Pergunta	Resposta GSMA
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.	O crescimento da Internet das Coisas (IoT), viabilizado por políticas e regulação flexíveis, balanceadas e neutras, vai permitir ao Brasil alcançar diversos benefícios socioeconômicos. O governo brasileiro deve garantir o estabelecimento de um ambiente que favoreça o investimento em toda a cadeia de valor da IoT. Flexibilidade regulatória, técnica e comercial é imperativa para permitir a formação de escala global consistente em plataformas confiáveis para provedores de serviço e fabricantes de dispositivos IoT. Formuladores de políticas públicas e reguladores devem reconhecer que a IoT uma indústria nascente, e que sua cadeia de valor, modelos de negócio e serviços são fundamentalmente diferentes de serviços tradicionais de voz e mensagens. Na maioria dos casos, serviços IoT formam um grupo fechado de usuários para o qual o acesso aberto à Internet ou chamadas de voz para qualquer dispositivo geralmente não são o propósito primário do serviço. Além disso, o usuário final do serviço não costuma ser pessoa física, mas pessoas jurídicas que requerem soluções IoT para garantir viabilidade econômica da prestação do serviço ou para permitir uma plataforma de gerenciamento consistente. Ainda, serviços IoT são caracterizados por receitas médias por conexão significativamente inferiores às dos serviços de voz e mensagens tradicionais. Tendo em vista que o ecossistema IoT e sua cadeia de valor são compostos por um grande número de players e pelo acelerado ritmo de mudança, o marco regulatório da Internet das Coisas no país deve se basear no conceito de serviços equivalentes para promover a competição e deve ser tecnologicamente neutro para ser à prova de futuro. Restrições tecnológicas podem reduzir a competição, aumentar custos, limitar investimentos e reduzir o bem-estar do consumidor.
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	A GSMA reconhece que existem diversas definições para M2M e IoT, e que ainda não há consenso na indústria sobre o melhor termo. A GSMA tem utilizado as seguintes definições: IoT: coordenação de máquinas, dispositivos e aplicações conectadas à Internet por meio de diversas redes. Dispositivos podem incluir ‘objetos’ do cotidiano como smartphones, tablets e outros aparelhos eletrônicos como veículos, monitores e sensores. Serviços conectados IoT: serviços oferecidos por meio de dispositivos cuja conectividade é viabilizada por autenticação de um SIM card, e que contam com pelo menos uma das seguintes características: • A conectividade móvel é utilizada para viabilizar função de valor agregado; acesso à Internet aberta ou chamadas de voz para qualquer dispositivo não são o propósito primário do serviço;

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. (...) • Esse enquadramento regulatório é adequado? Ele traz problemas ou limitações para os sistemas IoT? • 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. • A definição de IoT presente no Decreto n. 8.234/2014 é suficiente e adequada ou ela impede o desenvolvimento de alguma atividade? • Há a necessidade de se estabelecer um enquadramento regulatório de acordo com o nível de interação humana nos dispositivos M2M/IoT?	OU • O serviço tem um grupo de usuários fechado e o acesso à conectividade é gerenciado pelo provedor de serviço, excluindo livre utilização da Internet e de serviços de voz. Machine to Machine (M2M): dispositivos conectados sem fio ou via IP. Na maioria dos casos, comunicação acontece de forma autônoma, com intervenção humana limitada. M2M é parte fundamental da IoT. A GSMA reconhece, no entanto, que esforços para definir a IoT são prematuros, e podem ter consequências indesejadas ao reduzir o potencial de inovação da IoT, ou ao abrir caminho para uma regulação específica para IoT. Devido ao rápido ritmo de inovação na IoT, definições prematuras correm o risco de rapidamente se tornarem obsoletas. Também não é claro qual a necessidade de se definir IoT, a menos que se esteja considerando regulação específica. Na prática, a IoT deve ser entendida como um arranjo complexo de produtos e serviços, utilizando como subsídio e suporte os serviços de telecomunicações. Em seu relatório "Enabling the Internet of Things", o BEREC (Organismo de Reguladores Europeus das Comunicações Electrônicas) reconhece que "não é necessário determinar em detalhe qual definição [de IoT] é mais apropriada. Prender-se a uma definição de M2M ou serviços IoT só faz diferença crucial se as obrigações explicitamente dependerem dessa distinção". O BEREC fez um estudo abrangente sobre os serviços IoT na União Europeia (UE) sem precisar definir IoT. O governo brasileiro deveria seguir essa mesma linha. Com isso em mente, a definição utilizada no Brasil, adotada no Decreto n. 8.234/2014, merece revisão, com vistas, no mínimo, a remover a menção à intervenção humana, que gera incerteza no conceito.
