Produto 8

Relatório do Plano de Ação

Capítulo Regulatório

2017

BNDES O banco nacional do desenvolvimento

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

BRASIL GOVERNO FEDERAL

Sumário

1 CONTEXTO GERAL DESTE PRODUTO 4

2 ANÁLISE DE HORIZONTAIS 6

2.1 REGULAÇÃO DE TELECOMUNICAÇÕES 6

2.1.1 Conceitos inerentes ao desenvolvimento da IoT 6

2.1.2 A infraestrutura de telecomunicações 8

2.1.3 Aspectos relacionados à outorga para prestação de serviços de telecomunicações 10

2.1.4 Uso racional do espectro 17

2.1.5 Certificação e homologação de equipamentos 18

2.1.6 Obrigações de qualidade 21

2.1.7 Debate sobre a isenção do FISTEL 22

2.2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS 24

2.2.1 Necessidade de criação de Autoridade de Proteção de Dados Pessoais Privacidade e Proteção de Dados Pessoais 25

2.2.2 Experiências internacionais 28

2.2.3 Possibilidades regulatórias para a Autoridade Brasileira de Proteção de Dados Pessoais 35

2.3 SEGURANÇA DA INFORMAÇÃO 43

2.3.1 Governança e cooperação internacional 44

2.3.2 Arranjo institucional brasileiro 49

2.3.3 Incentivo à adoção de critérios para certificação de segurança dos diversos componentes de IoT 52

2.3.4 Segurança da informação em infraestruturas críticas 60

2.3.5 Tecnologia blockchain para a certificação de dispositivos e garantia de identidade digital 62

3 ANÁLISE DOS AMBIENTES PRIORIZADOS 66

3.1 CIDADES INTELIGENTES 66

3.1.1 Introdução 66

3.1.2 Privacidade em cidades inteligentes 72

3.1.3 Rede de energia elétrica inteligente 86

3.1.4 Iluminação pública inteligente 101

3.1.5 Mobilidade urbana 114

3.1.6 Segurança Pública inteligente 132

3.1.7 Aspectos regulatórios da contratação de soluções de Tecnologia da Informação e Comunicação pela Administração Pública 138

3.2 SAÚDE 151

3.2.1 Regulação da Agência Nacional de Vigilância Sanitária – ANVISA 152

3.2.2 Produtos para a Saúde 154

3.2.3 Regulação dos Conselhos de Medicina 163

3.2.4 Debates sobre Privacidade 164

3.3 RURAL 174

3.3.1 Uso de Remotely Piloted Aircraft Systems ("RPAS") em aplicações de IoT 174

3.3.2 Proteção e propriedade de dados e bases de dados 177

4 SUMÁRIO DE CONCLUSÕES DO CAPÍTULO REGULATÓRIO 181

4.1 HORIZONTAIS REGULATÓRIAS 182

4.1.1 Horizontal de Telecomunicações 182

4.1.2 Horizontal de Privacidade e Proteção de Dados Pessoais 183

4.1.3 Horizontal de Segurança da Informação 184

4.2 AMBIENTES PRIORIZADOS 186

4.2.1 Cidades Inteligentes 186

4.2.2 Saúde 191

4.2.3 Rural 193

1 Contexto geral deste produto

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

- **Diagnóstico Geral e Aspiração para o Brasil**: obtenção de visão geral do impacto de IoT no Brasil, entendimento das competências de TIC do País e definição de aspirações iniciais para IoT no Brasil;
- **Seleção de verticais e horizontais**: definição de critérios-chaves para seleção e priorização de verticais e horizontais;
- **Aprofundamento e elaboração de plano de ação (2018 -2022):** aprofundamento nas verticais escolhidas, elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2018-22;
- **Suporte à implementação:** apoio à execução do Plano de Ação 2018-22. As 3 primeiras fases são compostas de 9 produtos principais.

O presente documento apresenta o plano de ação regulatório para o desenvolvimento de IoT no país, dividido em dois grandes blocos: a) análise de horizontais; e b) análise de ambientes priorizadas.

Dentro do primeiro bloco, serão detalhadas as análises e recomendações relacionadas aos temas regulatórios horizontais, que têm sido investigados desde o início do estudo técnico, quais sejam: regulação de telecomunicações, privacidade e proteção de dados pessoais e segurança da informação.

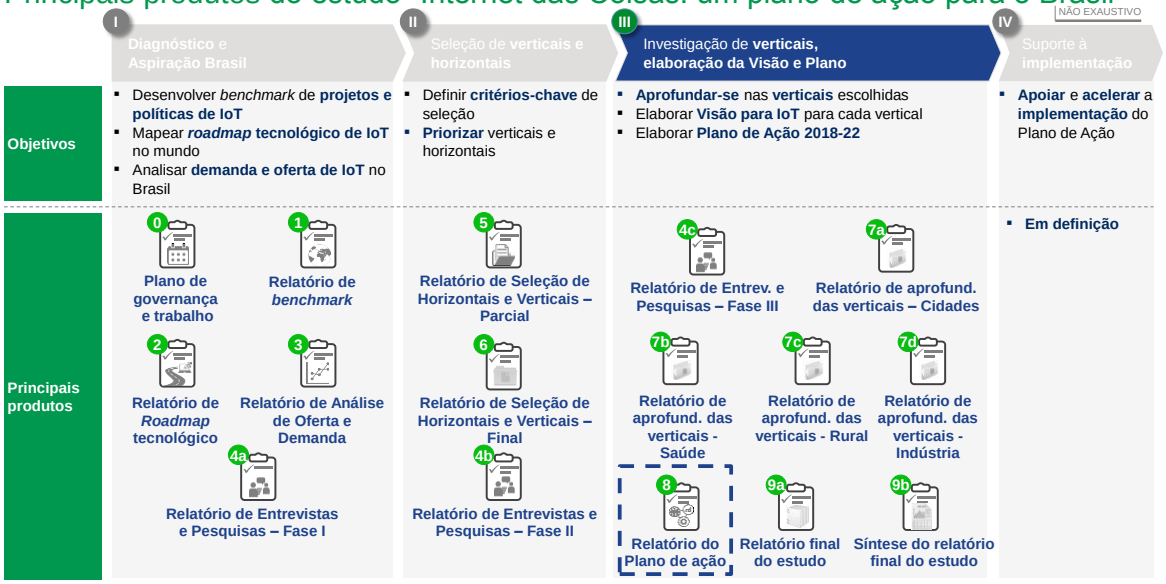
No segundo bloco será apresentado o aprofundamento jurídico realizado em relação aos três ambientes priorizados pelo estudo na Fase II: cidades inteligentes, saúde e rural.[1]

Esse documento faz parte do produto 8, inserido na Fase III do estudo, como descrito no **QUADRO 1** a seguir:

[1] O ambiente "indústria", por se tratar de frente mobilizadora, já conta com um grupo de trabalho específico, em andamento, no âmbito do MDIC, com a participação do MCTIC. Além disso, ao final de 2016, o MDIC publicou um estudo detalhado sobre o tema, intitulado "Perspectivas de especialistas brasileiros sobre oportunidades e desafios para a manufatura avançada no Brasil", o qual está disponível em: https://pt.slideshare.net/mdicgovbr/perspectivas-de-especialistas-sobre-a-manufatura-avanada-no-brasil-2016

QUADRO 1

Principais produtos do estudo “Internet das Coisas: um plano de ação para o Brasil”



FONTE: Análise do consórcio

2 Análise de Horizontais

2.1 Regulação de Telecomunicações

Esta parte do relatório aborda a horizontal regulatória de telecomunicações, como resultado de reflexão realizada a partir do diagnóstico relacionado a este setor, apresentados no Relatório da Fase I – Horizontal Regulatório. A partir dos temas mapeados, foi possível desenvolver recomendações para o endereçamento de questões relevantes para o desenvolvimento da IoT no Brasil.

Para esta finalidade, a presente seção divide-se nos seguintes blocos, a saber: (i) conceitos inerentes ao desenvolvimento da IoT; (ii) infraestrutura de telecomunicações necessária ao provimento de serviços de suporte às aplicações de IoT; (iii) aspectos relacionados à outorga para prestação de serviços de telecomunicações; (iv) uso racional do espectro de radiofrequência; (v) certificação e homologação de dispositivos; (vi) obrigações de qualidade; e (vii) taxas do FISTEL.

2.1.1 Conceitos inerentes ao desenvolvimento da IoT

Como foi reportado no Relatório da Fase I – Horizontal Regulatório, é relevante notar que não há um conceito preciso de IoT no ordenamento jurídico brasileiro. Esta imprecisão é compreensível diante do estágio inicial de desenvolvimento do mercado de IoT. Contudo, a definição de um conceito mais preciso aplicável ao mercado de IoT é importante para balizar eventual intervenção estatal nessa atividade, seja como agente normativo e regulador, seja como agente de fomento.

Entende-se, assim, como ponto inicial, **ser necessário revisitar a definição das comunicações M2M, conceito essencial para o funcionamento de inúmeras funcionalidades da IoT**. Tal constatação é amparada por uma série de contribuições recebidas na Consulta Pública de Internet das Coisas, que apontaram a necessidade de revisitar o conceito de *machine-to-machine* ("M2M") ou comunicação *máquina a máquina* presente no Decreto nº 8.234, de 2 de maio de 2014.[2-3]

O referido Decreto definiu que deverão ser considerados sistemas de comunicação M2M, para fazer jus aos incentivos fiscais previstos na Lei 12.715/2012, aqueles que, *sem intervenção humana*, utilizam redes de telecomunicações para transmitir dados a aplicações remotas, a fim de atender a objetivos que envolvem o monitoramento, medição e controle do dispositivo, do ambiente no qual este se insere ou sistemas de dados que estejam a ele conectados, por meio das redes utilizadas.

[2] Disponível em: http://participa.br/cpiot. Acesso em 24/08/17.

[3] A questão de extensão da desoneração do Fundo de Fiscalização das Telecomunicações ("FISTEL") será tratada em item próprio.

A dúvida surge quando se considera que muitos dispositivos dependem e dependerão de algum nível de interação com o usuário para seu adequado funcionamento. **Considera-se que o emprego do conceito de "intervenção humana" é insuficiente, pois diversas aplicações de IoT utilizam diferentes graus de interação com os usuários, dificultando o seu enquadramento.**

Existem iniciativas de revisão legal que procuram outorgar maior discricionariedade para a Anatel,[4] inclusive com definições que afastam a "interação humana" como ponto central do conceito de "sistemas de comunicação máquina a máquina".[5]

Tal dificuldade já foi enfrentada em outras jurisdições, dentre as quais destacamos, para fins de exemplificação, as definições adotadas pela Alemanha e pelo Canadá.

No primeiro caso, optou-se por definir comunicações M2M como aquelas que são "predominantemente automatizadas". A intervenção humana não seria usual, mas a sua presença, de forma limitada, estaria admitida e não afastaria a classificação de comunicação M2M.[6] Já no segundo caso, a comunicação M2M seria identificada naqueles dispositivos que se comunicam automaticamente sem a necessidade de intervenção humana "direta e consciente".[7]

Reconhece-se, assim, que a experiência estrangeira acabou por utilizar conceitos jurídicos indeterminados – i.e. intervenção humana "predominantemente" ou "direta e consciente" –, que demandam cautela do intérprete da lei.

De todo modo, é importante que a definição a ser utilizada no ordenamento jurídico pátrio traga segurança jurídica, para que não se crie distorções no mercado, notadamente se houver o estabelecimento de assimetrias fiscais ou regulatórias em favor de dispositivos IoT.

[4] Vide, por exemplo, o Projeto de Lei nº 7.656/2017 (de autoria dos Senhores Deputados Vitor Lippi e Odorico Monteiro, comentado pela Anatel). Disponível em https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4F5XiKYL1f8c-OplHKiusgnFeAtzDzvx7FNVl3h9VcWTOBPVj8nMPmHyacWmvXhRWWvB6-7AFm8UjEQ6cchyVg, acesso em 08/.09/.2017)

[5] Vide, por exemplo, o Substitutivo ao Projeto de Lei nº 7.406/2014, que no §1º do art. 38 propõe: "Para fins dessa Lei são considerados sistemas de comunicação máquina a máquina os dispositivos de comunicação para transmissão de dados e aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo ou ambiente ao seu redor ou sistema de dados a ele conectados por meio dessas redes." Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1510327&filename=Tramitacao-SBT-A+1+PL740614+%3D%3E+PL+7406/2014 . Acesso em 12/09/17.

[6] Alemanha. Definição de comunicação M2M adotada pelas autoridades alemãs disponível em: https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/TechnicalNumbers/IMSI_Extra-territorial.pdf?__blob=publicationFile&v=1 . Acesso em 21/08/17.

[7] Definição de M2M publicada pela Comissão de Telecomunicações do Canadá, disponível em: http://www.crtc.gc.ca/eng/dcs/current/faq_43.htm#a13. Acesso em 21/08/17.

Atualmente tramita no Congresso o Substitutivo do PL 7.406/2014, que em seu artigo 21 altera a redação atual do artigo 38 da Lei nº 12.715/2012. Pela redação do Substitutivo, o conceito de M2M passaria a estar definido na própria lei, e abarcaria *"os dispositivos de comunicação para transmissão de dados e aplicações remotas com o objetivo de monitorar, medir e controlar o próprio dispositivo ou ambiente ao seu redor ou sistema de dados a ele conectados por meio dessas redes"*. Embora trate-se de iniciativa louvável no intuito de trazer mais segurança jurídica, o conceito proposto pelo autor do Substitutivo pode ser interpretado como restrito demais para muitas inovações IoT. Isso porque, além de impreciso, sua definição em lei pode engessar futuras modificações no conceito.

Nessa linha, entende-se que o exemplo alemão, calcado na ideia de "predominância", tende a conferir maior flexibilidade para os modelos de negócio existentes e que venham a surgir, notadamente em comparação ao uso "indireto e inconsciente" proposto pelo direito canadense.

Admitindo, portanto, a necessidade de alterar o conceito de comunicação M2M existente no Brasil, recomenda-se avaliar a conveniência de propor-se a alteração do Decreto nº 8.234, de 2 de maio de 2014 para introduzir conceito que comporte o racional de "predominância" de automatização e que conduza à Anatel para promover a regulação de forma detalhada e que impeça distorções.

2.1.2 A infraestrutura de telecomunicações

Considerando que a infraestrutura de rede de telecomunicações necessária ao acesso à internet se constitui como premissa para o desenvolvimento da IoT, devem ser aqui abordadas possíveis ações que viabilizem mais investimento na ampliação de rede de acesso e transporte de telecomunicações no país.

A premissa a ser adotada neste ponto é a seguinte: com a previsão de conexão de milhares dispositivos às redes de telecomunicações do país e o consequente crescimento exponencial do tráfego de dados é fundamental criar incentivos para permitir novos investimentos na ampliação e massificação do acesso a estas redes.

Conforme apontado no Relatório da Fase I – Horizontal Regulatório, as políticas de massificação de acesso aos serviços de telecomunicações encontram desafios jurídicos. Sob esse aspecto, entende-se que o desafio principal já está suficientemente delineado e que existem soluções em tramitação para solucioná-lo.

Inicialmente, no que tange a fonte dos recursos para se viabilizar a massificação de acesso às redes de telecomunicações, três são os encaminhamentos identificados como prioritários:

a) O **PLC nº 79/2016 propõe a solução para duas questões: (i) a adaptação da modalidade de outorga de serviços de telecomunicações prestados sob o modelo de concessão para o modelo de autorização; e (ii) o endereçamento**

sobre a reversibilidade dos bens utilizados para a prestação dos serviços concedidos.[8]

De acordo com esta proposta de modificação da LGT, a alteração do regime de concessão na prestação de STFC pressupõe o pagamento de valor econômico a ser determinado pela Agência, o qual poderia ser utilizado para a expansão de banda larga no Brasil.

De fato, apesar de a proposta presente no PLC nº 79/2016 ainda não ter sido aprovada, é inegável que em caso de sucesso da iniciativa, os recursos oriundos da mudança de regime de prestação de serviço poderiam reverter em relevante fonte de investimento para ampliação do acesso à internet.

b) Além desta possibilidade, **deve ser discutida a aplicação dos recursos provenientes do FUST** para a massificação do acesso à internet em banda larga.[9] Embora seja o principal instrumento de universalização de serviços de telecomunicações, seus recursos praticamente não foram utilizados para tal finalidade.[10] Considerando o grande volume de recursos envolvidos e o sistema de financiamento eficaz utilizado pelo FUST, é importante solucionar esse gargalo como meio de fomentar soluções para IoT.

c) Por fim, não se pode deixar de mencionar a opção de expandir o acesso aos serviços de telecomunicação por meio da utilização de recursos provenientes de **Termos de Ajustamento de Conduta - TAC** eventualmente firmados entre a Anatel e as operadoras para substituir sanções por obrigações. Por meio destes instrumentos, a Agência pode substituir a aplicação de penalidades pecuniárias por obrigações de investimento e outros benefícios diretos aos usuários – o que também resulta na massificação de acesso ao serviço de telecomunicações.

Além de medidas para viabilizar fontes de recursos para a massificação do acesso à internet, é importante que haja uma adequada política pública para ampliar a capacidade

[8] Sobre a temática da reversibilidade dos bens, vale mencionar que a Portaria do Ministério das Comunicações nº 1.455/2016, que estabelece as diretrizes para atuação da Anatel no que tange a revisão do modelo de prestações de serviços, manifesta-se pela necessidade de eliminar este instituto. Disponível: http://www.anatel.gov.br/legislacao/normas-do-mc/899-portariamc-1455 . Acesso em 12/09/17.

[9] Vale citar, como exemplo, o já mencionado Substitutivo ao Projeto de Lei nº 7.406/2014, conforme parecer relatado pelo Deputado Jorge Tadeu Mudalen. Disponível em http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1509928&filename=PRL+5+PL740614+%3D%3E+PL+7406/2014 . Acesso em 18/09/17.

[10] De acordo com a recente análise feita pelo TCU (Acórdão 749/2017), apenas 0,002% dos recursos do FUST foram utilizados para a universalização dos serviços de telecomunicações. Vale mencionar ainda que de acordo com referida análise, 84% dos recursos arrecadados entre 2001 e 2016 para o FUST (aproximadamente 17,2 Bilhões de reais), já foram utilizados pelo governo para outras finalidades, que não a universalização dos serviços de telecomunicações. Disponível em: http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15B4A7944015B6411539954CA&inline=1. Acesso em 20/11/2017.

das redes de acesso e transporte de serviços de telecomunicações. A esse respeito, deve-se ressaltar que, de acordo com informações obtidas pelo Consórcio, esses pontos serão endereçados dentro do escopo do futuro Plano Nacional de Conectividade, colocado em consulta pública em 2017.[11]

Dessa forma, é fundamental a compatibilidade entre o Plano Nacional de IoT e o Plano Nacional de Conectividade, bem como eventuais outras políticas públicas de massificação de acesso a serviços de telecomunicações, tendo em vista que o sucesso do primeiro depende da efetividade do segundo.

