menção à ponderação de nota entre técnica e preço, e isso foi incluído no Art.30.

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

O papel das PPPs é muito importante em algumas verticais, principalmente a de cidades inteligentes. A PPP pode ser realizada em áreas nas quais o Estado não possui experiência e nem capacidade suficientes para realizar a gestão e o controle de operação e manutenção. Como exemplo, uma infraestrutura de telecomunicações dedicada a oferecer redes wi-fi em áreas da cidade. A operação continuada da rede depende de manutenção e atualização do sistema, a ser feita por parceiro privado. Outro exemplo, PPP que ofereça serviços do Estado ou Prefeitura à população e ainda com possibilidade de exploração de serviço podem ser boas alternativas, para evitar que as redes fiquem sem manutenção e sem atualização tecnológica.
Entende-se que as PPPs nos próximos anos deverão ser focadas em modelos de negócio nos quais seja demonstrada uma redução de custos, e não somente em projetos de grande valor que posteriormente impactem nas contas públicas Atualmente, os compromissos com o consórcio são pagos, porém não ocorre nenhum benefício financeiro para os Estados.
Na área de pesquisa, cabe destacar iniciativa da Comissão Europeia sobre PPPs para pesquisa e inovação, conforme o link (http://ec.europa.eu/research/industrial_technologies/ppp-in-research_en.html), a qual está funcionando no âmbito do H2020. Há três projetos, o "Factories of Future" (FoF), "Energy-efficient Buildings" (EeB) e "Sustainable Process Industry" (SPIRE), que serão implementados via chamadas abertas. Como exemplo cita-se o programa H2020 voltado para as fábricas do futuro (FoF) para 2014-2020, publicado em final de 2013, disponibilizou €1.15 bi para esse período. Nesse contexto, as empresas privadas que patrocinam os projetos, podem depois explorar os resultados como serviços profissionais, implementando as soluções e plataformas. As universidades continuam desenvolvendo com novas classes de soluções e novos algoritmos [1]. A governança do projeto é dividida entre as instituições parcerias.
[1] http://cordis.europa.eu/result/rcn/177872_en.html

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

A barreiras geradas por burocracia complexa existem em diversas áreas. Destaca-se o processo de abertura e manutenção de empresas, cuja formalização exige certidões de diversos órgãos públicos, pagamento de taxas e obtenção de alvarás, o que dura cerca de 83 dias, 3 a 4 vezes mais do que os países do Bric, segundo estudo "Doing Business" do Banco Mundial. Há variação por Estados, e no caso de São Paulo a obtenção do CNPJ leva cerca de 30 dias. Nos casos em que há capital estrangeiro, a depender do Estado, o prazo pode aumentar para 90 dias. Em relação aos custos, o valor total pode chegar a R$5.000,00. Outro aspecto é o regime tributário da empresa, pois a carga varia conforme o ramo: prestadores de serviço possuem tributos de 20% sobre o faturamento, e no ramo indústria e comércio a carga é 35% ou mais. Um indicador de complexidade de burocracia é o tempo necessário para pagamento de impostos, cerca de 2600 horas/ano, enquanto que na América do Sul, por exemplo, gasta-se 359 horas/ano.

Os processos de importação ou exportação podem ser melhorados para tornarem-se ágeis. Além deles, a complexidade tributária que é maior para quem produz - tanto para comercialização local quanto para exportação - do que para quem simplesmente importa desestimula a localização de produção no país. O fato de também existir possibilidade de greves de fiscais da Receita Federal em portos e aeroportos e que podem ficar semanas sem serem resolvidas, também faz com que players potenciais que poderiam ser fornecedores a partir do Brasil deixem de considerar o país como uma alternativa para isso, principalmente em um mercado altamente dinâmico, onde os prazos são curtos e os custos para a implantação de soluções são extremamente altos.
A Lei da Propriedade Intelectual (no 9279, 14/mai/96) necessita de atualização para avançar na proteção *patentária* de produtos tecnológicos, ativos intangíveis e outros, como biotecnológicos, oriundos de evoluções recentes. É necessária redução na burocracia exigida pela legislação atual, para que seja possível oferecer mais eficiência do sistema de proteção às inovações. A demora no processo para reconhecimento de direitos traz insegurança jurídica para o inventor que precisa negociá-los.

Além disto, os processos de certificação de equipamentos de radiofrequência pela Anatel precisam ter sua burocracia revista para serem rápidos, tornando possível absorver o grande número de dispositivos de IoT que é esperado. Isso envolve a agilização da etapa de realização de ensaios pelo OCD. Nesse sentido, a implementação de acordos de reconhecimento mútuo de certificação poderá agilizar todo o processo.

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

Os países que estão estabelecendo diretrizes para IoT, de uma forma geral ainda não tem políticas públicas claramente estabelecidas, mas há em andamento ações e iniciativas que visam incentivar o desenvolvimento de IoT em seus países.

Nos EUA vários projetos em diversas áreas de tecnologia estão sendo desenvolvidos para apoiar o crescimento de IoT, porém ainda são considerados isolados, de pequena escala, e sem coordenação central. Considera-se que o Governo não possui ainda uma visão estratégia nacional para IoT, mas que nos próximos anos isso será atendido, visando organizar o apoio para permitir a ampla adoção no país. Nesse sentido, no início de 2016, foi lançado o DIGIT Act (Developing Innovation and Growing the Internet of Things Act), baseado nas questões da consulta pública lançada pelo NTIA (NTIA RFC on the Internet of Things). O DIGIT Act orientará a Secretaria de Comércio no estabelecimento de grupo de trabalho de governo, indústria, consumidores e stakeholders da sociedade civil para desenvolver políticas e práticas para apoiar o desenvolvimento de IoT, propor políticas para melhorar a coordenação das agências federais nos aspectos de IoT e identificar oportunidades para as agências fazerem melhor uso de IoT. Além disso, ainda orientará o FCC sobre análise das necessidades de espectro atuais e futuras para IoT, apresentando recomendações para suprimir barreiras. Assim, o DIGIT Act apoiará o desenvolvimento de uma estratégia nacional.

Dentre os projetos mencionados, cita-se 1) NIST, com grupo de trabalho "Cyber-Physical Systems Public Working Group" (CPS PWG), Maio/2016, que publicou o "Framework for Cyber-Physical Systems"; com o grupo "Sensing and Perception Systems Group" para pesquisa de metrologia para manufatura inteligente; com projeto "Advanced Metering in Smart Distribution Grids" para melhoria de sensores de medidores inteligentes; relatório ""Big Data Interoperability Framework", em Set/2015, sobre informação técnica e de taxonomia, padrões e tecnologias para dados, particularmente em IoT. 2) FTC (Federal Trade Comission), orientação de alto nível orientado para negócios sobre segurança em produtos IoT, Jan/2015.

No Reino Unido há uma política governamental para o desenvolvimento de negócios em IoT. Destaca-se o programa "IoTUK", o qual é financiado como parte de programa integrado de 3 anos de £32m para acelerar IoT, lançado pelo Governo UK. O fundo do Governo em IoTUK é de £4m, que financiará todos os diferentes componentes do programa ao longo dos 3 anos. Nesse cenário, as empresas privadas podem financiar os projetos que se originem dos encontros promovidos. O IoTUK não investe em projetos, pois declaram que não são incubadora nem investidores. São um programa sem fins lucrativos, para trabalhar com corporações, universidades, setor público somente com sua capacidade de coordenação e gerência. Os parceiros de IoTUK terão oportunidades de investimento com os projetos que entrarem no programa. A função do IoTUK é ajudar nos relacionamentos, e não prover fundos diretamente.

A Comissão Europeia apoia o crescimento de IoT através do Programa H2020, Programa de Pesquisa e Inovação que dispõe de aproximadamente €80 bilhões em fundos para período de 7 anos (2014-2020), para atrair investimento privado para desenvolvimento dos projetos. Ao longo de 2014 foram feitas 100 chamadas abertas, que atraíram 31115 propostas, dentre as quais 4315 foram eleitas aptas para receber fundos. Nesse grupo, foram feitos 3236 acordos de recursos, assinados até Abril/2015, captando cerca de €5.5 bilhões. Ressalta-se as chamadas referentes a desenvolvimento de Cidades Inteligentes (p. ex. "SCC-01-2014 - Smart Cities and Communities solutions integrating energy, transport, ICT sectors through lighthouse (large scale demonstration - first of the kind) projects), H2020-SCC-2014". Com o objetivo de desenvolver e replicar soluções integradas de energia, transporte e ICT através de parcerias entre municipalidades e indústria, o ponto mais importante é a ação das empresas privadas envolvidas, que atuam como mantenedoras das infraestruturas instaladas. Essas empresas recebem reembolso de seus custos elegíveis do projeto, sendo assim remuneradas pelo esforço inicial, e depois se responsabilizam junto às prefeituras, realizando operação e manutenção para que as cidades efetivamente usufruam das melhorias, e as empresas privadas tenham receita a longo prazo do projeto instalado.

2.15 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?

O entendimento é que as demandas nacionais ocorram em função de necessidades locais, sejam em âmbito estadual ou federal, em áreas com maior carência, ou então por produtos e serviços que serão desenvolvidos no país e disseminados no mercado brasileiros. Por outro lado, o desenvolvimento de produtos e soluções que sejam aderentes à padronização internacional, a qual já se encontra em estágios mais avançados na definição de requisitos, vai permitir que os produtos nacionais sejam compatíveis com o mercado externo. Ressalta-se que as inovações brasileiras poderão ser compatíveis com o mercado internacional, e que podem atender mercados mais necessitados.

2.16 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?

3. Pesquisa & 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.

3.1 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?

Os mecanismos de incentivo à pesquisa, desenvolvimento e inovação são oferecidos através de programas e chamadas e embora não estejam todos disponíveis no momento, representam esforços estruturados para incentivos ao desenvolvimento de IoT em diversos setores de aplicação. Com isto, podemos citar:

1) FINEP com o Programa Inova Telecom (atualmente fechado), que na época do lançamento era de iniciativa conjunta do então MC, MCTI, Min Saúde e BNDES, para projetos de inovação com tecnologias em áreas alinhadas com IoT e M2M, tais como: "Comunicação Máquina a Máquina"; "Comunicações Estratégicas" (infraestrutura para processamento e armazenamento de dados no território nacional); TeleSaúde ("Sistemas de monitoramento, diagnóstico e tratamento remoto de pacientes, incluindo sensores e transdutores", e "Desenvolvimento, validação e avaliação da conformidade de softwares embarcados em dispositivos médicos"). As formas de apoio financeiro eram a própria FINEP, BNDES e Min Saúde.
2) Finame, BNDES e Funtec: Apoio financeiro não reembolsável a projetos de pesquisa aplicada, desenvolvimento tecnológico e inovação executados por Instituições Tecnológicas (IT), selecionados de acordo com os focos de atuação divulgados anualmente pelo BNDES. Os focos relacionados ao tema IoT são Semicondutores e Manufatura Avançada e Sistemas Inteligentes.
3) INCT (Institutos Nacionais de Ciência e Tecnologia) oferecem a possibilidade de delinear projetos de pesquisa em universidades onde podem ser estudados os problemas específicos na área de comunicação M2M e IoT. Permitem a formação de recursos humanos e capacitação de futuros profissionais.
4) EMBRAPII (Associação Brasileira de Pesquisa e Inovação Industrial) é qualificada como Organização Social pelo Poder Público Federal desde setembro/2013. O MCTIC e MEC repartem a responsabilidade pelo seu financiamento. Tem por missão apoiar instituições de pesquisa tecnológica, em selecionadas áreas de competência, para que executem projetos de desenvolvimento de pesquisa tecnológica para inovação, em cooperação com empresas do setor industrial.

5) Acordo de cooperação internacional: Chamada Conjunta RNP-NSF para projetos de Pesquisa e Desenvolvimento em Segurança Cibernética, entre Brasil e Estados Unidos. O objetivo é apoiar e promover projetos conjuntos de pesquisa e desenvolvimento na área, por meio de consórcios entre instituições científicas e tecnológicas e empresas brasileiras e americanas. Com prazo encerrado em dezembro/2016, os temas foram Segurança e Privacidade em Redes; Internet das Coisas, Sistemas Ciber-Humanos e Ciber-Físicos; e Detecção de Malware.

6) Acordo de cooperação internacional: 4ª Chamada Coordenada BR-UE em Tecnologias da Informação e Comunicação (TIC). Ação da RNP e a Secretaria de Políticas de Informática (Sepin) do MCTIC para trabalhos de desenvolvimento e inovação tecnológica, nas áreas de conhecimento: Computação em Nuvem, Internet das Coisas (projetos-piloto) e Redes 5G.

7) Projeto "Minha Cidade Inteligente" do MCTI (Decreto 8776 de 11 de maio de 2016) foi uma excelente iniciativa para iniciar o estimulo à comunicação M2M e IoT. Assim como a FINEP e FAPESP disponibilizaram R$ 10 milhões para a apoiar o desenvolvimento, por pequenas empresas, de produtos, processos e serviços inovadores em cidades inteligentes e sustentáveis.

8) A Lei de Informática (Geral e da Zona Franca de Manaus);

   A Lei 8.248/91, que concede incentivos fiscais relativos ao IPI para as empresas de manufatura que produzam no Brasil segundo as normas de um Processo Produtivo Básico (PPB) definido para cada tipo de produto, requer que essas empresas invistam um percentual de até 5% do seu faturamento com esse produto em atividades de pesquisa e desenvolvimento executadas no país. Esta obrigação representa um volume de recursos próximo de R$ 1,5 bilhão por ano, que as empresas beneficiárias aplicam em projetos na área de TIC em projetos de sua escolha.
   O Decreto 5.906/06, que regulamentou a Lei 8.248, previu, adicionalmente, a figura dos "programas e projetos de interesse nacional na área de informática e automação considerados prioritários pelo CATI [Comitê da Área de Tecnologia da Informação]", nos quais as empresas beneficiárias podem aplicar parte de suas obrigações.
   Outro ponto de interesse é o fato de que a Lei de Informática permite também a execução de atividades de P&D mediante intercâmbio científico e tecnológico com entidades tanto do Brasil quanto do exterior.
   Finalmente, a Lei de Informática admite investimentos em projetos de pesquisa e desenvolvimento executados por startups vinculadas a incubadoras credenciadas.
   Todos os mecanismos e obrigações descritos acima estão também presentes na Lei de Informática da Zona Franca de Manaus – Lei 8.387/91, regulamentada pelo Decreto 6.008/06.

   Ou seja, a Lei de Informática é um instrumento atual importante que fomenta o investimento em P&D nesta área. Recomendamos sua continuidade com as adaptações necessárias para alinhamento com as regras da OMC.

- Visando fomentar investimentos em P&D na área de IoT ligado à manufatura avançada, em especial em áreas estratégicas ligadas a impressão 3D, propomos a Inclusão das Impressoras 3D na "Relação de Bens de Informática e Automação" de forma a permitir o enquadramento de projetos de P&D realizados nesta área como contrapartida aos incentivos da Lei de Informática, conforme segue:

NCM 84.77 - Impressora 3D baseada em técnica digital, suas partes, acessórios e suprimentos.

- O Inova Empresas é um instrumento atual que deve ser mantido, sugerindo um Inova Manufatura Avançada ou Inova IoT que tenha um foco maior na área em questão, se possível com percentuais de subvenção econômica maiores do que as versões anteriores.

9) A Lei do Bem:

A Lei 11.196/05 ("Lei do Bem") provê a redução da base de cálculo do imposto de renda das empresas proporcionalmente ao volume de investimentos dessas em pesquisa, desenvolvimento e inovação tecnológica. Nesse caso, não há uma obrigação de investir, e sim um benefício de que as empresas podem desfrutar caso realizem os investimentos.
Também nesse caso, poderiam ser criados mecanismos específicos para o incentivo à realização de atividades de geração de inovação, mediante, por exemplo, o aumento do percentual de redução possível da base de cálculo caso as atividades se concentrem nas áreas de interesse. Esse benefício poderia ser progressivo, até um determinado limite, conforme a proporção dos investimentos efetuados nessas áreas em relação ao total.
Assim como na Lei de Informática, esse mecanismo dependeria de alteração na legislação em vigor.

Nesse cenário, as seguintes medidas poderiam ser adotadas:

- A criação, pelos respectivos Comitês, de Programas Prioritários (no âmbito da Lei Geral e da Zona Franca de Manaus) para fomento a projetos de P&D na área de IoT;
- A realização de Chamada Pública para a seleção de entidades executoras de tais Programas Prioritários, dentre Centros de P&D e Universidades, em diferentes partes do país. Tais entidades executariam projetos de P&D nas áreas de interesse, pré-aprovados, que poderiam receber aportes materiais ou financeiros das empresas beneficiárias sem risco de glosa;
- O incentivo à atração de especialistas de Centros de P&D e Universidades para ministrar palestras ou cursos de capacitação, utilizando-se de recursos da Lei de Informática na modalidade de intercâmbio científico e tecnológico. Nesse sentido, poderiam ser estruturados eventos para esse fim, patrocinados conjuntamente por empresas beneficiárias, o que potencializaria seus resultados;
- O incentivo à aplicação de recursos em startups voltadas a produtos ou serviços nas áreas de interesse;

- O incentivo à aplicação de recursos em programas de capacitação e formação de recursos humanos em tecnologias relacionadas a IoT, como eletrônica, computação, protocolos, cloud, big data, machine learning, etc., com o objetivo de massificar esse conhecimento e de provocar o interesse em torno do tema, promovendo o surgimento de novos agentes no ecossistema.
- Criação de linhas de crédito e/ou incentivo para aquisição de materiais, componentes e serviços (placas de prototipação, sensores, micro controladores, ambientes de desenvolvimento, hospedagem, etc.), nacionais e importados, para a criação, desenvolvimento, simulação e testes de soluções em IoT.
- Programa Nacional de incentivo a iniciativas empreendedoras aplicando tecnologia de IoT. Semelhante ao programa "Startup Brasil", porém, definindo políticas de incentivo e apoio específicos para áreas estratégicas (agrobusiness, otimização de cidades, saúde e assistência social).
- O Inova Empresas é um instrumento atual que deve ser mantido, sugerindo um Inova Manufatura Avançada ou Inova IoT que tenha um foco maior na área em questão, se possível com percentuais de subvenção econômica maiores do que as versões anteriores.
- Plataformas do Conhecimento – Lançar encomendas tecnológicas para projetos na área.
- Preferência em compras governamentais – Restituir este instrumento que expirou em 1/Dez/2016 para sistemas TIC, incluindo dispositivos e sensores, o qual fomenta a aquisição pelo governo federal de produtos da área desenvolvidos no Brasil.
- Reintegra – Alterar as regras de conteúdo local dos equipamentos de TIC para fomentar o desenvolvimento de equipamentos da área que possam ser exportados.
- Estabelecer uma plataforma/comunidade para intercâmbio de experiências, onde diversas indústrias / universidades / associações / organismos governamentais possam discutir e promover tópicos relativos a IoT/M2M (ex. "Plataforma Industrie 4.0" na Alemanha, "AIOTI" na Europa)
- Organizar uma colaboração eficiente com outras organizações (ex. "Plataforma Industrie 4.0" na Alemanha, "AIOTI" na Europa)
- Começar a desenvolver e incentivar uma estratégia de digitalização baseada nas indústrias mais representativas do Brasil (ex. Automotivo, Petróleo, Etanol, Minério, Química, Alimentos) envolvendo diversos stakeholders (ex. Industria, Academias, Associações, etc.), definir objetivos claros e plano de comunicação (ex. na Alemanha os objetivos são publicados no CeBit, Exposição Hannover Fair)
- Redefinir atividades para retomar a participação da Indústria no % do PIB brasileiro.
- Preferência por uma sistemática de uso/casos para distinguir entre diversos papeis (ex. usuários e fornecedores de tecnologia), para definir a

abrangência do tema e os benefícios do usuário no aumento da sua eficiência

- Identificar "key players" no mundo acadêmico, construir casos de sucesso e utilizá-los para educar os estudantes
- Utilities: Incentivos para adoção de geração distribuída de energia elétrica
- Transporte: necessidade de Transmissão de imagens em tempo real para órgãos de segurança pública, principalmente nos transportes rodoviário e ferroviário

As medidas acima podem ser executadas sob a égide da legislação atual, sem que estas necessitem de modificações.

Entretanto, se considerarmos a possibilidade de alteração na legislação, poderiam ainda ser criados incentivos adicionais para as atividades de P&D nas áreas de interesse.

Tais incentivos poderiam se dar sob a forma de um "bônus", válido por um período limitado, aplicado sobre as obrigações de investimento em P&D da Lei de Informática, quando aplicadas em projetos nas áreas de interesse, ou seja, para projetos nessas áreas cada real aplicado corresponderia a um valor x % maior para efeito de contabilização do cumprimento das obrigações. Este mecanismo, embora ocasione a redução do volume total de recursos aplicados em P&D, contribuiria para canalizar o objeto dos projetos para as áreas sob fomento, o que poderia resultar em um efeito global positivo para estas áreas. Para evitar redução excessiva, poder-se-ia definir um percentual máximo das obrigações da empresa elegíveis ao bônus.

Outra possibilidade seria a redução das obrigações de aplicação em pesquisa e desenvolvimento incidentes sobre o faturamento das empresas com produtos na área de IoT, à maneira da redução atualmente existente para os fabricantes de PCs e correlatos. Para tanto, é também necessária uma alteração na legislação para inclusão dos produtos relacionados a IoT na lista de bens de informática incentivados.

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

Para impulsionar PD&I no Brasil sugere-se a estruturação de redes de pesquisa aplicada orientadas para temas de IoT, unindo entidades como universidades, centros de pesquisa e empresas privadas em torno de temas/áreas específicas, tendo em vista o desenvolvimento de tecnologias e aplicações para IoT nas diversas áreas verticais, desenvolvimento e apoio a modelos de negócio em empresas existentes e startups, e esforços direcionados para impulsionar IoT no Brasil. A coordenação das redes deve ter grande conexão com setores do Governo relacionados ao desenvolvimento de IoT, em suas diversas áreas. Sugere-se que a governança seja conduzida por entidade privada, com definição de metas e acompanhamento da efetividade de todas as ações e atividades.