• Faz sentido ter um arcabouço regulatório especifico para IoT/M2M?	Não. Uma regulação específica de IoT iria restringir a inovação e gerar custos não-intencionais para a indústria, reduzindo o consumo e o investimento. Antes de regular uma indústria nascente como a IoT, tomadores de decisão devem considerar os seguintes princípios listados abaixo. • Definir um alto limiar para a intervenção regulatória, a ser estabelecido com base em estudos de impacto regulatório. Esta é uma boa prática adotada, por exemplo pelo regulador britânico, Ofcom, que sugere, em sua política de avaliação, que deve haver um "viés contrário à intervenção": "A opção de não intervir (...) deve ser sempre considerada. Às vezes o fato de que o mercado está agindo de forma imperfeita é utilizado para justificar uma ação. Mas nenhum mercado jamais atua perfeitamente, enquanto os efeitos (...) da regulação e suas consequências indesejadas podem ser piores que os efeitos do mercado imperfeito." Da mesma forma, o governo brasileiro deve resistir à tentação de intervir nessa nova indústria sem uma análise prévia e consistente do impacto das várias opções de políticas públicas. • Priorizar revisões e controles ex-post no lugar de regulações restritivas ex-ante. Regulações ex-ante tendem a ser prescritivas, o que, em uma indústria nascente como IoT, pode ser mais danoso que positivo para consumidores e para a indústria. Como reconhecido em diversos outros mercados digitais em crescimento, uma vez que as condições para um mercado saudável tenham sido criadas, uma

	regulação ex-post baseada na lei de competição é o melhor e mais seguro marco regulatório, pois permite flexibilidade técnica e comercial e garante que nenhum player tome proveito de arbitragem regulatória ou de pontos cegos de uma regulação prescritiva. • Promover e adotar políticas que estimulem investimentos. O governo brasileiro deve adotar políticas que facilitem a inovação e permitam que o fluxo de investimento siga livre de barreiras e incertezas regulatórias. • Reconhecer as peculiaridades da indústria de IoT. Ao contrário dos segmentos tradicionais de voz e dados, serviços IoT e M2M tipicamente envolvem mais players que os operadores móveis, incluindo fabricantes de dispositivos, desenvolvedores de plataformas online, integradores de sistemas e o setor público. • Preservar a neutralidade tecnológica e de serviços em todo o ecossistema IoT. O marco regulatório da IoT deve ser baseada em funcionalidade, deve garantir que serviços equivalentes sejam tratados da mesma forma, e e deve primar pela neutralidade tecnológica. Assim, o marco regulatório será custo-eficiente, moderno e à prova de futuro.
• O conjunto de dispositivos que requeiram conectividade deveria ter um arcabouço regulatório próprio, visto que as complexas obrigações das operadoras e os diretos e deveres dos usuários dos serviços de telecomunicações muitas vezes são inconsistentes no cenário de conectividade de máquinas?	Conforme explicado anteriormente, não é necessário arcabouço regulatório próprio para a Internet das Coisas; regulação prescritiva (ex-ante) pode causar distorções, engessar o mercado e impedir a inovação. Regulamentos gerais, ex-post, baseados em princípios e funcionalidade, são mais indicados para se adequar às rápidas mudanças na tecnologia, nos modelos de negócio e nas necessidades dos usuários.
• 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?	O arcabouço regulatório deverá garantir isonomia tributária para os serviços de IoT independentemente da radiofrequência utilizada, uma vez que os tributos são barreiras ao desenvolvimento de novos serviços desse segmento. Alternativamente, propor a alteração da Resolução nº 506/08 (art. 3º), de modo que a Anatel possa incluir, por intermédio de Ato, novas estações de radiocomunicação na lista de equipamentos de radiação restrita isentas de cadastramento ou licenciamento para instalação (pagamento de TFI) e funcionamento (pagamento de TFF).