2.1.3 Aspectos relacionados à outorga para prestação de serviços de telecomunicações

Eventual necessidade de obtenção de outorga para a prestação de serviços de telecomunicações é um ponto de atenção, conforme antecipado no Relatório da Fase I – Horizontal Regulatório. Assim, no presente documento, serão endereçadas discussões que têm suscitado dúvidas nos agentes privados interessados em atuar no setor de telecomunicações.

Inicialmente, registra-se que a oferta de aplicações de IoT demanda a contratação ou utilização de um serviço de telecomunicações como suporte. Esse serviço de telecomunicações pode ser prestado por meio de outorgas de Serviço de Comunicação Multimídia ("SCM"), Serviço Móvel Pessoal ("SMP") ou Serviço Limitado Privado ("SLP"). Importante aqui destacar que com a entrada em vigor da Resolução Anatel nº 680/2017, os serviços de SCM e de SLP, quando disponibilizados através de redes que utilizam exclusivamente meios confinados e/ou equipamentos de radiocomunicação de radiação restrita, dispensam a necessidade de obtenção de prévia outorga para a prestação de serviços de telecomunicações, bastando para tanto o cumprimento de outras obrigações regulatórias.

Neste contexto, é importante endereçar aqui alguns pontos identificados nas pesquisas realizadas durante a Fase III referentes (i) a oferta de conectividade embarcada em IoT e a necessidade de obtenção de prévia outorga para a prestação de serviços de telecomunicações; (ii) aspectos relacionados aos serviços de SLP para provimento de aplicações de IoT; (iii) limitações regulatórias na exploração de MVNO; e (iv) recursos de numeração e roaming internacional permanente.

i) Conectividade embarcada

[11] A consulta pública do futuro Plano Nacional de Conectividade foi lançada no dia 18 de outubro de 2017 e foi encerrada em 17 de novembro de 2017.

Como identificado no Relatório da Fase I – Horizontal Regulatória, a oferta de conectividade embarcada em dispositivos utilizados em soluções de IoT pode gerar dúvidas regulatórias uma vez que a distinção entre serviços de telecomunicações e Serviços de Valor Adicionado ("SVA") pode não ficar clara quando analisados os diferentes modelos de negócio adotados para o provimento de soluções de IoT, sobretudo nas situações em que há oferta integrada de ambos os serviços.

No atual marco regulatório, sempre que o provedor de aplicações de IoT ofertar, juntamente com as facilidades que caracterizam SVA, funcionalidade que caracterize prestação de serviço de telecomunicações, será necessária a obtenção de prévia outorga com o órgão regulador, salvo nas hipóteses de dispensa expressamente previstas na legislação e regulamentação do setor.

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

Desse modo, considerando a regulamentação atual e o entendimento externado pela Agência no Ofício Anatel nº 399/2010/PVCPR/PVCP, bem como o fato de a Anatel ter competência para deliberar sobre à interpretação da legislação de telecomunicações e os casos omissos (art. 16, XVI da LGT), entende-se necessário que essa Agência Reguladora avalie a possibilidade de editar Súmula para tratar desse tema, de modo a trazer segurança jurídica aos agentes de mercado interessados no provimento de aplicações de IoT.

Observe que a hipótese acima busca conferir maior segurança jurídica aos modelos de negócio de IoT em que a conectividade embarcada é contratada pelo provedor da solução de IoT como um serviço de um operador de telecomunicações. Nesse caso, a Súmula poderia contribuir para afastar eventuais discussões sobre uma possível revenda não autorizada de serviços de telecomunicações ao usuário de IoT.

Para a hipótese de conectividade embarcada oferecida pelo próprio provedor de IoT, seja por meio de rede de telecomunicações própria (SCM ou SLP) ou compartilhada de terceiros (MVNO), a oferta poderá depender, no atual regime regulatório, da obtenção de uma outorga específica para a operação do serviço de telecomunicações, mesmo que essa rede de telecomunicação seja destinada ao uso do próprio provedor de IoT. Nas

próximas seções serão tratados aspectos regulatórios relacionados a outorgas de SLP e MVNO, consideradas alternativas para alguns modelos de negócio em IoT.

ii) Aspectos relacionados ao Serviço Limitado Privado ("SLP") para provimento de aplicações de IoT

O SLP é regulado pela Resolução Anatel nº 617, de 19 de maio de 2013. A referida norma estabelece a necessidade de outorga de SLP para a prestação de serviço de telecomunicações, na modalidade restrita, que seja *explorado em favor do próprio executante ou prestado a determinados grupos de usuários a serem selecionados pela própria prestadora*.[12]

Esse modelo de prestação de SLP ganhou mais relevância com a entrada em vigor da Resolução Anatel nº 680/2017, que acrescentou à Resolução Anatel nº 617/2013 o artigo 5-A para dispensar a necessidade de outorga de SLP nos casos em que as redes de telecomunicações de suporte à exploração do serviço utilizarem exclusivamente meios confinados e/ou equipamentos de radiocomunicação de radiação restrita. Antes dessa mudança essa dispensa de outorga de SLP era apenas possível para categorias específicas de equipamentos de radiocomunicação de radiação restrita.[13]

Apesar de a Anatel nunca ter regulamentado quais seriam os limites da expressão "a determinados grupos de usuário", isto não resulta em qualquer tipo de insegurança jurídica aos agentes interessados na oferta de aplicações de IoT a um grupo predefinido de usuários, dentro das limitações do SLP. Como exemplo, tem-se a manifestação da Anatel no Ofício nº 1706/2017/SEI/ORLE/SOR-ANATEL[14] sobre o modelo de negócio de uma empresa de telecomunicações voltada para IoT que informava se enquadrar nessas condições:

> Reporta-se a Carta encaminhada por V. S.ª em 19 de maio de 2017, constante do processo n.º 53500.057940/2017-52, por meio do qual V. S.ª apresenta modelo de negócios referente a oferta de serviços IoT mediante o uso de equipamentos de radiação restrita operando nas faixas de 902-907,5 MHz, 915-928 MHz, para esclarecer e informar o que segue.

12 Resolução Anatel nº 617/2013, art. 3º: *"O SLP é um serviço de telecomunicações, de interesse restrito, explorado em âmbito nacional e internacional, no regime privado, destinado ao uso do próprio executante ou prestado a determinados grupos de usuários, selecionados pela prestadora mediante critérios por ela estabelecidos, e que abrange múltiplas aplicações, dentre elas comunicação de dados, de sinais de vídeo e áudio, de voz e de texto, bem como captação e transmissão de Dados Científicos relacionados à Exploração da Terra por Satélite, Auxílio à Meteorologia, Meteorologia por Satélite, Operação Espacial e Pesquisa Espacial."*

13 Antiga Resolução Anatel nº 506/2008, artigo 3º.

14 Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5qKCcRSzoq5DnXXPJM9hKqzeSvGfpxp0Fu_WoFxJu6rlRaCNKvC4RxM8uXVPEEW7BqBFNjtRWtYXl9RgoVX-6t

As estações de radiocomunicação, que fazem uso de equipamento, aparelho ou dispositivo, que utilize as faixas de 902-907,5 MHz, 915-928 MHz para aplicações diversas em que a correspondente emissão produza campo eletromagnético com intensidade dentro dos limites estabelecidos no Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita, aprovado pela Resolução n.º 680, de 27 de junho de 2017, estão dispensadas de licenciamento para instalação e funcionamento.

Ademais, foi informado pela empresa tratar-se de prestação de serviço a grupo determinado de usuários, o que se caracteriza como Serviço Limitado Privado - SLP. Uma vez que o SLP será prestado mediante o uso apenas de equipamentos de radiação restrita, a autorização da Anatel é dispensada, devendo-se comunicar o início de suas atividades, conforme dispõe o art. 5-A do Regulamento do Serviço Limitado Privado, adiante transcrito:

> Art. 5-A. Independe de autorização a exploração do SLP nos casos em que as redes de telecomunicações de suporte à exploração do serviço utilizarem exclusivamente meios confinados e/ou equipamentos de radiocomunicação de radiação restrita.
>
> **§ 1º A prestadora que fizer uso da dispensa prevista no caput deverá comunicar previamente à Agência o início de suas atividades em sistema eletrônico próprio da Anatel.**
>
> § 2º A prestadora que fizer uso da dispensa prevista no caput deverá atualizar seus dados cadastrais anualmente, até o dia 31 de janeiro, em sistema eletrônico próprio da Anatel.
>
> § 3º A dispensa prevista no caput não exime a prestadora da obrigatoriedade de atendimento das condições, requisitos e deveres estabelecidos na legislação e na regulamentação. (grifo nosso)

A comunicação deve ser realizada por meio de módulo do Sistema Mosaico, conforme orientações constantes na página http://www.anatel.gov.br/setorregulado/servico-limitado-privado.

Dessa forma, considerando o que foi exposto no documento apresentado (SEI n.º 1478325), ratifica-se o entendimento de que a operação proposta independente de prévia outorga da Anatel, nos termos do Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita, aprovado pela Resolução n.º 680/2017, do Regulamento do Serviço Limitado Privado, aprovado pela Resolução n.º 617/2013, e dos arts. 131, § 2º, e 163, § 2º, II, da Lei Geral de Telecomunicações - Lei n.º 9.472/1997.

Isto posto, o SLP é ferramenta importante na prestação de serviços de telecomunicação de escopo mais específico para suporte de aplicações IoT, não havendo barreiras para sua utilização atual.

iii) Mobile Virtual Network Operator - MVNO

A outorga do **MVNO** também pode ser empregada para a oferta de conectividade em IoT por meio do compartilhamento de rede móvel com prestadoras serviço móvel (SMP), possuindo atualmente duas modalidades previstas na regulação específica: a MVNO Autorizada e a MVNO Credenciada. Mais uma vez, cumpre destacar que as questões mais teóricas já se encontram mapeadas no Relatório da Fase I – Horizontal Regulatório.

Sobre a atual regulação, é válido apontar que as regras para configuração de MVNO encontram-se disciplinadas na Resolução Anatel nº 550, de 22 de novembro de 2010, a qual já passou por alterações pontuais desde a sua publicação para fins de expansão da adoção do modelo[15] – que tem sido objetivo de incentivo pelo órgão regulador.[16] No entanto, entende-se que seria interessante refletir sobre a necessidade de submeter o referido regulamento à revisão, tendo em vista que o contexto em que este foi formulado pode não ser mais compatível com a pretensão de expandir a IoT no Brasil.

Especificamente, é vedado que uma MVNO credenciada tenha contrato de representação com mais de uma prestadora numa determinada área de registro, o que obriga a operadora virtual a utilizar uma única rede como suporte para os seus serviços (limitação regulatória que pode inviabilizar modelos de negócio que exigem cobertura de todo o território nacional) ou a adotar o regime de autorizada, que por sua vez é mais complexo e custoso. A revisão dessa regra para permitir, por exemplo, a representação de mais de uma operadora poderia contribuir para que a MVNO pudesse utilizar a melhor rede disponível em um determinado momento e localidade, privilegiando os seus usuários.

A promoção de reflexões sobre a regulação de MVNO no Brasil ou a realização de pequenas alterações na Resolução Anatel nº 550, de 22 de novembro de 2010 pode contribuir para um ambiente mais favorável ao desenvolvimento do mercado de IoT. **De essencial, acredita-se que a Anatel tem papel importante na comunicação ao mercado de que a MVNO já se constitui como importante solução de acesso**.

iv) Roaming internacional permanente

15 Veja-se, por exemplo, a alteração trazida pela Resolução Anatel nº 663/2016, que excluiu a limitação voltada às MVNOs Credenciadas, de serem estas controladoras, controladas ou coligadas de outras MVNOs Autorizadas na mesma área geográfica de sua atuação.

16 "Como se tornar uma operadora MVNO", disponível em: http://www.anatel.gov.br/grandeseventos/pt-br/como-se-tornar-um-operador-mvno . Acesso em 22/08/16.

Outro aspecto que demanda atenção diz respeito ao uso de recursos de numeração estrangeira de forma permanente. É certo que os dispositivos inteligentes que serão utilizados no país necessitarão de recurso de numeração brasileiro, o qual é regulamentado pela Anatel, para se conectar a uma rede e fazer uso de um serviço de telecomunicação em território nacional.

Uma problemática que surge a partir deste pré-requisito de uso da numeração nacional é a que diz respeito aos dispositivos estrangeiros importados para o Brasil. Vale mencionar, que esse problema tem sido endereçado até o momento através da troca física do SIM card do aparelho. Com a instalação de um SIM card brasileiro que possua uma numeração nacional, é possível que o dispositivo se conecte à rede e usufrua de serviços de telecomunicação.

Entretanto, quando imaginamos um cenário de expansão do uso de dispositivos inteligentes que não comportam trocas físicas de chips, a emergência de novas tecnologias traz soluções alternativas a esse problema, muitas vezes provando, inclusive, serem mais eficientes.

Uma dessas novas tecnologias é a do e-SIM, que possui seu chip integrado fisicamente ao dispositivo. Embora não possa ser fisicamente substituído, ele pode ser reprogramado remotamente: o dispositivo equipado com este tipo de chip permite a substituição do recurso de numeração a ele associado mediante atualização *over-the-air*.

Isto significa que é viável alterar através da reprogramação remota a numeração do dispositivo e sua operadora sem que se troque fisicamente o SIM, o que solucionaria as questões envolvendo: (i) equipamentos importados; e (ii) dispositivos em que não seja viável a substituição física do chip – e.g. por questões de segurança.

O e-SIM se apresenta assim como uma alternativa para o problema da numeração nacional em dispositivos importados, afastando, assim, a necessidade de adotar modelos de negócio que utilizem recursos de numeração de prestadoras estrangeiras.

Ainda no que tange à utilização dessa tecnologia, vale ser mencionado que a Anatel se manifestou, em oportunidade anterior, sobre a impossibilidade de utilizar chips que não possibilitassem a portabilidade de operadoras.[17] Tal obrigação tem origem no texto da Súmula Anatel nº 8, de 19 de março de 2010, a qual positivou este direito dos consumidores.[18] À época, a apresentação de um chip que fosse integrado ao dispositivo

[17] ANATEL, Ofício nº 98/2015/SEI/PRRE/SPR-ANATEL. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?WwIhLN_g9R51QStF7kKYBHkoN4GOioaWR9LFGBGK627HLLLXn0lySP5NvKQPPiWBvcaCzM3y0c3MOWE17vgm14WMYQxiqVWaEwKY0c6tjm1UJcY093WgCCImLUr7hpXU . Acesso em 13/09/17.

[18] "O desbloqueio de Estação Móvel é direito do usuário do SMP que pode ser exercido a qualquer momento junto à Prestadora responsável pelo bloqueio, sendo vedada a cobrança de qualquer valor ao usuário pela realização desse serviço" Disponível em: http://www.anatel.gov.br/legislacao/sumulas/60-sumula-8 . Acesso em 13/09/17.

e que não permitisse o exercício do livre arbítrio do usuário quanto à operadora, de fato impedia seu uso. Entretanto, atualmente, o avanço das configurações do e-SIM já afastam preocupações neste sentido.[19]

Neste ponto, o uso do e-SIM pode se apresentar como uma alternativa à necessidade de se permitir o **roaming internacional permanente** para viabilizar o desenvolvimento de modelos específicos de negócios de IoT no Brasil. Conforme mencionado no Relatório da Fase I – Horizontal Regulatório, muitas das funcionalidades viabilizadas pela IoT envolverão a circulação de dispositivos provenientes de outros países, que estariam conectados a prestadoras também estrangeiras. Ocorre que até o momento, a Anatel tem sinalizado não concordar com este tipo de modelo, entendendo como sendo o roaming internacional permanente ato irregular.[20]

O fato do e-SIM ser remotamente reprogramável permite que os agentes troquem de operadora sem precisarem adquirir um novo SIM. Essa alteração facilitada de operadora, em consonância com a mudança de país do dispositivo, afastaria a necessidade de uso do roaming internacional permanente. [21]

Ainda no que tange esta discussão, deve ser destacado que considerando o estágio atual da regulação da Anatel, bem como o crescente desenvolvimento de funcionalidades adstritas à IoT, visualizam-se três cenários regulatórios passíveis de implementação:

a) Normatizar a escolha pela proibição total, tendo em vista que a Anatel ainda não editou regulamento que oficialize a vedação à prática, ação considerada fundamental para instituição de maior segurança jurídica aos players do mercado.

b) Em sentido completamente oposto, a Agência poderia adotar uma postura de liberação total para uso do roaming permanente no Brasil, o que demandaria extensos estudos, incluindo questões práticas (e.g. limitação de numeração), competitivas (e.g. inauguração de assimetria

[19] Para maiores informações, favor consultar: https://www.gsma.com/rsp/ . Acesso em 13/09/17.

[20] O assunto foi abordado pela Agência no Ofício Circular nº 43/2012/PVCPR/PVCP, de 28 de junho de 2012, em resposta aos questionamentos sobre a regularidade de utilização de terminais móveis com Simcard e recurso de numeração de prestadoras estrangeiras, com o intuito de oferecer SVA de forma permanente para usuários residentes no Brasil. Além disso, a Anatel manifestou-se neste sentido na Reunião da Comissão de Políticas Econômicas (SG3) da União Internacional de Telecomunicações ("UIT"), ocasião na qual se afirmou que "o roaming permanente poderia provocar o desbalanceamento na competição, já que acabaria sendo criada uma operadora de telecomunicações em escala global, que não pagaria os impostos das empresas locais". Informação disponível em: http://www.telesintese.com.br/brasil-diz-nao-ao-roaming-permanente/ . Acesso em 22/08/17.

[21] Apesar de não versar sobre roaming internacional, vale a lembrança de que a Súmula 1/1998 editada pela Anatel traz o precedente de obrigatoriedade de assinatura de acordo de roaming com outras operadoras em caso de ter sido ofertada esta opção a uma operadora específica. Tal entendimento poderia ser estendido ao cenário de acordos de roaming internacional, reforçando assim a viabilidade do modelo regulatório adotado pela Agência.

regulatória entre operadoras brasileiras e estrangeiras) e legais (e.g. eficácia do sistema de outorgas após a flexibilização).

c) Por fim, uma alternativa intermediária seria a opção de liberar parcialmente o uso do roaming permanente apenas para os dispositivos de comunicação M2M. Esta escolha exigiria a implementação de medida para coordenação de alocação de blocos de numeração que seriam previamente "reservados" para atender as aplicações integrantes.

Entende-se que a opção deve levar em consideração uma avaliação detida acerca do real impacto do roaming permanente à disseminação de aplicações IoT no Brasil, considerando alternativas a essa flexibilização – como o e-SIM ou o MVNO, apontados acima. Trata-se de consideração necessária, notadamente por envolver uma situação de mercado consolidada (situação "b") ou a criação de uma medida regulatória assimétrica (situação "c") – a qual, se não é novidade no setor, deve ser devidamente fundamentada.

Assim, crê-se que as principais questões que tangem ao tema outorga foram mencionadas.

2.1.4 Uso racional do espectro

É preciso abordar o **uso do espectro de radiofrequência**, insumo relevante no contexto da IoT. No Relatório da Fase I – Horizontal Regulatório foram expostas algumas questões que foram identificadas como relevantes para o debate acerca do aproveitamento eficiente do espectro.