Considerar o uso de padrões abertos, considerando o seguinte:

- A definição de uma rede de referência é essencial para o sucesso de uma solução desse tipo
- Propor estabelecimento de incentivos setoriais, relacionados com IoT e M2M, chamadas à indústria e academia para discussão de práticas a serem adotadas.
- Criação de um Plano de Evolução para TI do Governo contendo as intenções de uso de IoT pelos órgão governamental a curto/médio/longo prazo.
- Dada a configuração do governos do Brasil, um plano para implementação dos vários campi (Universidades, agentes sanitários, outras áreas da administração pública)
- Criação de um Plano Metropolitano para Cidades Inteligentes onde define as interfaces das cidades com o mundo externo e as metas de automação de produtos e logística

Adicionalmente, a criação de um benefício fiscal similar à lei de informática para equipamentos de infraestrutura utilizados em IoT, mas ao invés do benefício estar condicionado à necessidade de manufatura local, ele poderia estar condicionado à comprovação do desenvolvimento de uma parcela do software no país.

Considerando que o país dispõe de diversos mecanismos de fomento à pesquisa, desenvolvimento e inovação que poderiam ser utilizados, bastando para isso um direcionamento adequado voltado especificamente para a área de M2M / IoT. Note-se, entretanto, que algumas das ações propostas demandariam modificações na legislação vigente.

Além disso, poder-se-ia criar um Programa Nacional de incentivo às iniciativas empreendedoras em tecnologias de IoT, semelhante ao programa "Startup Brasil", porém definindo politicas de incentivo e apoio específicos para áreas estratégicas (agrobusiness, otimização de cidades, saúde e assistência social).

No tocante à provável revisão a ser feita na Lei de Informática em função do Painel da OMC e dependendo do efeito desse, eventualmente poderia ser incluído algum ajuste para incentivar PD&I em IoT e M2M.

Tal incentivo pela Lei de Informática teria que considerar IoT de forma ampla, onde ficasse claro que todo e qualquer investimento P&D em IoT e/ou em M2M fosse automaticamente considerado como investimento em TIC independentemente do campo de aplicação (se medicina, agricultura, biologia etc.) de forma a simplificar/evitar a discussão de enquadrabilidade dos projetos.

Isso passa por incentivar o PPB para produtos que possam se enquadrar em IoT e M2M, criando benefícios fiscais para a pesquisa e produção dos mesmos.

Reduzir a carga tributária para facilitar o acesso à aquisição de artigos importados de IoT e M2M e outros dispositivos relacionados a essas tecnologias de modo a permitir atualização do conhecimento do que há no mercado externo e facilitar o desenvolvimento de novas tecnologias localmente.

Adequar as Leis de incentivos existentes para que possam ser enquadrados os desenvolvimentos ligados à Manufatura Aditiva, Manufatura Avançada, Indústria 4.0, IoT e M2M de modo a incentivar o crescimento da Indústria Brasileira.

Criar leis de incentivo ao PPB para produtos que possam se enquadrar nestas tecnologias de comunicação, criando benefícios fiscais para a pesquisa e produção destes produtos.

Aumentar os benefícios (diminuição dos impostos de importação) para se ter acesso a aquisição dos artigos de IoT e M2M e outros dispositivos relacionados a esta tecnologia para facilitar o desenvolvimento e conhecimento de novas técnicas do mercado externo.

Adequar as Leis de incentivos existentes para que possam ser enquadrados desenvolvimentos ligados à Manufatura Aditiva, Manufatura Avançada, Indústria 4.0, IOT e M2M como principais fatores para o crescimento da Indústria brasileira.

3.3 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 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?

Os cursos na área de ciência e engenharia têm atratividade para pessoas com afinidade com as ciências exatas. No exame PISA 2016 quase metade dos estudantes brasileiros (44,1%) está abaixo do nível de aprendizagem considerado adequado em leitura, matemática e ciências que impacta negativamente na atratividade pelas ciências exatas.
Apesar do Brasil investir em Educação um percentual bem acima da média dos países da OECD (16,1% do PIB contra 11,3% do PIB na média), os investimentos são mal distribuídos e utilizados. É no ensino fundamental e médio que se precisa atrair os estudantes para áreas de ciências e matemática, básicas para o posterior direcionamento dos alunos para áreas de formação científica e tecnológica.
Possível complexidade na grade curricular, excessivo número de matérias e falta de clareza nos objetivos do curso, distanciamento da realidade do mercado de trabalho, falta de políticas universitárias de inserção no mercado, pouco alinhamento com demandas reais da indústria.
Tomando como base o relatório "Education at a Glance 2016" da OECD no resumo dos investimentos brasileiros, encontram-se alguns dados que ajudam a explicar parte do problema:

1) Os professores, no Brasil, têm legalmente o mesmo salário mínimo independentemente do nível em que lecionam (nota de EN – de imediato isso desestimula qualquer investimento pessoal em formação. Além disso, em alguns locais nem o salário mínimo é pago)
   a- Em paralelo, professores do nível terciário (EN superior) das universidades federais recebem de salário total (inclui férias, bônus etc.) valores maiores do que em muitos países da OECD e comparáveis aos salários praticados nos países nórdicos (nota de EN – isso esclarece em parte a questão de má distribuição de investimentos)
2) O Acesso à educação terciária (superior) é menor do que em outros países latino-americanos com dados disponíveis, com apenas 14% dos adultos atingindo esse nível. (nota de EN – novamente, o dado ajuda a esclarecer o efeito da má distribuição dos investimentos, pois em havendo melhor distribuição do investimento para o ensino fundamental e médio provavelmente a taxa de adultos a se interessarem pelo ensino superior aumentaria)

Para melhorar o cenário no longo prazo, deve-se investir na educação fundamental e média, formação de professores e em estratégias que mostrem aos alunos que a ciência e a matemática são úteis para resolver muitos problemas do cotidiano.
A curto e médio prazo, a criação de um programa de capacitação e formação, utilizando recursos da Lei de Informática, com o objetivo em atrair os interesses e capacitar tecnicamente os jovens para as áreas de tecnologia relacionadas ao ecossistema de IoT. Nesse contexto a disponibilização de bolsas aos participantes do programa, poderia aumentar a atratividade nas áreas de interesse.
Esse programa de capacitação poderia ser apoiado por eventos regionais, com a participação de universidades, professores, profissionais e empresas de relevância nacional/internacional, onde tendências, focos estratégicos e tecnologias seriam apresentados e discutidos, criando assim, uma comunidade em nível nacional com objetivos e interesses comuns na área de tecnologia.
Disponibilização de um programa Nacional de capacitação com diferentes níveis de público e certificação, que poderia ser promovido por empresas do segmento de tecnologia utilizando incentivos como Lei de Informática e/ou Lei de Bem.
   a- Conteúdo iniciante, seguindo as tendências mundiais de "makers" com disponibilização de KITs básicos associados a um currículo introdutório.
   b- Conteúdo intermediário, seguindo ainda a tendência "maker" baseado em um currículo mínimo básico, que pode sofrer adição de módulos específicos alinhados aos propósitos das empresas patrocinadoras. Estes dois níveis teriam o principal objetivo em atrair os interesses e capacitar tecnicamente os jovens para as áreas de tecnologia, com foco em IoT.
   c- Finalmente um conteúdo focado em negócios buscando apoiar as potenciais soluções e serviços originados nas edições básicas regionais, pré-selecionadas por um programa nacional, que tenham um potencial de

evolução para patentes, produtos ou serviços. Neste nível poderá haver a contribuição de aceleradoras e incubadoras para maturação dos projetos.

Todo esse programa de capacitação poderia ser apoiado por eventos regionais, com a participação de universidades, professores, profissionais e empresas de relevância nacional/internacional. Onde tendências, focos estratégicos e tecnologias seriam apresentados discutidos. Criando assim uma comunidade em nível nacional com objetivos e interesses comuns na área de tecnologia. Para tal a utilização de mídia e canais digitais, como redes sociais e comunidades deve ser empregado. Também seria muito importante atualizar conceitos da manufatura moderna para que possamos ter uma melhor qualidade no ensino e compatível com as necessidades atuais da Indústria de Centros de Pesquisas.

Além disso, é importante incluir o Ministério da Educação e Cultura nas discussões juntamente com MDIC e MCTIC. O MEC precisa estar nas discussões com a indústria, caso contrário, a formação estará cada vez mais afastada das suas necessidades e desincentivando a adesão dos estudantes, principalmente para os níveis mais avançados.

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

Antes de mais nada, entendemos por ecossistema de IoT um conjunto de atores e ações que giram em torno de três eixos: o do sentir (os dispositivos sensores), o do refletir (a serem feitas a partir das informações coletadas pelos sensores) e o do agir (serviços que serão desenvolvidos e oferecidos com base no resultado nas análises disponíveis). Assim, as políticas públicas de incentivo a PD&I (ou quaisquer outras) no âmbito desse ecossistema precisam tratar holisticamente todos os aspectos, abrangendo dos sensores aos serviços. Porém, o incentivo à PD&I para ecossistema de IoT ainda é tímido e necessita impulso para atingir empresas em todo o país. Conforme a Fapesp, em São Paulo aproximadamente 60% das empresas investem em pesquisa, e quando se considera o Brasil, o percentual cai para 39%. Torna-se necessário que o ambiente de empresas se descentralize, estendendo-se por todo o país e criando novos polos industriais. Ressalta-se a importância de estabelecer acordos e parcerias com instituições de educação para promover a inovação dentro de empresas.

Com relação às oportunidades, já existem programas que parecem estar no caminho certo ao ecossistema de IoT, pois incentivam a participação de ICTs e Institutos Federais de Educação juntamente com empresas o que, por um lado, ajuda a atrair e capacitar profissionais e, por outro lado, incentiva a introdução das inovações no mercado. Manter e/ou estender, por ainda serem tímidos, tais programas para IoT parece ser uma alternativa viável.

Oportunidades:

Seguindo os novos conceitos de manufatura aditiva, Indústria 4.0, IOT e M2M, existem inúmeras oportunidades que, para serem aproveitadas, exigirão ajustes rápidos na legislação e incentivos vigentes que, hoje, estão baseados em

conceitos rígidos com fronteiras bem definidas. Há necessidade de considerar um pensamento mais abrangente que leve em conta o desaparecimento de barreiras entre áreas de conhecimento (na educação, por exemplo) e as novas necessidades do mercado (muito mais voltadas a serviços do que antigamente, por exemplo).
Fixar um sistema de remuneração misto ao provedor de soluções de IoT, pagando um valor médio/baixo para a compra da solução e um bônus alto equivalente a um percentual do ganho de eficiência em cada projeto.
Planejamento de Ecossistemas (Cidades Inteligentes, Campi Inteligentes: Universidades, Unidades de atendimento ao Público, Saúde, rodovias federais)
Parcerias, como cidades inteligentes
A indústria necessita se modernizar e, por isso, pode saltar etapas e ter um grande acréscimo neste sentido
As mudanças na matriz energética e na malha, deixando a geração para o consumidor pequeno ou PME, o que pode induzir ao uso de produtos e serviços de IoT
O processo de importação, incluindo de protótipos, poderia ser simplificado para facilitar o acesso à equipamentos.
Desenvolvimento de players locais:

- Facilities – com foco em soluões para SmartCities;
- Serviços – com soluções de automação para uso comercial ou residencial, entretenimento e saúde;
- Integração – automatizada e otimizada de cadeias produtivas;
- Mobilidade – segmento automotivo, transporte público e logística.

Desenvolvimento de tecnologia local embarcada:

- Agrobusiness e mobilidade urbana.

Softwares e ferramentas para exportação:

- Aplicações para Fintech;
- Aplicações para Agrobusiness;
- UX/UI dedicados e otimizados para soluções de IoT;
- Serviços de integração e comunicação – Middleware.

Barreiras:
Com relação a barreiras, por existirem muitas áreas inexploradas para uso de IoT, onde o risco é maior, seria importante existir algum mecanismo de fomento baseado nos programas atuais que não exigisse contrapartida financeira, mesmo onde houvesse a participação de empresa (pequenas e média, principalmente) no desenvolvimento de tecnologias.
Além disso, como na questão 2 acima, é importante ajustar a Lei de Informática para incluir de forma ampla e clara a definição para P&D em IoT e M2M.
Também é importante avaliar a regulamentação para aquisição de equipamentos, componentes, licença de SW, etc. Precisaríamos de uma política pública que facilitasse a aquisição de assets, principalmente importados, para

a pesquisa científica não apenas nas questões de redução de taxas, mas também na burocracia envolvida.
A ausência de legislação clara sobre o tema; tributação excessiva; taxas como FUST, FISTELL e FUNTELL que podem incidir sobre IoT, além da já incidirem sobre as operações de telecomunicações; falta de informações aos gestores do setor público para disseminação do que é IoT e quais os seus benefícios; falta de suporte aos gestores públicos para realizar a contratação de projetos de IoT (ex.: suporte para uma licitação).
Falta de conceituação e processos específicos para prototipação, com um modelo flexível de importação de componentes para implementação de protótipos, pre-certificação, testes e homologação em agências reguladoras de novos conceitos e produtos.
Falta de conceituação e processos específicos para prototipação, pre-certificação, testes e homologação em agências reguladoras de novos conceitos e produtos.
Conceituação de modelo flexível para PPB com foco na manufatura em pequena escala de protótipos e produtos finais, porém com utilização de incentivos.

3.5 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?

Os problemas para a formação dessas redes podem estar relacionados ao distanciamento de foco existente entre centros acadêmicos, centros de pesquisa, universidades, devido a orientações distintas de linhas de pesquisa, de tal forma que há pouco alinhamento de interesses de estudos. Entende-se ser necessário promover a proximidade. Outro problema crucial é a escassez de recursos financeiros destinados a intercâmbios dessa natureza.

Embora existam mecanismos como Embrapii, Lei de Informática etc. que já incentivam o vínculo entre estes atores, questões financeiras e de Propriedade Intelectual, por exemplo, podem ser uma barreira para a união entre pesquisadores de universidades e ICTs (públicas principalmente) e empresas, diversas restrições de investimentos por região no país também gera barreiras.
A disseminação das informações sobre IOT, M2M, Indústria4.0 e Infraestrutura é essencial para que possamos ter mais sinergia entre Empresas, Universidades e ICTs nestes campos e isso só ocorrerá em um ambiente onde estes atores sintam-se à vontade para interagir. Assim, é fundamental que as regras sejam claras, pois se as discussões entrarem pelo campo jurídico certamente haverá entraves à formação de redes ou para o andamento de futuros trabalhos em conjunto.

3.6 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?

Antes de mais nada, é importante comentar que uma política para IoT não deve ser considerada uma política de TIC mas uma política bem mais ampla, pois IoT abrange outros campos do conhecimento e outras bases tecnológicas.

Nesse aspecto, algo a ser revisto é a Lei de Informática, por exemplo, que há muito tempo já traz a possibilidade de facilitar o relacionamento de startups com empresas estabelecidas ao permitir o uso da obrigação como participação no capital de empresas de base tecnológica em tecnologias da informação, vinculadas a incubadoras credenciadas. O que se incluiu na questão 2 a respeito de ajustar a lei para ficar mais alinhada com IoT implica em flexibilizar o termo "empresas de base tecnológica em tecnologias da informação", por exemplo, pois a pesquisa e o desenvolvimento para IoT não necessariamente estará atrelada a empresas dessa base tecnológica.
Quando olhamos para o cenário de startups no Brasil, é notório que está em franco crescimento, mesmo em momento de crise e aumento de desemprego, mas há impacto na permanência da empresa oriundo da carga tributária que a startup deve pagar, em torno de 30% do seu faturamento. Isso tem acarretado a taxa de mortalidade de startups de 25% ao ano. Há bons exemplos de conformação de startups e relacionamento com grandes empresas, mas o excesso de impostos coloca em risco as startups brasileiras, muito mais do que empresas em outros países. A preparação das startups no aspecto de negócios é importante e há bons resultados, alguns do programas do SEBRAE. Seria importante levar este tipo de preparação para sala de aula, ensinando visão de negócios junto com área tecnológica. Ressalta-se a necessidade de acompanhamento das startups e deveria existir organizações que atestassem o funcionamento, os resultados das empresas e seus produtos. Outra questão a ser destacada é a garantia de acesso à internet e infraestrutura de telecomunicações pelas startups, uso de datacenters e acesso a equipamentos a custo reduzido para realização de provas de conceito.

Assim como as startups, as aceleradoras deveriam ter apoio para planejamento, equipe reconhecida e um programa bem definido de atuação por área prioritária, ainda recebendo orientação em função dos resultados da FEP do BNDES e dos estudos da Câmara IoT. A distribuição de recursos deve ser bem definida e orientada por editais, tais como o Startup Brasil.

Por fim, a divulgação de recursos públicos alocados nas startups deve ser conhecido, assim como as etapas de implantação e demais informações, possivelmente por páginas oficiais na internet, sobre os responsáveis e documentação que a reconhece como empresa quando do recebimento de

recursos. Os recursos públicos alocados a startups devem ser em projetos de interesse público, e os recursos alocados para interesse privado devem ser alocado pelas empresas. Conforme o site Startup Brasil, não há editais e inscrições desde 2014. Ressalta-se o interesse em conhecer os resultados em termos de inovação e rentabilidade do dinheiro aplicado.

3.7 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.

Existe demanda reprimida, dado que os usuários finais ainda não compreendem como sanar seus problemas ou reduzir custos com uso de tecnologia. Ainda há poucos profissionais que podem dar suporte ao grande número de empresas. É sabido que do total de empresas brasileiras, apenas 43% delas tem uma área ou departamento de TI, e desconhecem a importância de Tecnologia da Informação na estratégia do seu negócio.

Existem algumas demandas nas áreas de segurança de informação e soluções para a área industrial com o objetivo de agilizar a automação da informação e diversas outras verticais.

Precisamos pensar o Brasil ingressando no conceito de Indústria 4.0 e nos prepararmos para sermos atores mundiais importantes na Manufatura Aditiva e IOT. Assim, existe demanda não somente de linhas de financiamento para P&D, mas também para modernização das regras jurídicas, tributárias e alfandegárias que precisam suportar a tomada de decisões e ações em tempo real, não apenas na execução da manufatura, mas também na gestão dos mais variados tipos de Indústria e de Serviços que surgirão a partir destas novas tecnologias.

Áreas como a do setor energético, por exemplo, necessitam de um agregado de inteligência em redes e distribuição. A área da saúde necessita melhores serviços no sistema público e, para isso, é fundamental que o sistema possa ser alimentado com mais e melhores informações.

Pesquisa, desenvolvimento e inovação em dispositivos inteligentes, impressão 3D, infraestrutura de comunicação, sensores, semicondutores, eletrônica orgânica, software embarcado, rádio frequência e automação, são essenciais para levarmos o Brasil para a vanguarda em comunicação M2M e IOT e, simultaneamente, darmos soluções para questões com a do parágrafo anterior.

Podemos citar também a Agricultura, Saúde, assim como verticais onde é possível implementar redução de custos (p.ex. iluminação inteligente, logística) através de Cidades Inteligentes. Além de PME e consumidor final possuem dificuldade em gerenciar e tornar seu espaço seguro. Técnicas de gerenciamento e serviços podem ser pesquisados.

E por fim, dispositivos, segurança, computação em núvem são demandas também vitais.

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

- Fundação de Apoio à Capacitação em Tecnologia da Informação (Facti) no projeto Plataforma IoT com foco na criação de aplicativos e uso de dados da comunicação Máquina a Máquina M2M para facilitar a vida da população na gestão de segurança pública, mobilidade e saúde em Fortaleza inicialmente.
- FIT Instituto de Tecnologia (P&D em IoT e Indústria 4.0 utilizando tecnologias como Lora, Sigfox, Wifi, Bluetooth, RFID, robótica para coleta de informação em tempo real, algoritmo de "Data mining", "Cloud" entre outras tecnologias para diversos setores e já com casos reais de IOT e Indústria 4.0 desenvolvidos para empresas como HP, Motorola e Flextronics)
- Instituto CESAR, lançou recentemente a plataforma KNoT (knot.cesar.org.br), plataforma capaz de interconectar as plataformas de IoT já existentes. Resultado de um projeto de pesquisa e inovação realizado pelo CESAR com parcerias, incluindo a UFPE e o Instituto Senai de Inovação.
- CEITEC (microeletrônica)
- Unicamp
- Instituto Eldorado
- CPqD
- USP com projetos de Smart Cities.
- Inatel em Minas Gerais
- PUC-Rio.
- Instituto Cesar.
- Instituto Atlântico (IA)
- Universidade Federal do Ceará
- Centro de Tecnologia da Informação Renato Archer (CTI)

Também devemos citar empresas como HP, Apple, Cisco, Flex, Ericsson, Qualcomm, Samsung, Nokia, IBM, Huawei, Telit, Advantech, ZTE, Intel, Novus, Siemens, Motorola, Dell, Lenovo, EMC, Icatel e HPE que também investem e apoiam pesquisas de IOT em Institutos e Universidades.

3.9 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?

O incentivo pode ser estrutura com fomento para promoção de encontros de empresas em função de necessidades específicas de algumas verticais, em ação que pode aproximar empresas pequenas a grandes investidores. Por exemplo, a Prefeitura pode disseminar conceitos de cidades inteligentes em uma cidade, não somente com editais, mas com consultas públicas e discussões na sociedade. A execução de projetos deve buscar resultados a médio e longo

prazo, de modo que haja retorno do investimento inicial, que pode ser sob forma de melhorias ou aumento de receita oriundo da exploração do resultado do projeto.