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:	O governo brasileiro pode usar como referência o estudo "Enabling the IoT" publicado pelo BEREC em fevereiro de 2016. Adicionalmente, o governo brasileiro pode considerar a Recomendação 26 de maio de 2016 da CITEL.
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	A GSMA entende que a interoperabilidade é fundamental para a sustentabilidade de qualquer sistema de comunicação. É importante que o ecossistema ofereça, ao mesmo tempo, mais confiabilidade e menor custo em toda a cadeia de valor; tais benefícios da economia de escala são viabilizados pela utilização de melhores práticas e padrões internacionalmente harmonizados. Assim, apesar de entender que a questão de interoperabilidade está relacionada com mecanismos de validação ou certificação, a GSMA acredita que, neste momento, desenvolver regras específicas e compulsórias de validação ou certificação para a IoT engessaria a inovação em uma indústria nascente: porque o futuro da IoT é,

ou voluntária, em sua opinião, qual se mostra mais adequada ao desenvolvimento do ecossistema de IoT no Brasil? Justifique.	em grande medida, incerto, a criação de padrões hoje poderia acarretar ineficiência e altos custos associados a path dependency. Em última instância, isso afeta negativamente o bem-estar do consumidor e a competitividade dos negócios no país. Alternativamente, a GSMA recomenda o uso de melhores práticas internacionais, que, por sua vez, oferecem condições equivalentes de confiabilidade e baixo custo para os clientes finais, com a vantagem, frente a certos padrões rígidos, de permitir a renovação e atualização conforme as necessidades da indústria.
1.6 Qual impacto a carga tributária do Brasil pode ter sobre o ecossistema de Internet das Coisas?	A GSMA apoia esforços como os adotados pelo Brasil de reduzir a carga tributária para conexões M2M, e nota que ações dessa natureza têm um importante efeito positivo sobre a adoção desses serviços, e para a sociedade e a indústria no país. A GSMA acredita que o governo brasileiro deve remover completamente as taxas específicas do setor de telecomunicações, uma vez que os impactos positivos na sociedade, na arrecadação governamental e no PIB resultantes dessa política vão superar quaisquer renúncias fiscais de curto prazo. A política tributária de um país deve reconhecer alguns importantes princípios para garantir sua efetividade: • A tributação deve ser genérica, não específica: tributação altera os incentivos de oferta e de procura, de modo que as distorções econômicas causadas pela aplicação de tributos só são minimizadas se a carga tributária for distribuída uniformemente pela economia. • A tributação deve considerar as externalidades dos setores e produtos: já é conhecido o argumento pelo qual a tributação se adapta às externalidades negativas de algumas indústrias e produtos, como, por exemplo, a indústria de tabaco. A mesma lógica, no entanto, deve ser aplicada para produtos e serviços que geram externalidades positivas. • O sistema tributário deve ser simples: incerteza e baixo nível de transparência em sistemas tributários podem desestimular o investimento, e geralmente implicam em maior custo de compliance para a indústria (e maior custo de enforcemente para o governo). Além disso, identificamos que, para a IoT, é importante que a tributação desestimule o investimento eficiente e a competição. A aplicação de taxas específicas para serviços IoT, por exemplo, pode gerar significativas distorções, inviabilizar investimento e inovação, e, em última instância, desacelerar o desenvolvimento da IoT no país.
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 pode ter um importante papel de gerador de demanda, como, por exemplo, na utilização de medidores inteligentes de energia elétrica. Além disso, é fundamental que o Estado remova as barreiras existentes hoje para o desenvolvimento desse ecossistema, tais como taxas específicas e sobrerregulação da indústria.
2.3 Seria interessante a atuação do Estado na formação de novos mercados de nicho para IOT? Por quê? Exemplifique.	Não é dever do Estado escolher campeões nacionais; um mercado sem barreiras será capaz de desenvolver, da forma mais eficiente, as áreas nas quais o país tiver melhores condições de ser competitivo.
2.9 Quais são as principais áreas de aplicações de IoT que podem melhorar os serviços públicos ou a gestão pública nas diferentes esferas?	Uma das principais áreas nas quais a IoT pode melhorar serviços públicos é nas Cidades Inteligentes, que incluem uma ampla gama de soluções para afetar positivamente a qualidade de vida dos cidadãos. Exemplos disso podem envolver de crowd management urbano, melhoria na malha de transporte público e privado, aumento da segurança pública e melhor gerenciamento dos serviços de energia elétrica.