Nesse caso, os comentários abrangem as formas de acesso à radiofrequência para servir de suporte às aplicações de IoT. O enfoque se dará sobre: (i) criação de mercado secundário de radiofrequência; (ii) regras de exploração industrial; e (iii) aumento do espectro não licenciado.

Em relação ao primeiro ponto, não há hoje um **mercado secundário de radiofrequência**, pois atualmente não é possível transferir a autorização, sem que seja também transferido o serviço de telecomunicação a esta vinculado. Entretanto, com a tramitação do já mencionado PLC nº 79/2016, surge a possibilidade de ser modificada a LGT também para prever a possibilidade de transmitir o uso de radiofrequência, sem vínculos. Se aprovada a redação, o Brasil passaria a integrar o rol de países que permite o mercado secundário de espectro.[22]

[22] RAMOS, Marcelo de Matos; LIMA Marcelo Sá Leitão Fiuza. *Sobre o uso eficiente do espectro radioelétrico.* Disponível em:http://seae.fazenda.gov.br/central-de-documentos/documentos-de-trabalho/documentos-de-trabalho-2006/DT_42.pdf . Acesso em 05/09/17.

Do ponto de vista regulatório a proposta é identificada como medida interessante para facilitar ainda mais o uso racional do espectro, o qual espera-se ser cada vez mais demandado – equilibrando assim a equação de oferta e demanda deste insumo. Num cenário em que a revenda de radiofrequência seja liberada, a flexibilização do uso do espectro seria maximizada, diferentemente do que ocorre atualmente.

Além disso, é importante que fique claro que o mercado secundário não se confunde com a possiblidade de cessão de radiofrequência por meio de **exploração industrial**, hoje regulamentada pela Resolução Anatel nº 671, de 3 de novembro de 2016.

A referida norma se configura como uma opção de uso mais eficiente do espectro, tendo em vista que, apesar de vincular a cessão de radiofrequência a uma série de requisitos e observância de um procedimento próprio, há em sua redação a previsão de casos que afastam a necessidade de anuência prévia da Agência (art. 41, § 6º). Seria importante avaliar, junto ao mercado, se as regras atualmente postas pela regulamentação são aptas a fomentar o uso eficiente de espectro.

Nesse sentido e considerando a novidade da regulação de exploração industrial, acredita-se que seria necessário **de pronto realizar mapeamento do uso do espectro licenciado no Brasil,** fazendo uso da previsão contida no art. 5º, I, da Resolução Anatel nº 671, de 3 de novembro de 2016 (comprovação periódica de uso efetivo de radiofrequências). **A partir da identificação adequada quanto à ausência de utilização do espectro pela operadora que detém seu uso, a Anatel poderia, motivadamente, avaliar a eventual necessidade de rever a regulamentação aplicável ou então adotar medidas para estimular a adoção desse modelo de negócio**.

Por ora, analisando a redação da Resolução acima citada, acredita-se ser necessário **discutir o porquê da vedação a cessão de uso de radiofrequência em uso primário.** Do ponto de vista jurídico, não se vislumbra qualquer impedimento para a liberação deste tipo de cessão para uso além do secundário.

Em relação ao terceiro ponto, sob a ótica jurídica, cumpre salientar apenas que **a alocação de espectro deve seguir os padrões de alocação internacionais, de forma a não gerar distorções e incompatibilidades entre equipamentos produzidos no Brasil e no exterior** – o que geraria uma série de prejuízo aos serviços.

2.1.5 Certificação e homologação de equipamentos

Outro bloco de grande importância está relacionado ao tema da certificação e homologação de equipamentos utilizados para a prestação de serviços de telecomunicações.

Como foi diagnosticado no Relatório da Fase I – Horizontal Regulatório, os procedimentos, que são regulamentados pela Anatel, para avaliação dos equipamentos

poderão constituir-se como entraves burocráticos à massificação do uso de dispositivos inteligentes.

Conforme consta no Relatório anterior, várias são as dificuldades relacionadas a esta questão, dentre as quais destacam-se: (i) o processo de certificação e homologação é extenso e demorado; (ii) não existem acordos de cooperação internacional que dispensem o procedimento de certificação já executado em outras jurisdições; (iii) não há critérios internacionais que viabilizem otimização dos testes realizados.

Tendo em vista que a demanda por certificação de homologação de equipamentos relacionados à IoT irá aumentar consideravelmente, não deve ser ignorado que obstáculos inerentes a estes procedimentos prejudicam a competividade na produção e comercialização dos dispositivos, além de impor possível atraso na entrada de novas tecnologias no mercado doméstico.

Considerando este cenário, a Anatel, lançou a Consulta Pública nº 34/2016, já finalizada, que propõe a revogação das normas e regulamentos técnicos de certificação de produtos para telecomunicações, a fim de uniformizar os procedimentos internos por meio da publicação de novos requisitos técnicos. [23]

Após o recebimento e análise das contribuições apresentadas, a Agência manteve o entendimento de que a inciativa é relevante para a promoção da desburocratização do processo de certificação, tornando-o mais célere. Atualmente, o processo que trata da proposta aguarda a apreciação do Conselho Diretor da Anatel.[24] **Isto posto, compreende-se ser a postura da Agência louvável por demonstrar o seu comprometimento com uniformização e desburocratização**.

Entende-se importante que a Anatel mantenha esse caminho. Adicionalmente, seria interessante prezar pela assinatura de Acordos de Reconhecimento Mútuo com outras jurisdições, de acordo com a conveniência e oportunidades identificadas pela Agência, tendo em vista que esta possibilidade já se encontra abarcada na regulação atual (Resolução Anatel nº 242, de 30 de novembro de 2000, art. 3º, I). Em que pese tal ato depender da vontade de outras jurisdições, também poderia contribuir para uma redução substancial na burocracia relativa à certificação de equipamentos.

Na mesma linha deve ser mencionado o recente Ato Anatel nº 11542, de 23 de agosto de 2017, que endereçou os requisitos técnicos para a avaliação da conformidade de

[23] Consulta disponível em: https://sistemas.anatel.gov.br/SACP/Contribuicoes/ListaConsultasContribuicoes.asp . Acesso em 18/09/17.

[24] Processo Anatel nº 53500.009149/2016-55. Acesso em 24/08/17.

equipamentos de radiocomunicação restrita.[25] Destaca-se que o referido ato não incluiu direcionamento para os equipamentos que fazem uso da tecnologia Chirp Spread Spectrum ("CSS")[26].

Segundo a própria Agência, este tipo de tecnologia, dentre outras, exigem a realização de estudos adicionais para a determinação dos correspondentes requisitos técnicos, o que não seria implementado diante do escasso período de tempo entre a publicação da Resolução Anatel nº 680, de 27 de junho de 2017 – aprovou o Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita - e a do referido ato.[27]

Diante deste cenário**, manifesta-se pela necessidade de realização de estudos adicionais que sejam eleitos pela Anatel como essenciais para definição de requisitos técnicos faltantes**, evitando assim a configuração de barreira de entrada a tecnologias específicas.

Por fim, e indicando uma postura ativa da Agência no tema, vale aqui mencionar também duas Consultas Públicas que foram lançadas no mês de Novembro de 2017 pela ANATEL, pouco antes desse relatório ser publicado: I) a Consulta Pública nº 27,[28] que visa atualizar o Ato Anatel nº 11542/2017 mencionado acima, em especial no que tange a possibilidade de utilização da tecnologia CSS; e II) a Consulta Pública nº 33,[29] que busca atualizar a Resolução nº 242, de 30 de novembro de 2000, que aprovou o Regulamento para Certificação e Homologação de Produtos para Telecomunicações, incorporando uma série de elementos aqui mencionados como essenciais para dar maior agilidade e eficiência para o processo de certificação e homologação de dispositivos IoT.[30]

25 ANATEL. Ato nº 11542, de 23 de agosto de 2017. Disponível em: https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=2128852&id_orgao_publicacao=0 . Acesso em 13/09/17.

26 Os equipamentos que seguem o padrão LoRa, exemplo de rede IoT LPWA, operam com a tecnologia CSS.

27 ANATEL. Contribuições recebidas à Consulta Pública nº 20/2017, resposta à contribuição nº 80860. Disponível em: https://sistemas.anatel.gov.br/SACP/Relatorios/RelatorioDadosBd.asp?pCodProcesso=C2017&pCodTipoProcesso=1&pTipoRelatorio=2 .Acesso em 13/09/17.

28 Disponível em: https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2037&Tipo=1&Opcao=andamento

29 Disponível em: https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2063&Tipo=1&Opcao=andamento

30 Vale aqui mencionar parte da justificativa contida na ANÁLISE Nº 160/2017/SEI/LM do Processo 53500.010924/2016-15 que deu origem a Consulta Pública: *"(...) Nesse sentido, suficiente mencionar, por exemplo, a revolução tecnológica encabeçada pela Internet das Coisas (ou, em inglês, Internet of Things – IoT), nova infraestrutura global para a Sociedade da Informação. Seus dispositivos inteligentes, interconectados física e virtualmente por meio das tecnologias da informação e comunicação, a cada dia se tornam mais disseminados, presentes e acessíveis. No núcleo dessa nova tendência tecnológica global estão os sistemas de comunicação máquina a máquina (em inglês, Machine-to-Machine – M2M). Tais sistemas são compostos por dispositivos de comunicação eletrônica dos mais variados tipos e funções; todos interligados ao ecossistema digital global e interagindo de forma autônoma por meio da Internet. A gama de aplicações para os sistemas que utilizam dispositivos M2M é incomensurável; engloba de meios de transporte e maquinário industrial a eletrodomésticos e peças do vestuário, apenas para citar alguns exemplos dos muitos dignos de menção. Em vista do volume e da variedade esperada no futuro próximo para esses*

2.1.6 Obrigações de qualidade

Tendo sido tratadas questões relacionadas ao procedimento de certificação e homologação de equipamentos, passamos para outra discussão de extrema relevância para a IoT no Brasil: as obrigações de qualidade mínimas na prestação de serviços.

Conforme mencionado no Relatório da Fase I – Horizontal Regulatório, a observância dos índices previstos nos RGQs para diversas aplicabilidades da IoT pode configurar-se como significativa barreira de desenvolvimento da IoT.[31] Como não há, atualmente, diferenciação quantos às funcionalidades viabilizadas por dispositivos que usam serviços de telecomunicações, todas as operadoras de SMP e de SCM devem assumir o mesmo nível de ônus regulatório[32].

Vale relembrar, ainda, que hoje apenas o quesito da velocidade é passível de maiores variações comerciais, sendo os demais, como latência, sujeitos a requisitos mínimos de qualidade. Essa restrição pode se mostrar inadequada para conferir maior liberdade às operadoras que prestam serviços de telecomunicações ou oferecem aplicações de IoT[33].

Nesse sentido, tendo em mente que a maior liberdade para as operadoras ofertarem planos adequados às aplicações IoT – v.g. com maior latência bidirecional – pode ser uma forma de baratear o custo da atividade, os RGQs podem representar um óbice a esse objetivo.

Tal objetivo encontra-se intimamente conectado à **relevância de ser elaborado um conceito claro e contemporâneo de comunicação M2M**. Com esta medida, ademais de ser viável a reconfiguração da hipótese de incidência do FISTEL, **seria possível ajustar pontualmente a regulação de qualidade para que os dispositivos M2M não se**

dispositivos que integram os sistemas de comunicação M2M, promover a avaliação da sua conformidade na forma atualmente estabelecida seria ineficiente e, muito provavelmente, impraticável. Assim, além de rever o procedimento para que seja mais abrangente e versátil, a fim de conferir mais qualidade ao processo de certificação e homologação de produtos para telecomunicações, a presente revisão normativa também representa uma oportunidade para simplificar e dar melhor consistência regulatória ao instituto."

31 Especificações quanto aos indicadores, coleta de informações, cálculos e outros assuntos relacionados aos requisitos de qualidade podem ser consultados nas seguintes normativas: (i) anexo da Resolução nº 574/2011, referente ao SCM; (ii) anexo da Resolução nº 575/2011, referente ao SMP; (iii) anexo da Resolução nº 605/2012, referente ao STFC; (iv) anexo da Resolução nº 411/2005, referente ao SeAC. Além disso, vale mencionar a Resolução nº 654/2015, que aprovou o Regulamento das Condições de Aferição do Grau de Satisfação e da Qualidade Percebida Junto aos Usuários de Serviços de Telecomunicações. Os dispositivos do Regulamento se aplicam às prestadoras do SMP, SMC, STFC e os serviços de televisão por assinatura.

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

33 É o caso do índice mínimo de tentativas bem sucedidas de conexão com a rede de dados (art. 20 do RGQ/SMP), bem como da latência bidirecional mínima de 80 milissegundos em 95% dos casos (art. 18 do RGQ/SCM), que correspondem a indicadores de qualidade que incidem sob qualquer conexão.

submetam a tais obrigações ou se submetam parcialmente (dentro de uma lógica de identificação de padrões mínimos que seriam considerados imprescindíveis).

Caso a Anatel compreenda que a realização de mudanças desse teor nos RGQs pode ser potencialmente prejudicial aos consumidores, propõem-se como possível solução **a flexibilização dos índices de qualidade para M2M apenas no nível de contratação para pessoas jurídicas**. Em conjunto com tal medida, destaca-se a importância de fazer uso dos procedimentos para solução de conflitos já presente na Anatel a fim de propiciar ambiente de maior segurança jurídica.

De todo modo, a agência reguladora parece estar atenta à necessidade de revisitar parâmetros de qualidade dos serviços de telecomunicações, visto que recentemente lançou a Consulta Pública n. 29/2017 para colher contribuições ao novo Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL[34]. Torna-se, imprescindível, portanto, que a Anatel leve em consideração a necessidade de alterações para fomentar aplicações de IoT.

2.1.7 Debate sobre a isenção do FISTEL

Por fim, a desoneração dos sistemas de comunicação M2M é ponto sensível para o desenvolvimento do universo IoT no Brasil – uma vez que o ARPU por conexão se torna extremamente baixo.[35-36]

A obrigação de recolhimento do FISTEL, desencadeada pelas estações utilizadas na prestação de serviços de telecomunicação, representa um ônus relevante. É verdade que os encargos envolvidos já foram em parte reduzidos, principalmente pela mudança trazida pelo art. 38 da Lei nº 12.715, de 17 de setembro de 2012: a taxa de fiscalização por

34 Disponível em: https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C2036&Tipo=1&Opcao=andamento

35 Segundo a GSMA, "[c]onexões M2M normalmente geram ARPU significativamente baixas quando comparadas às conexões pessoais, dessa forma a redução nas tributações associadas à M2M devem desempenhar papel importante no desenvolvimento do mercado." Tradução livre. Original disponível em: https://www.gsma.com/mobileeconomy/archive/GSMA_ME_Latam_2014.pdf . Acesso em 15/09/17.

36 Vale também destacar que o custo por uso de dados no Brasil encontra-se em significante redução. Segundo números da Anatel, desde 2010 até 2015, o valor médio mensal de 1Mbps caiu 71,7%, indo de R$ 21,18 para R$ 5,98. Além disso, a Anatel registou queda de 53,9% no ARPU da telefonia móvel do primeiro trimestre de 2009 ao segundo trimestre de 2015. Para maiores informações, favor consultar: http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=342736&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=342736.pdf e https://cloud.anatel.gov.br/index.php/s/VxuWaQltgEeQKyU/download?path=%2F&files=Relat%C3%B3rio%20de%20acompanhamento%20SMP%20-%201T16.pdf. Acesso em 11/09/17. http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=316693&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=316693.pdf . Acesso em 12/09/17.

chip a ser recolhida ao FISTEL passou de R$ 26,83 para R$ 5,86. Tal desoneração, contudo, não foi suficiente para dirimir o problema identificado.

Além do aumento da procura por soluções inteligentes em si, deve ser considerado que muitas das funcionalidades que envolvem o recolhimento do FISTEL tem valor de mercado menor que a taxas devidas por conexão – e.g. estação de telecomunicações. Isso pode inviabilizar, num primeiro momento a concretização do produto, ou, num segundo momento, a fruição pela população geral.

E como proposta para promover a difusão dos dispositivos inteligentes, o PL nº 7.656/2017 – já referenciado anteriormente, em trâmite na Câmara dos Deputados, propõe a alteração da Lei nº 12.715, de 17 de setembro de 2012 para reconhecer isenção total da taxa de fiscalização de instalação e de funcionamento para as estações móveis de serviços de telecomunicações que se caracterizam como comunicação M2M.[37]

Essencial apontar que a Anatel já se manifestou sobre o PL nº 7.656/2017, tendo destacado a relevância da proposição. Segundo a Agência,

> v) "*o impacto regulatório da proposição legislativa é insignificante. Tal aspecto foi levantado no âmbito do projeto estratégico de reavaliação do modelo de outorga e licenciamento de estações, tendo sido verificado que, em 2016, a arrecadação proveniente do recolhimento da TFF das estações 'máquina a máquina' foi de R$ 7.806.787,90 [...], enquanto a arrecadação com a TFF dos demais tipos de estações totalizou 2.424.589.731,00 [...]. Assim, tem-se que as estações 'máquina a máquina' correspondem a apenas 0,32% das receitas com a mencionada taxa, proporção que se mantém em relação à CFRP e à Condecine*"[38] (sem grifos no original)

A declaração da Anatel é de extrema relevância, pois afasta qualquer argumento no sentido de que a promoção da desoneração do FISTEL seria inviável por motivos de arrecadação.

Evidente que a forma como seria tomada a decisão para atingir o objetivo de desoneração poderá ser diferente da hipótese de alteração legislativa presente no PL nº 7.656/2017. A própria Anatel cogita a promoção de alteração na LGT, em seu art. 162, para excetuar da obrigação de licenciamento as estações M2M, o que consequentemente afastaria a incidência de todas as taxas e contribuições.[39]

[37] Projeto de Lei nº 7.656/2017, tramitação disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2137811 . Acesso em 10/08/17.

[38] Processo Anatel nº 53500.060180/2017-61, Informe nº 57/2017/SEI/PRRE/SPR.

[39] Processo Anatel nº 53500.060180/2017-61, Informe nº 57/2017/SEI/PRRE/SPR.

Dessa forma, deve-se ter em mente que a adoção de medida que reduza o custo de expansão dos dispositivos que utilizam a comunicação M2M são essenciais e devem ser postas em prática.

2.2 Privacidade e Proteção de Dados Pessoais

Para além de um possível aperfeiçoamento do arcabouço regulatório de telecomunicações, é preciso refletir sobre privacidade e proteção de dados pessoais no ecossistema de Internet das Coisas.

Com a proliferação de novos dispositivos conectados à Internet aptos a armazenar, coletar e tratar uma significativa quantidade de dados, tem sido recorrente a discussão sobre os usos legítimos dos dados e sobre as vulnerabilidades das bases de dados gerados. Em adição, a formulação de políticas públicas, a gestão eficiente e transparente dos órgãos governamentais e a criação de novos modelos de negócios são diretamente influenciados pelo crescimento exponencial de análises baseadas em grandes volumes de dados.