Também a implantação de um programa nacional que incentive o envolvimento e interação das empresas de médio e grande porte com o ecossistema emergente de startups nas modalidades de:

1- MENTORIA – onde as empresas atuariam como mentoras das novas empresas emergentes afins com seus negócios, dedicando parte do tempo de seus recursos humanos para o aconselhamento estratégico, financeiro, produtivo, marketing e comercial. Nessa modalidade não haveria transferência ou aporte financeiro direto da mentora para a mentorada.

2- TUTORIA – empresas de médio e grande porte poderiam "tutorar" emergentes afins com seus negócios diretos ou de suporte, permitindo a integração e compartilhamento de suporte operacional (P&D, RH, administrativo, marketing, produtivo e logístico) alavancando a capacidade das empresas emergentes em focarem nos desenvolvimento e conclusão de seu produto ou serviço. Nessa modalidade não haveria transferência ou aporte financeiro direto da mentora para a mentorada.

3- ADOÇÃO – Englobando todas as responsabilidades e direitos da TUTORIA porém com a possibilidade de aporte financeiro direto (não proveniente de incentivos) nas emergentes adotadas.

Como contrapartida as empresas MENTORAS, TUTORAS ou ADOTANTES receberiam incentivos governamentais na forma de renuncia ou abatimentos em determinados impostos. Com a possibilidade da aplicação de incentivos pré-existentes como Lei de Informática, em determinadas alíquotas que promovam atividades de P&D nas empresas emergentes. Percentuais de incentivo diferenciados devem ser aplicado em função da modalidade (Mentoria, Tutoria ou Adoção).

O Programa de Promoção da Economia Criativa é um exemplo de incentivo de ecossistemas. Esse programa é um modelo de Incubação e Aceleração de empresas de base tecnológica, que maximiza os benefícios da colaboração entre grandes empresas nacionais e multinacionais, pequenas empresas de base tecnológica e ambientes de inovação, sejam mecanismos de geração de empreendimentos ou ecossistemas de inovação, contribuindo para o aperfeiçoamento das ferramentas institucionais e atividades locais do Sistema Nacional de Inovação Brasileiro (SNI).

Esse programa representa um importante marco de inovação na interação e relações entre grandes empresas, startups, ambientes de inovação e governo. Além disso, o programa representa um modelo de referência para adoção e aplicabilidade dos diversos Fundos Setoriais e investimentos diretos de grandes e médias empresas no Brasil, como é o caso do projeto, que utilizou recursos da Lei de Informática no Brasil ao contexto do empreendedorismo de base tecnológica.

Os fundamentos jurídicos do programa são estruturantes e referência também para expansão através da utilização de outras modalidades financeiras de estímulo empreendedorismo intensivo em conhecimento, a exemplo de fundos setoriais como ANEEL e FNDCT, ou ainda e Lei do bem ou investimentos empresariais diretos. O programa Startups Economia Criativa Brasil propõe sua expansão institucional, ampliando apoio governamental à iniciativa.

Há que se considerar também como ponto de partida os dois principais problemas que uma startup enfrenta: capital e acesso a mercado para seus produtos. Assim, quando se fala em incentivar a criação de um ecossistema de startups com elevado grau de inovação em IoT através de apoio estatal, precisa-se tomar o cuidado de, além de fundos para investimento, prover/facilitar o acesso a mercados e esse último é mais complexo do que o simples investimento. Isso passa por questões tributárias, e burocráticas – a própria burocracia e os custos que existem hoje no País, por exemplo, para abertura e fechamento de empresas são barreiras que precisam ser tratadas. O fechamento de uma empresa é tão complexo que a maioria dos pequenos negócios optam por manter a empresa inativa - algo que não deveria ser opção, pois isso também consome tempo dos administradores que poderia ser dedicado a atividades mais nobres.

Também seria importante estender o mecanismo para programas como o Embrapii, por exemplo, permitindo o credenciamento de incubadoras como se fossem unidades ou polos Embrapii para realização de projetos em conjunto com empresas estabelecidas e ICTs.

De outra maneira, criar incentivos não reembolsáveis, mas com maior flexibilização para questões como propriedade intelectual, também poderia ser uma forma de apoiar as empresas nascentes para que encarem os riscos à inovação de forma mais adequada.

Outros aspectos:

- Redução de obrigações
- Determinação de linhas mestras para incentivo
- Entendimento mais aprofundado das aplicações de mercado e necessidades das empresas

3.10 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?

Destaca-se a necessidade de acompanhamento do mercado externo e incentivar as exportações de produtos e até de serviços. Também reduzir a burocracia e fomentar por via de consulados/embaixadas estrangeiras, visitas a outros mercados que necessitem de soluções existentes no Brasil. Outro aspecto a destacar é a realização de mapeamento de demanda e oferta locais, em termos de capacidade de atendimento das empresas locais e dos produtos disponíveis.

Identificar gaps na qualificação do corpo técnico e científico em Universidades e Institutos de Pesquisa e Educação. Incentivar cursos de pós-graduação, congressos técnicos e de negócio para difundir a informação técnica na área.

Infelizmente, dada a pouca cultura sobre a importância do investimento em P&D no país, ainda são necessários incentivos fiscais e obrigatoriedade para que tal investimento seja realizado. Dessa forma, as regras para tais incentivos precisam ser constantemente atualizadas.

Coordenar de forma efetiva as diversas frentes e grupos de IOT e Manufatura avançada dentro da Câmara de IOT é fundamental para que haja sinergia entre as diversas entidades.

4. Recursos humanos

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.

4.1 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;
  Todos os segmentos de formação profissional serão demandados com o advento da Internet das Coisas, entretanto as atividades ligadas a ciências exatas serão as mais requisitadas e as responsáveis em assegurar essa transformação. Formações tradicionais como Engenharia (todos os segmentos), Administração, Informática, Ciência da Computação, Analise de Sistemas, etc.; serão bem requisitadas dentro do ecossistema de IoT, uma vez que através dessas atividades ocorrerá a transformação gradativa das estruturas tradicionais existentes na sociedade para a estrutura utilizando-se IoT. Essa transformação exigirá dos profissionais a habilidade para criar pontes entre as operações existentes (tecnologia operacional ou mundo real) as tecnologias virtuais (mundo tecnológico).
  Dentro das profissões diretamente relacionadas à Tecnologia da Informação, destacam-se o surgimento de novas formações para o desenvolvimento do ecossistema de IoT, tais como as enumeradas abaixo. Entretanto cabe ressaltar

que algumas áreas e conhecimentos de alta demanda ainda surgirão à medida que novas tecnologias e aplicações comecem a serem desenvolvidas no mercado.

1. Cientista de Dados, Analista de *Bid Data* (ou Analista de Dados), *Analytics*, *Data Mining*: Devido ao grande volume de dados que serão gerados, oriundos de uma variedade distinta de fontes, tais profissionais terão a função de organiza-los e utiliza-los de forma eficiente e multidimensional do negócio. O trabalho com dados históricos, tendências, dados sociais, e análises preditivas será esperado no escopo de trabalho desses profissionais. Além dos aspectos técnicos voltados a função dessa profissão, também será requerido conhecimentos em estatística, matemática e algoritmos.
2. Desenvolvedores de Dispositivos (*hardware* e *firmware*); Desenvolvedores de Aplicações; Desenvolvedores com conhecimentos em lógica embarcada: Altamente requisitados, esses profissionais demandarão experiência para adaptar e acompanhar a evolução cada vez mais rápida do comportamento dos usuários, mantendo-os as aplicações atualizadas, funcionais, e interagindo com os inúmeros canais de comunicação do ecossistema de IoT.
3. Designers de Mídias Eletrônicas: no ecossistema da IoT os dispositivos estarão conectados e, portanto, irão requerer habilidades para integrar componentes eletrônicos a novos sistemas. Portanto isso irá requerer novos designs para funções ainda não exploradas anteriormente como por exemplo o consumo de energia, ou o número de sensores dos dispositivos. Adicionalmente tem-se a questão dos designers de microcontroladores, que tem a função de aplicar inteligência aos dispositivos, a fim de ajudá-los com a tarefa de processamento. Novos designes serão exigidos constantemente para atender à crescente demanda entre dispositivos.
4. Arquiteto em Segurança de Dados, Especialista em Redes e Protocolos: Tal função não tem apenas como objetivo o conhecimento de protocolos, ou a segurança de banco de dados (função hoje já existente no mercado profissional), mas adicionalmente a isso, esse novo profissional terá como desafio arquitetar soluções quando o assunto corresponde a dispositivos capazes de monitorar a vida de pessoas que estão conectados integralmente à internet. Em um ato constante, ativo e resiliente, esses profissionais possuirão o desafio de continuamente "assegurar" a segurança dos altos volumes de dados (estruturado e não estruturados) que serão trocados na rede, pelos dispositivos, em um ambiente extremamente dinâmico de equipamentos conectados.

Focando-se nas demais atividades de formação (área de humanas, e saúde), será necessário que os profissionais tenham uma formação mais holística envolvendo não apenas as áreas específicas de sua atuação, mas estendendo-se para uma rede multidisciplinar de conhecimento. Quanto mais holística for essa formação, maior será a diversidade de inovação na aplicação de conceitos específicos de cada profissão dentro do ecossistema de IoT.

Adicionalmente ao exposto acima sobre a reestruturação profissional gerada pela demanda da IoT, será necessário também a restruturação educacional já no ensino fundamental. A grade curricular deverá contemplar conceitos e

disciplinas anteriormente somente abordados no ensino médio ou técnico. Conceitos inovadores e disruptivos farão parte da base curricular no ensino fundamental, aonde a liberdade criativa, tecnologia básica, incentivos a inovação e empreendedorismo farão parte do cotidiano de ensino dos estudantes do ensino fundamental, em um esforço continuo de antecipar a construção do conhecimento para que a transformação para uma sociedade voltada para IoT ocorra já no ensino médio, e técnico.

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

  O processo educacional, não somente visando questão de IoT mas de uma maneira ampla, necessita de reformulação em suas grades curriculares. Alguns pontos a serem destacado correspondem as que seguem:

  1. A existência de poucas disciplinas com conteúdo específico que envolvem a temática de IoT.
  2. Incentivo ao desenvolvimento de projetos científicos, já no ensino fundamental. Incentivo a feiras de ciência congressos e conferência voltadas a esse fim.
  3. Criar a cultura da inovação desde o ensino fundamental, de forma lúdica e gradativamente conceitos mais consolidados no ensino médio.
  4. Fraco desempenho dos alunos em matemática, física, e áreas a fim, desde o ensino fundamental, passando pelo ensino médio e chegando até às universidades.
  5. Baixa procura dos cursos nas áreas de ciência exatas e engenharias, sendo reflexo da qualidade da educação no ensino fundamental e médio, aonde não se estimula áreas voltadas a ciências e matemática. Tais disciplinas que irão atrair o interesse do estudante a buscarem formação científica e tecnológica, e que consequentemente ao mercado de IoT.
  6. Aprimoramento do cenário da educação brasileira, com metodologias de ensino defasadas, com pouco ou nenhum espaço para a criação e inovação.
  7. Estagnação do modelo educacional e dos currículos dos cursos de formação, além da falta de recursos para
  8. Reforçar curriculum dos cursos superiores (Mecatrônica, Engenharia da Computação, Controle e Automação etc.) para desenho e integração de soluções de manufatura 4.0, IoT e M2M etc., aumentando-se o contato dos alunos com as tecnologias mais recentes.
  9. A formação de mão de obra a ser aplicável à IoT e M2M inicia em fases anteriores a formação universitária, nos ensinos fundamental e médio. Isso passa por uma redistribuição dos investimentos em educação no Brasil, para reforçar ainda mais a educação básica. É aposta de médio e longo prazo, até para que o país tenha recursos humanos melhor preparados para futuras tecnologias e não somente em IoT. Reforçar investimentos nas universidades (públicas, principalmente) pode agravar ainda mais a disparidade entre os vários níveis da educação no

país e provocar no longo prazo um quadro ainda pior para a formação de recursos humanos para áreas de ciência e tecnologia. O arranjo adequado passa por ajustar a participação do governo - MEC no caso da capacitação, pois MDIC e MCTIC que são os dois outros representantes do governo ligados de alguma forma a essa questão já estão melhor engajados nas discussões.

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

Os impactos podem ser entendidos como altamente positivos, pois a nova onda tecnológica criará a necessidade de serviços nunca oferecidos anteriormente, trazendo oportunidades de empregos no comércio e na indústria, abrindo postos de trabalho para novas funções. Mas como toda transformação, exigirá mudança e reformulação na estrutura de trabalho tradicional para uma nova estrutura de trabalho em IoT. Abaixo foram listados alguns tópicos referente a esse cenário:

1. Ganhos substanciais e efetivos de produtividade.
2. Planejamento detalhado e consequentemente redução significativa dos desperdícios.
3. Criação de novas competências profissionais especializadas para atender à tecnologia emergente, com a readequação de algumas funções para que passam atender as novas necessidades do mercado.
4. Geração de demanda por profissionais da área em empresas de segmentos atualmente não relacionados a TIC, mas que, com o advento das tecnologias M2M e IoT, necessitarão incorporar novas funcionalidades a seus produtos e serviços.

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

As novas tecnologias irão provocar um impacto positivo ao promover a formação e desenvolvimento profissional de um número maior de especialistas com maior capacidade de adaptação ao uso dessas tecnologias. Nesse contexto, ambos os setores (empregado e empregador) apresentarão benefícios, conforme segue alguns tópicos abaixo:

Para o empregado:

1. Necessidade de melhor preparo para o mercado de trabalho.
2. Maior flexibilidade para atualização técnica.
3. A transformação na maneira em que os serviços serão realizados, com menor esforço físico, com possível redução de atividades repetitivas para algumas funções.

Para o empregador:

1. Flexibilização de locais e postos de trabalho.
2. Segurança, produtividade, ganhos de escala, competitividade, empregabilidade.

3. Possibilidade no investimento de atividades que gerem inovação e novos produtos com a verba que antes era destinado para trabalhos manuais.
4. No setor público, com melhorias na oferta de serviços básicos para o cidadão, mais qualidade de vida nas cidades, na melhor gestão da máquina pública.

4.4 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?

Algumas questões relevantes, conforme listado abaixo:

1. Utilização de conceitos já desenvolvidos na indústria de manufatura, para o desenvolvimento de mão de obra para o IoT. Da mesma maneira que o sistema "S" foi um grande formador de mão de obra para a manufatura do passado, ele pode redirecionar seu ensino para a formação de profissionais que atuarão com IoT, como por exemplo, no manuseio, instalação e manutenção de gadgets, devices, etc.
2. Entretanto por ser uma tecnologia disruptiva e ubíqua a falta de mão de obra para criação, implantação, operação e manutenção corresponde a uma realidade. O plano nacional deve envolver rapidamente a formação desde o nível médio, e técnico, para que no espaço de tempo relativamente curto (1 a 2 anos) o país tenha técnicos voltados para essa área de atuação sendo absorvidos pelo mercado de trabalho.
3. Do ponto de vista regulatório – legislação, tributação, etc. – ainda há pouquíssima ou nenhuma oferta de cursos focados nas novas necessidade de IoT.
4. Diferentes abordagens deverão ser adotadas, no pais. Isso devido as realidades socioeconômica das regiões brasileiras, com diferentes níveis de infraestrutura existente nessas regiões que naturalmente será um limitador para o desenvolvimento de projetos voltados a IoT.

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

Entende-se que ainda o arranjo entre governo, universidade e empresa não tenha atingido a dinâmica e sinergia adequada para a formação de mão de obra aplicada a IoT, visando superar os desafios existentes. Abaixo segue algumas considerações a respeito dessa temática, que deveriam ser superadas a fim de se construir um ambiente propício para a formação profissional adequada para atender todas as áreas de IoT.

1. O diálogo entre estes atores ainda é distante e muitas vezes os esforços da academia estão distantes das necessidades do mercado e das empresas. Ainda há muita resistência da academia em aproximar-se das

empresas e fazer pesquisa aplicada. Por outro lado, algumas empresas ainda não enxergam todo o valor de um pesquisador.

2. Nesse sentido reforça-se a necessidade de incentivar a aproximação e o intercâmbio entre profissionais e pesquisadores, incentivando a aplicabilidade de pesquisas já desenvolvidas nas universidades ao mercado de trabalho.
3. A academia possui uma agenda diferente e está afastada do mercado. As mudanças no mercado ocorrem cada vez mais rapidamente e as universidades não estão reagindo na velocidade necessária. A criação e/ou facilitação de mecanismos que permitam PPP em atividades diretas de treinamento e capacitação podem ser um fator diferencial para potencializar e acelerar a criação de mão-de-obra qualificada e em curto prazo para atuação no domínio de IoT, envolvendo principalmente, mas não apenas eletrônica, computação e serviços (principalmente ligados a midleware de comunicação e cloud);
4. Investimento do governo ampliando o número de bolsas de pesquisa para alunos de mestrado, doutorado, e pós-doutorados, bem como atualização do valor das bolsas, com o objetivo de incentivar pesquisas nesse sentido.
5. Incentivo à formação de redes de colaboração entre as diversas áreas relevantes na área de IoT.
6. Incentivar a aproximação das empresas e escolas a fim de promover o contato dos alunos com as tecnologias mais atuais, buscando incentivá-lo a estudar ciências e matemática de forma que possam sentir-se mais confortáveis para seguir carreiras técnicas.
7. Criação de núcleo de pesquisas através de uma associação entre universidades, empresa privada e prefeituras, a fim de serem desenvolvidos estudos de soluções a serem aplicados nos problemas vivenciados e trazidos pelas prefeituras ao núcleo de estudo.

5. Oferta tecnológica e composição de ecossistemas

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.

5.1 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?

A Abinee é uma sociedade civil sem fins lucrativos que representa os setores elétrico e eletrônico de todo o Brasil, sendo sua diretoria, com mandato de quatro anos, composta e eleita pelas próprias associadas. Fundada em setembro de 1963, possui como associadas, empresas nacionais e estrangeiras, instaladas em todo país e de todos os portes.

O quadro de associadas da ABINEE inclui as maiores e mais relevantes empresas do setor, contando inclusive com uma Comissão de IoT, dedicada ao estudo do tema e que congrega as mais importantes provedoras de tecnologia, soluções e serviços do mercado.

O quadro completo de empresas associadas à ABINEE pode ser encontrado em: http://www.abinee.org.br/abinee/associa/

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

- Fundação de Apoio à Capacitação em Tecnologia da Informação (Facti) no projeto Plataforma IoT com foco na criação de aplicativos e uso de dados da comunicação Máquina a Máquina M2M para facilitar a vida da população na gestão de segurança pública, mobilidade e saúde em Fortaleza inicialmente.
- FIT Instituto de Tecnologia (P&D em IoT e Indústria 4.0 utilizando tecnologias como Lora, Sigfox, Wifi, Bluetooth, RFID, robótica para coleta de informação em tempo real, algoritmo de "Data mining", "Cloud" entre outras tecnologias para diversos setores e já com casos reais de IOT e Indústria 4.0 desenvolvidos para empresas como HP, Motorola e Flextronics)
- Instituto CESAR, lançou recentemente a plataforma KNoT (knot.cesar.org.br), plataforma capaz de interconectar as plataformas de IoT já existentes. Resultado de um projeto de pesquisa e inovação realizado pelo CESAR com parcerias, incluindo a UFPE e o Instituto Senai de Inovação.
- CEITEC (microeletrônica)
- Unicamp
- Instituto Eldorado
- CPqD
- USP com projetos de Smart Cities.
- Inatel em Minas Gerais
- PUC-Rio.

- Instituto Cesar.
- Instituto Atlântico (IA)
- Universidade Federal do Ceará
- Centro de Tecnologia da Informação Renato Archer (CTI)

Também devemos citar empresas como HP, Apple, Cisco, Flex, Ericsson, Qualcomm, Samsung, Nokia, IBM, Huawei, Telit, Advantech, ZTE, Intel, Novus, Siemens, Motorola, Dell, Lenovo, EMC, Icatel e HPE que também investem e apoiam pesquisas de IOT em Institutos e Universidades.

5.3 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?

Conforme indicado no item 5.1, as ofertas de tecnologia, produtos e serviços para os segmentos econômicos podem ser identificadas por áreas verticais, a saber: Automotivo, Cidades Inteligentes, Casa Inteligente e Agricultura (com soluções de drones).

Como exemplo cita-se a área de automotivo, no qual há expectativa de que o uso de veículos inteligentes e autônomos promova benefícios sociais e econômicos na prevenção de acidentes. De acordo com OMS, em 2013 ocorreram 1,25 milhões de óbitos no mundo devido a acidentes em estradas. No Brasil, no mesmo período houve 42291 óbitos. Verifica-se que o erro humano é responsável por 90% dos acidentes com veículos, e que veículos autônomos possam prevenir cerca de 90% desses acidentes.
Entende-se que a transformação digital vai gerar novos modelos de negócios através de quatro elementos-chave:

1. Transformação da infraestrutura híbrida
2. Proteção da empresa digital
3. Potencialização da produtividade no local de trabalho
4. Capacitação das organizações orientadas a dados

Em termos de ofertas de tecnologias, destacam-se:

- Produtos de consumo (os geradores de ação em IoT)
- Sistema de gerenciamento de produtos IoT (principalmente sistema de borda inteligentes)
- Sistemas de gerenciamento de Campus
- Serviços de instalação e gerenciamento de sistema de borda e campus
- Serviços de análise de dados (na borda ou nuvem)
- Serviços de consultoria (geração de ecossistemas)

Duas demandas principais vindas da maioria dos segmentos econômicos brasileiros: aumento de produtividade e diminuição de custos. As tecnologias citadas acima serão a plataforma para que essas demandas possam ser endereçadas e atingidas.
Em relação à tecnologia, tem-se:

- Infraestrutura de rede compatível com os requisitos de dispositivos IoT.