2.10 Ainda nesse contexto, que problemas específicos você sugeriria que o Governo	A aplicação de soluções em IoT pode ajudar na solução de desafios enfrentados pela administração pública hoje. Abaixo seguem dois exemplos de soluções baseadas em IoT.

resolvesse por meio dessas novas tecnologias e quais seriam as áreas prioritárias de atuação e os meios de contratação existentes mais adequados?	Crowd management Capacidade de monitorar, e, quando necessário, direcionar um grupo de pessoas para garantir sua segurança. A mesma solução pode ser utilizada para mover grupos de pessoas para seus destinos e planejar a oferta de serviços baseando-se em seu comportamento. Gerenciamento de recursos hídricos Soluções inteligentes de gerenciamento de recursos hídricos utilizando sensores IoT permitem o monitoramento do ambiente em tempo real, viabilizando melhor controle e menores tempos de resposta em situações de crise.
2.14 Quais são atualmente os países de referência em políticas públicas de IoT?	Há diversos países ao redor do mundo nos quais as Cidades Inteligentes têm ganhado importância. No Oriente Médio, há diversas cidades, especialmente Dubai, que se comprometeram em implementar uma série de serviços avançados até 2020. Cingapura, por sua vez, lançou um programa de cidades inteligentes sob o título "Nação Inteligente", e que tem como objetivo introduzir novas soluções para todos os aspectos da vida urbana. Nos EUA, diversas cidades, de Chicago a Atlanta, estão proativamente implantando soluções de cidades inteligentes em parceria com operadoras móveis.
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 uso de tecnologias globalmente padronizadas, como as redes móveis, significariam que as inovações desenvolvidas no Brasil poderiam ser exportadas. Da mesma forma, soluções desenvolvidas fora poderiam ser adquiridas integral ou parcialmente, e utilizadas com pouco ou nenhum problema de integração.
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?	Algar Telecom, Claro, Nextel, Oi, Sercomtel, TIM e Vivo são as operadoras móveis nacionais que apoiam a IoT em termos de conectividade e serviços de valor agregado.
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?	Operadoras móveis estão bem posicionadas para apoiar a IoT no Brasil por meio de diferentes serviços. Comunicações otimizadas Diversas operadoras têm redes 4G bem estabelecidas, alcançando alta largura de banda, atendendo requerimentos de baixa latência, e com planejamento sobre a qualidade de serviço para suportar escala, segurança e serviços de emergência. Operadoras móveis também conseguem suportar requerimentos de menor largura de manda por meio de redes 2G e 3G, que estão sendo suplementadas pelas redes Low-Power Wide Area (LPWA). As tecnologias LPWA, pensadas especificamente para a IoT Móvel (Mobile IoT), são baseadas em padrões 3GPP e podem suportar diversas bandas móveis e requerimentos de performance, e são adequadas para diversos tipos de aplicações IoT. IoT Móvel Redes para IoT Móvel podem suportar grande volume de conexões de dispositivos de baixo custo e com longa vida útil em espectro licenciado. Esses serviços podem, por exemplo, habilitar aplicações do tipo on/off, como

	smart meters, postes inteligentes, e atualizações básicas de status de diversos tipos de sensores e equipamentos, mesmo que estejam em locais remotos. Como a IoT Móvel opera em espectro licenciado, congestão não é um risco, e a cobertura do serviço, indoors e outdoors, favorece a penetração dos serviços de IoT. Gerenciamento de dados e Big Data A IoT será responsável por enormes volumes de dados advindos dos dispositivos móveis conectados. Esses dados podem ser utilizados para gerar insights sobre gerenciamento e eficiência que até então não eram evidentes. Essas informações podem ser utilizadas em tempo real ou armazenadas para análise histórica. O potencial desses dados pode ser maximizado se o acesso a esses dados for facilitado, por exemplo, por um mercado virtual, facilitando não apenas o desenvolvimento de abordagens e serviços inovadores, mas também de APIs e de formatos harmonizados de acesso aos dados. Autenticação e identificação Desenvolvido pela GSMA e seus membros, o Mobile Connect é uma solução segura e universal de single sign-on (SSO). A IoT pode se beneficiar de soluções de autenticação e identificação ao facilitar a forma que os usuários interagem com serviços digitais e aumentar a segurança ao fazê-lo. Por exemplo, seria possível um motorista se identificar para um carro ao começar a dirigir para fins do seguro. Soluções de segurança Para garantir que novos serviços IoT oferecidos no mercado sejam seguros, operadoras móveis vêm trabalhando com demais empresas do ecossistema para desenvolver expertise e aplicar no mercado. A GSMA publicou um guia de melhores práticas de segurança na IoT, disponível no seguinte endereço: www.gsma.com/iotsecurity.