Nesse cenário, o desenvolvimento de soluções Internet das Coisas perpassa pela edição de normas sobre proteção de dados pessoais que lide com a complexidade e as nuances dos dados pessoais, e que seja capaz de trazer segurança jurídica à essa nova fronteira da vida em sociedade.

Mais do que a edição de norma específica sobre proteção de dados pessoais, também se faz necessária a existência de instância regulatória para lidar com os desafios da atual sociedade da informação, por se fazer necessária a existência de uma autoridade capaz

de apresentar opiniões técnicas específicas a este novo ambiente e realizar controle unificado e homogêneo do cumprimento das disposições sobre proteção de dados pessoais.

2.2.1 Necessidade de criação de Autoridade de Proteção de Dados Pessoais Privacidade e Proteção de Dados Pessoais

No presente tópico, serão apresentadas considerações sobre possíveis desenhos institucionais para uma Autoridade de Proteção de Dados Pessoais no Brasil. Partimos da premissa de que um dos consensos obtidos durante o processo de formulação e consultas públicas relacionadas ao plano nacional de IoT foi justamente a necessidade de criação de uma autoridade de proteção de dados pessoais.

Desse modo, serão brevemente descritas as experiências institucionais da União Europeia e dos Estados Unidos - que são centrais no atual debate mundial sobre a proteção de dados pessoais e possuem modelos institucionais distintos entre si. Além disso, analisaremos a autoridade constituída no Uruguai, exemplificando a forma como essa instituição vem sendo formulada na América do Sul. Também serão analisadas as propostas normativas sobre o tema atualmente em tramitação no Congresso Nacional. Em seguida, serão indicadas possibilidades regulatórias para a instituição de Autoridade de Proteção de Dados Pessoais no país.

O regime jurídico de proteção à privacidade apresenta significativas lacunas no Brasil, devido à ausência de legislação bem como de institucionalização a respeito do tema. Um dos problemas atuais é o fato de que a observância ("enforcement") de normas relativas à privacidade serem objeto de fiscalização e atuação de múltiplas entidades consecutivamente: SENACON (ligada ao Ministério da Justiça), Ministério Público Federal, Ministério Público Estadual e assim por diante. A **aprovação de lei específica e a criação de Autoridade de Proteção de Dados Pessoais** pode mitigar esse problema. Além disso, pode prevenir abusos na coleta e tratamento de dados pessoais dos usuários de Internet e nos sistemas de Internet das Coisas. Atualmente, os contornos legais da proteção de dados pessoais no Brasil são fornecidos primordialmente pelo Marco Civil da Internet e pelo Decreto nº 8.771/2016. Mesmo prevendo parâmetros mínimos de proteção da privacidade na Internet, como a exigência de que dados pessoais somente poderão ser fornecidos a terceiros quando houver consentimento livre, expresso e informado do usuário (art. 7º, VII), **o próprio marco regulatório existente prescreve a necessidade de haver norma específica** que verse em maior detalhe sobre a proteção desses dados (art. 3º, III).

Em uma sociedade cada vez mais orientada pela análise de dados[40], tal vácuo normativo é preocupante não apenas para cidadãos, mas também para o setor privado e para o próprio Estado. Isto porque, com a proliferação de novos dispositivos conectados à Internet capazes de coletar dados diversos, como é o caso de tecnologias de IoT, mais recorrentes e comprometedores serão os ataques a *data bases* e a ocorrência de uso indevido de dados pessoais. Em adição, a capacidade gerencial desses atores se tornou condicionada e tem sido incrementada pela coleta, armazenamento e processamento automatizado de dados realizados com auxílio de elaborados algoritmos. A formulação de políticas públicas, a gestão eficiente e transparente dos órgãos governamentais e a criação de novos modelos de negócios[41] são diretamente influenciados pelo crescimento exponencial de análises baseadas em grandes volumes de dados.[42]

Nesse cenário, o desenvolvimento de soluções para a comunicação máquina a máquina perpassa pela edição de normas específicas sobre a proteção de dados pessoais que lidem com a complexidade e as nuances dos dados pessoais, e que sejam capazes de trazer segurança jurídica à essa nova fronteira da vida em sociedade, especialmente considerando que a expansão de IoT pode ter o condão de potencializar violações à privacidade dos cidadãos.

Mais do que a edição de normas específicas sobre proteção de dados pessoais, também se faz **necessária a existência de instância regulatória capaz de apresentar opiniões técnicas específicas** à proteção da privacidade nos diferentes segmentos de mercado e de realizar controle **unificado e homogêneo** do cumprimento das disposições sobre proteção de dados pessoais.

Para estruturar essa instância, é necessário refletir sobre os **modelos de regulação existentes**, sendo os principais deles os de **regulação estatal, co-regulação e auto-**

[40] No artigo **The promise and the peril of data-driven society**, publicado no *The New York Times* em 25.02.2013, discute-se o conceito de sociedades orientadas por dados, tratando do impacto do *big data* no uso de redes sociais, nas decisões empresariais e nas questões de privacidade *online*. Disponível em: https://bits.blogs.nytimes.com/2013/02/25/the-promise-and-peril-of-the-data-driven-society/?_r=0. Acesso em 21.08.2017.

[41] As variadas técnicas de tratamento e análise de dados permitem a disponibilização de uma série de funcionalidades e serviços digitais, dentre as quais estão a publicidade digital direcionada e o uso de *big data* por empresas de telefonia para auxiliar a administração pública. Mais informações em: http://www.inova.jor.br/2017/08/07/big-data-telecomunicacoes-cidades/. Acesso em 21.08.2017.

[42] Conforme a revista *The Economist*, em edição de maio de 2017, as mesmas preocupações regulatórias que existiam no século passado com a indústria do petróleo ressurgem agora com a ascensão das grandes empresas do mundo digital. O controle que essas empresas têm sobre os dados de seus usuários lhe dá grande poder econômico. Com o aumento de aparelhos conectado à Internet, o volume de dados que essas empresas detêm tende a crescer exponencialmente. Disponível em: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. Acesso em 18.08.2017.

regulação.[43] O modelo recorrentemente encontrado no Brasil é o de **regulação estatal**, em que a organização de determinado segmento de mercado é concentrada e conduzida por órgão da Administração direta ou indireta, como é o exemplo das Agências Reguladoras (Agência Nacional de Energia Elétrica - ANEEL e Agência Nacional de Telecomunicações - ANATEL, por exemplo).[44]

Em pólo diametralmente oposto e menos recorrente no país se encontra a **auto-regulação**[45], consistente na regulação conduzida pelos próprios agentes de mercado e no desenvolvimento e implementação de mecanismos destinados ao cumprimento desses parâmetros normativos.[46] Nesse cenário, as possibilidades de imposição de sanção diferem do poder de polícia estatal e são aplicadas pela própria comunidade auto-regulada. Os resultados dessa atuação são de características diversas, como a elaboração de códigos de conduta, modelos de contratos, códigos de ética e de selos de qualidades. Embora não sejam novidade, as experiências de auto-regulação têm expandido significativamente após o surgimento da Internet e sua efetividade varia de acordo com fatores diversos, como a existência de incentivos governamentais, a composição e transparência da instância de elaboração e aplicação das regras criadas.[47]

Por fim, iniciativas de **co-regulação** são definidas pelo compartilhamento de responsabilidades entre governo e agentes privados em atividades como a formulação de normas e padrões regulatórios e seu *enforcement*.[48] Esse modelo de regulação se exterioriza de diversas maneiras e com diferente intensidade, como a auto-regulação supervisionada por órgãos governamentais ou a elaboração negociada de normas (*negotiated rulemaking*). Referido modelo tem sido adotado com o intuito de reunir

43 HIRSCH, Dennis D. **The Law and policy of online privacy:** Regulation, self-regulation, or co-regulation? 34 Seattle U. L. Rev. 439, 2010-2011, p. 451.

44 KLEINSTEUBER, Hans. J. **Self-regulation, co-regulation and state regulation**, p. 62. Disponível em: http://www.osce.org/fom/13844?download=true. Acesso em 25.08.2017.

45 POULLET, Yves. **How to regulate Internet**: New paradigms for Internet governance self-regulation: Values and limits. 1999, p. 84-88. Disponível em: http://www.crid.be/pdf/public/4656.pdf. Acesso em 25.08.2017.

46 Como exemplo nacional temos o Conselho Nacional de Auto-regulamentação Publicitária - CONAR.

47 Sobre o tema, vide relatório do *Selfregulation.info*. Disponível em: http://www.law.uni-sofia.bg/Kat/T/IP/T/PM/DocLib/Internet%20Self-Regulation%20An%20Overview.htm Acesso em 28.08.2017.

48 Para Kleinsteuber, se o Estado e os reguladores privados cooperam em instituições conjuntas, há a co-regulação. (Idem, p. 63). Segundo Christopher T. Marsden, o termo co-regulação abrange uma variedade de diferentes fenômenos regulatórios, que têm em comum o fato de que o regime regulatório é estruturado a partir de uma interação complexa entre a legislação em vigor e entidades auto-reguladoras. Os variados interesses desses atores resultam em diferentes incentivos para que eles cooperem. In: **Internet co-regulation and constitutionalism**: Towards a more nuanced view. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328&rec=1&srcabs=1988369&alg=1&pos=1. Acesso em 25.08.2017.

diferentes *stakeholders* na elaboração de normas que contarão com incentivos e fiscalização conduzidos com respaldo estatal.[49]

Diante das possibilidades regulatórias apresentadas, primeiramente se faz necessário ressalvar que a escolha do modelo regulatório para a autoridade de proteção de dados pessoais deve levar em consideração o contexto local, não sendo recomendável a apresentação de solução *blueprint* replicada em diversos países e que desconsidera o cenário de recursos governamentais, da capacidade organizacional dos setores relevantes e de vontade política.[50]

De todo modo, pesquisas desenvolvidas nas últimas décadas indicam que as Autoridades de Proteção de Dados Pessoais existentes que se mostram mais efetivas são as que contam com o devido engajamento dos diversos setores interessados ("multistakeholderism" ou "multissetorialismo"), que possuem mecanismos reais de absorção da colaboração apresentada por esses atores, e que apresentam altos índices de transparência e responsividade.[51]-[52] Outra característica relevante dessas autoridades está relacionada às suas competências e ações, como o comprometimento com a promoção de educação e conscientização da comunidade sobre a proteção de dados pessoais no uso da Internet.

Assim, **o desenho da instância reguladora a ser criada deverá levar em conta o contexto político-institucional local e ser adequado à dinamicidade e complexidade técnica da Internet**. Além disso, deverá estabelecer reais processos participativos para a tomada de decisões e dispor de capacidades institucionais para fornecer ao mercado parâmetros de conduta e também fiscalizar o cumprimento da legislação relacionada.

2.2.2 Experiências internacionais

Nesta seção, serão brevemente descritas as experiências normativas e institucionais dos Estados Unidos, União Europeia e Uruguai quanto à privacidade e à proteção de dados pessoais. Para além de sua relevância em matéria de proteção à privacidade, os modelos

49 MARSDEN, Christopher T. **Internet co-regulation and constitutionalism**: Towards a more nuanced view. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328. Acesso em 31.08.2017.

50 RODRIK, Dani. **Institutions for high-quality growth**: What they are and how to acquire them. Cambridge: NBER, 2000 (Working Paper, n. 7.540). Disponível em: http://www.nber.org/papers/w7540. Acesso em 26.08.2017.

51 United States Chamber of Commerce; Hunton & Williams LLP. **Seeking solutions**: Attributes of Effective Data Protection Authorities, 2016. Disponível em https://www.uschamber.com/sites/default/files/023052_dataprotectionhuntonpaper_fin.pdf. Acesso em 23.08.2017.

52 Em 1999 a *Bertelsmann Foundation* indicou a necessidade de envolvimento dos atores privados nas práticas de *enforcement* estatais devido à falta de capacidade do governo em lidar com a natureza global, técnica e cambiante do ambiente virtual. Mais que isso, sugeriu que intermediários da Internet sejam compreendidos como potenciais aliados para promover a governança e combater irregularidades na rede "Bertelsmann Foundation. **Self-regulation of Internet content**, 1999, p. 49. Disponível em: https://cdt.org/files/speech/BertelsmannProposal.pdf. Acesso em 25.08.2017.

regulatórios dos EUA e da UE possuem arranjos bastante diferentes entre si para lidar com o assunto, o que justifica sua escolha para exemplificar como a comunidade internacional tem lidado com a questão da proteção dos dados pessoais de seus cidadãos. O Uruguai, por sua vez, detém papel de destaque na proteção de dados pessoais na América Latina, sendo tal proteção considerada direito humano pela Constituição uruguaia. No país, a proteção de dados pessoais é regida por lei específica e existe órgão competente para lidar com o assunto.

Os três modelos exigem o consentimento do usuário para a coleta, tratamento e uso de dados pessoais, estipulam obrigação de transparência, consistente na necessidade de fornecer ao titular dos dados algumas informações básicas, e concedem o direito de acesso, retificação e eliminação de dados.[53] Entretanto, esses modelos divergem quanto aos papéis do Estado e do mercado na regulação e *enforcement*.[54]

Nos Estados Unidos, o papel do Estado é reduzido às normas setoriais, sendo o Poder Judiciário a instância final para a resolução de conflitos. Na Europa, a Autoridade de Proteção de Dados detém grande parte da competência normativa e atua na resolução administrativa de conflitos, de modo a evitar a judicialização de conflitos. De forma semelhante ao modelo europeu, o Estado possui papel importante no Uruguai, principalmente em relação à fiscalização de condutas, já que é exigido cadastramento prévio de bancos de dados, a cargo da autoridade de proteção.

Quanto ao papel do mercado, a regulação esparsa no caso estadunidense exige que a maioria da prática comum sobre dados pessoais e privacidade seja definida pelos seus próprios agentes, por meio de práticas autorregulatórias, como a celebração de contratos, sempre sujeita ao crivo judicial. A União Europeia, por sua vez, faz uso de mecanismos advindos do mercado para incentivar a adesão a padrões de tutela já definidos nas normas sobre proteção de dados. O sistema uruguaio, por fim, é semelhante nesse sentido ao da Europa, pois permite, perante à autoridade de proteção e desde que estes estejam de acordo com a legislação, o registro de códigos de conduta elaborados por associações e entidades representativas de responsáveis por bancos de dados de titularidade privada.

a) União Europeia

A proteção de dados pessoais na União Europeia é atualmente regulada pelas Diretivas nº 95/46/CE e nº 2002/58/CE, editadas entre meados de 1990 e início dos anos 2000 pelo Parlamento e pelo Conselho Europeu, com o objetivo de harmonizar a legislação

53 GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 21.08.2017.

54 Ibid., p. 19-24.

existente sobre o assunto nos Estados-membros.[55] A primeira delas é a principal regulamentação de proteção de dados pessoais em vigor no sistema jurídico europeu[56], enquanto a segunda aborda o tratamento de dados pessoais e a proteção da privacidade nas comunicações eletrônicas.[57]

Em janeiro de 2012, a Comissão Europeia propôs uma **reforma das regras vigentes** sobre proteção de dados pessoais, culminando na edição da Regulamentação nº 2016/679 (*General Data Protection Regulation* - GDPR) e da Diretiva nº 2016/680 do Parlamento e do Conselho. Essas novas regras buscam permitir ao usuário controlar a coleta, tratamento e uso de seus dados pessoais e almejam também simplificar o ambiente regulatório sobre o tema. As regras foram publicadas em maio de 2016 e passarão a vigorar a partir de maio de 2018.[58]

Especificamente em relação à existência de Autoridade destinada à proteção de dados pessoais, os Estados-membro observam o art. 8º da Carta de Direitos Fundamentais da União Europeia[59], que requer a existência de órgão independente. Em primeiro lugar, tem-se a **Autoridade Europeia para a Proteção de Dados** (EDPS)[60], **entidade supervisora e consultiva independente**, responsável por assegurar que as instituições e órgãos da União Europeia respeitem obrigações no que concerne à proteção de dados. Dentre as competências da EDPS estão o controle do tratamento dos dados pessoais, o aconselhamento de instituições e organismos da UE e o processamento de queixas e inquéritos.

Por sua vez, o **Grupo de Trabalho** instituído pelo artigo 29 da Diretiva nº 95/46/CE é um órgão consultivo independente sobre proteção de dados e privacidade, sendo constituído

55 **Manual da Legislação Europeia sobre Proteção de Dados do Conselho da Europa (CE) e do Tribunal Europeu dos Direitos do Homem (TEDH)**, 2014, p. 18. Disponível em: https://rm.coe.int/16806ae65f. Acesso em 29.08.2017.

56 A Diretiva determina normas gerais sobre a legitimidade e limites do tratamento de dados pessoais, estipula direitos dos titulares desses dados, e prevê também autoridades de supervisão independentes nacionais. Mais informações em: http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_5.12.8.html. Acesso em 29.08.2017.

57 Para uma revisão do histórico da regulação da Internet na União Europeia, ver FEELEY, Matthew J. **EU Internet regulation policy**: The rise of self-regulation, 22 B.C. Int'l & Comp. L. Rev. 159 (1999). Disponível em: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1216&context=iclr. Acesso em 29.08.2017.

58 A *General Data Protection Resolution* consagraria modelo de co-regulação, no qual o Poder Público estabelece padrões normativos amplos para a proteção de direitos, mas, ao mesmo tempo, abre espaço para a iniciativa privada estabelecer regulações privadas com vistas ao desenvolvimento do setor tecnológico. Conforme https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017#_edn3. Acesso em 29.08.2017.

59 Os artigos 7º e 8º da Carta reconhecem o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais estreitamente relacionados, conquanto distintos. A Carta está integrada no Tratado de Lisboa, que estabelece certos princípios para a proteção da privacidade, e é juridicamente vinculativa nas instituições e órgãos da União e nos Estados-Membros quando aplicam legislação da União Europeia.

60 Em inglês, *European Data Protection Supervisor*.

por representantes das autoridades nacionais de proteção de dados dos Estados-membros, da EDPS e da Comissão Europeia. De forma geral, esse órgão **emite recomendações, pareceres e outros documentos**.[61] Nos termos da nova legislação que entrará em vigor em 2018, ele será substituído pelo Comitê Europeu para a Proteção de Dados.[62] Há também o ***Data Protection Officer***, no âmbito da Comissão Europeia, responsável por garantir que a Comissão aplique adequadamente a legislação concernente à proteção de dados pessoais. Além de cooperar com a EDPS e informar os departamentos da Comissão que coletam dados pessoais e as pessoas titulares dos dados sobre seus respectivos direitos e obrigações, o *Officer* **mantém base de dados** com o registro de todas as operações da Comissão que tenham envolvido dados pessoais.[63] Por fim, no âmbito dos Estados-membros, **há autoridades nacionais de proteção de dados**, que atuam em conjunto com as entidades descritas acima.

