Contribuições à Consulta Pública do Ministério de Ciência, Tecnologia e Inovação para a constituição de um Plano Nacional de Internet das Coisas

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE - ABES

Janeiro de 2017

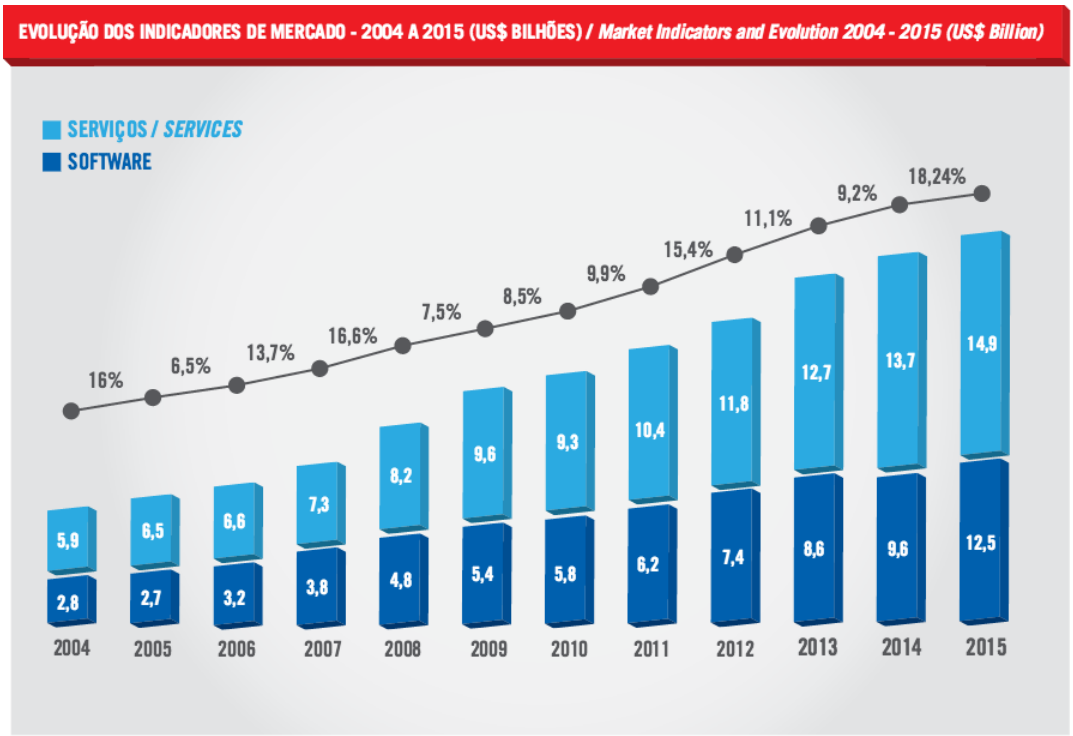
I. Introdução

Vivemos uma transformação digital com amplitude similar à que teve a Revolução Industrial. Bilhões de dispositivos conectados ao redor de nós já estão colaborando para que isso seja cada vez mais verdade e parte indispensável da nossa sociedade, do setor produtivo e da gestão pública. E as "coisas" conectadas seguem a se multiplicar e enriquecer nossas vidas: termostatos inteligentes, dispositivos médicos, automóveis, dispositivos vestíveis, câmeras de vigilância com alarmes integrados e todo tipo de equipamento industrial já estão se conectando e apresentando um estimulante cenário para a inovação, para os negócios e para novos benefícios para a sociedade brasileira.

A ABES - ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE reconhece que a Internet das Coisas (IoT, na sigla em inglês) está radicalmente mudando a maneira como as empresas operam e as pessoas interagem com o mundo físico. Louvamos a iniciativa do Ministério de Ciência, Tecnologia, Inovação e Comunicações (MCTIC) em ouvir a sociedade brasileira por meio de uma Consulta Pública para a construção de um Plano Nacional de Internet das Coisas. Colocamos a nossa experiência e expertise à disposição do governo brasileiro para colaborar amplamente com essa iniciativa. Nesse sentido, gostaríamos de abordar alguns pontos que permeiam a consulta pública e que julgamos pertinentes serem considerados no futuro Plano Nacional de IoT.