- Plataformas de conectividade, armazenagem e análise de dados.
- Desenvolvimento de aplicações para as múltiplas verticais de aplicação de IoT, como: cidades inteligentes, energia, saúde, manufatura avançada.
- Integração de sistemas.
- Dispositivos e gateways.
- Computação em nuvem, big data, analytics

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

As alianças internacionais que tiverem requisitos para interoperabilidade atraentes para os produtos a serem desenvolvidos no Brasil, e processo de certificação acessível em termos de custo para os produtos de IoT desenvolvidos no país. Nesse sentido, cita-se:

1) AllSeen Alliance: organização sem fins lucrativos dedicada ao desenvolvimento de interfaces para interoperabilidade entre dispositivos, viabilizando IoT com base na arquitetura aberta AllJoyn, baseada em Linux, para áreas e produtos de áudio, plataformas de desenvolvimento, gateways, automação residencial, iluminação, conexão com nuvem. Atualmente possui mais de 200 fabricantes.
2) Open Connectivity Foundation: Possui framework de software livre IoTivity, também registrado no Linux Foundation. As áreas são: setor automotivo, eletrônica do consumidor, automação residencial, industrial, saúde e segurança, com produtos de áudio/vídeo, gateways, media renderer, servidores de mídia, servidores de nuvem.
3) OneM2M: Padronização para camada de serviço M2M comum ("middleware") destinado a ser embarcado em diversos hardwares e softwares para oferecer interoperabilidade entre soluções. Tem coordenação com 8 organismos de padronização mundiais (ARIB, Association of Radio Industries and Businesses, Japan; ATIS, Alliance for Telecommunications Industry Solutions, US; CCSA, China Communications Standards Association; ETSI, European Telecommunications Standards Institute; TIA, Telecommunications Industry Association, US; TSDSI, Telecommunications Standards Development Society, India; TTA, Telecommunications Technology Association (TTA), Korea; TTC, Telecommunication Technology Committee, Japan; 6 consórcios (Broadband Forum, CEN, CENELEC, GlobalPlataform, New Generation M2@M Consortium Japan e Open Mobile Alliance) e cerca de 200 empresas.
4) Outras comunidades podem vir a ter um papel relevante no ecossistema de IoT, incluindo:
    a. Thinger.io
    b. OpenIoT
    c. MQTT.org

5) Ecossistemas centrados em reputadas Universidades e Institutos de Pesquisa nacionais e Internacionais terão também um papel relevante dentro do universo de IoT

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

- Componentes, incluindo Semicondutores, sensores, atuadores, componentes eletrônicos, circuitos integrados, antenas
- "Coisas" conectadas, exemplo: *wearables,* eletrodomésticos, veículos, cidades inteligentes, Industria 4.0 e quaisquer outras verticais de IoT
- Produtos, softwares e serviços para Manufatura Avançada, Industria 4.0
- Terminais, dispositivos, módulos, sistemas embarcados
- Infraestrutura de conectividade, redes, telecomunicações, interconexão
- Infraestrutura e plataformas de IT, incluindo Cloud, Storage, Data Centers, virtualização
- Gestão e gerência de operações e negócio
- Plataformas para Internet das Coisas
- Segurança da informação, soluções, produtos, softwares e serviços
- Serviços de conectividade incluindo operadoras de telecomunicações
- Serviços, exemplo; consultoria, implementação, gestão, integração de plataformas, operação e suporte
- Desenvolvimento de Software, incluindo Big Data, Analytics, aplicações, ciência de dados
- Produtos e soluções como serviço (*as a Service)*
- Soluções integradas, incluindo terminais, redes, plataformas e serviços para aplicações de consumidor final, corporativas, governo e outras
- Novos materiais, biotecnologia, nanotecnologia
- Novos procolos, matemática, estatística, *analytics*

5.6 Que nichos de mercado apresentam potencial para desenvolvimento de players locais?

Identificamos potencial para o desenvolvimento de players locais no desenvolvimento de soluções para as seguintes áreas e verticais:

- Facilities – com foco em soluções para Smart Cities;
- Serviços – com soluções de automação para uso comercial ou residencial;
- Logística – automação e otimização de cadeias produtivas;
- Mobilidade – segmento automotivo, transporte público;
- Manufatura avançada;
- Agroindústria;
- Energia;
- Saúde;
- Entretenimento; e
- Meio ambiente

5.7 Em quais aplicações o Brasil pode ser competitivo em semicondutores?

Entende-se que na área de semicondutores o Brasil não tem condições de ser competitivo com produtos internacionais, embora possa desenvolver produtos e soluções de qualidade, para competir com produtos importados.
A competitividade poderá vir da escala da demanda de algum produto commodity, como por exemplo:

- Design de chips
- Eletrônica orgânica
- RFID
- Desenvolvimento de sensores e MEMS
- Desenvolvimento de ASICS para dispositivos IoT

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

- equipamentos para meios de pagamentos disruptivos
- Agrobusiness e mobilidade urbana
- Dispositivos e gateways IoT
- Sensores com e sem fios
- Aplicativos para dispositivos móveis

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

Em aplicações IoT praticamente todo software será baseado em web e comercializado como serviço. O Brasil tem potencial para desenvolver aplicações IoT e oferecer o serviço globalmente. Há também oportunidades de desenvolvimento de aplicativos para dispositivos móveis e software para integração de sistemas legados a plataformas IoT.

- Aplicações para Fintech
- Aplicações para agrobusiness
- Agronegócio
- UX / UI dedicados e otimizados para soluções de IoT
- Serviços de integração e comunicação - Middleware

5.10 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?

ABINEE- Associação Brasileira da Indústria Elétrica e Eletrônica.

6. 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.

6.1 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?

O ecossistema de IoT é caracterizado principalmente por ser área de inovação. Houve esforços iniciais na direção de cidades inteligentes, direcionados para cidades digitais, mas há esforços significativos na direção da Internet do Futuro. No entanto não há financiamento para projetos estruturantes e há falta de condições para projetos colaborativos interdisciplinares, tais como consórcios entre empresas, universidades, usuários finais, nos quais a aplicação dos conceitos de IoT seria revertida em benefícios para a sociedade.

O Estado Brasileiro oferece atualmente diversos mecanismos de incentivo à pesquisa, desenvolvimento e inovação tecnológica de caráter geral que seriam aplicáveis aos setores relacionados a IoT.
Dentre estes, podemos destacar:

- A Lei de Informática (Geral e da Zona Franca de Manaus); também é importante, mas precisa ser adequada para a Indústria 4.0, a Manufatura Aditiva e serviços de startups. Além disso, é fundamental uma atualização e flexibilização na lista de bens de informática para que manufatura aditiva, indústria 4.0, IoT etc. sejam considerados.
- A Lei do Bem;
- O Programa BNDES Funtec com recursos não reembolsáveis;
- A oferta de recursos via FINEP.
- O Inova Empresas é um instrumento atual que deve ser mantido, sugerindo um Inova Manufatura Avançada ou Inova IoT que tenha um foco maior na área em questão, se possível com percentuais de subvenção econômica maiores do que as versões anteriores.
- Finame e Cartão BNDES para facilitar a aquisição de máquinas e equipamentos necessários às atividades de P&D.

6.2 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?

No cenário atual em que ainda não se destacam fontes de financiamentos para IoT, ressalta-se a necessidade de disseminação do conceito de IoT como prioritário para o desenvolvimento sustentável do País e a criação de canais de financiamento para projetos consorciados de IoT, relacionados a tecnologias habilitadoras, ao desenvolvimento de modelos de negócio e a governança, a novas aplicações e serviços, com valorização da participação das pequenas e médias empresas.

Os mecanismos existentes são adequados, sendo que, no caso dos instrumentos de financiamento pelo BNDES, FINEP e agências estaduais, sua eficácia depende da efetiva oferta pública dos recursos alocados.

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

É necessário incluir IoT, M2M e Indústria 4.0 nas linhas de financiamento e fomento ou criar linhas específicas para isso.

6.4 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?

Ainda que já existam estruturas no Brasil seguindo o modelo americano do Vale do Silício e o modelo Europeu, a atuação ainda é incipiente quando comparada a esses mercados mais maduros em empreendedorismo e inovação. A atuação de Investidores-anjo e VCs não deve ser vista de maneira isolada como uma operação de capital de risco, mas sim como parte de uma conjuntura muito maior de atratividade e exequibilidade de novos investimentos no país.

Entre as principais limitações ao empreendedorismo no Brasil estão:

- Alta carga regulatória em múltiplos segmentos do mercado
- Burocracia na abertura, fechamento e operação de empresas
- Burocracia na obtenção de alvarás e permissões diversas
- Altas taxas de juros, aumentando a atratividade da renda fixa
- Custo elevado de crédito bancário
- Direito societário desatualizado, incluindo falências, proteção a investidores minoritários, cumprimento de contratos
- Complexidade exagerada e elevada carga tributária
- Infraestrutura deficiente em muitas partes do país
- Registro e defesa de propriedade intelectual
- Baixos acesso e qualidade média da educação fundamental e superior

7. 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

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

Aplicações de IoT em diversos setores públicos, a saber:

1. Gestão de infraestruturas públicas e cidades inteligentes, incluindo: rodovias, ferrovias, hidroviário, aeroportos, gestão de sistema de transporte público, controle de tráfego, semáforos e estacionamentos, segurança pública, energia, água, zeladoria urbana,
2. Melhoria de serviços de saúde no tocante a conectividade das unidades de saúde, da gestão de ativos, controle de temperatura e umidade em salas de operação e quartos de pacientes, uso de tecnologia de conectividade de dispositivos de monitoramento de pacientes, gerência de distribuição de medicamentos em hospitais e clínicas, a informatização do SUS, identificação única de pacientes, registro eletrônico de pacientes, construção de datacenters.
3. Área de Educação, considerando inicialmente a disponibilização de conectividade em banda larga: implementar uso de plataformas de ensino, soluções de controle de bens e equipamentos em escolas, centralização de informações em Secretarias de Educação e desenvolvimento de conteúdos pedagógicos.
4. Meio ambiente, rastreabilidade de produtos, monitoração de qualidade de ar, agua, dentre outros, monitoração aérea de meio ambiente etc, prevenção e detecção de desastres naturais,

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

Ainda não há dados consolidados para o Brasil em relação ao impacto no setor público, mas cita-se que o aumento de banda larga tem correlação com o aumento do PIB nos municípios (refletindo possivelmente a inclusão digital e novos serviços) pois em países menos desenvolvidos, cada 10% de aumento na banda larga representa +1,38% do PIB, conforme referência do Banco Mundial.

Como exemplo de impacto de projetos de cidades inteligentes, cita-se o caso da cidade de Milton Keynes, no Reino Unido, classificada como uma das "Top 10 UK Smart City". Nessa cidade foi realizado projeto de central de coleta de dados de gerência de vários sistemas (consumo de energia e água, transporte obtidos com registro de imagens por satélite, bancos de dados sociais e econômicos e dados de mídia social), visando crescimento econômico, tendo sido implementado por parceria entre prefeitura, consórcio de empresas (British Telecom e outras) e universidade. Em termos de impacto, foi previsto crescimento da economia em 64% em 2026, a redução em 20% de consumo de água e redução de trânsito em 50%. Outro aspecto importante foi a incubação de 90 novas pequenas e médias empresas para aplicações IoT, com criação de

centenas de empregos. A prefeitura identificou mais de £ 105 milhões em redução de custos, além da geração de novas receitas.

Para o setor público global, cita-se que IoT poderá gerar $4.6 trilhões em 2022 a partir do aumento da produtividade, da melhoria de eficiência dos sistemas militares de defesa, da redução de custos, da melhoria da experiência dos cidadãos com serviços públicos e aumento de receita dos governos.

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

Dentre as barreiras na esfera pública, estão o excesso de burocracia na aquisição de soluções, geração e uso isolados de dados isolados, falta de coordenação no setor público entre órgãos do Governo, Planejamento, falta de cooperação com o setor privado, falta de agilidade na tomada de decisões e gestão de recursos, além de aspectos legais quanto ao monitoramento, coleta e uso de informações.

7.4 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?

O Governo deve investir em tecnologia inteligente para projetos de infraestrutura pública com vistas a aumentar a segurança, reduzir os seus custos de manutenção e melhorar o dia-a-dia gerencial/operacional. Além disso, esses projetos gerarão dados valiosos que deverão ser disponibilizados ao público e a iniciativa privada para promover a inovação e o consequente desenvolvimento de novos produtos e serviços de IoT.

Neste sentido, é importante ressaltar que a IoT irá gerar uma quantidade sem precedentes de dados. Os dados coletados de dispositivos conectados oferecem uma miríade de benefícios potenciais para usuários, pesquisadores, Governo e iniciativa privada, e se esses conjuntos de dados forem compartilhados, esses benefícios podem ser multiplicados. Podemos inicialmente pensar que há apenas uma razão para coletar dados, contudo, uma infinidade de aplicações de IoT pode ser criada a partir da análise destes dados, aprimorando continuamente o bem-estar social e auxiliando o crescimento econômico.

Para maximizar os benefícios do IoT, os Órgãos e Agências do Governo devem reestruturar suas práticas em torno dos benefícios oferecidos pelos produtos e serviços de IoT disponíveis, demonstrando como e quanto a tecnologia pode influenciar o bem-estar econômico e social do país.

Além disso, como já ressaltado em tópicos anteriores, vislumbramos a necessidade de revisão de regulamentos que possam afetar negativamente o ecossistema de IoT.

Por fim, existem ainda aspectos absolutamente sensíveis e que são pressupostos para a viabilidade do modelo de IoT nas demandas públicas, quais sejam:

a. Segurança jurídica para a coleta e tratamento de dados públicos e privados;

b. Modelos de contratação e/ou parceria em linha com a sofisticação das soluções existentes, levando em consideração não apenas o valor, mas também outros critérios como performance, melhor tecnologia disponível, benefícios sociais dentre outros;
c. segurança jurídica na contratação, dotada de matriz de riscos, limitação de responsabilidades, remuneração adequada, juntamente com sistema de garantias apto ao recebimento de grandes investimentos;
d. políticas públicas menos restritivas ao ingresso de tecnologias internacionais;
e. sistema de fomento, com possível transferência de recursos inter-federativos para viabilizar projetos em grandes conglomerados urbanos.

b) Demanda privada

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

- **<u>Saúde</u>**
  - Monitoramento preventivo de saúde com monitoramento dos sinais vitais e emissão automática de alertas médicos
  - Diagnóstico remoto com aplicativos para consultas médicas
  - Autoatendimento e tratamento remoto
  - Prontuário único do paciente
  - Inventário e localização de equipamentos em UPAs e hospitais
  - Monitoramento da condição de idosos e PNEs
  - Controle da cadeia do frio de fármacos, vacinas e hemoderivados
  - Controle na distribuição e administração de medicamentos, materiais e suprimentos
  - Rastreamento de medicamentos (controle de estoques, gestão inteligente de datas de validade, etc.)
  - Unidades de Terapia Intensiva com equipamentos de monitoração integrados aos dados sobre estado geral do paciente
  - Quartos "inteligentes" que interagem com o paciente por meio de IoT e Computação Cognitiva
  - Monitoramento e otimização da disponibilidade de equipamentos de diagnóstico
  - Realidade virtual para treinamento médico
  - Consultas remotas com vídeo
  - Cirurgias remotas através de robôs controlados a distância

- **<u>Agricultura</u>**
  - No caso de agricultura de precisão, a tecnologia pode contribuir tanto com a otimização, racionalização ou redução das perdas da produção,

assim como também contribuir para reduzir o impacto ambiental. Os exemplos existentes são:

- Detecção, monitoração da variabilidade espacial e temporal dos sistemas de produção agropecuários;
- Rastreabilidade da produção, para controle de qualidade e procedência;
- Melhoria do uso e manejo do solo por meio do seu monitoramento;
- Economia com irrigação (irrigação inteligente);
- Redução de perdas por questões climáticas;
- Planejamento operacional (forecast de tempo, detecção e gestão de pragas com analytics, planejamento de safra com analytics, consumo de insumos (pesticidas, agua) eficientemente com agricultura de precisao, localização e controle de gado, controle de estoque e logística de transporte) ;
- Modelos de analise de preços de comodities e de mercado;
- Gestão remota;
- Troca de informações e de conhecimento;
- Controle de rebanhos (saúde e inventário);
- Monitoramento do armazenamento de Leite;
- Controle automatizado da qualidade de alimentos;
- Rastreamento da semente à colheita para otimização de produtividade;
- Veículos agrícolas inteligentes e autônomos, como colheitadeiras;

- **Infraestrutura**
  - Transporte público: com a utilização da localização dos smartphones e de vestíveis é possível saber onde há mais demanda por transporte público e qual é o modal mais indicado.
  - Transporte de carga: monitoramento de cargas em rodovias, ferrovias e hidrovias para otimizar o transporte de carga modal.
  - Engenharia de tráfego: monitoração de veículos, passageiros e cargas em ruas, avenidas e estradas para garantir a melhor fluidez do tráfego.
  - Construção civil: predios inteligentes, eficiencia de consumo de agua, energia, etc.
  - Energia: indústrias, comércios e residências inteligentes com controle automatizado do uso de energia, bem como distribuição inteligente da mesma por parte das concessionárias.
  - Recursos hídricos: controle do consumo e de perdas na distribuição de água tratada
  - Logística: localização de bens e inventário, otimização inteligente de estoques

- **Petróleo e gás**
  - Monitoramento de vazamentos e perdas na distribuição de gás e derivados do petróleo
  - Automatização de segurança e de controles de meio ambiente;

- Instrumentação, sensorização e monitoração complementados com serviços remotos
- High performance computing e modelos matemáticos avancados
- Redução de custo de manutenção e aumento de eficiencia operacional;
- Modelos de negociação comercial automatizados;
- Garantia de segurança de trabalhadores em situação de risco (monitoramento remoto dos trabalhadores);
- Uso de sensores e equipamentos para manutenção e trabalhos em áreas de alta profundidade e difícil acesso (com condições precárias de luminosidade, alta pressão, corrosão de materiais, etc.)
- Monitoramento da qualidade e "saúde" dos de ativos;
- Manutenção preditiva de equipamentos.

- **Automotivo**
  - Veículos autônomos e inteligentes
  - Carro conectado, incluindo atualização de software
  - Comunicação veículo a veículo
  - V2X (veículos, pedestre e infraestrutura)
  - Carros elétricos, redução de emissão e demanda por combustíveis fósseis
  - Serviços baseados em localização (LBS), incluindo GPS com informação instantânea de tráfego, integração com concessionárias, oficinas, postos
  - Economia compartilhada
  - Plataforma de serviços incluindo seguro, assistência e socorro
  - Estradas inteligentes, monitoramento de tráfego, platooning

- **Bens de consumo e varejo**

  Com os mundos físicos e digitais se fundindo em uma única realidade, os objetos do dia-a-dia hoje desprovidos de conectividade e computação serão inseridos no mundo digital através de ambientes inteligentes.

  Exemplos:
  - Consumidores mais informados, novos tipos de consumidores requerem transformação da industria;
  - Omni-channel viabilizado pela digitalização;
  - Integração da cadeia do valor;
  - Personalização de produtos e da experiência do cliente;
  - Globalização;
  - Individualização de marketing;
  - Estabelecimento de canais diretos entre produtores e consumidores;
  - Otimização e integração de estoques;
  - Diferenciação da experiencia do cliente
  - Tecnologias vestíveis, Wearables (para bem-estar, monitoramento preventivo de saúde)
  - Identificação e monitoramento do comportamento do consumidor

- Monitoramento em lojas físicas (por meio de conectividade com pontos de acesso wifi ou ibeacons por ex) do comportamento do comprador para melhor atendimento, controle de estoque e supply chain);
- Monitoramento de condições de calor, ventilação e ar condicionado em lojas físicas (conjugação com serviços de meteorologia);
- Utilização de analytics ou serviços de previsão meteorológica para previsão de demanda de produtos em curto, médio e longo prazo

- **Energia**
  - Com o uso das SmartGrids será possível gerir a demanda por energia, reduzindo o desperdício;
  - Integração entre medidores de energia, água e gás;
  - Desenvolvimento do AMI para redução de perdas técnicas e não técnicas, redução de tempo de falha, interrupção e restauração ao consumidor final, em casos de falha na rede elétrica (self-healing: recuperação automática do sistema elétrico);
  - Rastreabilidade – gestão de ativos;
  - Manutenção preditiva e pro-ativa;
  - Previsibilidade de consumo;
  - Geração de Energia distribuída fotoelétrica em casas e PME;
  - Novas modalidades de tarifação de consumo de energia, água e gás;
  - Monitoramento de linhas de transmissão para identificação precisa de pontos de falha;
  - Serviços analíticos e de previsão meteorológica para previsão de quedas de energia;
  - Monitoramento e uso racional dos recursos pelos usuários intermediários e finais.
  - A digitalização de subestações, na Distribuição, Transmissão e Geração é regulamentada pela ANEEL e englobada IoT e M2M, onde a segurança cibernética é fundamental para evitar ataques cibernéticos a infraestrutura critica;
  - Na medição, os dados dos sensores podem ser usados para detectar fraudes e roubos de energia na rede elétrica;
  - Gestão de Ativos para as concessionárias de energia, onde através dos dispositivos integrados a rede, pode-se realizar a manutenção preventiva dos equipamentos, evitando falhas no fornecimento de energia.
  - Otimizar a energia elétrica gasta com a iluminação, por meio de sensores inteligentes, realizando, por ex. a dimerização da Luz da iluminação publica e a detecção automática de falhas de iluminação.