5.4 Que alianças internacionais, no contexto da IoT, são relevantes para o desenvolvimento da IoT no Brasil?	Redes A GSMA e seus membros apoiam a utilização de melhores práticas e padrões internacionais na camada de rede, tendo em vista que isso promove segurança, replicabilidade e economias de escala. Nesse contexto, o órgão de padronização 3GPP é fundamental no desenvolvimento de um padrão de conectividade para a IoT. Aparelhos Na camada de dispositivos, uma importante aliança é a OneM2M. (http://www.onem2m.org/) Smart Home Há diversas alianças sobre o tema de Smart Home, incluindo a AllSeen Alliance (https://allseenalliance.org/) e o Open Internet Consortium (http://www.openinterconnect.org/). IoT Industrial O Industrial Internet Consortium foi fundado pela Intel, Cisco, AT&T, GE e IBM com o objetivo de desenvolver padrões específicos para as aplicações industriais da IoT (http://www.iiconsortium.org/).

	Cidades Inteligentes Abordagens quanto às cidades inteligentes ainda são bastante fragmentadas internacionalmente, mas a GSMA tem trabalhado com seus membros para desenvolver o mercado (http://www.gsma.com/smartcities). Big Data e IoT Abordagens sobre Big Data e IoT também são fragmentadas internacional, e a iniciativa da GSMA sobre Big Data e IoT busca estabelecer uma abordagem comum sobre o compartilhamento de dados da IoT para estimular a inovação (http://www.gsma.com/connectedliving/iot-big-data/).
5.5 Identifique quais são os subsetores da cadeia de TIC mais relevantes para o desenvolvimento de IoT.	Redes – redes móveis – 2G, 3G, 4G, IoT Móvel Dispositivos – módulos, aparelhos, plataformas de gerenciamento de aparelho Serviços de gerenciamento – plataformas de serviço, integradores de sistema Gerenciamento de dados e inteligência – analytics, machine learning, big data, inteligência Aplicações – visualização, aplicações para usuários
9.6 Com base nesse contexto, quais os desafios para a implementação dessas camadas de capacidade de segurança em dispositivos M2M/IoT?	A GSMA possui um abrangente guia de implementação para dispositivos IoT dentro das nossas diretrizes de segurança de IoT – o documento CLP.13 "IoT Security Guidelines Endpoint Ecosystem".
Em sua opinião, existe no contexto de M2M/IoT a necessidade de novos mecanismos de segurança, devido a particularidades desses novos ambientes?	O desenvolvimento de mecanismos de segurança inteiramente novos não é necessário para garantir serviços IoT seguros, visto que já existe uma ampla gama de soluções comprovadamente seguras, como a utilização de um Cartão de Circuito Integrado Universal (UICC) para proteger a identidade do dispositivo, assim como utilizar credenciais criptografadas dentro de dispositivos IoT. O desafio para a IoT é que muitos desses mecanismos ainda não foram amplamente adotados pelos serviços IoT, e, portanto, é preciso considerar o custo de utilizar os mecanismos já existentes para esses novos dispositivos.
Poderia citá-los juntamente com os cenários de uso?	Para mais informações e exemplos, consulte também o documento da GSMA Solutions to Enhance IoT Authentication Using SIM Cards (UICC)".
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?	A escolha da melhor solução de criptografia deve ficar a cargo do provedor de serviço, posto que há diversas soluções criptográficas robustas e padronizadas disponíveis, mesmo para dispositivos de menor custo.