Dessa forma, quanto à proteção da privacidade e de dados pessoais, a União Europeia possui **modelo predominantemente regulatório** - dado que as Diretivas determinam como se dará a proteção de dados pessoais e que existem autoridades responsáveis por sua aplicação tanto no nível nacional quanto no supranacional -, **com indicações significativas de co-regulação**. Um exemplo de formas de co-regulação no continente europeu são as normas vinculantes advindas de entidades privadas (*binding corporate rules - BDRs*), em que empresas europeias e estrangeiras definem contratualmente regras para a proteção de dados pessoais em suas trocas transnacionais. Contudo, essas normas corporativas passam por processo de homologação perante a autoridade de proteção de dados de cada país envolvido na operação.[64] Mais especificamente, a **legislação implementada em 1995 permite que países-membros utilizem abordagens co-regulatórias na proteção de dados pessoais**. Nesse sentido, cada país implementa sua legislação sobre proteção de dados pessoais e convida representantes de determinado setor para elaborar um "código de conduta" para o segmento, que poderá ser aprovado e obter força de legislação.

b) Estados Unidos

Diferentemente, os Estados Unidos **não possui legislação federal específica e consolidada** sobre a proteção de dados pessoais. A matéria é regulada por uma série de **leis federais setoriais e por leis estaduais**, além da existência de códigos de conduta e

61 De forma específica, suas tarefas estão definidas nos artigos 30 da Diretiva nº 95/46/EC e no artigo 15 da Diretiva nº 2002/58/EC.

62 Mais informações sobre o *Article 19 Working Party* em: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. Acesso em 29.08.2017.

63 Ferramenta disponível em: http://ec.europa.eu/dpo-register/search.htm. Acesso em 29.08.2017.

64 Mais informações em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017. Acesso em 29.08.2017.

regulamentos estipulados pelo setor privado. A legislação federal que versa sobre a proteção de dados pessoais diz respeito a setores específicos, como saúde e seguros (*Health Insurance Portability and Accountability Act* - HIPAA), bancário (*Gramm-Leach-Bliley Act* - GLB), telecomunicações (T*elecommunications Act*) e questões consumeristas (*Children's Online Privacy Protection Act* - COPPA). A maioria dos Estados possuem legislação específica sobre proteção de dados pessoais, mas o Estado da Califórnia se destaca no cenário da privacidade por ter editado as primeiras e mais dinâmicas leis na área.

Diante desse cenário regulatório difuso, **inexiste nos Estados Unidos órgão específico** que concentre aspectos de privacidade e proteção de dados pessoais. Quem exerce autoridade sobre essas questões em âmbito federal são instâncias independentes com competência para regulamentar e assegurar o cumprimento de normas setoriais. Como exemplo, o *Department of Health and Human Services* - HHS normatiza e assegura o cumprimento da proteção a dados na área da saúde, e o *Consumer Financial Protection Bureau* tem adotado parâmetros para a defesa desses direitos dentro do escopo da *Gramm-Leach-Bliley Act*, que diz respeito ao setor financeiro.

Fora do contexto industrial, a ***Federal Trade Commission* - FTC[65] assume papel de destaque na regulação e *enforcement* da privacidade**. A *Section 5* do *Federal Trade Commission Act* é a principal ferramenta utilizada pela instituição para garantir a privacidade dos cidadãos, já que a norma constitui em cláusula geral de proteção ao consumidor, proibindo atos ou práticas injustas (*unfair*) ou enganosas (*deceptive*) no ambiente consumerista.[66] Embora a mencionada norma não conceda à instituição poder de aplicar multas, permite que a Comissão **aplique medidas contra violações de suas regras**, e essas medidas comumente têm gerado ordenações administrativas que proíbem companhias de executarem novas condutas negligentes e possivelmente resultam em auditorias bianuais por um período de até 20 anos.

Ainda, a **FTC possui prerrogativas de investigação** sobre o cumprimento das normas dentro do escopo de sua atuação.[67] De forma geral, a Comissão instaura reclamação (*files a complaint*) quando possui motivos para entender (*reason to believe*) que um determinado

65 A *Federal Trade Commission* foi criada em 1914 com a assinatura do *Federal Trade Commission Act*. É agência governamental independente chefiada por cinco comissários nomeados pelo Presidente dos EUA - sendo a nomeação confirmada pelo Senado federal - para mandato de 7 anos. Seus objetivos primordiais são a proteção dos consumidores e garantia da competição no mercado. Mais informações em: https://www.ftc.gov/about-ftc/our-history; https://www.law.cornell.edu/uscode/text/15/41. Acesso em 28.08.2017.

66 "*Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful*" [15 U.S.C. § 45(a)].

67 Entre os fatores para iniciar tal processo estão reclamações de consumidores, pesquisas internas, recomendações de organizações da sociedade civil e do setor privado, notícias publicadas na mídia, e prioridades de políticas públicas. Mais informações em: http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/Estados-Unidos-Anexos.pdf. Acesso em 28.08.2017.

indivíduo esteja se utilizando de (i) método injusto de competição ou (ii) ato ou prática injusto ou enganoso. Em seguida, o juízo administrativo (*administrative law judge - ALJ*) recebe e analisa o pleito, sendo que as partes podem apelar da decisão para a composição total da Comissão. Esse processo pode resultar em ordem de cessação de conduta (*cease-and-desist order*), a qual a FTC pode fazer cumprir através de liminar (*injunction*) ou pedido de penalidade civil (*civil penalties*) nas cortes federais.[68]

Nos âmbitos estaduais, procuradores-gerais também possuem competência para aplicar medidas de *enforcement* na ocorrência de atos ou práticas comerciais que sejam consideradas injustas ou enganosas, e também para tratar das violações definidas por leis estaduais de proteção à privacidade.

Além desse panorama institucional, podemos dizer que **nos Estados Unidos há consideráveis práticas de auto-regulação**. Tendo em vista as preocupações relativas à privacidade e ausência de regulamentação estatal específica, entidades privadas adotaram, por exemplo, políticas de privacidade e passaram a utilizar selos e outros mecanismos capazes de certificar que determinada companhia segue as políticas que adotaram.[69] Esse regime **coexiste com fragmentado regime de co-regulação** desempenhado pelas agências setoriais, através da implementação de medidas de *private enforcement*. Ou seja, há a imposição de sanções decorrentes do descumprimento de códigos de conduta, códigos de ética e cláusulas-tipo formuladas pelas próprias empresas e homologadas perante o órgão regulador.[70]

c) Uruguai

O Uruguai tem desempenhado papel de destaque na América Latina em relação à proteção de dados pessoais. Foi o segundo país da região a obter reconhecimento pela União Europeia de que promove adequada proteção de dados e foi o primeiro país não europeu a ratificar a Convenção 108 do Conselho Europeu.[71]

[68] Mais informações em https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/understanding_differences.html e https://www.law.cornell.edu/uscode/text/15/45. Acesso em 28.08.2017.

[69] BOWIE, Norman E.; JAMAL, Karim. **Privacy rights on the Internet**: Self-regulation or government regulation? Business Ethics Quarterly, Vol. 16, No. 3 (Jul., 2006), pp. 323-342. Disponível em: http://www.jstor.org/stable/3857919. Acesso em 26.08.2017. Em pesquisa realizada pelos autores (p. 332), dos 100 endereços eletrônicos de alto tráfego selecionados, 34 tinham um selo de certificação. Todos esses 34 *websites* e mais 63 (de um total de 66 *websites* que não possuem tal medida) disponibilizam política de privacidade.

[70] SOMBRA, Thiago. **A regulação da transferência internacional de dados**. JOTA, 06.07.2017. Disponível em https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-regulacao-da-transferencia-transnacional-de-dados-06072017. Acesso em 28.08.2017.

[71] A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares é o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Busca "garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida

A **proteção de dados pessoais no Uruguai é prevista constitucionalmente como direito humano** (art. 72) e encontra-se definida na Lei nº 18.331/2008 (*Ley de Protección de Datos Personales y Acción de Habeas Data* - LPDP).[72] Esse estatuto garante ao titular dos dados o direito de controlar o seu uso, estejam eles armazenados em meios físicos ou digitais. Assegura, inclusive, a possibilidade de ser apresentado *habeas data* a entidades públicas e privadas para exercer tal direito.[73]

O órgão competente para assegurar o cumprimento desse direito é a ***Unidad Reguladora y de Control de Datos Personales* - URCDP**, instituído pela LPDP como **órgão com autonomia técnica** vinculado à Agência de Desenvolvimento do Governo para Gestão Eletrônica (AGESIC).[74] A URCDP é vinculada ao orçamento da AGESIC[75] e possui **competências de normatização, fiscalização, cooperação, sancionamento e gestão da transferência internacional de dados**. A URCDP também emite opiniões (*dictámenes*)[76], elabora guias de boas práticas (*guías de ayuda*)[77], assessora o Poder Executivo e emite pareceres a pedido de outras entidades. Em relação às sanções, a LPDP garante à URCDP **poderes para aplicar sanções administrativas** como a observação, advertência, multa, suspensão e encerramento de base de dados, promovidas com apoio do Poder Judiciário.

A URCDP é dirigida por um **Conselho Executivo**, composto por três membros, sendo um o Diretor Executivo da AGESIC e dois membros nomeados pelo Poder Executivo, que devem possuir histórico pessoal, profissional e de conhecimento na temática. Essas especificidades buscam assegurar que os membros da autoridade possuam independência, eficiência, objetividade e imparcialidade no desempenho de suas funções (art. 31 da LPDP). Com exceção do Diretor Executivo da AGESIC, os outros membros têm mandato de quatro anos, podendo ser reconduzidos. Os diretores mantêm seus cargos até o fim de seus mandatos, salvo nos casos de remoção a cargo do Poder Executivo por inaptidão, omissão ou crime, observado o devido processo legal.

privada, face ao tratamento automatizado dos dados de caráter pessoal". Mais informações em: http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_5.12.8.html. Acesso em 31.08.2017.

72 A LPDP foi regulamentada pelo Decreto nº 414, de 2009.

73 GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**, p. 22. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 21.08.2017.

74 Em espanhol, *Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento*.

75 Anexo à resposta ao Ofício nº 259/2015/GAB-SAL-MJ (Processo nº. 08027.000032/2015-11). Informações recebidas da Embaixada do Brasil no Uruguai. p. 3. Disponível em: http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/22-Uruguai.pdf. Acesso em 30.08.2017.

76 Disponíveis em: https://www.datospersonales.gub.uy/inicio/Resoluciones+y+dictamenes/dictamenes/. Acesso em 30.08.2017.

77 Disponíveis em: https://www.datospersonales.gub.uy/inicio/publicaciones/Guias+de+ayuda/. Acesso em 30.08.2017.

Como estrutura de suporte ao Conselho Executivo, a LPDP estabeleceu a designação de um **Conselho Consultivo multissetorial**, composto por cinco membros, representantes do Poder Judiciário, do Ministério Público, da academia, do setor privado, e que possuam reconhecida trajetória na defesa e promoção dos direitos humanos. O Conselho Consultivo pode ser acionado pelo Conselho Executivo para analisar as matérias de sua competência, sendo obrigatória a sua consulta nos casos de exercício regulatório pelo Conselho Executivo.

Os responsáveis por banco de dados abarcados pela lei devem proceder ao registro obrigatório junto a URCDP.[78] Com base nesse registro, a URCDP cumpre com seu mandato de divulgar de maneira gratuita a qualquer indivíduo a existência de bancos de dados pessoais, suas finalidades e a identidade dos seus responsáveis. A LPDP define ainda que nenhum banco de dados pode ter finalidades que violem direitos humanos ou sejam contrárias às leis ou a moral pública.

Além disso, **podem ser registrados perante a URCDP os códigos de conduta** elaborados por associações e entidades representativas de responsáveis por bancos de dados de titularidade privada, desde que sejam considerados adequados à legislação pela URCDP.

2.2.3 Possibilidades regulatórias para a Autoridade Brasileira de Proteção de Dados Pessoais

Nesta seção, pretende-se propor alternativas de desenho institucional para a Autoridade de Proteção de Dados Pessoais a ser concebida no país. De início, serão apresentadas as provisões regulatórias trazidas por cada um dos Projetos de Lei sobre proteção de dados pessoais que tramitam atualmente no Congresso Nacional. Em seguida, serão feitos apontamentos sobre possíveis modelos regulação e as relacionadas formas de financiamento, composição e competências.

a) Modelos de regulação propostos pelos Projetos de Lei de proteção de dados pessoais

Como já mencionado acima, o Brasil não possui legislação específica para a proteção de dados pessoais, resultando na defesa difusa e setorial da privacidade de usuários de internet por diversos órgãos, como a ANATEL, o CADE, a SENACON, os Procons e o Ministério Público. No Congresso Nacional, tramitam atualmente três projetos de leis relacionados à proteção de dados pessoais, que objetivam regular a necessidade de consentimento para a coleta, tratamento e uso de dados, e estabelecer regras sobre o compartilhamento, exclusão e transferência de dados a terceiros nacionais ou no exterior.

[78] Conforme detalhado no Decreto nº 414/2009.

As alternativas regulatórias ao cenário da proteção de dados pessoais estabelecidas por cada uma das propostas serão descritas a seguir.[79]

O *Projeto de Lei nº 5.276/2016*, de iniciativa da Presidência da República, **prevê genericamente a criação de órgão competente** para adotar políticas de conscientização e garantia de proteção de dados pessoais, sem apresentar sua vinculação, composição e orçamento. Dentre suas competências estão a condução de auditoria nas práticas de tratamento de dados pessoais, promover ações de cooperação entre autoridade de proteção de dados pessoais e estabelecer normas complementares para as atividades de comunicação de dados pessoais. Determina também que as sanções aplicáveis a pessoas jurídicas pelo descumprimento das normas prescritas na proposta serão a imposição de multas; a publicização da infração; a anonimização, o bloqueio ou o cancelamento de dados pessoais; a suspensão de operação de tratamento de dados pessoais e a suspensão do funcionamento das operações com dados pessoais. A proposta em questão também **institui um Conselho Nacional de Proteção de Dados Pessoais**, com capacidades essencialmente consultivas e composto majoritariamente por representantes do governo, que significa poucos assentos para representantes da sociedade civil e da iniciativa privada. Aparentemente, o Conselho será vinculado ao Ministério da Justiça, que terá a competência para designar os representantes governamentais, que serão indicados pelos respectivos órgãos e entidades.

O *Projeto de Lei nº 330/2013*, de iniciativa do Senado Federal e emendado pela CMA (Comissão de Meio Ambiente, Defesa do Consumidor e Fiscalização e Controle), **prevê a existência de órgão que terá competências relacionadas à normatização, fiscalização e sanção relacionadas à coleta, tratamento e uso de dados pessoais**. Mais especificamente, o órgão terá competência para (i) regulamentar o disposto na proposta; (ii) autorizar e fiscalizar a transferência internacional de dados; (iii) tomar iniciativa diante de incidentes de segurança; e (iv) aplicar sanções ao descumprimento da lei. A proposta de lei não indica, contudo, o desenho, composição e orçamento dessa autoridade competente - e não poderia fazê-lo sob o risco de incorrer em inconstitucionalidade formal. No entanto, expressamente menciona a possibilidade de demais autoridades competentes atuarem na fiscalização e cumprimento das regras sobre privacidade e proteção de dados pessoais, de modo a criar sistema similar ao dos Estados Unidos, ou seja, sem homogeneidade institucional no cuidado de dados pessoais. Ainda, o projeto prevê a criação de mecanismos de participação do titular de dados em um programa de

[79] Corroboram para essa análise os relatórios da Artigo 19, intitulado **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional; e do Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI/USP), **Xeque-mate**: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. Disponíveis, respectivamente, em: http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf e https://gpopai.usp.br/wordpress/wp-content/uploads/2016/06/Xeque-Mate.pdf. Acesso em: 21.08.2017.

governança em privacidade criado pelo responsável do tratamento (conforme artigo 29, em especial o inciso I, "e").

Finalmente, o *Projeto de Lei nº 4.060/2012*, de autoria do Deputado Federal Milton Monti (PR/SP), **não prevê a existência de Autoridade Central** e reconhece a capacidade de "autoridades competentes" em editar normativos a respeito da proteção da privacidade. A proposta também prevê a **possibilidade de ser instituído Conselho de Auto-regulamentação** destinado a elaborar balizas para o tratamento de dados pessoais.

Em síntese, os Projetos de Lei nº 5.276/2016 e nº 330/2013 preveem a existência de órgão competente para lidar com a temática de dados pessoais, mas não especificam seus contornos institucionais. O Projeto de Lei nº 5.276/2016 prevê como competências do órgão a elaboração de diretrizes e a adoção de medidas para a garantia da proteção de dados pessoais, mas não lhe atribui expressamente a competência para aplicar as sanções prescritas. Também não descreve com precisão qual será a vinculação institucional ou fonte de recursos dos órgãos cuja instituição determina, embora haja indícios de que o Conselho pertencerá à estrutura do Ministério da Justiça. Igualmente, o Projeto de Lei do Senado nº 330/2013 apenas prescreve ao órgão a competência para normatizar e fiscalizar práticas relacionadas a dados pessoais da Internet, sem especificar seu desenho institucional e ainda prevendo competências compartilhadas com outros órgãos de governo. Finalmente, o Projeto de Lei nº 4.060/2012 não prevê órgão para a proteção de dados pessoais e confirma a possibilidade de ser instituída instância de auto-regulação.

Uma recomendação essencial com relação aos Projetos de Lei diz respeito à distinção de tratamento à questão da privacidade e proteção de dados pessoais no setor privado e no setor público. É essencial que essa distinção não prospere na Lei de Proteção aos Dados Pessoais que vier a ser aprovada no país. A proteção aos dados pessoais deve ser a mesma tanto para dados coletados no setor privado quanto no setor público, salvo hipóteses específicas[80]. A privacidade de dados no setor público é o pilar estruturante da construção de aplicações em cidades inteligentes, monitoramento de dados, coleta, tratamento e análise de quais dados obtidos pelo setor público. Nesse sentido, o setor público deve também se subordinar à lei e tratar os dados pessoais com as mesmas cautelas necessárias em face do direito à privacidade e vida privada. Uma proteção robusta à privacidade, tanto no setor privado quanto no público no que tange a dados pessoais, é a base para o desenvolvimento seguro, transparente, equilibrado e sustentável de aplicações da IoT.

b) Autoridade com modelo de co-regulação e alternativa imediata de auto-regulação

Nesta seção, discute-se o possível modelo regulatório e desenho institucional de uma Autoridade de Proteção de Dados Pessoais brasileira. O objetivo é discorrer brevemente sobre o estado da arte do debate e, em seguida, apresentar reflexões sobre as alternativas

[80] É o caso da coleta de dados pessoais para a prestação de serviços públicos essenciais, conforme melhor argumentado na sessão de privacidade em cidades.

apresentadas, com foco no tipo de modelo regulatório cabível e na sua subsequente forma de composição, financiamento e arranjo de competências.

Tendo em vista as considerações ora apresentadas, considera-se que **o modelo regulatório mais adequado para regulamentar e fiscalizar a privacidade na Internet consiste na instituição de autoridade central em modelo de co-regulação** e o incentivo de práticas transitórias de *auto-regulação*. Isto é, enquanto não aprovada legislação específica para a proteção de dados pessoais e instituída autoridade competente em modelo de co-regulação, deverão ser estimuladas iniciativas do setor privado que proponham códigos de conduta e regras setoriais para a proteção de dados pessoais na Internet.