A emergência da IoT é uma oportunidade ao desenvolvimento econômico brasileiro
Encorajamos o governo brasileiro a perseguir um planejamento de médio e longo prazo para o desenvolvimento do ecossistema de IoT no país. Entendemos que essa é uma grande oportunidade para o desenvolvimento interno, com a criação de soluções e aplicações para a melhoria das condições de produção e de vida da população brasileira. Trata-se também de uma relevante oportunidade para a inserção global do Brasil no ecossistema global de IoT, sobretudo no que tange à exportação de serviços.

Os setores de software e de serviços de tecnologia da informação são essenciais para o desenvolvimento da IoT no país
O Brasil é um celeiro de empresas na área de software e de serviços de TI, um setor competitivo que não para de crescer. Segundo o estudo Mercado brasileiro de Software e Serviços 2016, produzido pela ABES em parceria com a IDC, o mercado de TI no Brasil cresceu 9.2%, em 2015, enquanto que a média de crescimento global foi de 5,6%. Somente o segmento de software cresceu 30% entre 2014 e 2015, ano em que o país enfrentou uma recessão econômica com queda do PIB superior a 3% (vide gráfico abaixo).



Fonte: ABES e IDC, estudo *Mercado Brasileiro de Software e Serviços 2016*
Disponível em: http://central.abessoftware.com.br/Content/UploadedFiles/Arquivos/Dados%202011/ABES-Publicacao-Mercado-2016.pdf

O desenvolvimento de IoT merece estímulo e monitoramento ao invés de uma regulamentação específica para IoT

O rápido avanço do desenvolvimento das aplicações e soluções baseadas em IoT é extraordinário, tal como exemplificado pelas inovações em tratamento de dados, em especial, pela inteligência artificial. Muitos dos desafios colocados por essas aplicações e soluções tal como a proteção dos dados e informações pessoais, estão sendo tratadas por legislações específicas (tal como Marco Civil da Internet ou o Código de Defesa do Consumidor) ou são motivos de discussão legislativa (tal como os projetos para a criação de uma Lei Geral de Proteção de Dados Pessoais). Como a tecnologia e as suas diferentes possibilidades de uso evoluem rapidamente, a imposição prematura de regulamentação específica para IoT criaria restrições que poderiam sufocar a emergência dessas novas aplicações e tecnologias.

De certa forma, a emergência da IoT hoje apresenta as mesmas características dos primórdios da Internet quando estávamos aprendendo e desenvolvendo novos produtos e serviços que permitiram a explosão de conhecimentos atuais e o aumento brutal dos dados e da produtividade mundial. Eventuais lacunas devem ser trabalhadas, sempre que possível, pelos mecanismos tradicionais de mercado, como auto-regulamentação, contratos padronizados, sempre com foco na competição e na livre-iniciativa.

A cooperação com entidades internacionais e com outros países para identificar áreas de interesse comum, visando participar da definição de normas, padrões e protocolos, desencorajando, sempre que possível, medidas unilaterais de criação de normas, protocolos, padrões, como, por exemplo, a localização forçada de dados em determinadas áreas geográficas, são bem-vindas e teriam alto potencial para beneficiar as tecnologias emergentes, tal como a IoT.

Essas medidas poderiam ser fonte de estímulo e fortalecimento do Brasil como exportador de serviços de tecnologia de informação com soluções de IoT escaláveis globalmente.