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	A GSMA facilita a cooperação e o compartilhamento de ameaças de segurança entre seus membros e o amplo ecossistema por meio do Grupo de Segurança e Fraude. Os membros do grupo utilizam as informações ali disponibilizadas para implementar processos operacionais ou soluções de rede específicas com vistas a mitigar ataques e reduzir riscos. A GSMA também disponibiliza diretrizes e guias de melhores práticas, como o GSMA

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?	IoT Connection Efficiency Guidelines, para proteger redes de comunicações contra ataques de negação de serviço (DDoS).
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?	A GSMA e seus membros têm ampla experiência em questões de segurança e privacidade, e têm trabalhado com as empresas parceiras em IoT para incluir segurança e privacidade nas tecnologias IoT e na experiência do consumidor como um todo. Essa colaboração vai permitir que a indústria seja capaz de identificar e mitigar os riscos à privacidade do consumidor no contexto da prestação do serviço. Para maximizar as oportunidades da IoT, no entanto, é fundamental que os consumidores tenham confiança nas empresas que estão ofertando os serviços IoT e coletando dados a seu respeito. A GSMA e seus membros acreditam que a confiança do consumidor só pode ser alcançada quando os usuários sentem que sua privacidade é devidamente respeitada e protegida, sem, no entanto, afetar a customização dos serviços que lhe são ofertados. Esse esforço envolve dois princípios gerais: 1) Abordagem baseada em risco: práticas de proteção de dados para um serviço IoT devem refletir o risco para a privacidade do indivíduo e o contexto em que os dados sobre o indivíduo são coletados e utilizados. Intervenções regulatórias devem ser limitadas às áreas em que um risco identificado se concretiza e as medidas existentes são insuficientes para solucionar a questão. 2) Accountability do provedor de serviço: o governo brasileiro pode apoiar ações da indústria no sentido de identificar e mitigar riscos à privacidade, por meio dos quais os provedores de serviço podem demonstrar accountability. Essa medida pode incluir tecnologias e ferramentas que facilitam o controle da privacidade pelo usuário. No caso de muitos serviços IoT, além da operadora móvel, outros players frequentemente estão envolvidos – fabricantes, desenvolvedores de plataformas e até mesmo a administração pública. Com isso em mente, é importante ressaltar o risco que pode ter a incerteza jurídica e regulatória, e se faz mister que as regras de privacidade e proteção de dados sejam aplicadas de forma consistente sobre toda a cadeia de valor da IoT, de forma tecnologicamente neutra.
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	Um arcabouço de proteção de dados que seja à prova de futuro deve compreender que boa parte dos dados captados por sensores IoT não são dados pessoais (já que a maior parte do uso de IoT é em aplicações comerciais e industriais e em serviços públicos), e não devem, portanto, ser tratados como tais. Ainda que os dados coletados sejam pessoais, é fundamental que o regime de proteção de dados permita a coleta e o tratamento desses dados, a fim de não inviabilizar o importante mercado de big data. Há de se considerar também que os projetos de lei de proteção de dados em trâmite no Congresso Nacional têm forte ênfase no consentimento expresso e explícito; tal ênfase pode se tornar uma grande barreira para o desenvolvimento da IoT no país, uma vez que as máquinas, incapazes de consentir, iriam constantemente requerer novas autorizações, interrompendo atividades importantes e gerando, no consumidor, *privacy fatigue* e uma cultura de consentimento desinformado.

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.	
• Quais padrões e modelos de anonimização de dados devem ser implementados de modo a possibilitar o não confinamento de dados em IoT?	Não deve ser adotado nenhum padrão específico de anonimização, sob risco de engessar a inovação e deixar, em pouco tempo, o país preso a um modelo atrasado. O ideal é que, se necessário, o marco regulatório adote a anonimização como um princípio e faça controle ex-post, a fim de permitir que a indústria, os consumidores finais e a própria administração pública tenham liberdade de escolher a opção mais eficiente a cada período.
• Até que ponto a premissa de liberdade na aplicação dos dados pode ser utilizada de maneira virtuosa para o conjunto da sociedade?	A liberdade deve ser absoluta, e o controle final sobre ela deve permanecer nas mãos do usuário. Com transparência e acesso a ferramentas de controle, o usuário deve ser capaz de tomar decisões informadas sobre o seu ponto de equilíbrio entre privacidade de dados pessoais e serviços customizados. O usuário deve ser livre, inclusive, para permitir consentimento inferido a partir do contexto da utilização de serviços.