- **Logística**
  - Rastreamento da distribuição de produtos até entrega ao consumidor,
  - Inventário inteligente,
  - Detecção de danos em embalagens por câmaras

- Manutenção preventiva de empilhadeiras e máquinas
- Gestão de EPIs
- Monitoramento das condições de armazenagem e transporte de mercadorias sensíveis à temperatura
- Integração de fornecedores e tracking do ciclo de vida dos produtos tornando a produção mais flexível/adaptável às demandas de mercado e disponibilidade de suprimentos.
- Monitoramento do comportamento do motorista;
- Monitoramento dos veículos para aumento da eficácia de manutenção;
- Compartilhamento de ativos (caminhões, carretas, barcas) para a sua otimização e redução dos custos
- Meios de transporte conectados e autônomos
- Drones para entregas logísticas – e-commerce

- **<u>Aeroespacial</u>**
  - Sensorização, automação, sistema conectados, equipamentos inteligentes, analytics como ferramentas para melhorar eficiencia e qualidade;
  - Ameaças de segurança cibernética de Nation States e terroristas
  - High performance computing e processamento de imagem
  - Novos materiais e desenvolvimento de pesquisas
  - Rastreamento de peças e componentes na composição de aeronaves;
  - Manutenção preditiva;
  - Utilização de dados gerados em tempo de operação de aeronaves para melhoria de serviço de manutenção ou "retrofit" com time de engenharia para correção de falhas em tempo de projeto.

- **<u>Eletrônicos avançados</u>**

  Desenvolvimento de produtos com conectividade e aplicações de gerência de uso, como por exemplo:
  - Sensorização embarcada;
  - Sensores inteligentes aplicados a vestíveis
  - Acessórios de Realidade Virtual;
  - Transformação de eletrodomésticos em geral em coisas conectadas, permitindo "hardware as a service" (identificação, auto-diagnóstico, manutenção, medição de uso e reposição de suprimento em dispositivos)

- **<u>Mineração</u>**
  - Gerência de operações de máquinas, gerência de processos, controle de inventário
  - Controle de movimentação de veículos e materiais

- Sensorização e automação para aumento de eficiencia, segurança e monitoração de meio-ambiente (interação homem-máquina; conversão de digital para físico);
- Maximização de uso de ativos e manutenção preditiva;
- Conectividade em áreas remotas
- Monitoramento de estruturas para prevenção de acidentes
- Garantia de segurança de trabalhadores em situação de risco (monitoramento remoto dos trabalhadores, dos equipamentos, controle de insalubridade de ambientes);
- Monitoramento de saúde de ativos;
- Manutenção preditiva de equipamentos.
- Automatização e maior eficiência na cadeia de armazenamento e transporte de minérios em todas as etapas do ciclo logístico Mina-Ferrovia-Porto-Navio

- **Telecomunicações e mídia**
  - Digitalização e disseminação do conteúdo
  - Streaming 4K para dispositivos móveis
  - Shows e esportes interativos ao vivo
  - Broadcast pessoal em 3D a partir de dispositivos móveis
  - Broadcast remoto para TV & Mídia
  - Jogos em realidade aumentada / realidade virtual
  - Internet táctil
  - Realidade aumentada & virtual como interface de mídia e comunicação
  - NFV (Network Function Virtualization) e SDN (Software Defined Networks com capacidades avançadas de segurança, gerenciamento, virtualização e engenharia de tráfego)

- **Serviços bancários**
  - Agregação de rastreamento de itens com serviços de seguro e serviços de aluguel de veículos, com controle remoto de operação e monitoramento de uso.
  - Uso massivo de analytics e big data poderá incrementar as ferramentas de predição, tornando a concessão de crédito mais segura e, consequentemente, mais barata.
  - Pagamento por dispositivos móveis e wearables
  - Manutenção preditiva de ATMs;
  - Engajamento com cliente por meio de monitoramento de dispositivos móveis;
  - Monitoramento em agências (por meio de conectividade com pontos de acesso wifi ou ibeacons por ex) do comportamento do comprador para melhor atendimento, controle de estoque e supply chain);
  - Monitoramento de condições de calor, ventilação e ar condicionado em agências (conjugação com serviços de meteorologia)
  - Mobile wallet, mobile payment, mobile money

- Seguros baseados no comportamento e estilo de vida do usuário Banco
- Mobile & Omni channel
- Personalização de serviços e ofertas baseado em analytics
- Block chain
- Mudança dos perfis das agencias
- Segurança da informação

- **Cidades inteligentes**
  - Transporte (estacionamentos inteligentes, previsibilidade de transito, previsibilidade de transportes públicos, compartilhamento de transportes de baixo volume etc);
  - Saúde (atendimento remoto, prontuário único de paciente, rastreabilidade de medicamentos, controle de descarte de medicamentos etc);
  - Meio Ambiente (rastreabilidade de produtos, monitoração de qualidade de ar, agua, dentre outros, monitoração aérea de meio ambiente etc);
  - Segurança (rastreabiliadade de pessoas, detecção por face);
  - Infraestrutura (otimização de consumo de energia, água, conectividade em qualquer lugar e em qualquer momento, mudança no perfil de uso de serviços de conectividade, etc);
  - À partir de um sistema de iluminação inteligente é possível desenvolver toda uma gama de soluções em IoT passando por semáforos inteligentes, integrados com câmeras de segurança, etc;
  - Controle de resíduos/lixo/bueiros;
  - Aplicações de acesso pelo cidadão;
  - Informações sobre disponibilidade de áreas de estacionamento;
  - Acionamento da coleta de lixo pela ocupação dos containers;
  - Centros de Monitoramento de emergências integrados com serviços policial, bombeiros, guarda civil e de previsão meteorológica para primordialmente coordenação de ações preventivas;
  - Monitoramento de frota de transporte público com frotas conectadas para otimização de rotas, monitoramento do comportamento do motorista, monitoramento dos veículos para aumento da eficácia de manutenção e manutenção preditiva;
  - Monitoramento da rede de abastecimento de água por meio de sensores que detectem com precisão pontos de falha ou que possam mesmo antever estes pontos de problema;
  - Monitoramento da rede de abastecimento de energia e implementação de “smart grids”;
  - Integração dos meios de transporte públicos para incremento na agilidade de locomoção dos cidadãos por meio de indicação da conjunção dos meios mais eficientes para alcance de um destino.

- **Indústria 4.0**

- Digitalização de processos industriais, realidade aumentada
- Conectividade e integração de informação em toda da cadeia de valor (horizontal) e entre todos os niveis do processo da indutria (vertical);
- Informação transformando o valor / diferenciando os produtos da Industria: devices inteligentes conectados geram dados, dados (estruturados e não estruturados) analisados geram insights e valor agregado;
- Equipamentos e Máquinas conectadas e integradas para redução de perdas e paradas em produção
- Controle de logística de produção
- Automação da manufatura, Manufatura aditiva – Impressão 3D, RFID
- Sensores para notificação e gestão de manutenção preditiva, preventiva e corretiva.
- Video para monitoramento de ativos e processos
- Sensores machine-to-machine
- Segurança remota de plantas
- Controle em real-time de robôs
- Uso de especialistas remotos para reparos em campo
- Micro-robôs para verificação do processo produtivo
- Informação embutida em ativos como matérias primas e peças
- Produtos inteligentes capazes de transmitir informações de uso
- Cadeia produtiva, logística, de venda e suporte integradas com rastreabilidade
- Equipamentos auto-suficientes, auto-reparadores e auto-programáveis
- Garantia de segurança de trabalhadores em situação de risco (monitoramento remoto dos trabalhadores);
- Monitoramento de saúde de ativos;
- Manutenção preditiva de equipamentos.

- **<u>Escritórios e residências inteligentes</u>**

  Automação residencial e de ambientes de escritório, aplicações para gestão de consumo como:

  - Controle dos dispositivos de iluminação, ar condicionado, mídias, consumo geral (água e energia).
  - Controle de entrada e saída de pessoas (acesso e segurança).
  - Interatividade em eletrônicos e eletrodomésticos: geladeira que notifica a falta de um determinado produto; lavadora de roupas que altera a programação mediante o tipo de roupa; TVs que ajustam a programação conforme o usuário; banheiras que ajustam a quantidade de água e temperatura previamente; sensores de luz que acionam a abertura/fechamento de cortinas; espelhos inteligentes touch screen com acesso à internet, etc.
  - Assistentes virtuais que entendem o contexto onde as pessoas estão inseridas, viabilizando, junto a sensores de presença e atividade, ambientes que apoiam e ampliam a execução das atividades do dia-a-dia.
  - Gerenciamento à distância dos equipamentos domésticos.

- Monitoramento de 'Telhados Fotovoltaicos'.
- Robôs domésticos: aspiradores e limpadores de chão, limpa-vidros.

- **Pequenas e médias empresas**

  Entendemos que este segmento não carece de uma vertical específica já que se submetem às mesmas situações que empresas de maior porte (prédio inteligente, manutenção preditiva, logística otimizada).

  Além de consumidor, este segmento pode ser visto como um segmento que buscará explorar oportunidades neste novo ambiente. Novas empresas surgirão para explorar as oportunidades do novo ambiente de negócios propiciado pela IoT.

  De qualquer forma, listamos os exemplos que podem se inserir neste item:

  - Automação de processos;
  - Redução de custos;
  - Melhorias na gestão de máquinas e equipamentos;
  - Melhorias em produtividade;
  - Gestão assertiva de estoques e ativos;
  - Gestão de compras e interações com fornecedores de forma automatizada;
  - Processos de devolução mais rápidos e eficientes de forma a não penalizar o cliente;
  - Controle efetivo da qualidade dos produtos e serviços;
  - Melhor entendimento e engajamento do cliente

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

Educação

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

Aplicações de IoT são todas ainda incipientes frente ao seu potencial. As mudanças mais impactantes na vida das pessoas devem ser na área de saúde e bem estar, monitoramento ambiental, agroindústria e cidades inteligentes. Alguns exemplos de white spaces:

- Integração entre elementos de informática com ambientes operacionais,
- Análise de comportamento de pequenas atividades do dia a dia, através do uso de big data
- Aplicações na área da agricultura

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

O impacto estimado de IoT na economia brasileira em relação ao setor privado pode ser mensurado por quantidade de dispositivos conectados e montante de investimentos. Cita-se a previsão da IDC Brasil de 130 milhões de dispositivos conectados em 2015, o que corresponderia a quase metade de "coisas" conectadas na América Latina. O mercado de Business Intelligence e Analytics teria ao final de 2015, investimentos de US$ 788 milhões no Brasil. Para 2016, a IDC estimou que esse mercado movimentaria expressivos US$ 4,1 bilhões no Brasil. Na América Latina, o mercado de IoT crescerá de US$ 7,7 bilhões, registrado em 2014, para cerca de US$ 15,6 bilhões em 2020. Atualmente 59% das empresas avalia iniciativas e projetos orientados ao conceito de Internet das Coisas na AL.

Em termos globais, há estimativa da categoria de IoT voltada para área comercial e industrial atingir US$ 7 trilhões em 2030, que envolve áreas de manutenção preventiva de equipamentos, gerências de iluminação, ar condicionado e aquecimento, gerência de transporte de frotas, e outras melhorias, que contabilizadas em larga escala refletem grande redução de custo e consumo de energia, e aumento de produtividade e eficiência. Cerca de 70% do valor potencial de IoT é oriundo de aplicações comerciais e industriais.

Nesse contexto, são citadas as seguintes melhorias:

- Surgimento de novas empresas explorando novas oportunidades de negócios viabilizados pela tecnologia.
- Aumento da eficiência (redução de perdas e consumo consciente) de água potável
- Aumento da produtividade no agronegócio
- Redução de congestionamentos em grandes cidades, com consequente redução no consumo de combustível e na emissão de poluentes. Aumento da produtividade da população.
- Novos serviços. Toda uma gama de novos serviços irão surgir, seja a partir da criação de novos dispositivos ou a partir de novos serviços criados a partir dos dados coletados: novos aplicativos, novos serviços B2B ou B2C baseados em dados, empresas especializadas em camadas intermediárias do tratamento e armazenamento de dados, etc. Saber estimular o desenvolvimento dos novos serviços das cadeias em tornos dos dados poderá ser um diferencial para a competitividade brasileira no cenário global.
- Mudança na composição das ofertas de emprego. Com a sensorização haveria uma mudança nas oportunidades do mercado de trabalho. Algumas profissões deixarão de existir (como por exemplo o funcionário que monitora nas residências o consumo de água ou de energia) e uma gama nova de profissões será criada, em especial, em torno dos serviços ligados aos dados (como, por exemplo, os cientistas de dados, o técnico e o engenheiro de privacidade e segurança da informação, etc.).

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

Barreiras que impedem o desenvolvimento de pequenas e médias empresas (excessiva tributação, burocracia na abertura de empresas, custo elevado de pessoal CLT)

7.10 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?

8. Aspirações

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

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

Promover o crescimento econômico do país permitindo a expansão do mercado, a geração de empregos, o desenvolvimento profissional em diversos níveis, a melhoria da gestão da máquina pública, o melhor controle de gastos públicos, o atendimento a serviços básicos do cidadão como saúde, educação e transporte.
Sugere-se que o Governo estabeleça um plano de metas para adoção de soluções de IoT , por exemplo no caso de Cidades Inteligentes, através da definição de percentuais a serem implementados em períodos de tempo a serem definidos (p.ex. nos primeiros três anos, entre três a cinco anos, etc.).

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

As aspirações voltadas para o crescimento econômico através de apoio aos negócios serão de grande impacto no Brasil. Nos EUA e Reino Unido destacam-se iniciativas voltadas para incentivo ao desenvolvimento do mercado através de apoio a negócios de empresas emergentes. Nos EUA destaca-se o consórcio de empresas IIC, que embora seja de eco industrial, está fortemente voltado para a produção de produtos e soluções por empresas de pequeno e médio porte, seguindo padronização e arquitetura desenvolvida para Internet das Coisas. No Reino Unido, destaca-se o forte apoio financeiro do Governo para iniciativas tais como o IoTUK, dedicado a apoiar novas empresas. O IoTUK recebe do Governo um fundo destinado à sua operação (equipes e recursos materiais). Desta forma, o escopo é promover encontros entre empresas, através de chamadas de projetos direcionados para demandas específicas, para os quais se apresentam desenvolvedores de soluções ou fabricantes de produtos. Na Comunidade Europeia destaca-se o Programa H2020, em particular as chamadas para projetos de cidades inteligentes. Essas chamadas são estruturadas de forma a serem atendidas por parcerias entre universidades, centros de pesquisa e empresas privadas, de forma que os recursos financeiros dados pelo Governo são destinados para reembolso de custos elegíveis (com algumas variantes entre os tipos de reembolso) das empresas e de pessoal envolvido. Com esse formato, o projeto pode ser desenvolvido e então implantado por empresas privadas que depois farão a operação e manutenção das infraestruturas (p. ex iluminação pública com postes inteligentes), tendo receita e sustentando a implantação, para real usufruto da cidade. Configura-se assim um investimento público com resultados que se mantêm a médio e longo prazo.

9. 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

9.1 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:

1. 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.

2. 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.
3. 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.

O uso generalizado dos serviços de IoT oferece uma grande oportunidade para o crescimento econômico e para o benefício da sociedade como um todo, como já apontado ao longo de nossas contribuições.

Para que esta oportunidade seja amplamente utilizada pelo Brasil, o Estado precisa conjugar a proteção à privacidade e à segurança nacional e o equilíbrio com as práticas adotadas pelo mercado de IoT, que vem diariamente aprimorando suas práticas nestes campos para salvaguardar a privacidade dos dados dos seus usuários.

Do ponto de vista tecnológico, a segurança e a privacidade devem ser abordadas no dispositivo, na camada de aplicação, na camada da conectividade e na nuvem. Os dispositivos IoT devem ter mecanismos de segurança resilientes para evitar ataques massivos de DDoS. Na camada da conectividade, redes móveis oferecem mecanismos robustos de segurança e privacidade. As redes móveis de segunda geração (GSM) foram as primeiras a ter funções de segurança padronizadas e integradas, que evoluíram através

de redes 3G e agora 4G. As redes móveis 4G atuais oferecem um alto nível de segurança e confiabilidade para usuários e operadoras. Além disso, as recentes tecnologias 3GPP, como o LTE-M, o NB-IoT e o design de EC-GSM-IoT para suportar o caso de uso do IoT, são soluções superiores projetadas para atender aos requisitos de segurança e privacidade do IoT/M2M. E, embora o padrão 5G ainda esteja em desenvolvimento, é esperado que os sistemas 5G futuros2 suportem um ecossistema avançado e confiável, que endereçará novos modelos de negócio IoT/M2M e demandas de segurança.

O Estado deve concentrar seus esforços na elaboração de uma Política Nacional de Segurança Cibernética adequada para identificar, responder e, em última instância, prevenir ameaças cibernéticas aos sistemas IoT/M2M e às infraestruturas críticas. A elaboração desta política deve ser precedida por uma ampla discussão com todos os setores da sociedade, seguida por um esforço de implementação que garanta sua plena adoção pelos entes governamentais, setor privado e sociedade civil.

Diferentes organizações apontaram a necessidade de reforçar a cibersegurança. Recentemente, a Comissão Interamericana de Telecomunicações (CITEL) da OEA recomendou aos Estados membros que promovam a colaboração com a indústria para incentivar a adoção de medidas de segurança adequadas no que diz respeito aos serviços IoT/M2M, inclusive em suas cadeias de valor e educando os usuários finais sobre IoT/M2M, para evitar vulnerabilidades cibernéticas e prevenir ataques cibernéticos, e revisar os requisitos de certificação de equipamentos para facilitar a adoção de serviços IoT/M2M, quando tal se justifique.

Ref. 1: Ericsson White Paper 5G Security Scenarios and Solutions

Ref. 2: CITEL PCC.I/REC. 26 XXVIII-16 - Recommendation to incentivize greater adoption of IoT/M2M services

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

9.2 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

9.3 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.

9.4 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.

9.5 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:

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.

9.6 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?

O desafio consiste justamente no desenvolvimento de uma camada ou plataforma que trate as questões de segurança de aplicação, rede e dispositivos conectados de forma integrada. Existe sim esta demanda por novos mecanismos de segurança porque, por exemplo, no aspecto de segurança mencionado podem ser necessárias APIs (RESTful, por exemplo) que permitam à camada de aplicação gerenciar dispositivos com base em credenciais de acesso e autorização que ela fornece aos dispositivos.

Uma vez que os dispositivos ou as fontes de dados podem ser diversos, esta abstração da camada de segurança baseada em credenciais padronizadas permite que tanto a captação de dados quanto a interação com sensores ocorram de modo seguro. Esta arquitetura também permite que se enderecem aspectos de diagnóstico de estado dos sensores, determinação de problemas de conectividade entre aplicação e sensores (inclusive com determinação de falhas de rede) e armazenamento de dados provenientes dos sensores.

Além disso, muitos dispositivos IoT utilizam plataformas com poder de processamento e memória restritos, além de operarem desconectados da rede elétrica. Por essas razões, versões "leves" de mecanismos tradicionais devem ser criadas, respeitando-se as limitações existentes. Existem algumas instituições de P&D com capacidade para desenvolvimento desses tipos de mecanismos, além das principais universidades brasileiras.

Há, ainda, a necessidade de se considerar a limitação de recursos de alguns dispositivos de IoT, além de novas tecnologias e protocolos de interconexão. Por exemplo, é necessário criar mecanismos de segurança que possam ser executados em dispositivos que usam uma pilha de relógio que deve durar por meses, possuem conectividade limitada ou mesmo que se comunicam com dispositivos que se encontram fisicamente próximos.

Também existe oportunidade de desenvolvimento local de novos mecanismos de segurança, mas acreditamos que isso só deve ser considerado se forem seguidos padrões internacionais, adaptando-os de acordo com necessidades da legislação local.

Ainda é interessante se notar que podemos considerar normas e padrões mínimos para diferenciar um dispositivo considerado seguro para uso e não seguro. Por exemplo, dispositivos médicos (bombas de insulina, marca-passos), que envolvem transações financeiras, dados confidenciais (roteadores de rede, dispositivos de armazenamento), integridade física, bens patrimoniais (fechaduras, controle de acesso), etc, teriam um nível de segurança maior.

Objetos do cotidiano, como lâmpadas, equipamentos de limpeza ou de menor risco, estariam em uma categoria diferente. Órgãos certificadores e programas de capacitação poderiam ser criados para estabelecer e certificar os equipamentos mais sensíveis à problemas de segurança da informação. A

indústria nacional teria, então, diretrizes mínimas de segurança da informação a serem atendidas por seus produtos e serviços de M2M/IoT.

9.7 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?

Nos últimos anos, diversos grupos de pesquisa em criptografia no mundo estudaram versões leves de algoritmos e protocolos criptográficos, que fossem adequados para dispositivos restritos. Fontes sobre o assunto incluem a página do CryptoLUX e o DRAFT NISTIR 8114 do NIST.

Os dispositivos em si são apenas a origem de dados que terão maior valor agregado após seu processamento em soluções analíticas, por exemplo. Neste sentido, não há necessidade, com algumas exceções, de soluções robustas de criptografia na ponta na maioria dos casos de soluções IoT. Não obstante, a oferta crescente de dispositivos que possuam não apenas microcontroladores mas também microprocessadores capazes de rodar sistemas operacionais, permite que eventualmente esta criptografia seja já tratada com propriedade na origem dos dados. Há que se relembrar ainda que, tal qual explanado no item 1, é necessária integração entre a camada de dispositivos com as camadas de rede e aplicação para garantia total de segurança.

Desta forma, defendemos, além da aplicação de padrões internacionais, a criação de um programa de certificação específica para a indústria de IoT, de forma a auditar que os produtos implementem e usem de forma correta protocolos e algoritmos considerados de melhor prática pelo mercado.

9.8 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?

Ataques de negação de serviço realizados recentemente, como o que vitimou os sites Twitter e Spotify, utilizaram dispositivos IoT, como câmeras IP e set-top boxes, por exemplo, os quais foram invadidos por meio da exploração de vulnerabilidades simples, como uso de senhas de fábrica ou inexistência de autenticação. Para que esse tipo de problema seja eliminado, é fundamental que dispositivos IoT sejam desenvolvidos por meio de ciclos de desenvolvimento seguro de software e hardware, que considerem segurança em todas as etapas do processo.