O Estado pode ser um importante indutor do desenvolvimento de IoT

A introdução da digitalização aplicada a processos e produtos é seguida por reduções de gastos e de recursos. Nesse contexto, o Estado pode ser um importante indutor do desenvolvimento de IoT no país, seja estimulando a introdução de produtos e processos digitalizados na administração pública (ativos, serviços públicos, etc.) como também por meio de linhas de financiamento. Por exemplo, o BNDES e a FINEP podem ter relevante atuação com a priorização de linhas de créditos voltadas o desenvolvimento da IoT e da economia digital.

Mecanismos alternativos de garantias a empréstimos, que permitissem a redução dos *spread* e de *del crederes* bancários seriam relevantes para impulsionar o empreendedorismo de pequenas e médias empresas na área digital, tais como duplicatas, contratos de serviços futuros, propriedade intelectual e outros.

Segurança e Privacidade devem ser elementos centrais do Plano Nacional de IoT

O ponto crítico nas aplicações de IoT é a segurança. Ela é a primeira camada de privacidade e passa pelo envolvimento do governo, das empresas e da educação da população em geral.

Temos acompanhado e contribuído com as discussões no Congresso Nacional para a criação de uma Lei Geral de Proteção de Dados Pessoais. Entendemos que o tema é relevante e que a promulgação de tal legislação será um importante passo para a proteção dos indivíduos e para a segurança jurídica no país. Entendemos, todavia, que é preciso uma legislação madura e equilibrada (aplicada a empresas, governos e entidades sem fins lucrativos), que seja baseada em princípios e que proteja os indivíduos sem bloquear a inovação e a nova economia movida por dados. Isso seria prejudicial não somente às empresas e governos, como também aos próprios indivíduos que se beneficiam dos diversos serviços privados e públicos disponíveis atualmente.

Os formuladores de políticas públicas deveriam encorajar práticas como segurança e privacidade "*by design*" para otimizar proteções à segurança e à privacidade. Para tal finalidade, políticas de estímulos a boas práticas seriam mais eficazes que regulamentações detalhadas.

As ameaças cibernéticas que rondam organizações e cidadãos se modificam diariamente e se distinguem significativamente de um setor para outro. Dada a natureza mutante dos ataques cibernéticos, seu combate requer grande velocidade e agilidade, gerenciamento de riscos e inovação em medidas defensivas. Nesse sentido, o estabelecimento de um conjunto de princípios para a segurança e a privacidade serão mais eficazes no combate a esses ataques do que quaisquer requisições delimitadas *a priori*.

Privacidade e proteção de dados pessoais devem ser pensados como elementos indissociáveis da segurança cibernética e da governança da informação. Por isso, é importante que o governo avance na implantação e efetivação da Estratégia Nacional de Governança Digital, do Ministério do Planejamento, Orçamento e Gestão, e da Estratégia Nacional de Segurança da Informação e Comunicações e da Segurança Cibernética, do Gabinete de Segurança Institucional da Presidência da República.

Governos devem garantir o fluxo de dados para apoiar o crescimento de IoT
Os dados são o novo recurso natural do século XXI, constituindo-se no fluido vital que move a economia global. No mundo conectado de hoje, o comércio internacional simplesmente não funcionaria sem os fluxos constantes de transferência de dados entre as fronteiras nacionais. O livre movimento dos dados permite às empresas brasileiras de todos os tamanhos e de todas as indústrias trazer inovações do mercado global, guiar seus investimentos, crescer e criar empregos. O fluxo de dados transfronteiras permite, particularmente às pequenas e médias empresas, competir na economia global por meio do acesso a produtos e serviços digitais, tal como as aplicações em nuvem, que lhes proporcionam tecnologia de ponta a custos competitivos, permitem que ingressem nas cadeias globais de valor e tenham acesso direto a clientes em mercados externos.
Infelizmente há alguns governos que consideram implantar (ou já criaram) barreiras ao comércio digital. Empresas brasileiras e aquelas que operam nesses países têm muito a perder se tais barreiras forem implementadas.