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.	A interoperabilidade entre os sistema é um fator crítico de sucesso. Na primeira geração da IoT, cada serviço geralmente foca em uma área em particular e atua de forma independente, como, por exemplo, um veículo inteligente ou um serviço de saúde móvel isolado. No entanto, os benefícios crescem exponencialmente se, no futuro próximo, for possível trocar dados com diferentes serviços e aplicações. Um exemplo disso é em uma cidade inteligente com diversos sistemas IoT em operação, tais como uma casa de shows e os dados sobre a venda de ingressos, o Instituto de Meteorologia utiliza sensores espalhados pela cidade, e o transporte público é inteligente e conectado com os semáforos. Se os dados desses sistemas é compartilhado, decisões em tempo real podem ser feitas sobre o funcionamento dessa cidade, como no caso de, no dia de um esperado concerto, os sensores indicarem previsão de chuva pesada, mais ônibus e táxis podem ser enviados para as estações mais próximas do local do evento para ajudar a atender a demanda localizada. Esse tipo de serviço só é possível se dados de serviços individuais, mesmo que pertencentes a diferentes players, forem compartilhados para permitir a geração de serviços inovadores.
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	A camada de suporte a aplicações e serviços é fundamental para a IoT, visto que viabiliza a interoperabilidade, análise de dados, tomada de decisão e interação com o usuário. Alguns serviços IoT podem vir a ser serviços relativamente simples de coleta de dados ou tomada de decisões simples, como parquímetros inteligentes, sensores climáticos, ou sensores de status de algum equipamento. Assim, por exemplo, caso o status do equipamento mude para off-line, por exemplo, é possível gerar um alerta.

desnecessário? Se sim, quais as principais facilidades que tal camada deveria ter? Quais oferecem oportunidades para desenvolvimento local? Justifique e dê exemplos.	Entretanto, a maioria dos benefícios da IoT advém da possibilidade de tomar decisões complexas e responder ao conjunto de dados coletados pelos dispositivos. Dessa forma, se o status de um equipamento mudou para off-line, seria possível fazer análises adicionais para gerar um diagnóstico. Na medida em que se coletam mais dados, a análise de dados vai ajudar a medir a performance de cada equipamento, bem como as causas e efeitos de falhas. Esses serviços adicionais requerem a camada de suporte a aplicações. Se, por um lado, coletar dados é um primeiro passo positivo, ser capaz de responder e aprender com os dados coletados, por outro, será responsável por gerar insights fundamentais. A camada de suporte a aplicações e serviços é também importante para garantir a interoperabilidade. Como discutido acima, interoperabilidade e processamento de dados são primordiais para viabilizar a usabilidade de casos além da simples coleta de dados. APIs permitem que serviços e dados sejam acessados por terceiros, viabilizando, então, que sistemas de IoT possam interagir uns com os outros.
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?	Utilizar uma única solução significa que players atuando nesse setor estariam sujeitos a um único fornecedor, o que traz limitações inerentes, como limitações na escolha de funcionalidades, preços menos competitivos, alto custo de mudança para uma solução alternativa, dentre outros. Em contrapartida, uma abordagem baseada em melhores práticas significa que diversas empresas estariam desenvolvendo seus produtos de acordo com uma especificação acordada pela indústria. Para o consumidor, isso significa maior poder de escolha, na medida em que seria possível escolher e misturar componentes. A interoperabilidade entre as soluções na camada de dados pode ser obtida se o ecossistema adotar uma abordagem comum (APIs, modelos e formatos) para a troca de dados da IoT. Isso significa que os dados transferidos já estariam em um formato que poderia ser combinado com dados de outras fontes, e que dados de organizações parceiras, por exemplo, poderiam ser acessadas pelo mesmo método. Uma abordagem unificada para Big Data em IoT significa que uma aplicação desenvolvida em um local pode ser reaplicada em outro local sem a necessidade de incorrer em altos custos de adaptação. A GSMA vem trabalhando com seus membros para atingir esse objetivo por meio de sua iniciativa Big Data em IoT: http://www.gsma.com/connectedliving/iot-big-data/.