Em relação ao estado atual da discussão sobre a Autoridade competente, os participantes das audiências públicas conduzidas na Câmara dos Deputados sobre proteção de dados pessoais apresentaram certa uniformidade em torno das características gerais[81] que devem guiar a criação da autoridade.[82] Em geral, mas com alguma divergência[83], considera-se que **deverá haver autoridade única, centralizada[84], permeável à participação de atores relevantes, composta por corpo técnico especializado e dotada de independência financeira e decisória**.[85] Há, todavia, vozes contrárias à instituição de nova autoridade, vez que já existe no país órgãos com competência normativa ou para fiscalizar a aplicação da legislação vigente.[86]

81 Entre tais características, estariam agilidade e flexibilidade, ou seja, capacidade de reagir a novas tecnologias e novos modelos de negócios); especialização técnica; estabilidade e visão de longo prazo; relacionamento cooperativo com setor privado, sociedade e o próprio governo; articulação institucional, com, por exemplo, autoridades em outros países e empresas multinacionais, tendo em vista a dimensão transnacional do mercado.

82 InternetLab, **O que está em jogo no debate sobre proteção de dados pessoais no Brasil?**, 2016, p. 18-19. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em 25.08.2017. Esse relatório teve como base as contribuições enviadas ao Ministério da Justiça por meio da plataforma "Pensando o Direito" durante todo o período da consulta pública do texto do Anteprojeto de Lei, que aconteceu entre os dias 28 de janeiro e 05 de julho de 2015.

83 Grupo de Pesquisa em Políticas Públicas para o Acesso da Universidade de São Paulo sugeriu que os Estados, o Distrito Federal e os Municípios deveriam ter o condão de criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa. Ibid., p. 24-25.

84 A Câmara BR argumenta que a criação de um único órgão responsável pelo assunto seria a forma mais eficiente de existir consistência nas interpretações e certeza regulatória. Ibid., p. 19.

85 Para acessar as contribuições dos atores sobre desenhos institucionais da autoridade de proteção na audiência pública realizada pela Câmara dos Deputados sobre os PLs nº 4.060/2012 e nº 5.276/2016 em 31.05.2017, ver: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-publicas. Acesso em 31.08.2017.

86 Ibid., p. 18-19.

Isto posto, a preocupação apresentada pelos participantes das audiências públicas seria exequível especialmente com os modelos de regulação e co-regulação[87], desde que o órgão instituído possua capacidade decisória, autonomia financeira e seja permeável e responsivo às demandas setoriais. Importante ressalvar que esse diagnóstico não afasta a coexistência de iniciativas auto-regulatórias, desde que observem a legislação vigente e os normativos editados pela autoridade competente.[88]

De todo modo, não se considera que a auto-regulação seria suficiente para devidamente normatizar e fiscalizar o respeito à privacidade na Internet, especialmente no médio e longo prazo. Isso porque **experiências de auto-regulação muitas vezes não são multissetoriais (*"multistakeholder"*)**, dependendo de adesão voluntária dos diversos atores. Ainda, as normas editadas por meio da auto-regulação não são cogentes e o órgão deterá limitadas capacidades sancionatórias.

No mesmo sentido, **modalidades puramente regulatórias não se mostram adequadas, tendo em vista sua excessiva impermeabilidade setorial, o que poderia acabar engessando não só o desenvolvimento de aplicações de internet, mas também os modelos de proteção aos dados pessoais e outros temas conexos**. Com efeito, os existentes órgãos governamentais brasileiros não se revelam hoje com as capacidades necessárias para atender satisfatoriamente à questão, carecendo ora de *know-how*, ora de capacidade organizacional, ora dos recursos necessários para atuar na regulação e fiscalização da proteção aos dados pessoais.

O presente contexto de corte de gasto também reduz a possibilidade de expandir capacidades governamentais já existentes ou de ser instituído novo órgão dentro da estrutura da Administração pública direta ou indireta, como seria com a expansão organizacional e técnica da Senacon ou com a criação de Agência Regulatória específica para a proteção de dados pessoais.[89]

Partindo desse cenário, o modelo de co-regulação mostra-se uma alternativa viável para tratar de questões de dados pessoais na Internet. Isso porque reduz o ônus financeiro e organizacional do Estado, compartilhando responsabilidades, e representa uma ferramenta capaz de combinar a flexibilidade da auto-regulação com o caráter cogente de normas governamentais. Em outras palavras, o modelo de co-regulação permite uma

87 Já que a questão da proteção de dados pessoais, por ser estipulada como direito fundamental na Constituição (inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, no art. 5º, X), pressuporia algum nível de envolvimento estatal.

88 Esse é o exemplo dos Estados Unidos, em que a regulação setorial editada pelas agências coexiste com mecanismos de auto-regulação.

89 Essa foi a proposta do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (CTS-FGV), que sugeriu a criação de uma autarquia ou um sistema nacional de proteção de dados pessoais. In: InternetLab, **O que está em jogo no debate sobre proteção de dados pessoais no Brasil?**, 2016, p. 20. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em 25.08.2017.

estrutura atrelada aos canais democráticos que informam a autoridade competente, ao mesmo tempo em que é capaz de lidar com debates técnicos complexos e com as necessidades do crescente mercado de uso intensivo de tecnologia, primordialmente transnacional e com forte assimetria de informações, sendo, portanto, visto com muito mais abertura pelo setor privado.[90]

A esse respeito, o Estado brasileiro possui interessantes experiências de co-regulação, exemplificada pela Câmara de Comercialização de Energia Elétrica (CCEE), no âmbito da regulamentação desse setor. A Câmara é pessoa jurídica de direito privado sem fins lucrativos instituída por lei e fiscalizada pela Agência Nacional de Energia Elétrica (ANEEL), com finalidade de viabilizar a comercialização de energia elétrica entre os atores do setor.[91] Composta por consumidores e agentes vinculados aos serviços e às instalações de energia elétrica, seu patrimônio é composto primordialmente por contribuição de seus agentes e eventuais doações. Assim, a CCEE é organização privada, custodiada por recursos privados, instituída mediante autorização legislativa e regulada e fiscalizada pela ANEEL. Além disso, possui competência para mediar transações em setor regulado e apresentar à Agência propostas de alteração das regras de procedimento de comercialização de energia elétrica.

De forma análoga, vale mencionar a experiência do NIC.br, que se configura também como associação privada, com a capacidade de regular o sistema de números e nomes de domínio na Internet do país. Essa organização é integralmente financiada por recursos próprios, gerados através do valor arrecadado com registros de domínio com a terminação ".br". Apesar de não atuar como órgão normativo, atua com capacidade consultiva em diversas instâncias, tendo inclusive recebido reconhecimento legal do Marco Civil da Internet, com respeito à sua contribuição para questões envolvendo exceções ao princípio da chamada neutralidade da rede.

Esses exemplos apontam para a viabilidade da criação de uma Autoridade de Proteção de Dados Pessoais em modelo de co-regulação. A seguir apresentamos outros exemplos institucionais que podem servir de modelo para sua implantação. Em primeiro lugar, é recomendável a **criação de uma autoridade <u>central</u> e <u>independente</u>, salvaguardada da possibilidade de captura por pressões políticas ou por um setor específico**.

Trata-se do caso, por exemplo, da Autoridade Europeia para a Proteção de Dados, já descrita em detalhes acima, que consiste em entidade central para garantir a privacidade

[90] Ibid., p. 441. Kamara (2017) afirma que a emergência de novas tecnologias cria a necessidade de se pensar modelos de auto e co-regulação, como a emissão de padrões técnicos para a proteção de dados pessoais. Contudo, observa-se que a auto-regulação é mecanismo limitado, pois, sendo flexível e dirigido pelo mercado, pode levar à promoção de interesses tão somente de grupos privados. In: KAMARA, Irene. **Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'**. European Journal of Law and Technology, Vol. 8, No. 1, 2017.

[91] Cf. Lei nº 10.848/2004, Decreto nº 5.177/2004 e Resolução Normativa nº 109/2004.

em todos os Estados-membros, dotada de capacidade para aconselhar as instituições da União Europeia e das autoridades nacionais, checar o cumprimento das normas e impulsionar processos investigatórios.

Em relação à sua composição, a autoridade deverá ser **dotada de corpo técnico** - não só no âmbito estritamente tecnológico, mas também jurídico, econômico e mercadológico. Isso se justifica pela sofisticação e rápida mudança das questões envolvidas e pelo fato de que uma regulação pulverizada, conduzida por autoridades distintas, permite a consolidação de ambiente regulatório e fiscalizatório inadequado e com altos custos de transação. Além disso, a entidade precisa contar com a velocidade de ação necessária para lidar com questões complexas e imediatas, como o vazamento de informações, ou ainda, situações de crise e ataques cibernéticos.

Hoje, a resposta a cenários como esses depende exclusivamente de instituições como o Poder Legislativo ou o Poder Judiciário, que não possuem a velocidade ou a capacidade técnica para lidar com um tema muitas vezes imediato e complexo.

Além da especialização para lidar com os distintos contornos da proteção da privacidade em aplicações de IoT, a autoridade deverá trabalhar com múltiplos setores, envolvendo representantes do governo, do setor empresarial e industrial, da comunidade científica, da sociedade civil, academia, dentre outros. A produção de normas envolvendo atores diversos atribui legitimidade e estimula o cumprimento voluntário e independente das normas geradas, independentes da possibilidade posterior de sancionamento. Aproxima-se desse modelo o desenho do Conselho Consultivo da URCDP e o Grupo de Trabalho instituído pelo art. 29 da Diretiva nº 95/46/CE do Parlamento Europeu, que possuem composição multissetorial e dão suporte à política de proteção de dados no Uruguai e na União Europeia. Nos Projeto de Lei em tramitação não há especificação sobre a composição da autoridade competente, havendo esse detalhamento apenas em referência ao Conselho Nacional de Proteção de Dados Pessoais (previsto no Projeto de Lei nº 5.276/2016). Todavia, a composição desse conselho participativo não pode ser denominada de *multistakeholder* porque seus membros seriam essencialmente representantes de órgãos governamentais (menos de metade dos membros são privados) e não há exigência de conhecimentos técnicos específicos para lidar com a proteção de dados pessoais. Em verdade, a composição tal como descrita resultaria em maioria de profissionais de carreiras jurídicas sem algum conhecimento técnico específico para lidar com questões tecnológicas.

No que concerne às **competências** da autoridade, elas variam especialmente em relação à capacidade de editar normas cogentes e à possibilidade de adotar atividades de fiscalização e *enforcement*. As propostas normativas ora em debate no Congresso Nacional preveem a possibilidade de a autoridade **editar normas complementares à legislação federal, realizar auditoria no tratamento de dados pessoais, promover ações de educação sobre proteção de dados, adotar providências quanto a incidentes de**

segurança, gerir a transferência de dados pessoais para o exterior e impor sanções diversas (como a advertência, imposição de multas e a suspensão de atividades).

Considera-se adequado o leque de competências prescritas nos Projetos de Lei, especialmente em virtude da capacidade para promover conscientização social, exercer fiscalização, impor sanções, emitir pareceres opinativos e editar normas relacionadas à proteção de dados pessoais e à publicização de bases de dados públicas.[92] A URCDP no Uruguai detém similares competências, atuando na normatização, fiscalização e sancionamento. O exercício dessas competências é acompanhado de exigência de cadastramento por parte de empresas que desenvolvem atividades de coleta, tratamento de transferência de dados pessoais. Adicionalmente, considera-se benéfica a **possibilidade dessa autoridade chancelar e verificar o cumprimento de normas ou códigos de conduta** elaborados em regime de auto-regulação, a exemplo das *binding corporate rules* na União Europeia. Competência adicional seria sua **atuação como *ombudsman***, com mecanismos para receber e investigar reclamações individuais contra a má-administração de dados pessoais por empresas e autoridades públicas. As atribuições do *Data Protection Officer* da Comissão Europeia possuem alguma similaridade com essa ideia, na medida em que coopera com as autoridades dos países membros da União Europeia, possui diálogo com titulares de dados coletados e mantém registro de operações conduzidas pela Comissão que envolvam dados pessoais.

Um ponto essencial é que a autoridade de proteção aos dados pessoais deve ter competências únicas e idênticas para tratar tanto da coleta, uso, tratamento e outras operações de dados realizados no setor privado e no setor público. Uma proteção robusta à privacidade é a base para o desenvolvimento de aplicações de cidades inteligentes, de governo aberto, bem como de quaisquer outros serviços governamentais que se utilizem de dados. Nesse sentido, o setor público também deverá observar e estar sujeito às diretrizes adotadas pela autoridade de proteção aos dados pessoas, salvo restritas exceções descritas no tópico de privacidade em cidades inteligentes deste Estudo. A Constituição Federal não faz qualquer distinção relacionada ao direito à privacidade e à vida privada no setor privado e no setor público, de modo que, do ponto de vista institucional, recomenda-se que a lei e a autoridade devem tratar a questão com isonomia, sem adotar distinções dependendo do setor que será objeto de análise.

Por fim, com relação às formas de **financiamento**, a solução mais simples seria a dotação orçamentária específica. Isso assegura regularidade organizacional, e consiste no modelo vigente atualmente na União Européia e nos Estados Unidos. De todo modo, há outras possibilidades. Por exemplo, algumas soluções mencionadas nas audiências públicas, tal como o modelo implantado na Espanha, em que a *Agencia Española de Protección de Datos*

92 Sugestão apresentada em audiência pública pelo Instituto de Tecnologia e Sociedade. Conforme será abordado neste relatório, há diversos pontos de tensão entre a proteção de dados pessoais e a publicização de bases de dados públicas.

(AEPD) é sustentada pelas multas por ele aplicadas.[93] Todavia, referido modelo possui o condão de estimular a imposição de multas com finalidades arrecadatórias sem a necessária observação de coerência decisória na imposição de sanções a práticas de coleta, tratamento e compartilhamento de dados pessoais.[94]

Outra solução para o financiamento da autoridade brasileira seria uma adaptação do mencionado modelo uruguaio, que exige o registro obrigatório de bancos de dados. Neste caso, o valor cobrado para a realização do registro poderá ser revertido para o financiamento da instituição. Contudo, existem algumas barreiras à consecução desse modelo de financiamento, entre elas, a necessidade de previsão legal expressa e a cobrança de adicionais, bem como a imposição de custos de transação adicionais para o setor, capazes de desestimular a realização do registro.[95] Dentre as possibilidades existentes também é possível o financiamento mediante contribuição de setores interessados. Nesse caso, uma crítica eventual seria a possiblidade de captura do órgão por parte dos agentes financiadores.

Em todo caso, independente do modelo final que venha a ser adotado, o benefício sistêmico da criação de uma autoridade unificada de proteção aos dados pessoais no país ultrapassaria e muito todo e qualquer custo incidente. A situação atual é de crescentes custos de transação e regulatórios relativos a esse tema. A incerteza atualmente gerada pelo vigente sistema legislativo em relação à proteção de dados pessoas e custos decorrentes dessa incerteza são, sem dúvidas, muito maiores do que o custeio de uma autoridade de proteção em qualquer um dos modelos descritos acima.

2.3 Segurança da Informação

Diante do desenvolvimento da Internet das Coisas no Brasil, da expansão de vulnerabilidades em redes e da natureza "sem fronteiras" de incidentes em segurança da informação, a discussão sobre medidas relacionadas à cibersegurança nos âmbitos do Poder Público e da iniciativa privada ganha destaque.

93 Em 2013, foram arrecadados 22 milhões de euros em multas pela agência, sendo seu custo de financiamento de 13 milhões de euros naquele ano. O excedente entre o custo de manutenção da agência e o total do valor arrecadado é direcionado para a Fazenda Pública. InternetLab, **O que está em jogo no debate sobre proteção de dados pessoais no Brasil?**, 2016, p. 23. Disponível em http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em 25.08.2017.

94 Sobre esse respeito, importante delinear a destinação das verbas provenientes das multas aplicadas pelo órgão, de modo a evitar sua destinação a fundos genéricos ou contingenciados.

95 Modelo semelhante ao uruguaio é o do Reino Unido, que exige o registro obrigatório de *data controllers*. O *Data Protection Act* de 1998 requer que qualquer organização processadora de informações pessoais realize registro junto ao *Information Commissioner's Office* (ICO), sob pena de configuração de infração penal. Disponível em: http://www.legislation.gov.uk/ukpga/1998/29/contents. Acesso em 3108.2017.

Discutem-se modelos de governança tanto para a cooperação internacional, quanto em relação ao arranjo institucional interno brasileiro. No âmbito local, faz-se necessário, ainda, encontrar alternativas para incentivar a adoção de medidas protetivas à segurança da informação pela iniciativa privada, seja pela adoção de mecanismos voluntários de certificação de dispositivos ou pelo respeito a critérios mínimos de segurança em infraestruturas críticas.

Um dos pontos em que se prevê a adoção de medidas concretas é a certificação voluntária sobre a segurança de dispositivos ligados à Internet das Coisas. A estruturação de sistema de certificação baseado na auto-avaliação voluntária, sem a imposição de obrigações legais aos aderentes, tem o potencial de criar cultura de transparência na prestação de informações ao usuário e incentivar a adoção de alto padrão de segurança pela iniciativa privada. Para viabilizá-lo, uma alternativa seria a criação de "aliança" por representantes da iniciativa privada, a qual poderia ser responsável pela organização estrutural e elaboração de diretrizes. Abaixo, apresentamos os encaminhamentos identificados.

2.3.1 Governança e cooperação internacional

Diante da natureza "sem fronteiras" de incidentes em segurança da informação e da expansão de vulnerabilidades em redes com o desenvolvimento da Internet das Coisas, discute-se atualmente a possibilidade de adoção de novo modelo de governança internacional no tema de cibersegurança.

Uma possibilidade ventilada é a possibilidade de a União Internacional das Telecomunicações ("UIT") liderar a discussão, possivelmente por meio de uma Cúpula Mundial de Cibersegurança. Esta possibilidade seria baseada no modelo instituído pela Cúpula Mundial da Sociedade da Informação, adotada em 2003 no âmbito da UIT.[96] O objetivo seria a criação de ambiente dedicado especificamente à segurança da informação entre países, com estrutura organizada para fomentar a cooperação internacional.

No entanto, entende-se que a UIT não é o foro apropriado para eventual medida, por não se tratar de foro multissetorial.[97] A tomada de decisões no âmbito da organização envolve de forma primordial Países-Membros e a iniciativa privada, sem a presença de uma

[96] Cabe notar o tópico da segurança da informação já consta na Declaração de Princípios no âmbito da Cúpula Mundial sobre a Sociedade da Informação em 2003. Ver Documentos da Cúpula Mundial sobre a Sociedade da Informação: Genebra 2003 e Túnis 2005 / International Telecommunication Union. São Paulo: Comitê Gestor da Internet no Brasil, 2014.