Como exemplo podemos entender que uma vez que as camadas de sensores, rede e aplicações estejam integradas, é possível imaginar uma arquitetura de

credenciamento e autorização onde o acesso à camada de aplicação, por exemplo, passe por um serviço de subscrição no qual os dispositivos tenham de ser validados com identificadores e chaves únicos dentro da camada de rede. A aplicação só poderia ser invocada por meio de dispositivos devidamente autorizados e credenciados por ela. Uma camada de rede que possa associar os dispositivos corretos à aplicação que processará os dados enviados na rede filtra cada requisição de acesso por meio de validação do dispositivo como fonte segura de dados. Um ambiente integrado por si só representa um ambiente cooperativo para detecção de falhas de segurança com respectivas ações de correção.

Também é necessário incentivar mecanismos que permitam a pesquisa e divulgação de vulnerabilidades. Porém, a legislação ainda não é clara com relação à forma correta de se fazer a divulgação de vulnerabilidades, o que afasta pesquisadores. Muitas vezes, por medo de represálias e processos, tais informações ficam indisponíveis aos fabricantes e acabam sendo usadas para fins ilícitos. Para garantirmos o fluxo de informações a respeito de vulnerabilidades e ataques a equipamentos e infraestrutura precisamos de uma melhor definição legal das atividades de análise de segurança e testes de penetração.

Além disso, um programa de certificação de segurança implementado de forma gradual, com selo de qualidade estampado nas embalagens dos produtos, forçaria os fabricantes a aumentar a qualidade e segurança de seus dispositivos, ao passo que os consumidores passem a cobrar por esse selo.

Por fim, também sugerimos acompanhar os projetos internacionais de segurança, após identificação de atores relevantes na área como, por exemplo, o OWASP, a arquitetura do IIC, o NIST com projeto de cibersegurança

9.9 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.

Para que haja uma massiva adoção das aplicações de IoT pela sociedade deve-se garantir aos usuários que se trata de um ecossistema seguro para o tráfego de seus dados. Neste sentido, aplicações desenvolvidas com base nos princípios da "Privacy by Design" e da "Security by Design", além de redes de telecomunicações robustas e seguras, tornam-se itens fundamentais para assegurar o pleno desenvolvimento e aceitação da IoT entre a população brasileira.

Logo, em relação à privacidade, a ABINEE entende que as empresas de tecnologia responsáveis pelo desenvolvimento de produtos e serviços de TIC devem adotar o já citado princípio da "Privacy by Design" com o objetivo de criar salvaguardas para a privacidade dos usuários desde a sua criação, passando pela fase de elaboração até o lançamento de seus produtos e/ou serviços, buscando prever potenciais ameaças desde o seu processo de concepção. Deve-se dar ênfase à inovação técnica em tecnologias de aprimoramento da privacidade para permitir que os indivíduos gerenciem e controlem seus dados pessoais de forma mais intuitiva e eficaz.

Outrossim, tendo em vista que o ecossistema de IoT é florescente, torna-se impossível tentar prever todos os possíveis pontos relacionados à proteção de dados que poderão influenciar a Internet das Coisas. Não nos parece salutar a ideia de propor uma lei de proteção de dados pessoais estática para aplicação exclusiva no universo de IoT, que se apresente como uma fotografia do período no qual foi criada.

Propor este tipo de regulamentação para algo dinâmico e inovador como IoT pode paralisar sua evolução no país. Não se deve olvidar que boa parte das aplicações de IoT que auxiliarão o desenvolvimento da economia, assim como da própria sociedade, ainda não foram inventadas.

Pelo contrário, o Estado deve buscar a edição de lei específica sobre proteção de dados pessoais, de natureza principiológica e genérica, que abarque fundamentos que garantam a privacidade dos usuários no mundo online e off-line, e que não fique ultrapassada em razão do desenvolvimento tecnológico, podendo ser aplicada diretamente no ecossistema de IoT.

Outra questão importantíssima a ser observada e garantida na elaboração desta futura lei de proteção de dados é o livre fluxo internacional de informações. Este ponto é de suma relevância para garantir o crescimento da IoT no Brasil e do processo de inovação.

Acreditamos firmemente que a lei de proteção de dados pessoais de qualquer país deve ter em conta a natureza global das cadeias de valor de dados atuais e o papel crescente dos mercados globais de serviços digitais para a Internet das Coisas. Neste sentido, a promoção de fluxos transfronteiriço de dados será fundamental para o crescimento dos negócios e da sociedade.

Muitas transferências internacionais importantes estão acontecendo, por exemplo, com relação a impedir fraudes e corrupção, protegendo os funcionários e acionistas contra a perda de rendimentos, sendo os processos de denúncias apenas um exemplo. Outro exemplo de transferências que geralmente devem ser aceitas e estar sujeitas às medidas ordinárias de proteção de manipulação é quando há interesse legítimo, por exemplo, no caso de resolução de problemas técnicos, em que a transferência de dados é temporária, de baixo volume e não frequente por natureza. Portanto, propomos que os fluxos de transferências internacionais de dados não sejam restritos quando forem necessários para os fins de interesses legítimos perseguidos pelo responsável ou por quem manipula os dados, que não são anulados pelos interesses ou direitos e liberdades do titular dos dados, e quando o responsável ou operador tiver analisado todas as circunstâncias da operação de transferência de dados ou do conjunto de operações de transferência de dados.

Os projetos de lei de proteção de dados pessoais em discussão no Congresso Nacional têm como ponto comum a previsão de que a transferência internacional de dados pessoais será permitida para países que oferecem nível equivalente ao do Brasil de proteção estabelecido por regulamento. No entanto, o problema que antevemos é a transferência internacional no contexto de um mundo baseado na comunicação entre "coisas", onde será inviável impor limites ao fluxo de dados.

Outra questão relevante é a exigência de consentimento para a transferência internacional de dados, que pode vir a minar a capacidade do Brasil de se beneficiar da Internet das Coisas.

Um exemplo simples seria imaginar a dificuldade de um usuário estrangeiro, que utiliza um dispositivo para monitorar sua informação de saúde, como diabetes, ter seu dispositivo bloqueado simplesmente por estar visitando o Brasil. Seria inexequível para uma empresa monitorar onde seus usuários estão o tempo todo e notificá-los ao entrar em um país com rígidas regras de consentimento ou, até mesmo, interromper o funcionamento do dispositivo enquanto não houver autorização.

Dada a natureza global dos fluxos de dados modernos e atividade econômica, acreditamos que seja importante incluir mecanismo de transferência internacional compatível com o de outras jurisdições e regiões. Desta forma o país terá a possibilidade de gerar, trocar e processar informações com diferentes partes do mundo, criando maior capacidade de análise e desenvolvimento de novos produtos e serviços para o ecossistema de IoT que poderão ser comercializados mundialmente.

Logo, a futura norma sobre privacidade deve buscar o equilíbrio entre os anseios da sociedade e da iniciativa privada, para que não haja prejuízo para

quaisquer das partes ou impactos negativos na economia digital brasileira, em especial, para o desenvolvimento do florescente ecossistema da IoT.

Por fim, é flagrante os inúmeros benefícios que o mundo conectado pode trazer para a sociedade e economia brasileira, sejam nas áreas de saúde, educação, administração pública, entre outros. A variedade de dispositivos e aplicações de IoT vão das cidades inteligentes ("*Smart Cities*"), aos carros conectados, passando ainda pelas casas inteligentes e *Smart Grids* (redes elétricas inteligentes). Para que estes benefícios sejam usufruídos, uma abordagem eficaz para garantir a segurança cibernética demanda o trabalho conjunto entre empresas e o Estado para a elaboração e promoção de melhores práticas voluntárias (incluindo testes de segurança e análise de risco) nas áreas de segurança e privacidade de IoT.

Conjugado com a elaboração destas melhores práticas, entendemos ser mandatório o engajamento do Estado brasileiro na elaboração e edição de uma Política Nacional de Segurança Cibernética, aplicável aos setores público e privado, contendo objetivos e metas claramente estabelecidos, enfatizando a proteção à infraestrutura crítica brasileira, quais sejam, energia, transporte, abastecimento de água, petróleo e gás, comunicações e sistema financeiro. O processo de elaboração desta Política Nacional deverá contar com um amplo debate com a participação de todos os setores da sociedade e sua implementação deverá ser observada atentamente pelo Estado com vistas a garantir sua eficácia.

Busca-se desta forma garantir resiliência cibernética do Brasil, trazendo segurança para o ecossistema de IoT e possibilitando à sociedade brasileira que ingresse totalmente no ecossistema de aplicações de IoT.

9.10 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.

9.11 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?

  Para que o não-confinamento de recursos possa ser adotado em larga escala, auxiliando o desenvolvimento de IoT e impulsionando o processo de inovação no Brasil, mas, ao mesmo tempo, resguardando os direitos individuais dos usuários, a utilização de tais dados deverá ocorrer no contexto do tratamento de dados pessoais em prol do bem-estar social e não em prol de um indivíduo identificável. Fomentando, desta forma, a utilização de mecanismos de anonimização de dados conjugados com a adoção do *Big Data* e do *Data Analytics* que permitam àqueles que tenham acesso a grandes bancos de dados processar estas informações para descaracterizá-las, não infringindo direitos individuais. Assim teremos condições de desenvolver iniciativas tanto no ambiente público quanto privado que nos permitam encontrar respostas que auxiliem em seu desenvolvimento e bem-estar, p.ex., a realização de campanha de vacinação para prevenir o surto de determinada doença em um período específico do ano, pois através dos dados tratados via *Data Analytics* será possível mapear que naquele mesmo período, em anos anteriores, houve um aumento desproporcional da doença.

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

  O compartilhamento de informações e a adoção de padrões abertos que garantam a segurança de dispositivos IoT é uma preocupação constante dos agentes deste mercado. Neste sentido, a adoção de padrões interoperáveis virá como uma iniciativa natural destes agentes para o compartilhamento de informações, sem demandar qualquer ação do Estado que possa vir a ser prejudicial para os processos de desenvolvimento e inovação de IoT.

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

  Entendemos que a definição de padrões e modelos não deve ser feita pelo Estado. Pelo contrário, o Estado deve deixar que o mercado

decida quais padrões e modelos são mais adequados de acordo com os diferentes tipos de produtos e serviços de IoT disponíveis. Caberá ao mercado fazer a "seleção natural" dos mecanismos que garantam maior segurança no ambiente de IoT e, ao mesmo tempo, permitam o não-confinamento de dados.

Entender o mercado de IoT como guia e aquele que detém maior experiência para fazer este tipo de seleção não é incorreto. Devemos recordar que as empresas que atuam neste mercado lidam diariamente com a confiança de seus usuários e são as maiores interessadas para que a credibilidade em relação aos seus produtos e serviços seja garantida.

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

Para que a sociedade possa alcançar o máximo de benefícios do universo de IoT precisamos permitir o maior grau de liberdade possível na utilização destes dados. Contudo, tomando o cuidado para que estes dados sejam sempre que possível anonimizados, afastando-se a possibilidade de utilização de dados de um usuário específico ou identificável.

Importante recordar que a tecnologia é apenas o meio, o recurso para implementação de soluções de IoT. Em geral, a viabilidade tecnológica não é um problema para implementação das soluções, tendo em vista que sensores podem ser desenvolvidos para aplicações inéditas, dados podem ser ou não criptografados, e os acessos a estes dados são por premissa de visualização e consumo controlados.

Isto posto, na hipótese acima de confinamento, é possível que uma câmera possa tanto servir a um monitoramento de cerca geo-espacial virtual (segurança) quanto para leitura de um QRCODE que identificará unicamente um dispositivo colocado à sua frente. A limitação do hardware é relativa, podemos ter, por exemplo, um microcontrolador compartilhando dados de temperatura de um ambiente, mas aberto a ser conectado a outros tipos de sensores sem grandes esforços operacionais. Não obstante, o acesso aos dados pressupõe uma camada de segurança que os exponha apenas a entidades autorizadas a este acesso e, portanto, o consumo destes dados é muito mais submetido à análise do caso de uso específico do que a limitações de uma plataforma de armazenamento por exemplo.

Em outras palavras, o acesso aos dados pode ser autorizado a qualquer um o que vai nortear este acesso e deverá seguir políticas de privacidade, necessidade ou mesmo observação de preceitos éticos e de transparência. Sobre os aspectos de virtuosidade na aplicação dos dados, trata-se de um aspecto muito mais condicionado aos casos de uso desenhados do que ao que eventualmente a tecnologia passivamente seja colocada a viabilizar.

A tecnologia blockchain é um bom exemplo de segurança e compartilhamento de informações na rede com foco na confiança dos

participantes. Com a criação de redes de compartilhamento de informações criptografadas baseadas em blockchain com controles de acesso, abre-se a possibilidade de segurança e confiabilidade caminharem juntas de maneiras sem precedentes.

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

Não podemos cansar de estressar a importância da palavra confiança na relação entre usuários e empresas no ecossistema de IoT. Sendo assim, o usuário deve confiar nos dispositivos existentes e a indústria deve, constantemente, desenvolver novos mecanismos de segurança e zelar pela transparência na relação com este usuário, através da indicação da finalidade para a qual os dados foram coletados e a forma de seu tratamento.

Ademais, para que a indústria consiga gerenciar com êxito esta relação com os usuários, um fator fundamental passa a ser o processo de educação, tanto com a geração de uma massa crítica e qualificada para trabalhar no ecossistema de IoT, quanto através do investimento no processo de educação da sociedade para aprender como incorporar a tecnologia no seu dia-a-dia, estando ciente dos seus benefícios e riscos, habilitando-se de forma adequada para entrar definitivamente na era da economia digital.

Desta forma, é necessário incluir disciplinas obrigatórias de segurança da informação nos currículos de cursos de computação das universidades brasileiras, pois a grande maioria dos engenheiros e cientistas de computação não conhece o mínimo necessário para desenvolvimento de dispositivos e software seguros. Sem essa massa crítica, dispositivos IoT continuarão sendo implementados de maneira insegura e contribuindo para a execução de ataques.

Quanto à sociedade, esta deverá ser conscientizada dos riscos e vantagens de se utilizar dispositivos capazes de coletar informações e influenciar em sua vida cotidiana.

10. Gerenciamento da 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, aprovisionamento e configuração dos dispositivos sensores e atuadores, elementos de rede e infraestrutura computacional, suportando toda a operação.

10.1 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.

O Governo deve concentrar seus esforços na criação do ambiente regulatório moderno, não burocrático, com o objetivo de preservar os direitos e garantias fundamentais dos cidadãos, com interferência mínima nos modelos de negócios de IoT, evitando tornar-se proprietário de infraestrutura de IoT cuja mudança e atualização é muito rápida.

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

Os dispositivos de IoT têm criticidades distintas. Um dispositivo somente de medição ou monitoramento, aplicado em uma variável não crítica e sem possibilidade de atuar sobre qualquer sistema, não demanda nenhum requisito especial além da compatibilidade com a infraestrutura de comunicação. Já um dispositivo capaz de acionar ou desligar sistemas, como iluminação, distribuição de água ou equipamentos, bem como dispositivos que monitoram dados críticos, como tarifação e dados privados, precisam operar em um nível de segurança mínimo para instalação.

10.3 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.

A disseminação de dispositivos conectáveis só será possível se o processo de conexão à infraestrutura de rede for simples, instant-on. Inserção de SIM cards ou necessidade de conexão a um computador para realizar a configuração serão barreiras à disseminação da IoT.

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

10.5 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.

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

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

10.8 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.

Inexistindo problemas relacionados à privacidade e segurança dos cidadãos, eventuais bancos de dados existentes ou a serem gerados com a adoção de soluções de IoT deveriam ser disponibilizados os atores do setor privado para que possam criar produtos, serviços e soluções. Seria uma importante fonte de incentivo à inovação.

10.9 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?

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

Para atender adequadamente as novas demandas de serviço de IoT/M2M, as operadoras precisarão aumentar a densidade da rede usando Small Cells, que por sua vez exigirá uma infraestrutura de rede mais densa, especialmente em áreas urbanas / suburbanas.

As regulamentações devem permitir a expedição de licenças para a construção de infraestrutura de rede, bem como a permissão do acesso a postes públicos, dutos, conduítes, direitos de passagem, e prédios públicos, para permitir uma implantação econômica de redes (multi-serviço) para as verticais do mercado.

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

11.1 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, consequentemente, 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.

Enquanto a indústria ainda busca a convergência em torno de padrões IoT mais específicos, consideramos que a Interoperabilidade não deva ter caráter obrigatório, mas sim muito desejável e muito importante para o sucesso de IoT, devendo ser constantemente perseguida.

A interoperabilidade é proporcionada pela adoção de padrões de indústria que definem uma plataforma comum de comunicação capaz de conectar e gerenciar diferentes tipos de dispositivos, independentemente do seu formato, sistema operacional, vertical, fabricante, provedor de serviços ou país.

Através de padrões, recursos IoT são expostos a outros dispositivos IoT e acessados de maneira homogênea e segura.

O uso de plataforma em Nuvem permite que os micro-serviços ou APIs relativos a cada uma das camadas relacionadas conversem entre si e com outros sistemas.

Não obstante, esta plataforma e cada um dos serviços devem estar em conformidade com aspectos de segurança privacidade (mascaramento de dados, criptografia etc) que garantam que os dados se mantenham seguros e íntegros.

Citamos como exemplos o consórcio Open Connectivity Foundation (OCF) e a sua plataforma de referência open-source IoTivity, assim como a aliança AllSeen e a sua plataforma de referência open-source AllJoin.

Consideramos que o uso de soluções e plataformas open-source, não deva ter caráter obrigatório, mas seu uso é igualmente muito desejável para a rápida disseminação de IoT.

11.2 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.

Ao contrário de ser considerado "overhead", o uso da camada de aplicação tende a ser comum na maioria dos casos de uso, na medida em que proporciona a produtividade e a agilidade para o desenvolvimento de aplicações, entrega o máximo de interoperabilidade em menor prazo possível, suporta as necessidades de múltiplas verticais ou mercados e a escalabilidade necessária para a expansão de redes IoT.

A definição das interfaces de aplicações por padrões devem ser flexíveis de modo a atender tantos a dispositivos IoT mais leves e restritos assim como os mais complexos e "inteligentes".

Importante ainda lembrar que a Lei de Moore avança no sentido de reduzir o custo do poder computacional e comunicações, de modo que mesmo dispositivos pequenos e leves poderão suportar interfaces comuns proporcionadas pela camada de aplicações IoT.

Dentre as facilidades, esta camada deve oferecer serviços de provisionamento e mesmo controle de versionamento próprios a fim de que as soluções tenham um ciclo de desenvolvimento ágil tanto no aspecto de produção de código quanto no aspecto de escalabilidade e rapidez entre testes, homologação e produção.

11.3 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?

Um modelo rígido e excludente não parece fazer sentido. Ao mesmo passo em que iniciativas de código aberto podem facilitar a prática de IoT, já que envolvem baixos investimentos para manutenção de aplicativos e soluções, por outro lado há soluções e aplicativos mais focados em necessidades de negócio específicas, desenvolvidos com fins comerciais, que envolveram investimentos em P&D ou aplicação de conhecimentos das empresas e justificam serem de código fechado.

Mesmo aplicações de código fechado tendem a ser comercializados e disponibilizados em modelo de serviços (pague por uso) o que envolve investimentos significantemente mais baixos que os modelos por licenciamento. O mesmo pode ocorrer com aplicações em código aberto.

Em suma, um modelo híbrido entre códigos aberto e fechado parece atender de modo muito mais compreensivo as demandas do mercado, assegurando competitividade e liberdade de modelo de negócios, assim como acontece no mercado atual de IT.

11.4 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?

As funcionalidades IoT não devem estar ligadas a soluções, mas sim à convergência de padrões na indústria, de modo a evitar a fragmentação em nichos isolados em indústrias específicas, que não podem se comunicar facilmente.

Atualmente podemos observar convergência em IoT em torno de OCF (Open Connectivity Foundation) que reune trabalhos de diferentes consórcios: OIC (Open Interconnect Consortium), UPnP (Universal Plug and Play) e AllSeen Alliance.
Não necessariamente todas as funcionalidades deveriam ser providas por uma única solução porque isto potencialmente inviabilizaria integração com sistemas importantes legados de alguns consumidores de IoT.
A abordagem mais racional seria o provisionamento de ferramentas de integração que viabilizem a interoperabilidade das aplicações. Estas mesmas ferramentas de integração seriam a solução a endereçar a interoperabilidade das soluções fora de uma camada de suporte.

11.5 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?

Esta nuvem será pública, privada ou mista de acordo com as necessidades específicas de cada consumidor das soluções. Ainda há setores, como o bancário por exemplo, que relutam em migração de todas as suas soluções, ou ao menos as mais críticas, para nuvens públicas. No entanto, algumas indústrias já se mostram muito mais flexíveis aos modelos públicos e adotam este formado sem qualquer receio. As soluções que com efeito apresentam dificuldades de migração para nuvens públicas em geral não se referem a casos de IoT. Soluções IoT têm como premissa fácil escalabilidade e rápido provisionamento, condições melhor atendidas por nuvens públicas. Em relação a ofertas de Infraestrutura, Plataformas e Software como serviço sim, no Brasil já há presença sólida de empresas que provêm estas ofertas com capacidade de atender tal demanda uma vez que em geral são empresas que cobrem a mesma demanda em nível global.

11.6 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.

Técnicas de Inteligência Artificial tais como Machine Learning e Deep Learning poderão potencializar a utilização de aplicações IoT, considerando a quantidade de informação gerada por IoT e a capacidade dessas técnicas de IA reconhecerem padrões existentes e aprenderem novos padrões.
Um exemplo é o uso de assistentes inteligentes ao usuário em dispositivos e redes IoT, capazes de a tornar a interface com usuários mais natural e produtiva.
Tal qual mencionada nos ítens anteriores, a presença de uma camada ou plataforma que permita rápida e fácil integração entre APIs e aplicações é importante para desenvolvimento de soluções de IoT. Isto posto, Machine Learning também deve ser encarado como um serviço a ser disponibilizado nos mesmos moldes, melhor cenário em nuvem, para que se concretize sua integração com, por exemplo, serviços também em nuvem e na mesma camada

de BigData, Analíticos etc. Um exemplo poderia ser uma camada que contenha um micro-serviço que facilite conectividade com sensores (mensageria, segurança e armazenamento embutidos) e que possa se integrar com um serviço de armazenamento de dados que possa estar também facilmente conectado com um serviço de machine learning que provenha resultados baseados nestes dados captados e armazenados.