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?	A infraestrutura de computação em nuvem deve variar a depender do uso, dos requerimentos de segurança e do tipo de usuário que deve acessar os dados e as aplicações. Em geral, a combinação de nuvens pública e privada é uma abordagem razoável. Existe uma grande oportunidade para Inteligência / Plataforma / Software como serviço na IoT, uma vez que muitos dos serviços de IoT advêm da coleta, processamento e troca de dados.
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.	Machine Learning tem a capacidade de identificar novas conexões entre diferentes unidades de informação que talvez não fossem intuitivamente óbvias por analistas humanos, ou que teria altos custos se feito de outra forma. No contexto da IoT, machine learning deve ser capaz de peneirar volumes imensos de dados e identificar correlações que podem ser utilizadas para lidar com problemas reais ou para apoiar a tomada de decisão. Alguns exemplos de Big Data para IoT incluem: • Utilizar sensores nas águas dos mares e rios, e, em conjunto com dados sobre a previsão do tempo, fazer previsões sobre a possibilidade de enchentes.

	• Utilizar sensores de qualidade do ar em prédios, veículos, e, no futuro, sensores individuais, que, em conjunto com dados sobre velocidade e direção do vento, podem identificar a origem de determinados poluentes do ar. • Utilizar sensores automotivos em conjunto com informações sobre os trajetos dos usuários para identificar gargalos no sistema de trânsito e permitir a modelagem dos mecanismos de controle de tráfego.
11.7 Qual o impacto do Machine Learning para IoT e quais oportunidades existem para o desenvolvimento local?	O principal impacto de machine learning é permitir que insights sobre dados sejam obtidos rapidamente, e que hipóteses sejam testadas muito mais rapidamente que quando um algoritmo tradicional é utilizado. Normalmente, algoritmos são simplificados porque o grau de influência que uma ampla gama de variáveis tem sobre o resultado é difícil de ser previsto antecipadamente por quem escreveu o algoritmo. No caso de machine learning, o sistema é capaz de avaliar as contribuições relativas de cada fator no resultado, e aplicar mecanismos de feedback, permitindo a melhoria do modelo. Esse processo também pode ser contínuo, na medida em que mais dados são acrescentados, aumentando ainda mais a eficiência do modelo. Apesar de que machine learning geralmente requer supercomputadores para funcionar, há uma grande oportunidade para o desenvolvimento de expertise local nessa área, inclusive no que tange ao ensino dessa área da computação nas universidades.
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?	O ponto de partida seria o fato de haver oportunidades para empresas locais desenvolverem novos dispositivos IoT que sejam relevantes para o mercado nacional, e potencialmente para exportação. Instituições de ensino superior poderiam oferecer cursos voltados para a implementação da IoT e das indústrias correlatas, como Big Data. Na medida em que o volume de dados de IoT cresce no país, haverá também demanda para a utilização de algoritmos mais avançados nas fronteiras das redes (inclusive machine learning). A área de Edge Computing, que leva as aplicações, serviços e dados do nódulo central para os extremos da rede, será uma área de grande crescimento no futuro da computação.
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?	Atualmente, as redes móveis no Brasil, as quais operam sob espectro licenciado, suportam mais de 12 milhões de conexões M2M celular. A rápida evolução da tecnologia IoT Móvel – inclusive o 5G no futuro próximo – significa que o espectro licenciado tem se tornado cada vez mais importante para a IoT no país. Assim, é essencial que os serviços IoT baseados em espectro licenciado continuem a ser apoiados pelo governo brasileiro. O país já conta com boa quantidade de espectro para assegurar cobertura (isto é, abaixo de 1GHz) e capacidade (isto é, acima de 1GHz). Isso significa que as redes móveis já possuem a capacidade de suportar significativo crescimento de tráfego de IoT. Por sua vez, o espectro licenciado é capaz de garantir serviços de alta qualidade em amplas áreas, tendo em vista que as operadoras não têm risco de interferência e podem controlar níveis de uso. Como resultado, a IoT Móvel pode vir a ser a única escolha para serviços que necessitem de garantias concretas, como aplicações de médicas e de segurança. O espectro licenciado também estimula investimentos de longo prazo nas redes. Dessa forma, o governo brasileiro deve garantir que o mercado de IoT tenha acesso aos benefícios ímpares viabilizados pelo espectro licenciado.