Para apoiar o crescimento do ecossistema de IoT e estimular a competitividade da economia, o governo brasileiro deve ter uma posição ativa na proteção do livre fluxo de dados entre fronteiras através de acordos de comércio bilaterais e plurilaterais. Nesse sentido, a participação do Brasil nas discussões do Acordo de Serviços (*Trade in Services Agreement* – TiSA) poderia ser uma oportunidade para endereçar esse tema e ajudar a pavimentar o caminho para futuros acordos comerciais. Em especial, essas discussões devem incluir disposições compulsórias (*binding*) para a proteção do fluxo de dados transfronteiras e evitar medidas unilaterais de localização forçada de dados (como, por exemplo, a obrigação de armazenar dados em data centers locais).

Os padrões abertos são essenciais para o desenvolvimento de aplicações e serviços de IoT
A tarefa de conectar bilhões de dispositivos entre uma multidão de diferentes atores é demasiado complexa. Para tanto, ganha relevância o estímulo à adoção de padrões abertos tanto em termos de conectividade de dispositivos quanto de redes, por meio do qual se avança rumo à interoperabilidade global. Ferramentas e recursos de código aberto possibilitam a uma ampla gama de pessoas e empresas a entrar no mercado e no ecossistema de IoT.

Nesse contexto, é importante que o governo estimule e promova a inovação e o desenvolvimento de novas aplicações e serviços e ao mesmo tempo que tenha políticas enérgicas de proteção à propriedade intelectual e de combate à pirataria.

O Plano Nacional de IoT deve promover a inovação e estimular a competição
A emergência da IoT abre um período de transformações e, aproveitadas as oportunidades, de prosperidade. Muitas das possibilidades e desafios que virão com essa tecnologia ainda são desconhecidos. Dessa maneira, na medida em que novas questões críticas surgirem com o amadurecimento de aplicações e soluções em IoT, é importante que as respostas governamentais permaneçam abertas à flexibilidade e encorajem a continuidade da inovação e da competição.

II. Desafios a serem considerados no contexto de IoT

Com o avanço das aplicações e soluções baseadas em IoT, há a permanência e, em alguns casos, o aprofundamento de alguns desafios a serem considerados por governos e organizações, tais

como a segurança, a privacidade, a interoperabilidade dos sistemas e a responsabilização dos agentes.

Interoperabilidade dos sistemas
A interoperabilidade dos sistemas é a habilidade das "coisas" se comunicarem entre si de maneira concisa e eficiente. Tem sido um tradicional desafio do setor de tecnologia a ser solucionado. Devido à complexidade e amplitude dos sistemas e conexões baseados em IoT, a interoperabilidade é fundamentalmente importante para que todo o ecossistema de IoT se desenvolva. Nesse cenário, não é aconselhável que busquemos padrões próprios, mas que, antes, nos apoiemos nos padrões globais universalmente reconhecidos.

Segurança
A segurança tem sido um elemento crítico para qualquer tecnologia. O crescimento de aplicações e soluções baseadas em IoT aumenta sua importância devido ao aumento do escopo dos desafios de segurança tanto para empresas quanto para usuários finais (sejam eles governos ou cidadãos). Potenciais ataques podem consistir na obtenção de dados privados ou confidenciais, na manipulação ou controle de dispositivos ou em confundir ou negar serviços para aplicações que usam e fornecem dados dentro de um sistema de IoT.

Serão grandes os riscos para os sistemas de IoT que suportam indústrias, produção e transmissão de energia, transportes e outros setores importantes da economia. Na medida em que as infraestruturas industriais se tornam conectadas, tornam-se potenciais alvos de ataques. Para ajudar a proteger esses sistemas, o próprio sistema e seus responsáveis devem entender como os dados fluirão – de dispositivo para dispositivo, entre data centers e até mesmo entre fronteiras – e desenvolver protocolos de segurança e privacidade que coletarão e protegerão dados de maneira confiável, com apropriada gestão de riscos e em concordância com as obrigações regulatórias. Organizações focadas na padronização (tais como ISO, NIST, ETSI, CERT e AIOTI) propiciam excelente apoio com recomendações de abordagens para processamento e manuseio seguro de dados tal como solução de vulnerabilidades, resposta à incidentes de segurança e à incidentes de vazamento de dados. Há uma série de guias, recomendações e padrões publicados ou em desenvolvimento por essas organizações que podem ser usadas para apoiar inovações seguras em sistemas de IoT.