[97] Não obstante o criticismo à possibilidade de inclusão da agenda de segurança da informação em instrumento internacional pela UIT, a agência atua de forma positiva em diversos aspectos relacionados ao tema. O braço da agência responsável por padronização (ITU-T) já emitiu centenas de padrões técnicos em segurança da informação, o que se mostra positivo à iniciativa privada. Em paralelo, a UIT assiste a países em desenvolvimento na criação de Centros de Tratamento de Incidentes de Redes (CTIR). Ver https://www.itu.int/en/wcit-12/Documents/WCIT-background-brief6.pdf.

pluralidade de atores e setores da sociedade na discussão, requisito considerado essencial para a construção de políticas bem-sucedidas em segurança da informação. O Brasil defendeu essa posição no âmbito da Comissão Interamericana de Telecomunicações ("CITEL"), parte da Organização dos Estados Americanos ("OEA"). Na contribuição da CITEL à Conferência Mundial de Telecomunicações, sediada pela UIT em 2012 ("CWG-WCIT12"), o país defendeu que aspectos de segurança nacional e Cibercrime não sejam endereçados por regulações no âmbito da UIT.[98]

Não obstante as críticas em relação à possibilidade de incursão da UIT na temática, a discussão sobre a cooperação internacional entre países para proteção contra crimes cibernéticos é essencial no contexto da Internet das Coisas, para a garantia de ambiente seguro para o desenvolvimento e operação de soluções e aplicações. Para tanto, entende-se ser necessário aprimorar os mecanismos atuais para a prevenção e tratamento de incidentes entre países, o que será endereçado a seguir.[99]

O instrumento internacional de referência em vigor para a cooperação policial em segurança cibernética é a Convenção sobre Cibercrime de Budapeste ("Convenção sobre Cibercrime"), adotada em 2001 no âmbito do Conselho Europeu e ratificada por 52 países até o momento, com maioria composta por Países-Membros da União Europeia.[100] O instrumento estabelece padrões mínimos de proteção, a fim de permitir a obtenção de dados e meios de armazenamento de dados por autoridades estrangeiras. Embora o texto não defina como cada País-Membro deva legislar, define os atributos específicos que devem ser incluídos no escopo da legislação interna. No entanto, há entendimento de que a Convenção de Budapeste encontra-se em diversos aspectos ultrapassada por conta das mudanças tecnológicas desde sua aprovação. Mais do que isso, o instrumento não encontrou adesão maciça no cenário internacional, tendo sido ratificada por apenas 52 país.

O Brasil não aderiu à Convenção sobre Cibercrime.[101] Uma das razões é o fato do país não ter participado das negociações dessa convenção, o que vai de encontro à prática do país de apenas aderir a tratados internacionais dos quais tenha participado das negociações. Outra razão são as inúmeras críticas ao texto da Convenção em função do

98 Disponível em https://www.cept.org/Documents/com-itu/7628/.

99 European Union Agency for Network and Information Security (ENISA), 2015, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, v. 1.0.

100 Disponível em http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf.

101 O tema já foi objeto de questionamentos no âmbito da Câmara dos Deputados. Os requerimentos REQ 307/2013 CREDN (arquivado), RIC 3.464/2013 (arquivado), RIC 3.465/2013 (arquivado), solicitam informações sobre a adesão do Brasil à Convenção sobre Cibercrime. Em paralelo, os Projeto de Lei nº 3.175/2012 e 4.424/2008, preveem a alteração do Código Penal para harmonizar o ordenamento jurídico nacional com a Convenção.

descompasso resultante da evolução tecnológica posterior à sua adoção em 2001, como dito, e à falta de equilíbrio entre as medidas previstas para cooperação policial e o respeito a direitos fundamentais do indivíduo.[102] Se por um lado, a Convenção permitiria, em tese, maior consistência entre o ordenamento jurídico dos Países-Membros, mediante os critérios mínimos de proteção estabelecidos, essa harmonização chegaria hoje tardiamente. Isso porque alguns dos principais países-Membros, notadamente os países europeus, estão revendo seus normativos internos sobre cibersegurança e até mesmo revogando por completo regimes de retenção de dados correlacionados à Convenção, especialmente depois da decisão da Corte de Justiça Europeia que considerou como "inconstitucionais" em face dos normativos europeus as leis nacionais de retenção de dados.

Face ao cenário e às alternativas expostas, entendemos ter um efeito adverso qualquer movimentação no sentido de se aderir à Convenção sobre Cibercrime. Isso porque a adesão poderia representar possibilidade de conflito com o quadro legal brasileiro. Cita-se, de forma preliminar, a exigência de respeito aos direitos fundamentais do indivíduo pela Constituição Federal, como o direito à liberdade de expressão e privacidade.[103]

Um caminho mais recomendável para lidar com a questão da cibersegurança em IoT no plano internacional seria buscar outras formas de cooperação internacional, levando em consideração os esforços que vêm sendo feitos nesse sentido a partir de países como Estados Unidos, Canadá, Japão, China e Coreia.

Como alternativa à adesão à Convenção sobre Cibercrime para cooperação internacional, países podem se engajar de forma bilateral em Acordos de Troca e Proteção Mútua de Informações Classificadas, estratégia adotada pelo Brasil. Essa estratégia produziria efeitos mais eficazes do que aderência a uma Convenção que se mostra antiquada e pendente de atualização. Nesse sentido, o Brasil já possui uma série de acordos bilaterais em vigor, com países como China, Canadá, Cuba, México, França, Nigéria, Panamá, Suriname, EUA, Colômbia, Peru, Portugal, Espanha, Rússia, Itália, Israel, Reino Unido, Suécia.[104] A busca por novos acordos permitiria enriquecer o ordenamento jurídico

[102] A Convenção sobre Cibercrime influenciou, em grande medida, o Projeto de Lei nº 84/1999, proposto pelo Senador Eduardo Azeredo e rejeitado majoritariamente em suas principais propostas. O projeto de lei alçou amplo debate entre o público, incluindo petição online com dezenas de milhares de assinaturas contrárias à sua aprovação. O Congresso iniciou discussão no Poder Legislativo, culminando na conclusão de que um projeto de lei criminal não poderia ser considerado como a melhor opção para regular a internet no país.

[103] Constituição Federal de 1988, disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

[104] Para panorama dos Acordos de Troca e Proteção Mútua de Informações Classificadas, ver FORNAZARI JÚNIOR, M. PF em pauta – Cooperação jurídica internacional, disponível em https://jota.info/artigos/pf-em-pauta-cooperacao-juridica-internacional-17032016. Para detalhes sobre as diligências permitidas e os requisitos necessários para concessão, ver a Cartilha de Cooperação Jurídica Internacional em Matéria Penal, publicada pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça. Disponível em

interno, ao mesmo tempo em que asseguraria que o mesmo permaneceria *pari passu* com o que há de mais contemporâneo com relação ao arcabouço normativo de cibersegurança.

Tais acordos permitem, por exemplo, o auxílio direto ativo e passivo entre países e a troca de experiências institucionais e melhores práticas. Por exemplo, é possível expedir, durante investigação criminal ou ação penal, ordem de auxílio ativo, para que o Judiciário do país de destino avalie o mérito da solicitação de cooperação, de acordo com a sua legislação interna. Por sua vez, o auxílio passivo permite o caminho inverso, para que uma autoridade estrangeira envie demanda de cooperação às autoridades brasileiras.

Se comparada com a adesão à Convenção sobre Cibercrime, a celebração de Acordos de Troca e Proteção Mútua de Informações Classificadas traz benefícios, tais como a flexibilidade decorrente da opção de criar parcerias específicas com países em que há interesse, sofisticação e maior atualização possível quanto ao modelo de tratamento do ordenamento jurídico. É necessário ressaltar, entretanto, que a sistemática falha em corresponder ao fluxo transfronteiriço de dados. Em certos casos, não há certeza sobre quais informações podem ser obtidas por autoridades, com quem e em quais condições.[105] No contexto do desenvolvimento de soluções em IoT, ressalta-se que essa problemática pode ser potencializada. Uma das dificuldades previstas seria a identificação do provedor de aplicação responsável por uma solução IoT e, principalmente, a localização de sua base de dados, em razão do suposto aumento da complexidade no fluxo de dados entre os diversos atores envolvidos na prestação de uma solução.[106] No entanto, entendemos que uma revisão permanente do texto-base para esses acordos passa a ter um efeito positivo para todo o ordenamento, provocando, quando necessário, a atualização de acordos anteriores.

Outro caminho é facilitar a cooperação policial internacional, com respeito às garantias de direitos fundamentais estabelecidas pelo ordenamento jurídico nacional, estabelecendo novos instrumentos para tanto e revendo outros instrumentos atualmente em vigor. Por exemplo, deve ser incentivada a adoção de instrumentos internacionais que promovam incentivos à troca de informações estratégicas e o intercâmbio de recursos humanos entre agências de proteção à segurança da informação dos países, como sugere

http://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf.

105 Ver Access Now – Mutual Legal Assistance Treaties - Policy Analysis, disponível em http://mlat.info/policy-analysis.

106 Para ilustração dos desafios envolvidos obtenção de informações para pedidos de auxílio no ambiente digital, ver FORCE HILL, J. Problematic Alternatives: MLAT Reform for the Digital Age, Harvard Law School, National Security Journal, 2015. Disponível em http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/. Acesso em 9 de outubro de 2017.

o documento base da Estratégia Brasileira para a Transformação Digital, elaborado pelo Grupo de Trabalho Interministerial criado pela Portaria nº 842, de 17/02/2017.[107]

De forma complementar, sugerimos, também, o reforço da atuação brasileira com a atuação da OEA, como forma de fortalecer a cooperação regional e internacional em cibersegurança. A interface com a OEA é historicamente relevante para o desenvolvimento da política nacional em segurança da informação e cibersegurança. O Brasil já promulgou a Convenção Interamericana sobre Assistência Mútua em Matéria Penal por meio do Decreto Legislativo nº 272/2007.[108] No âmbito da organização, ainda, o Comitê Interamericano Contra o Terrorismo ("CICTE") desenvolve o Programa de Segurança Cibernética, com foco em segurança e infraestrutura crítica. O CICTE tem sido relevante para o amadurecimento do tema nos Países Membros da OEA, incluindo o Brasil.

Outro movimento importante é o acompanhamento efetivo do país nos processos de definição de standards internacionais, bem como de autorregulação ou de regulação híbrida com relação a temas de cibersegurança. Incentivar ou até mesmo exigir que fornecedores de equipamentos, software e outros insumos de IoT estejam certificados por organizações internacionais (como a IEEE, dentre outras) é um caminho efetivo, de baixo custo institucional e capaz de produzir resultados imediatos. Nesse sentido, a promoção e acompanhamento de processos de definição de standards e outras medidas de coordenação com respeito a esse tema é recomendável.

Além disso, há outro tema a ser considerado de ajuda recíproca e mesmo de fomento ao desenvolvimento internacional relacionado à questão da cibersegurança. A razão para isso é que países em desenvolvimento como o Brasil, acabam inevitavelmente por razões econômicas utilizando um grande volume de dispositivos conectados de baixo custo, que não atendem a padrões de segurança mínimos, ou que não encontram condições para sua manutenção e atualização em termos de segurança. O conjunto de dispositivos acaba então se convertendo em custos, disseminados na forma de externalidades negativas, como bem-representado por ataques de negação de serviço realizados através de botnets como a *Mirai* ou a *Persirai*. Nesse sentido, é do interesse da comunidade internacional e dos países que compõe a OCDE desenvolver mecanismos de fomento ao desenvolvimento, na forma de linhas de crédito, empréstimo, e outros fundos, capazes de incrementar as capacidades de países em desenvolvimento para lidarem com essas questões. Isso evitaria que os custos gerados por esses dispositivos conectados

[107] Disponível em http://www.mcti.gov.br/documents/10179/2100710/04.08+Estrat%C3%A9gia+Brasileira+para+Transforma%C3%A7%C3%A3o+Digital/cdbc34bf-e9d0-48ae-a8aa-aa4b4b4886af.

[108] Decreto Legislativo nº 272/2007, disponível em http://legis.senado.gov.br/legislacao/ListaTextoIntegral.action?id=235170&norma=256138.

implicassem risco para infraestruturas críticas situadas em outros países. Nesse sentido, nossa conclusão é que um dos componentes do fomento ao desenvolvimento internacional hoje deve ser o tema da cibersegurança. Investir agora nesse campo implica poupar grandes custos no futuro, tanto para países em desenvolvimento como para membros da OCDE.

2.3.2 Arranjo institucional brasileiro

Para o desenvolvimento de qualquer modelo de cibersegurança efetivo – e notadamente, de Internet das Coisas – é fundamental promover instituições cujo norte comum seja o multisetorialismo, isto é, a cooperação entre diversos setores como o Poder Público, setor privado, academia, comunidade técnica e científica, sociedade civil, dentre outros. A razão é que nenhuma política de cibersegurança será efetiva se apenas conduzida por um desses setores (ou por um deles majoritariamente). Para que a cibersegurança seja efetiva é necessário contar com mecanismos de resposta rápida que conjuguem a cooperação entre todos esses setores distintos.

Embora haja normas sobre segurança da informação em vigor atualmente no país, não é possível identificar uma governança definida entre estes atores, nem a existência de uma instituição que promova o multisetorialismo nessa área. Face a esse cenário, sugerimos que a definição de estratégia de segurança da informação no âmbito da Administração Pública Federal envolva a criação ou designação de órgão ou entidade que possa coordenar as atividades baseadas em segurança da informação. Esse órgão deverá ter o papel efetivo de "coordenador", no sentido de funcionar como um fórum (ou hub) para a atuação conjunta multissetorial. Há uma série de alternativas factíveis para a designação ou criação deste órgão, como será demonstrado a seguir.

De imediato, ressalta-se que o modelo de governança institucional sobre segurança da informação no Brasil poderia ser construído para ser eficaz a partir da necessidade de interação entre o Estado, iniciativa privada, academia e sociedade civil. Essa é uma recomendação tratada como pressuposto pela literatura especializada,[109] incluindo debates governamentais e de políticas públicas[110], e até mesmo contribuições recebidas

[109] Veja-se, como referência, KELLO, LUCAS. The Virtual Weapon and International Order. NEW HAVEN; LONDON, Yale University Press, 2017; TROPÍNA, T., CORMAC C. Self-and Co-regulation in Cybercrime, Cybersecurity and National Security. Heidelberg: Springer, 2015; WEBER, R. Governance of the Internet of Things – From Infancy to Frist Attempts of Implementation? Laws, v. 5, n. 3, p. 28, 2016.

[110] NETMundial, The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness, disponível em http://content.netmundial.br/contribution/the-importance-of-a-multistakeholder-approach-to-cybersecurity-effectiveness/180.

de atores do setor privada[111], ou ainda, autoridades públicas no exterior.[112] Em outras palavras, há evidências apontando na linha de que o caráter multissetorial atua no sentido de promover eficácia a qualquer instituição que trate do tema da cibersegurança.

Vale ressaltar que a iniciativa de criação de órgão específico no âmbito da Administração Pública Federal para lidar com o tema da segurança da informação deve ser originada da Presidência da República, conforme a regra de competência privativa estabelecida pela Constituição Federal.[113]

Dentre os modelos institucionais possíveis, está a criação de um conselho permanente multissetorial de segurança da informação, com a participação de membros do Poder Público, iniciativa privada, comunidade científica, sociedade civil e academia em sua composição. Do ponto de vista material, o conselho poderia atuar em caráter consultivo para a elaboração das políticas nacionais de cibersegurança e funcionar também como um "*hub*" de articulação, prevendo, por exemplo, a criação de mecanismos de resposta a incidentes em segurança da informação (*rapid response)*, sempre que necessário, valendo-se para isso da capacidade de articular os diversos setores da sociedade para alcançar o máximo de efetividade.

Este conselho deve ser composto por estrutura adequada para a proteção da segurança da informação, incluindo no contexto do desenvolvimento de IoT, e para a coordenação da cooperação entre os órgãos e entidades do Poder Público. Como exemplo, há a possibilidade de ele estar ligado a um Ministério específico, como o Ministério da Justiça, o que poderia habilitá-lo para atuar de forma técnica e transversal no âmbito da Administração Pública Federal. Além disso, no âmbito do Ministério da Justiça o conselho estaria integrado com a Polícia Federal, permitindo ampliar ainda mais a capacidade de resposta a incidentes de segurança que afetem a infraestrutura crítica do país, bem como conjugar as questões de cibersegurança como o combate aos cibercrimes. Essa estrutura não seria nova no âmbito do Ministério da Justiça já que este tem experiência na condução de comitês multissetoriais, como é o caso do Conselho Nacional de Combate à Pirataria, dentre outros, além da interface direta com o GSI/PR.

111 Ver a posição da Microsoft, disponível em https://blogs.microsoft.com/microsoftsecure/2017/06/07/nist-cybersecurity-framework-building-on-a-foundation-everyone-should-learn-from/.

112 No âmbito da União Europeia, a necessidade de criação de ambiente multissetorial está refletida na Estratégia de Cibersegurança, publicada em 2013. Ver Comissão Europeia, Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido, JOIN(2013) 1 final, disponível em http://www.dgpj.mj.pt/sections/informacao-e-eventos/2013/encontros-de-direito/downloadFile/attachedFile_3_f0/ESTRATEGIA_EUROPEIA_CIBERSEGURANCA.pdf?nocache=1400574470.82. A posição está alinhada com o Fórum Econômico Mundial, de acordo com o documento "Global Agenda Council on Cybersecurity", disponível em www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

113 O artigo 61, § 1º, inciso II, alínea e, da Constituição Federal de 1988 estabelece que é de iniciativa privativa do Presidente da República a lei que disponha sobre a criação de órgãos da administração pública.

Como pontos positivos deste modelo, está a abertura à participação colaborativa entre órgãos da Administração Pública Federal, iniciativa privada, sociedade civil e academia. O modelo pode criar impacto positivo na criação de um ambiente de confiança entre o Poder Público e a iniciativa privada, público e academia. Confiança essa essencial para tratar de temas de cibersegurança. Outro ponto positivo decorrente da proximidade com setores civis é a atuação complementar ao GSI/PR, que, por sua vez, tem como foco a defesa da informação no âmbito exclusivo da Administração Pública Federal. Esse caminho seria também recomendável pela desnecessidade de se ampliar ainda mais a máquina pública.

No futuro, caso seja viável, entendemos que outra possibilidade para gerir a segurança da informação no país no longo prazo seria a criação de agência reguladora independente especializada em segurança cibernética. A agência deve ser competente para atuar com a gestão de risco, prevenção de incidentes, programas de educação, cooperação internacional, bem como para elaborar diretrizes de boas práticas com foco na iniciativa privada, certificação de dispositivos e definição de critérios mínimos de segurança. O mesmo elemento de cooperação multissetorial deve estar presente também nesta eventual agência. Como benefícios deste arranjo, está a possibilidade de estabelecimento de cooperação com representantes da academia, sociedade civil e indústria, como forma de evitar que a atuação da agência gravite excessivamente em torno do Estado, ou do setor privado, configurando o fenômeno de "captura" da agência por seus próprios regulados ou outros grupos de interesses especiais.