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

Técnicas de Inteligência Artificial tais como Machine Learning e Deep Learning têm grande sinergia com IoT, e oferecem grandes oportunidades no Brasil, na indústria de desenvolvimento de Software para soluções de problemas locais e específicos.

A presença de uma solução que possa aumentar a eficácia na tomada de decisões a partir de dados coletados por sensores é atrativa.

Podemos citar os seguintes casos de uso:

- Aprendizado sobre o comportamento de hábitos do usuário e ajuste de um sistema ou dispositivo em resposta a essa aprendizagem. Exemplo: Análise do consumo de energia em casa, bairro, cidade, e ajuste na demanda de energia na grid;
- Previsão e antecipação de eventos. Exemplos: Indústria 4.0: auxiliar a indústria a não somente predizerem falhas em equipamentos como também com antecedência já decidirem pela melhor abordagem para tratamento desta falha; Análise das informações de voos de um avião e previsão antecipada de falhas de um elemento do avião.

11.8 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?

Computação Cognitiva incluindo Big Data e Data Analytics é sem dúvidas outra área a se prestar atenção. A replicação do modo de pensar humano em modelos computacionais permite um nível de sofisticação em soluçÕes de IoT onde, por exemplo, ao invés de se instalar um sensor de temperatura em uma caldeira com algum gatilho de alarme estabelecido para superaquecimento, simplesmente pode-se lançar mão de uma solução cognitiva à qual você tenha apenas de solicitar que mantenha a caldeira em seu melhor nível de eficiência e ela será capaz de tratar alarmes e ações de modo autônomo. Hoje a dificuldade reside em se encontrar empresas que já possuam soluções cognitivas maduras e já estabelecidadas no modelo de plataforma (e nuvem) para que possam ser acopladas nativamente a outros serviços, incluindo serviços IoT de mensageria etc como já mencionado.

11.9 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.

Novamente, a camada de suporte deve ser abrangente o suficiente para contemplar serviços e APIs de analytics que possam facilmente se conectar aos

demais serviços. Voltando-se à questão 1, dentro deste ecossistema de IoT os dados necessitam de soluções analíticas para que seja criado valor e complexidade de integração da camada analítica com as demais passa a virtualmente inviabilizar a criação de soluções. Um caso de uso poderia ser o monitoramento de um equipamento, coleta de telemetria acerca de variáveis que sejam importantes para por exemplo, a partir de uma solução analítica e dados históricos, se poder prever uma eventual falha de funcionamento. Se a sensorização do equipamento não for facilmente integrada com a coleta e armazenamento de dados bem como a capacidade analítica para a solução, a solução final se torna desprovida de valor.

11.10 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.

A camada de suporte deve apresentar um serviço/API que permita que estes dados de local e tempo possam trafegar dentro do mesmo protocolo de envio de dados de telemetria ou afins. Não obstante, o formato do pacote de dados a trafegar por este protocolo também deve ser flexível o suficiente para que a carga destes dados não seja grande (IoT demanda pacotes leves para envio de dados) e para que a interpretação de todos os dados enviados possa ser a mesma.

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

É primordial que este suporte e o desenvolvimento de aplicações sejam estabelecidos em ambiente e plataformas seguras. Neste sentido este serviço ou implementação de aspecto de segurança, desde a conectividade até o analítico, deve ser nativo às camadas de suporte. Além disto é fundamental manter a interoperabilidade com padrões de mercado.

12. 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.

12.1 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).

O desenvolvimento da tecnologia possui ciclo natural e melhorias são incorporadas em função de novas demandas e da penetração no mercado. O contexto de IoT demandará qualidade de transmissão, confiabilidade e aspectos de segurança cada vez mais críticos. Entende-se que as tecnologias de conectividade existentes e as redes disponíveis atualmente possuem capacidade para atender as demandas específicas de IoT. Essa evolução será natural. As tecnologias que não atenderem os requisitos de IoT serão rapidamente descartadas.

Arquiteturas de solução e padrões IoT bem definidos devem incluir uma camada de Abstração da Conectividade, capaz de gerenciar a conexão segura ponto a ponto, identificação, aprovisionamento, atualização de software, diagnóstico, gerenciamento entre os diferentes recursos e dispositivos IoT, independentemente dos protocolos de acesso utilizados na camada inferior de Hardware, sejam eles Ethernet, Wifi, Bluetooth, Zigbee, GSM, 3G, LTE, RFID, etc.

Os padrões de acesso existentes têm evoluído rapidamente, com novas versões de WiFi e Bluetooth sendo adaptadas às necessidades de IoT, chegando ao mercado com maior alcance, velocidade e volume de dados, de modo que não vemos a necessidade de desenvolvimento de novos padrões de acesso para necessidades específicas de IoT.

O Brasil deve adotar uma postura de total alinhamento tecnológico a ecossistemas globais no que tange tecnologias e padrões de acesso. Há hoje uma grande quantidade de tecnologias disponíveis nos domínios de PAN, LAN e WAN e a aplicabilidade de cada uma delas determinará quais prevalecerão e quais serão eventualmente eclipsadas por outras.

O Brasil tem uma grande oportunidade em inovação, criando dispositivos, aplicações e plataformas para a Internet das Coisas, que podem ser alavancadas através do emprego de tecnologias comerciais harmonizadas globalmente, com escala, padronização e interoperabilidade

12.2 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?

O 5G se mostra como o principal domínio tecnológico para suportar IoT no futuro, bem como uma plataforma de inovação e criação de serviços future proof. O 5G terá um papel habilitador e acelerador de IoT, ainda que a realidade de IoT seja agora e a introdução do 5G no país deva ocorrer a partir de 2020.

As tecnologias com mais potencial são aquelas com base em LPWAN (NB-IoT, LTE Cat-0, Cat-1, Cat-M em faixa licenciada, e tecnologias proprietárias em alguns nichos de mercado) com aplicações em algumas verticais. Também se menciona as tecnologias de curto alcance para uso doméstico com padrões IEEE, para as quais é necessário utilizar mais banda não licenciada (p.ex 5 GHz) com maior quantidade de espectro, assim como o surgimento de novas tecnologias WLAN (LTE-U e LAA) que complementam as coberturas outdoor. Destaca-se a viabilização do uso de femtocells para aumentar a penetração de cobertura.

Além disso, a Internet das Coisas será de natureza heterogênea, com outras tecnologias de acesso de nicho compondo um ecossistema de vasto, uma vez que toca aplicações e dispositivos muito diferentes entre si, com os mais diversos requisitos de qualidade de serviço.

Além disso, a capacidade instalada em conexões fixas é fundamenta para o desenvolvimento da camada de conectividade. A expansão de capilaridade e capacidade da última milha – banda larga - junto com a camada de agregação e transporte e interconexão são pilares fundamentais para suportar a imensa demanda de IoT.

12.3 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).

Independentemente da interoperabilidade, que se torna mais complexa à medida que novos padrões forem surgindo, entende-se que é muito importante o desenvolvimento de novos padrões para atender a missão crítica e o massivo. A tecnologia 5G possui características para atender essas demandas. Para tal, destaca-se a importância de novas faixas de espectro para 5G.

O Brasil deve adotar uma postura de total alinhamento tecnológico a ecossistemas globais no que tange tecnologias no core da rede. De maneira complementar ao que acontece no acesso, as arquiteturas de evolução de core são definidas em fóruns e grupos e trabalho internacionais, assegurando escala, padronização e interoperabilidade.

12.4 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?

As tecnologias de core mais interessantes são aquelas que sejam dinâmicas e que permitam inteligência tais como SDN (Software Defined Networks com capacidades avançadas de segurança, gerenciamento e virtualização e engenharia de tráfego) e NFV (Network Function Virtualization, que ajudam a reduzir os custos de hardware em datacenters e fornecem agilidade de tempo de implantação de soluções). Além disso estão sendo consideradas nos planos de adoção de 5G, especialmente para suportar um dos principais focos da tecnologia, o. Massive Machine Type Communications. Os desafios estão nos custos de licenças para adoção de funcionalidades.

12.5 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).

Os protocolos para IoT operam nas diferentes camadas OSI e são desenvolvidos pelo IETF, IEEE, ITU e outros organismos, visando atender necessidades atuais e futuras de IoT. Para cada camada há disponível um conjunto de protocolos com diversas características para atender diferentes tipos de aplicações, conforme largura de banda, nível de transmissão, alcance, confiabilidade, necessidade de transmissão em tempo real e tipo de consumo de energia. Também a topologia da rede, a quantidade de nós, tipo de ambiente indoor ou outdoor são critérios que definem as soluções.

Além disso, os protocolos de gerência IoT permitem a comunicação heterogênea entre camadas de enlaces distintas, e exercem um papel relevante em IoT devido à diversidade de protocolos e padrões em todas as camadas. A necessidade de comunicação heterogênea e amigável entre diferentes protocolos na mesma ou por diferentes camadas é crítica para aplicações IoT.

O aspecto de segurança deve ser atendido em todas as camadas, e os protocolos devem oferecer modos de tratamento. Ou então, quando não houver esse mecanismo embutido, é necessário verificar abordagens para atender esse requisito.

Por outro lado, a aplicação pode oferecer um nível adicional de segurança usando TLS ou SSL como protocolo de transporte. Além disso, autenticação fim a fim e algoritmos de encriptação podem ser usados para lidar com diferentes níveis de segurança, conforme requisitado. Ressalta-se que as abordagens de segurança estão sempre em evolução para atender os aspectos dos dispositivos IoT.

Da mesma maneira, o Brasil deve adotar uma postura de total alinhamento tecnológico a ecossistemas globais no que tange tecnologias no core da rede. No que se refere a protocolos, o Brasil pode e deve participar de fóruns internacionais, colaborando na definição e construção de protocolos

harmonizados globalmente. Só assim podemos contar com a interoperabilidade que existe na Internet atual também na IoT.

Por fim, os desafios que surgem com a criticidade das aplicações e a evolução das demandas, que são aspectos de mobilidade, confiabilidade, escalabilidade, gerência, disponibilidade e interoperabilidade, são indutores naturais da evolução dos padrões e seus protocolos, ou, quando necessário, estimulam a criação e desenvolvimento de novos padrões para atender as demandas mencionadas.

12.6 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?

Na camada de transporte, TCP para aplicações gerais e UDP para aplicações massivas e de broadcast de mídia

Na camada de rede, IPv4 para compatibilidade com redes legadas e para PANs e LANs e IPv6 para WANs e aplicações gerais

Na camada de enlace e física deve ser alinhado à tecnologia de acesso (ethernet, WiFi, LTE, etc)

12.7 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?

A IoT irá certamente impactar o core da rede, quando se considera que bilhões de dispositivos estarão conectados. A tecnologia 5G já contempla implantações do tipo Massive Machine Type Communications, como caso de uso na sua padronização. Mas o uso massivo de dispositivos não impactará somente o core da rede, mas também o uso do espectro, que também deve acompanhar o mesmo crescimento. Nesse sentido, deve-se pensar em grandes quantidades de espectro para este tipo de comunicação, tanto abaixo de 6 GHz como acima de 6 GHz (Faixas da Res. 238 do WRC-19 e outras como 28 GHz e 31-33 GHz).

Independente dos cenários de uso do chamado Enhanced Mobile Broadband, ou seja, aplicações que demandarão mais banda (como vídeos de ultra alta definição), a IoT certamente irá impactar o core das redes atuais, tanto do ponto de vista de demandar muito mais espectro, como do ponto de vista da arquitetura das redes. Em razão da grande quantidade de dispositivos a serem conectados ao mesmo tempo (pelo menos 1 milhão de dispositivos por km2, de acordo com os requisitos para IMT-2020 descritos no anexo 5.8 do mais recente relatório do Chairman do WP5D da UIT-R, doc. 5D/374), quantidade significativa de espectro será exigida para acomodá-los e com uma qualidade de serviço adequada. Em relação a topologia das redes móveis de quinta geração (5G), algumas das mudanças e novos conceitos que estão sendo discutidos em âmbito da 3GPP podem ser aplicadas, embora não

exclusivamente, a IoT: SCEF (Service Capability Exposure Function), que permite abrir algumas das funcionalidades do core da rede através de APIs voltadas a terceiros, aumentando ainda mais as possibilidades de aplicações IoT; GENCEF (Group based enhancements in the network capability exposure functions), controle de sinalização em grupo para reduzir a necessidade de recursos de sinalização; Network slicing, que consiste na separação em múltiplos "cores" de redes lógicos. Estes são temas são apenas alguns tópicos atualmente em discussão e em vias de padronização, e que irão, portanto, impactar tanto a IoT, como as redes da próxima geração.

Com o aumento do número de dispositivos e do volume e da heterogeneidade do tráfego gerado e endereçado a dispositivos IoT, uma nova arquitetura de core se tornará o padrão em redes convergentes. A virtualização de funções de rede, incluindo gerência, suporte, operação, banco de dados, sinalização, aplicações e roteamento é um evolução que já está em andamento, com arquiteturas baseadas em cloud.

Neste novo paradigma de core de fixas e móveis, funções das mais diferentes naturezas são virtualizadas em hardware multi-purpose e orquestradas dinamicamente, assegurando capacidade de conexões simultâneas, volume de sinalização e tráfego.

Na arquitetura 5G, a evolução do core das redes atais, composto por Packet Core, HLR/HSS, IMS, PCRF e tantas outras plataformas, além de OSS/BSS, dará lugar a uma camada horizontal de virtualização chamada SDI – Software Defined Infrastructure. É dentro do conceito de SDI que serão construídas por software as funções de rede, permitindo-se assim o Network Slicing, onde diferentes tipos de serviço são instanciados e orquestrados simultaneamente, seja para atender a um alto volume de tráfego de dispositivos como câmeras de alta definição, para um grande número de dispositivos (IoT Massivo) ou para aplicações com alta prioridade e baixa latência (IoT para missão crítica)

12.8 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 servem 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?

O principal desafio dessas tecnologias é que sejam transparentes ao usuário final, de forma que os dispositivos IoT entrantes numa rede de acesso sejam do tipo "plug and play", onde haja mínima ou nenhuma intervenção do usuário final. Também considera-se que permitam a localização geográfica dos dispositivo por meio de tecnologias como GPS, iBeacons, LBE, QR Codes, NFC ou LBS.

O fato de ser "plug and play" traz grandes desafios ao provedor de serviços, desde o ponto de vista de ativação do dispositivo até o processo de seu monitoramento.

No Brasil há possibilidade de desenvolvimento com intervenção de protocolos que permitam atender estes dois objetivos ("plug and play" e localização), empregando engenharia de serviços e suporte com resposta rápida.

Quanto a equipamentos de rede, entende-se que há espaço para a indústria nacional, para área de programação/software de camadas de serviço superiores, além da camada de acesso físico. Na área de desenvolvimento, cita-se algoritmos de roteamento e sistemas de gerência que permitam identificação de dispositivos em uma região.

Outros desafios a serem mencionados em IoT é a disponibilidade dos dados, pois além do que já se dispõe para redes banda larga (taxa de transmissão, latência, jitter e perda de pacotes), para IoT será fundamental a baixa latência, confiabilidade e disponibilidade do dado, a serem atendidos em requisitos de desempenho. Tais requisitos deverão ser suportados pelas tecnologias 5G em desenvolvimento. Estes itens são incrementados quando do uso de faixa licenciada na interface macro-célula ou em redes WMAN, ou ainda podem ser controlados com engenharia em redes WLAN para faixa não licenciada.

As tecnologias para acesso sem fio se agrupam em 3 distintos grupos:

1. PAN: Personal Area Network – redes de curtíssimo alcance, tipicamente alta velocidade de transferências de dados e aplicações dentro de um domínio: wearables, office space, car. Por exemplo: Bluetooth, NFC
2. LAN: Local Area Network – tecnologias para redes locais, de curto alcance, como uma casa, um escritório ou centro comercial. Exemplos: WiFi, ZigBee
3. WAN: Wide Area Network – tecnologias para redes de grande alcance, celulares e com cobertura cidades ou países.

a. Não licenciadas: tecnologias de nicho, proprietárias, com baixa capacidade e não padronizadas, operando em frequência não licenciada, como SigFox e LoRa
b. Licenciadas, genéricas: redes móveis baseadas em tecnologia padronizada, harmonizada globalmente e interoperável, de alta capacidade e confiabilidade, como GSM (2G), WCDMA (3G) e LTE (4G)
c. Licenciadas, específicas: também de tecnologia padronizada assim como (b) porém usando implementações específicas para IoT visando aumentar a capacidade de dispositivos, melhorar cobertura, diminuir consumo de bateria e aumentar a eficiência espectral e uso de bandas 3GPP disponíveis, como EC-GSM, LTE-M e NB-IoT

O grupo 3(b) é extremamente relevante, por constituir o principal meio de acesso a ser desenvolvido de maneira robusta para aplicações de Internet das Coisas. Três principais tecnologias se destacam:

1. EC-GSM: implementação do padrão GSM onde parâmetro de tempo, sensibilidade e tráfego são ajustados permitindo que a mesma potência ofereça maior raio de cobertura para dispositivos IoT na transmissão de dados sobres redes 2G. Essa tecnologia pode ser ativada por software sobre redes GSM existentes que cobrem quase a totalidade da população brasileira, e por usar padrão GSM o custo do dispositivo é bastante reduzido se comparado a tecnologias mais sofisticadas como o 4G. O consumo de bateria também é bastante reduzido.

2. LTE-M: implementação do LTE usando canais que ocupam 1.4MHz de espectro, portanto muito mais estreitos que as portadoras usadas tradicionalmente de 10MHz ou 20MHz. Isso permite melhor adequação a diferentes larguras de canal que eventualmente já estejam disponíveis para operadoras móveis, sobretudo em frequências baixas e de uso por tecnologias legadas. 450MHz, 800MHz, 850MHz, 900MHz são algumas faixas nas quais se pode aumentar o fator de ocupação ('spectrum depth') ao usar canais menores, dedicados a IoT. A grande vantagem é de usar a interface aérea de LTE, que tem eficiência espectral bastante superior àquela do GSM.
3. NB-IoT: de maneira semelhante ao LTE-M, o NB-IoT também é uma implementação particular do LTE, que faz uso de canais ainda mais reduzidos ocupando 200kHz, o mesmo que uma portadora GSM. Pode ser intercalado com portadoras GSM usando os mesmos rádios multi-tecnolgia, ou ainda ser sobreposta a portadoras LTE em operação, já que a interferência co-canal produzida vai ser rejeitada pelo LTE não usando os Resource Blocks mapeados para a sub-portadora OFDMA interferida.

12.9 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?

As aplicações IoT/M2M estão surgindo sobre diferentes alternativas tecnológicas. Entre todas, as redes celulares oferecem o maior potencial de adoção maciça de serviços IoT/M2M, devido à sua cobertura nacional e implantações onipresentes, facilidade de atualização para lidar com muitos casos de uso potenciais de IoT/M2M com curto tempo de entrega para o mercado e alta qualidade de serviço. Além disso, as recentes tecnologias 3GPP, tais como, Band-IoT (NB-IoT), Cat-M1 e Extended Coverage-GSM-IoT (EC-GSM IoT), já suportam diferentes casos de uso de IoT e o futuro padrão 5G suportará casos de uso avançados de IoT.

O espectro não licenciado pode ser adequado em alguns casos específicos, como por exemplo, de uso indoor, no entanto, limitar as aplicações de IoT a este espectro não seria apropriado, já que comprometeria severamente o potencial de desenvolvimento de IoT no Brasil.

Naturalmente, há aplicações e uso para os dois tipos de espectro, nos quais já ocorre operação conjunta das múltiplas tecnologias, visando oferecer soluções para vários cenários. Exemplos: uma operadora celular (LTE) em cobertura outdoor que se comunica com small cells (LTE-U/LAA), ou operador celular LTE que faz uso de rede Wi-Fi através agregação de enlace (LWA). Na banda não licenciada de 5GHz tem sido possível obter coexistência dessas tecnologias.

Nesse contexto, o governo brasileiro deve alocar espectro suficiente para a expansão dos serviços 4G atuais, bem como planejar novas bandas de espectro necessárias para a introdução inicial de serviços 5G até 2020 ou antes1, 2. A disponibilidade oportuna, global ou regional, de quantidades suficientes de espectro harmonizado em bandas de baixo e alto espectro é importante para a introdução inicial de serviços de IoT/M2M e para seu posterior crescimento. Nenhuma banda única fornecerá uma solução completa para os requisitos de 5G IoT. Portanto, o espectro será necessário em faixas de banda baixa, média e alta frequências. O espectro licenciado para operadoras através de leilões de espectro continuará a ser o modelo que oferece previsibilidade para investimentos comerciais e assegura qualidade de serviço adequada. Dedicar espectro para serviços específicos de IoT/M2M deve ser evitado tanto quanto possível, a fim de assegurar o desenvolvimento saudável do ecossistema e evitar a fragmentação do mercado. O governo deve facilitar frequências de espectro para os testes do 5G, bem como, apoiar pesquisas na padronização do 5G.

Em particular, o governo brasileiro deve considerar a alocação de novas faixas de espectro identificadas na recente Conferência Mundial de Radiocomunicações IT-R 2015 (WRC-15), incluindo a banda C (3,4-3,6 GHz), banda L (1,427-1,518 MHz) e 614-698 MHz. Além disso, considerar as faixas de 3,3-3,4 GHz e 3,6-3,7 GHz, que foram identificadas por outros países vizinhos na América Latina, e assignar faixas já identificadas em Conferências Mundiais de Radiocomunicações, como a de 2,3 GHz.