Privacidade e Proteção de Dados Pessoais
A privacidade e a proteção de dados pessoais têm sido um importante elemento nas discussões normativas brasileiras, com destaque para a emergência do Marco Civil da Internet e, mais recentemente, nos projetos de lei sobre o tema em discussão no Congresso Nacional. Esses elementos ganham relevância na medida em que o ecossistema de IoT se desenvolve. Por exemplo, para salvaguardar a privacidade será necessário, como já mencionado acima, avançar em conceitos como o privacidade e segurança "*by design*" de modo que esses elementos sejam contemplados em todo o ciclo de vida de um produto, sistema ou serviço desde a sua concepção. Ao mesmo tempo, é preciso que se tenham princípios claros e estabelecidos, tais como a transparência e o direito de escolha dos titulares dos dados. Como novos desafios surgirão na medida em que avançarmos nas implementações de IoT, uma abordagem principiológica (baseada em princípios e não em regulamentações prescritivas) combinada com uma mudança nos processos produtivos que incorpore segurança e privacidade desde o início produzirá melhores resultados tanto para a proteção à privacidade quanto para a inovação.

Responsabilidade civil
A matriz de responsabilidade civil dos agentes e os riscos envolvidos não é um tema novo. As tecnologias de IoT criam interdependência entre múltiplos desenvolvedores para um mesmo produto, prestadores de serviços para uma mesma solução, entre usuários dos dados e usuários finais. Esse tipo de interdependência já está presente em outros tipos de tecnologia que estão incluídas em cadeias produtivas complexas. Dessa maneira, consideramos que já existe marco legal, em especial na relação contratual, para endereçar esses novos desafios e que não é necessária uma nova categoria para a responsabilização jurídica dos agentes. Uma complexidade adicional pode vir a ser criada no futuro a partir de sistemas completamente autônomos, tal como os carros autônomos, mas nesse caso também seria importante uma cuidadosa avaliação da situação e a identificação dos problemas antes de avançar com novas regras ou modernizar as existentes.

Educação
A educação segue sendo um desafio. Faz-se necessário um aprimoramento dos esforços para a melhoria da educação, em especial em disciplinas que envolvem matemática, estatística, física, engenharia. No contexto de rápido avanço da IoT e da economia digital, torna-se relevante a disseminação de conteúdos e disciplinas nas áreas de programação, segurança, privacidade, ciência de dados.

Neutralidade da rede
A neutralidade da rede também é um elemento importante para o estímulo do desenvolvimento de IoT no Brasil, na medida em que garanta que os dados de IoT serão capazes de se movimentar livremente nas redes de comunicações. Importantes avanços nesse campo foram alcançados com o Marco Civil da Internet. Encorajamos o governo a seguir atento a esse importante elemento.

Migração para o IPv6
Ainda no que tange às condições elementares para o desenvolvimento de IoT, recomendamos que o governo siga atento à necessária migração do padrão IPv4 para o IPv6. Essa medida se faz necessária na medida em que avança rapidamente o número dispositivos conectados. Com o IPv6, teremos:

- Espaço para endereços de IP mais longos que os atuais, podendo acomodar mais dispositivos sendo diretamente conectados à rede;
- A possibilidade de dispositivos tendo múltiplos endereços IPs
- Maior suporte para comunicações seguras
- A possibilidade de grupos de comunicação (tipo multicast) e redes de comunicação (anycast).