Além disso, o governo brasileiro pode considerar novas faixas de espectro atualmente em estudo para a próxima Conferência Mundial de Radiocomunicações UIT-R 2019 (WRC-19) na faixa de 24,25 a 86 GHz, incluindo blocos de espectro 24,25-27,5 GHz, 31,8-33,4 GHz, 37,0-43,5 GHz, 45,5-50,2 GHz, 50,4-52,6 GHz, 66-76 GHz e 81-86 GHz.

Em alinhamento com outras nações líderes, o governo brasileiro pode considerar a possibilidade de designar novas bandas para os serviços 5G antes da ITU-R WRC-19, em particular, as bandas de 26 e 28 GHz, que estão sendo apoiadas pelos governos do Japão, Coréia, Europa e EUA.

Além disso, será necessário um espectro adicional para o backhaul de micro-ondas para fazer face à evolução dos serviços 4G e 5G; particularmente para novas faixas, como a banda V (57-66 GHz) e a banda E (71-76 / 81-86 GHz), prioritárias para backhaul de micro-ondas na região da América Latina.

O preço do espectro por MHz deve ser mantido o mais razoável possível de acordo com a situação econômica local, para permitir grandes investimentos de capital necessários para uma introdução bem-sucedida dos serviços de IoT.

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

A Introdução do 5G nas redes móveis, tanto em frequências novas como evolução da cobertura atual é um passo importante para a maturidade de IoT. O 5G será um grande habilitador de casos de uso como por exemplo aplicações de missão crítica que requerem altíssima prioridade, confiabilidade,

segurança e latência reduzida a 1ms ou menos. Será também um grande acelerador para aplicações massivas e de alta demanda de tráfego, permitindo volume de dados, performance e quantidade de dispositivos conectados ordens de grandeza maiores que as atuais com redes até quarta geração.

As redes de quinta geração (5G) vão se constituir na principal plataforma das aplicações IoT, promovendo o desenvolvimento destas em toda a sua potencialidade. As redes de comunicações móveis hoje existentes não foram projetadas para suportar o aumento de dispositivos conectados previstos para os próximos anos.

1. mMTC: um dos requisitos mínimos de performance definidos pela recomendação M.2083 da UIT-R e atualmente em progresso (Anexo 5.8 do mais recente relatório, 5D/374, do Chairman do WP5D) para as tecnologias de interface de rádio candidatas para o IMT-2020 (5G) é a densidade de conexão, que consiste no número total de dispositivos capazes de prover uma qualidade de serviço específica por unidade de área (por km2). Para definir esta densidade de conexão considera-se largura de banda mínima capaz de entregar mensagens de tamanho específico em determinado tempo e com determinada probabilidade de sucesso. Este requisito foi proposto neste documento da ITU-R para o cenário definido como mMTC (Massive Machine Type Communications). O mínimo requisito para densidade de conexão é de 1 milhão de dispositivos por km2. Como exemplo cita-se medidores da área de utilities (energia, água, gás) operados por bateria. Esses medidores operam tipicamente com baixas taxas de dados, enviando mensagens curtas e intermitentes, mas requerem baterias de longa duração para funcionamento por anos, e também são capazes de serem atendidos por cobertura, uma vez que muitos são instalados no interior de prédios
2. LLC: "Ultra-Reliable and Low Latency Communications", o qual não apenas irá incluir IoT, mas também irá garantir a segurança dos usuários envolvidos, como por exemplo dos veículos/carros autônomos. Nestes cenários, a confiabilidade (probabilidade de sucesso de transmissão com baixa latência) da transmissão entre os veículos vizinhos, ou entre um veículo/carro e a infraestrutura rodoviária ao seu redor, e o suporte a alta mobilidade serão também fatores chaves. Baseado nos últimos requisitos em desenvolvimento, o 5G vai garantir uma comunicação extremamente confiável (pelo menos 1-10-5 de probabilidade de sucesso de transmissão) e baixa latência (de até 1ms) em veículos com velocidades de até 500km/h. Considerando todas estas características juntas, o 5G irá resultar em redes móveis robustas que darão conta de todo esse tráfego e de todos estes cenários. Como exemplo, automação de processo industrial ou comando e controle de drones, o que requer latências melhores que dezenas de milissegundos disponíveis atualmente
3. eMBB: oferecer altas taxa de dados para oferecer mais capacidade para crescente demandas de vídeo e melhorar experiência do usuário. Assim, as características do 5G para atender as novas demandas serão a melhoria do throughput (ondas milimétricas acima de 24GHz), uso de antenas inteligentes MIMO, ampla cobertura (para locais indoor),

forte segurança (aplicações de saúde, governo e sistema financeiro), alta confiabilidade (1 pacote perdido em 100 milhões), baixa latência (tipicamente 1 milissegundo), mobilidade sem falhas, banda larga extrema (multi Gpbs), grande capacidade (ex vídeo 4K UHD), alta densidade de "coisas" e baixo consumo de energia (baterias com vida útil de 10 anos ou mais).

O 5G terá operação em diversas faixas de frequência, oferecendo suporte a dispositivos IoT massivos em faixas abaixo de 1GHz (grandes distâncias), baixa latência para a faixa entre 1 e 6GHz (mais largura de banda e missão crítica), e operação em faixa acima de 24GHz (ondas milimétricas) com ampla largura de banda, oferecendo comunicação entre redes de forma transparente para o usuário. O item 1.13 da CMR-19 (Conferência Mundial de Radiocomunicação de 2019) da UIT-R objetiva a identificação de faixas de frequência relacionadas a 5G (IMT-2020) e será capaz de prover escalabilidade com maiores larguras de banda no médio e longo prazo.

Finalmente, o 5G será um elemento fundamental na aceleração da Internet das Coisas. Vale ressaltar no entanto que IoT já é uma realidade hoje, fazendo uso de tecnologias móveis (GSM, WCDMA, LTE, LTE-A) e outras, incluindo de curto alcance e não licenciadas. O 5G é será realidade comercial a partir de 2020. Assim, há uma série de evoluções das tecnologias móveis atuais que terão um papel fundamental na habilitação e aceleração de casos de uso para IoT – EC-GSM, LTE-M e NB-IoT. Estas tecnologias criam o caminho de evolução das redes atuais para o 5G.

12.11 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.

Com o aumento exponencial de dispositivos conectados, IPv6 será o protocolo de endereçamento de-facto da Internet das Coisas. IPv6 já é uma realidade em redes públicas e privadas e será fundamental para habilitar bilhões de dispositivos conectados a redes heterogêneas.

Ainda que possamos definir casos de uso onde diferentes dispositivos possam estar conectados a redes locais com IP privado – como uma casa ou um carro conectado – onde um gateway representa o ponto de agregação e portando o endereço público – é importante fatorar que um grande volume de conexões de dispositivos se dará por redes móveis, sem passar por gateways locais, fazendo, portanto, uso de endereços IPv6 públicos.

12.12 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?

Considerando que o desenvolvimento de tecnologias IoT permitirá conectar bilhões de dispositivos à rede até o ano 2020, com consequências para quase todos os aspectos da vida cotidiana, estamos agora enfrentando o desafio de

atender aos requisitos de padronização de muitos sistemas verticais Indústrias que aplicam as TIC como tecnologias habilitadoras.

Isto se manifesta, principalmente, no campo da IoT, onde algumas plataformas IoT estão sendo desenvolvidas de forma independente, de acordo com as necessidades específicas de cada setor. Estas divergências no desenvolvimento e implantação de IoT pressionaram as partes interessadas para se reunirem para mitigar o risco de "silos" de dados emergentes em diferentes indústrias.

Neste sentido, é necessário trabalhar em coordenação com os organismos de normalização internacionais e regionais (por exemplo, ITU-T, 3GPP) e outras organizações relacionadas para integrar melhores frameworks de normalização, cobrindo uma ampla variedade de aplicações com diferentes objetivos e requisitos.

A fim de construir um diagnóstico abrangente dos desafios e oportunidades da IoT no Brasil em relação às questões de padronização, consideramos que a Câmara IoT deve levar em consideração os fóruns da indústria e os projetos de parceria das organizações de desenvolvimento de normas que estão desenvolvendo especificações técnicas para IoT visando reduzir o tempo e o custo para implementar IoT com benefícios em termos de economias de escala. Isso deve encorajar a cooperação entre as agências relevantes, a fim de aumentar o desenvolvimento de normas internacionais de telecomunicações que facilitem e garantam a interoperabilidade dos serviços de IoT.

Além disso, deve ser levado em consideração o trabalho realizado pela UIT-T e sua Comissão de Estudo 201, que é responsável pelos estudos e trabalhos de padronização relacionados com IoT e suas aplicações, incluindo cidades inteligentes e comunidades. É importante mencionar, por exemplo, a Recomendação UIT-T Y.4000 / Y.2060 sobre a visão geral da IoT, que define a IoT como "uma infraestrutura global para a sociedade da informação, permitindo serviços avançados através da interconexão (física e virtual) baseadas em tecnologias existentes e em evolução de informação e comunicação interoperáveis "; e a Recomendação UIT-T Y.4702, sobre requisitos e capacidades comuns de gestão de dispositivos no IoT, que estabelece requisitos comuns e capacidades de gestão de dispositivos no IoT para diferentes cenários de aplicação.

Além disso, seria desejável considerar o trabalho da Comissão de Estudos 13 da UIT-T: Redes futuras, incluindo computação em nuvem, redes móveis e de próxima geração, especialmente as atividades relacionadas com a padronização de tecnologias 5G emergentes e como interagirão em redes futuras para apoiar o desenvolvimento de sistemas 5G.

Por último, tendo em conta que os endereços IP são recursos fundamentais que são essenciais para o desenvolvimento futuro das redes TIC baseadas em IP, é essencial promover a consciencialização da importância da implantação do IPv6 e da sua vantagem sobre IPv4 considerando o IoT, dado a demanda substancial por endereços IP para dispositivos IoT.

Consequentemente, a administração do Brasil deve considerar garantir que equipamentos de rede, equipamentos de computação e software recém-implantados tenham capacidade IPv6, conforme apropriado. Deverá facilitar as atividades de treinamento conjuntas, envolvendo peritos competentes das entidades relevantes, a fim de fornecer informações, incluindo roteiros e orientações, e prestar assistência no estabelecimento contínuo do IPv6 no país, em colaboração com as organizações pertinentes.

Ref. 1: ITU-T SG20: IoT and its applications including smart cities and communities

13. 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.

13.1 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?

No momento as tecnologias estão mais maduras que o próprio mercado. Esforço deve ser aplicado para identificar as oportunidades de mercado (problemas a serem resolvidos) e formatar a solução tecnológica dos produtos e serviços a oferecer. Há pleno espaço para empresas nacionais competirem globalmente.

Para os gateways as oportunidades estão no desenvolvimento de software embarcado nestes dispositivos que permitam segurança, monitoramento e melhor aproveitamento dos dispositivos utilizados numa área de cobertura. No Brasil é possível desenvolver, verificar e certificar/homologar este software/middleware como sendo seguro para o usuário. O Inmetro é o organismo que pode estabelecer os procedimentos de teste, assim como no caso de medidores inteligentes de energia elétrica.

13.2 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?

SoC (System on a Chip) é uma solução com potencial para IoT, já que une o elemento de processamento com outros, como memória e rádio, em um mesmo chip. Outra solução é o SDR (Software Defined Radio) que pode incorporar diversos protocolos em um mesmo rádio, definindo as características desse rádio por meio de software, como, por exemplo, utilizar Thread ou ZigBee(*) no mesmo rádio 802.11(redes Wi-Fi.
Não existe a necessidade de desenvolver soluções em âmbito nacional. O mercado já pode ser atendido com a tecnologia atual.
(*) ZigBee: conjunto de especificações para a comunicação sem-fio entre dispositivos eletrônicos, com ênfase na baixa potência de operação, na baixa taxa de transmissão de dados e no baixo custo de implementação. Não vemos espaço para desenvolvimento nacional de novas arquiteturas de processadores. As empresas nacionais devem focar nos dispositivos e aplicações de IoT, onde há maior valor e onde temos recursos humanos em abundância.

13.3 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?

As baterias químicas de lítio, alcalina, chumbo-ácido, níquel-cádmio apresentam características de peso, recarga e preço que atendem inúmeros produtos, mas as novas demandas estão levando a tecnologia de baterias para outro patamar, buscando novos materiais e modos de operação. Algumas tendências tecnológicas são a recarga rápida (p. ex 7 minutos com bateria superiônica), de recarga típica de uma vez por semana para celulares (bateria de aço inoxidável), busca de novos metais e substâncias como íon sódico e substrato de cobre e novos tipos como baterias de estado sólido que substituem lítio líquido por grafite. Outras tendências são a obtenção de energia a partir do movimento humano e uso de som para transferir energia. De forma geral, busca-se encontrar um eletrólito que tenha custo mais baixo e seja menos raro do que o lítio, o que permitiria estender a vida útil por ter mais densidade de energia.

Os impactos no ecossistema IoT estão relacionados principalmente à operação dos dispositivos nas redes, vida útil e custo. A energia requerida por um dispositivo IoT depende do tipo de transmissor, do protocolo, dos sensores e eletrônica da operação, e um sensor envia tipicamente kbytes de dados. Alguns dispositivos sensores de janelas e portas, movimento ou fumaça, não necessitam conectar diretamente na Internet, podendo fazer uso de hubs para enviar seus dados. Um exemplo típico de consumo de um transmissor deste tipo é de 23mA. Outro caso de uso é uma rede mesh de múltiplos nós que leva o sinal para o gateway passando por um nó de cada vez. Tipicamente, o consumo varia entre 5 e 34 mA de acordo com a configuração. Nesse contexto, o ecossistema IoT é estruturado com dispositivos e roteadores ou hubs em função da característica de conectividade e têm apresentado perfis específicos de consumo de energia, principalmente por ficarem longos períodos em modo desligado e somente serem ativados para tarefas específicas (p. ex medição), empregando baixa potência em muitos casos. No modo desligado o consumo é muito baixo, mas quando requisitados para operar, precisam de um pico de potência.

Os avanços da tecnologia 5G incluem dispositivos com baterias de vida útil longa e muitos dispositivos de baixa complexidade e trarão benefícios ao ecossistema IoT. Aspectos de otimização na interface aérea e no core da rede reduzem a complexidade e aumentam a vida útil das baterias, principalmente devido aos modos avançados de economia de energia e sinalização mais eficiente. No LTE citam-se dois tipos de operação, PSM (Power Save Mode), que reduz sinalização entre transmissões, e recepção descontinuada (eDRx, Extended discontinuous receive), que aumenta o período de monitoração por mensagem da rede. Também reduzem medições do canal para permitir economia de consumo.

13.4 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.

Desenvolvimento de sensores MEMS é uma ótima oportunidade de aplicação dos recursos humanos e materiais desenvolvidos nos últimos anos para atuação em microeletrônica no Brasil.

Eletrônica impressa encontrará muita aplicação na área de wearables e saúde, duas aplicações importantes em IoT.

13.5 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

Importante destacar que órgãos internacionais de padronização têm trabalhado na convergência de padrões e no desenvolvimento das respectivas implementações de referência em código aberto.

Citamos como exemplo o consórcio Open Connectivity Foundation (OCF) e a sua plataforma de referência com software e hardware aberto IoTivity, compatível com diferentes sistemas operacionais embarcados: Linux, Android, arduino, Tizen.

Outro exemplo é a Aliança AllSeen e a sua plataforma de referência em código aberto AllJoin,

Recentemente AllSeen, assim como outro consórcio importante uPnP (Universal Plug and Play) se uniram à OCF, consolidando um grande número de empresas e organizações.

A adoção desses padrões e plataformas facilita a adoção de boas práticas de segurança e interoperabilidade, ao mesmo tempo que abstrai os protocolos de comunicação utilizados, tais como Wifi, Bluetooth, NFC e Zigbee.

[Sistemas operacionais abertos como Tizen e Google Android Things são maduros o suficiente para atenderem os casos de uso de IoT.

- Tizen: Tizen é um sistema operacional baseado em Linux Kernel e é utilizado em dispositivos embarcados, como Smart TV, Wearables e Internet das Coisas;
- Google Android Things: É a aposta da Google em suprir um gap de sistemas operacionais para IoT com foco em segurança. O foco deste sistema é para dispositivos com microprocessadores.

13.6 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.

No futuro espera-se que haja espaço para várias configurações, a depender da característica da solução, quantidade de sensores e nós de rede.

No entanto, enquanto não estiver consolidada uma infra-estrutura de comunicação direta com a Internet (LPWA) que atenda os requisitos de cobertura, segurança, privacidade, desempenho, custo e consumo de energia exigidos por muitos dispositivos de IoT, o papel do gateway será essencial na maior parte das aplicações.

Redes locais de processamento distribuído podem ser uma saída para evitar introduzir uma maior capacidade de processamento em dispositivos que não demandam deste potencial, mas que poderão utilizar outros elementos na rede para processamento dos seus dados.

Gateways podem ser utilizados para fazer a interface entre redes celulares (3G, 4G/LTE, etc) e dispositivos não celulares (Wi-Fi, Bluetooth, Zigbee, etc), viabilizando que dispositivos restritos, com menor capacidade de processamento, comunicação e energia, tipicamente de menor custo, possam acessar a internet.

O Gateway é um elemento capaz de agregar mensagens de diversos tipos de dispositivos, sensores e diferentes protocolos, inclusive dispositivos que passam a maior parte do tempo "hibernando" para menor consumo de energia, e encaminhá-las em menor volume de mensagens diretamente para o servidor de aplicações ou "nuvem".

Alguns produtos já disponibilizam essas funções integradas em uma única placa, tais como ARTIK, com suporte a diferentes protocolos, acesso a redes celulares e interfaces com arquitetura em nuvem ARTIK Cloud, de modo a agilizar a expansão de redes IoT.

13.7 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.

Em IoT tem que se considerar as tarefas de tempo real, sem a necessidade de utilizar o processamento na nuvem. Esse processamento seria realizado pelo dispositivo, ou o conjunto de elementos na rede, criando uma zona de processamento local.
Em alguns casos não faz sentido ter um processamento de maior capacidade para tomar decisões locais, como no caso de uma lâmpada, mas em casos como um refrigerador, o processamento poderá e deverá ser maior. A tendência é de ter dispositivos/gateways com mais poderosos, conforme a

evolução para consolidar a processamento "na ponta". Cita-se como exemplo o 5G, quando o processamento é distribuído entre macrocells e small cells. Este cenário pode oferecer uma solução mais rápida e com menos custos de processamento nos datacenters.

13.8 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?

Protocolos abertos podem favorecer a adoção mundial, como o IoTivity e AllJoyn que já estão em cooperação, agora pela OCF - Open Connectivity Foundation.
É essencial que a adoção vise uma interoperabilidade entre os sistemas e dispositivos, a fim de fomentar o desenvolvimento de dispositivos terceiros.
O nível de maturidade deve considerar:

- a adoção por diferentes fabricantes e fornecedores de IoT e a consequente penetração desses padrões no mercado,
- a capacidade de prover suporte e serviçoes a diferentes indústrias (verticais),
- a facilidade oferecida à comunidade de desenvolvedores de software através de plataformas de referência em código aberto e
- a existência de procedimentos de certificação que assegurem que as especificações estejam sendo suficientemente obedecidas de modo a assegurar os benefícios citados nos itens acima.

Outro aspecto relevante a ser considerado na adoção de uma infraestrutura interoperável é a integração entre verticais. Por exemplo, o cenário de colaboração entre as verticais de Casa Inteligente e Saúde Conectada, onde um usuário de uma casa inteligente possa se comunicar com o sistema de Saúde em caso de emergência médica. Vemos os protocolos MQTT e CoAp, acrescidos de segurança TLS quando necessário, como duas alternativas adequadas para troca de mensagens entre dispositivos.

13.9 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?

Como Gateways fazem o papel de agregadores de mensagens em redes IoT, há de se considerar o número de dispositivos conectados ao Gateway, o tamanho médio das mensagens geradas por estes dispositivos e a frequência com que mensagens são acumuladas repassadas a servidores e/ou à "nuvem".
A utilização de padrões como OCF reforçam a adoção de técnicas de criptografia e conexões suficientemente fortes e, ao mesmo tempo, leves, tais como CoAP (Constrained Application Protocol) sobre DTLS (Datagram Trasnport LAyer Security) .

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

Verifica-se o uso potencial de smartphones como gateways nas tecnologias IoT móveis e pessoais, que incluem vestíveis, relógios e monitores de saúde que se conectam à internet através de conexão wireless ou por smartphones. A característica dessa categoria é a natureza móvel da aplicação IoT e da dependência com a existência da conexão wireless.

Nos casos que envolvem mobilidade, espera-se que seja comum o uso do smartphones com a função de Gateway IoT viabilizando casos de uso em diferentes áreas e verticais, por exemplo:

- Saúde: dispositivos vestíveis com sensores biométricos, tais como relógios inteligentes e pulseiras de ginastica com sensores cardíacos e de movimento e equipamentos individuais de saúde (ex: glicosímetro) possam acessar diretamente a internet;
- Carro Conectado: onde informações capturados de dispositivos de diagnostico (e.g. ODBC), sensores de segurança do veículo e informações sobre o usuário do carro sejam agregadas pelo smartphone e enviadas via rede celular.

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

A capacidade de atender a nova demanda de banda larga e móvel, principalmente tecnologias como 4G e 5G, já que será necessária uma maior capacidade de Internet para atender a crescente demanda em IoT.
Considerando a amplitude territorial do Brasil e limitações nacionais de redes celulares urbanas e rurais, a arquitetura em Gateways pode viabilizar que dispositivos possam acessar a internet (“nuvem”) mesmo sem conexão celular, usando protocolos leves e seguros, viabilizando aplicações diversas, por exemplo, em Cidades Inteligentes e Agricultura.
Em um mercado ágil, com lançamento constante de novos produtos, milhões de dispositivos entrando no mercado em um curto intervalo de tempo, os procedimentos, exigências e custos da certificação ANATEL precisam ser urgentemente revisados.