III. Conclusão

O rápido avanço da digitalização e dos dispositivos conectados coloca na ordem do dia a existência de políticas públicas consistentes para o desenvolvimento dos ecossistemas de Internet das Coisas no Brasil. Nesse contexto, software e serviços de tecnologia da informação têm um papel essencial para o desenvolvimento da IoT no Brasil e sua inserção nas cadeias globais de valor e deveriam ser objetivo de políticas públicas de estímulo e de fomento.

Chamamos a atenção para desafios importantes a serem considerados no Plano Nacional de IoT, como a interoperabilidade dos sistemas, a segurança, a privacidade, a educação, a neutralidade da rede e a importância da infraestrutura. Nesse contexto, desaconselhamos que haja uma regulação específica para IoT e que o Estado paute suas ações imbuído do seu importante papel de indutor ao desenvolvimento e da necessária segurança jurídica para os empreendedores.

IV. Sobre a ABES

A ABES – ASSSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE, é uma Entidade de Classe Patronal, a nível nacional, com abrangência em todo o Território da República Federativa do Brasil, que congrega em seu quadro associativo, nesta data, 1047 empresas associadas e aproximadamente 1000 empresas conveniadas, dentre as quais se incluem empresas desenvolvedoras, produtoras, distribuidoras e revendedoras de programas de computador e prestadoras dos serviços técnicos complementares necessários ao adequado uso desses sistemas.

A entidade também congrega como seus conveniados pólos tecnológicos regionais como: Porto Digital, Parque Tecnológico BH Tech, Parque Tecnológico Tech Vitória, Incubadora da USP Cietec, Rede Paulista de Inovação (RPI), Softex Campinas, Centro Internacional de Tecnologia de Software (CITS), Parque Tecnológico de Itaipú (PTI), Associação Catarinense de Empresas de Tecnologia (ACATE) e Softsul. Entendemos que o trabalho conjunto é importante para o desenvolvimento do setor tecnológico brasileiro.

A Associação foi fundada em 1986 e nesses trinta e um anos de atividade tem participado ativamente da formulação da política nacional de informática, tendo participado, na pessoa de seus presidentes, dos organismos federais formuladores da Política Nacional de Informática, quais sejam, o CONIN – Conselho Nacional de Informática e Automação, do CATI - Comitê da Área de Tecnologia da Informação e do CICE - Comitê Interministerial do Comércio Eletrônico.

A ABES integra o Painel de Colaboradores do CNCP – Conselho Nacional de Combate à Pirataria, no Ministério da Justiça, órgão criado pelo governo Federal do qual fazem parte representantes do Ministério da Justiça, de outros seis Ministérios, da Receita Federal do Brasil, da Polícia Federal, da Polícia Rodoviária Federal, da secretaria Nacional de Segurança Pública (SENASP), da Câmara dos Deputados e do Senado Federal.

A associação é Conselheira do SOFTEX – Associação para Promoção de Excelência do Software Brasileiro, OSCIP no âmbito do ministério da Ciência e Tecnologia que promove o desenvolvimento do software nacional e também conselheiro do ITS – Instituto de Tecnologia do Software de São Paulo.

A ABES também participa do processo legislativo nos âmbitos municipal, estadual e federal, apresentando propostas de leis e emendas aos projetos de lei em tramitação, tendo participado ativamente da elaboração diversos projetos de interesse do setor.

A Associação mantém ativas, nos últimos 30 anos, ações e campanhas institucionais de combate à violação dos direitos autorais de programas de computador e, mais recentemente, da campanha "Brasil País Digital", que busca mostrar iniciativas que transformam dados em informações

valiosas para indicação de tendências, tomadas de decisão e resolução de problemas importantes para toda a sociedade.

Diante do exposto, demonstramos que a Abes tem se preocupado em representar os polos e as empresas que inovam e fomentam este país, para que possamos juntos promover o desenvolvimento econômico. A Abes coloca o seu time de colaboradores e parceiros para agregarem aos projetos do MCTIC.

Agradecemos desde já a atenção recebida.

Atenciosamente,

Francisco Camargo
Presidente