Por sua vez, fazemos notar que a Política Nacional de Segurança da Informação, a ser lançada em 2017 e descrita no documento base da Estratégia Brasileira para a Transformação Digital, publicado pelo MCTIC prevê a criação de espinha dorsal por meio do GSI/PR, posição esta reforçada pela Estratégia de Segurança da Informação e Comunicações e da Segurança Cibernética da Administração Pública Federal do Brasil para 2015-2018.[114] Caso esse modelo venha a ser implementado, sugere-se que ele possua o mesmo grau de multissetorialismo de forma institucionalizada, conforme descrito acima. Isso permitirá maior eficácia nas políticas de cibersegurança, a criação de mecanismos de resposta rápida, melhor coordenação entre atores, fomentando assim um ambiente de confiança entre os diversos setores internamente.

114 BRASIL. Presidência da República. Gabinete de Segurança Institucional. Estratégia de Segurança da Informação e Comunicações e da Segurança Cibernética da Administração Pública Federal do Brasil para 2015-2018: versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília: Presidência da República, 2015 p. 47. "O estabelecimento de um modelo de Governança Sistêmica de SIC e SegCiber na APF, com a coordenação executiva, de acompanhamento e de avaliação do órgão central (GSI/PR), é essencial para a efetiva coordenação executiva das ações de Segurança da Informação e Comunicações e de Segurança Cibernética da APF, de modo a atender a transversalidade do tema, e contemplar ações multissetoriais que perpassem as competências dos órgãos da APF".

2.3.3 Incentivo à adoção de critérios para certificação de segurança dos diversos componentes de IoT

Do lado do usuário, seja um indivíduo ou mesmo empresa (*business-to-business*), umas das principais problemáticas relacionadas à adoção de dispositivos em IoT se refere à falta de informações a respeito das medidas de segurança e outras características funcionais dos dispositivos conectados. Em geral, há pouca clareza sobre os riscos à privacidade e segurança decorrentes do uso de um dispositivo, bem como sobre as práticas e cuidados do provedor da solução.[115] A partir da prestação de informações acessível sobre, por exemplo, criptografia e gestão de acesso, o consumidor final poderá realizar escolhas mais conscientes a respeito do dispositivo adquirido. De forma ilustrativa, deve haver medidas de conscientização que permitam ao consumidor evitar adquirir solução em IoT que possa, por exemplo, causar curto circuito, vazar dados pessoais ou permitir que seus dispositivos domésticos conectados sejam controlados por terceiro não autorizado.[116]

Do lado do desenvolvedor, um modelo de certificação criaria incentivo para que empresas aumentem seus padrões de segurança, prestem informações com transparência e invistam na criação de cultura de confiança.

Para possibilitar esse cenário, sugerimos a adoção de sistema de certificação voluntária, com a adoção de selos e sistemas de sinalização ("certificação voluntária"). O objetivo é a criação de mecanismo para a demonstração de prestação de informações e compromissos por parte de fornecedores e fabricantes para com boas-práticas.

De imediato, ressaltamos que não se propõe a substituição de obrigações de avaliação de conformidade compulsória aplicáveis a produtos, serviços e processos, como no âmbito do INMETRO ou da ANATEL. Pelo contrário, o que se sugere é a adoção de ferramenta adicional à avaliação de conformidade obrigatória pelo Estado, com foco em medidas de privacidade e segurança por desenho (*privacy* e *security by design*).

115 O uso de dispositivos em Internet das Coisas envolve uma série de riscos em segurança da informação, dado o cenário em que consumidores são alheios às particularidades técnicas dos dispositivos e, como consequência, aos riscos de segurança decorrentes. Alguns casos são paradigmáticos desse cenário. Para panorama abrangente, ver LEVERETT, É. CLAYTON, R. ANDERSON, R. "Standardisation and Certification of the 'Internet of Things" (2017), disponível em https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf.

116 Em caso paradigmático do impacto causado pela inobservância a critérios de segurança em dispositivos conectados à internet em 2016, objetos desprotegidos como câmeras de segurança, conversores de TV à cabo, roteadores, gravadores digitais de televisão e similares foram utilizados para ataque de negação de serviço. O tráfego de dados decorrente de milhões de objetos foi utilizado para atacar os servidores de empresa norte-americana. Os objetos utilizados pelo ataque compartilhavam das mesmas características: baixa proteção por criptografia, falta de proteção por senhas ou o uso de senhas padrão (como "admin, admin'). Para mais informações, ver SCHNEIER, Bruce. Lessons from the Dyn DDoS Attack. Disponível em https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

Em ambos os casos citados, exige-se a certificação de produtos que podem ser ligados à Internet das Coisas, sob pena de infração na hipótese de descumprimento. No âmbito do INMETRO, pode ser o caso de "brinquedos", "equipamentos para consumo de água" e "segurança de aparelhos domésticos e similares".[117] No plano da ANATEL, exige-se a certificação e homologação de produtos para telecomunicação.[118]

Como reflexo da medida, entendemos que a adoção de modelo de certificação voluntária poderia levar, ainda, ao incentivo ao compartilhamento de informações sobre vulnerabilidades, com o engajamento da academia e comunidade de pesquisa em segurança da informação.[119] Embora haja benefícios ao mercado como um todo no compartilhamento de informações sobre riscos e ataques conhecidos, o maior desafio continua sendo na dificuldade de compartilhar informações relevantes publicamente e na falta de incentivos para isso. Esse gargalo é ampliado pela ausência de um modelo pré-definido para o compartilhamento de informações.[120] Outro desafio é a falta de clareza à iniciativa privada sobre os benefícios decorrentes da partilha de informações sobre vulnerabilidades. Por fomentar a criação de ambiente de confiança, o modelo de certificação de dispositivos pode, como consequência, incentivar o compartilhamento de informações sobre vulnerabilidades por desenvolvedores de dispositivos IoT.

Como forma de instrumentalizar o procedimento de certificação, sinalização e indicação, sugere-se a criação de "aliança", formada por representantes relevantes da iniciativa privada engajados no desenvolvimento de dispositivos em IoT, em modelo de auto-regulamentação, baseado em consenso multissetorial.[121] Entendemos tratar-se do modelo

117 Como referência, a lista de produtos com certificação compulsória do INMETRO consta em http://www.inmetro.gov.br/qualidade/rtepac/compulsorios.asp. Já há, inclusive, a previsão de avaliação a dispositivos IoT por parte do INMETRO. O Regimento Interno do órgão estabelece como competência do Laboratório de Informática desenvolver programas de avaliação de software em Internet das Coisas. Portaria nº 2 de 4 de janeiro de 2017 do Ministério do Desenvolvimento, Indústria e Comércio Exterior (Regimento Interno do INMETRO), art. 84, disponível em https://www.diariodasleis.com.br/legislacao/federal/exibe_artigo.php?ifl=235081.

118 Resolução nº 242, de 30 de novembro de 2000, da ANATEL (Regulamento para Certificação e Homologação de Produtos para Telecomunicações), disponível em http://www.anatel.gov.br/legislacao/resolucoes/15-2000/129-resolucao-242.

119 Online Trust Alliance, 2017. Disponível em https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.

120 Cabe notar, ainda, segundo relatório publicado pela Agência Europeia de Segurança das Redes e da Informação, os modelos mais comuns para compartilhamento de informações em países da União Europeia e da Área Econômica Europeia envolvem auto e corregulação, em detrimento de legislação específica. Ver European Union Agency for Network and Information Security (ENISA), 2015, Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, p. 6.

121 Trata-se do modelo implementado na Alemanha, com o Conselho de Cibersegurança (Cyber-Security Council), criado em 2012. O órgão alemão inclui como participantes especialistas em cibersegurança e em políticas públicas, além de membros da iniciativa privada, dentre médias e grandes empresas e operadores de infraestrutura crítica. O Conselho é composto por Comitê Executivo, Presidente e Vice-Presidente. Mais informações em

mais vantajoso em um primeiro momento. Primeiro, a iniciativa privada opera parte significativa das soluções adotadas em IoT e detém *expertise*, razão pela qual qualquer iniciativa de certificação deve ser organizada em torno da indústria. Segundo, o modelo permite que os custos sejam internalizados pelos próprios atores, ao invés do Estado.[122]

Uma possibilidade é a adoção de modelo com dez grandes atores e vinte organizações de menor porte, envolvendo membros da iniciativa privada e academia.[123] Como ponto focal da iniciativa, entendemos ser possível considerar a designação da Câmara IoT, fórum ligado ao MCTIC, como ponto focal para estruturar a criação desta "aliança".

Caberia à "aliança" creditar laboratórios para realizar a avaliação de conformidade da certificação de produtos. Sugere-se que esta, na sequência, crie website dedicado para a certificação de dispositivos de IoT, bem como para a publicação de relatórios periódicos de informações relevantes, vulnerabilidades e respostas coordenadas.

Como exemplo relevante, vale mencionar a *Commercial Product Assurance* (CPA), autoridade britânica responsável pela certificação em segurança da informação, que disponibiliza relatórios e diretrizes por meio de seu website a qualquer interessado em atuar como entidade certificadora, bem como para o público em geral. Os relatórios podem delimitar os procedimentos para certificação, balizas para a operação e governança dos laboratórios, além de permitir maiores detalhes à população sobre as informações disponibilizadas em selos de certificação.[124]

É necessário ressaltar que não há modelo único de certificação, sinalização e indicação, mas uma miríade de possibilidades**. Dentre as alternativas possíveis, sugere-se o modelo "voluntário", sem a imposição de obrigações legais aos aderentes. Nele, a prestação de informações é iniciada pelo próprio desenvolvedor, não por obrigação legal**.

Seria importante que a iniciativa privada reconhecesse a certificação não como custo, mas como possibilidade de agregar valor a produtos, com engajamento à longo prazo. Isso passa pela conscientização dos consumidores, que, devidamente informados, poderão – a seu critério – dar preferência à aquisição de equipamentos certificados e com maior grau de segurança, o que poderia ser visto como um diferencial competitivo para o mercado. Nesse sentido, o modelo de certificação guarda paralelo com iniciativas relevantes de conscientização, em particular o mecanismo de compartilhamento de

http://www.cybersicherheitsrat.de/english/about-us/.

122 HATMANN, I. A. A Autorregulação pelo Código: Características, Impacto e Limites de um Novo Modelo. In: LEAL, F. (coord.) Direito privado em perspectiva: teoria, dogmática e economia – São Paulo: Malheiros, 2016.

123 BIHR, P 2017, *Trustmarks for IoT: ThingsCon Report,* encomendado pelo Open IoT Studio da Fundação Mozilla.

124 Disponível em https://www.ncsc.gov.uk/articles/become-cesg-approved-test-facility.Acesso em??

informações sobre incidentes em segurança da informação do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil ("CERT.br"), órgão que atua como ponto focal à iniciativa privada em caso de incidentes e ataques.[125]

Sugere-se modelo de auto-avaliação para a certificação de dispositivos. De acordo com este modelo, o próprio provedor do dispositivo submete as informações relevantes a respeito do equipamento ao órgão responsável pela certificação. Para garantir credibilidade, sugere-se que os interessados submetam uma auto-avaliação às entidades credenciadas pela "aliança" formada, responsáveis por verificar as informações e conceder selo de certificação.[126]

O modelo de certificação implementado não pode representar barreira de entrada a atores menores no mercado ou refletir os interesses de atores específicos. Dessa forma, entendemos que o desenho do modelo de autorregulação denota flexibilidade para evitar o fechamento (*lock in*) a determinadas tecnologias. Uma possibilidade para evitar esse cenário é o foco na certificação de tecnologias não proprietárias ou a criação de perfis de certificação tecnologicamente neutros, ou seja, que não considerem tecnologia específica, mas apenas critérios mínimos de segurança.

Este arranjo deve, ainda, representar baixo custo a interessados, dada a necessidade de permitir que atores pequenos e produtos com curto ciclo de existência possam fazer parte do sistema. Em certas jurisdições, a certificação de dispositivo IoT pode chegar a 500.000 euros, como é o caso da certificação de medidores inteligentes de energia elétrica na União Europeia, por meio do método de credenciamento *Common Criteria* (CC).[127] Nesse contexto, o modelo voluntário de auto-avaliação permite agilidade e menor custo aos interessados em obter a certificação.

Ressaltamos que a adoção de estratégias de segurança da informação baseadas em autorregulação ("*bottom-up*"), em detrimento da regulação estatal, não é inédita. Pelo contrário, é iniciativa comum em outras jurisdições. Como destaca a organização

125 O CERT.br é o órgão responsável por atuar como centro para o tratamento de incidentes de segurança da informação no âmbito do Núcleo de Informação e Coordenação do Ponto BR ("NIC.br"). O órgão ainda publica relatórios periódicos, com o objetivo de promover uma cultura de conscientização sobre a importância de proteção cibernética e capacitação.

126 Online Trust Alliance, 2017. Disponível em https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.

127 Conforme Avaliação de Impacto (*Impact Assessment*) da Proposta de Regulação do Parlamento e Conselho Europeu sobre a ENISA, de 2017 e disponível em http://eur-lex.europa.eu/resource.html?uri=cellar:2413e286-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF, p. 24. O modelo Common Criteria é reconhecido pelos órgãos nacionais de certificação dos países signatários do instrumento internacional Common Criteria Recognition Arrangement ("CCRA").

DigitalEurope, o modelo é tendência em países como Reino Unido, Estados Unidos, Japão e Itália.[128]

Na União Europeia, cabe destacar a iniciativa de certificação Trusted-IoT, discutida como alternativa aos modelos regulados pelo bloco econômico.[129] Em outro modelo, a *Online Trust Alliance*, ligada à *Internet Society*, se dedica não apenas ao fomento da certificação de dispositivos em IoT, mas também à participação da elaboração de políticas públicas em segurança da informação.[130] Destaca-se, também, por seu caráter aberto e inovador, a iniciativa de certificação *#iotmark*, caracterizada pela transparência na elaboração dos critérios de certificação.[131]

Notamos que a certificação de dispositivo deve ser pautada pela transparência, não apenas no momento da criação de perfis de certificação, no âmbito da "aliança", mas também na disponibilização de informações sobre produtos ao consumidor final. Dentre as informações incluídas, ressalta-se a importância de temas como: (i) segurança do dispositivo, com informações sobre medidas de segurança adotadas e dados sobre funções e processamento; (ii) credenciais e possibilidades de acesso de usuários; (iii) conectividade; (iv) atualização remota de medidas de segurança.

O objetivo é reduzir a assimetria de informações entre o desenvolvedor da aplicação e o consumidor final, possivelmente desinformado das características técnicas do produto. Para tanto, sugerimos que a informação seja disponibilizada por meio de recursos visuais claros e de fácil compreensão para o consumidor, como por selo (*label*) ou marca de confiança (*trustmark*) ostentado no produto ou na embalagem. Nesse sentido, a

128 DigitalEurope, "DigitalEurope's views on Cybersecurity Certification and Labelling Schemes", 2017, disponível em http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2365&language=en-US&PortalId=0&TabId=353.

129 A Trusted-IoT Label não é ligada aos mecanismos de reconhecimento internacionais da União Europeia, como o mecanismo Common Criteria ou SOG-IS. Para mais informações, ver Comissão Europeia, "Digital Single Market – Digitising European Industry Questions and Answers", disponível em http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm.

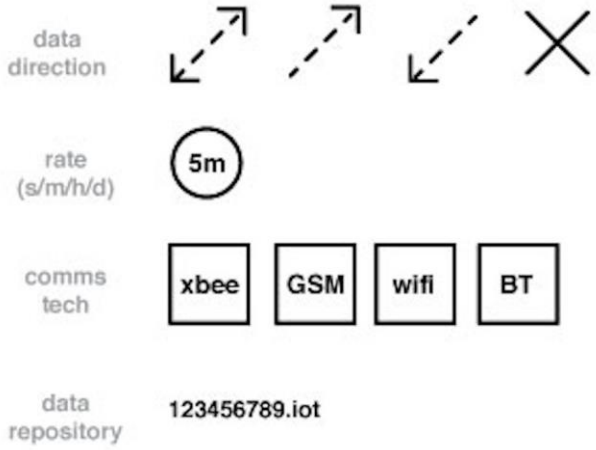
130 A Online Trust Alliance possui diretrizes e checklists em fácil acesso, por meio do website https://otalliance.org/HonorRoll. A atuação da entidade é descrita em detalhes no relatório "2017 Online Trust Audit & Honor Roll", disponível em https://otalliance.org/system/files/files/initiative/documents/2017trustaudit.pdf.

131 O texto-base elaborado pela *#iotmark*, bem como as notas e comentários dos participantes, está disponível para acesso em https://docs.google.com/document/d/1b_0Wz6pEM8282t8H4MMfBpfCBkxwNGYR1enJOTuolJ4/edit#. O texto estabelece cinco pilares para avaliação de segurança de dispositivos: (i) *backend* de sistemas (e.g., criptografia, resiliência à ataques, procedimentos para atualização de *software* e configuração de dispositivos); (ii) robustez para definição de senhas; (iii) especificações do dispositivo (e.g., tipos de *firmware* e mecanismos de criptografia utilizados, segurança no *setup* e controle de dados); (iv) especificações adicionais (e.g., opções de segurança do *hardware*, resiliência a ataques locais); (v) especificações comerciais (e.g., identificação clara sobre os meios de contato e ciclo de vida do dispositivo, política de privacidade, conformidade com legislação local em proteção de dados pessoais, testes de penetração de segurança, aviso sobre o uso de código aberto). Disponível em https://iotmark.wordpress.com/security/.

experiência pode seguir o precedente do Programa Brasileiro de Etiquetagem ("PBE"), coordenado pelo INMETRO e focado na prestação de informações sobre eficiência energética por meio de etiquetas ao consumidor final.[132]

A seguir apresentamos exemplos concretos, conforme desenvolvido por trabalho comissionado pela Fundação Mozilla:[133]

Modelo de selo para produto desenvolvido pela agência Designswarm, disponibiliza informações em nível básico sobre o tráfego de dados a partir do dispositivo IoT.

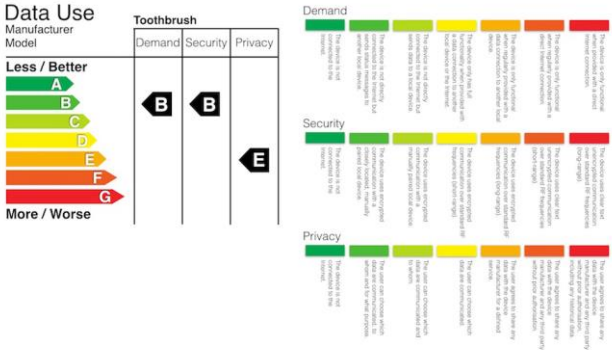


Modelo de selo para produto desenvolvido pela agência Beyond.io, disponibiliza informações básicas sobre o compartilhamento de dados pessoais coletados por solução IoT.

132 Disponível em http://www2.inmetro.gov.br/pbe/pdf/folder_pbe.pdf.

133 Disponível em Bihr, P 2017, *Trustmarks for IoT: ThingsCon Report*, commissioned by the Mozilla Foundation's Open IoT Studio, p. 67 – 71, 76.

Modelo de selo para produto desenvolvido por Boris Adryan, disponibiliza informações técnicas sobre consumo de dados, segurança e privacidade.



Modelo de selo para produto desenvolvido por Thorne & Bihr, disponibiliza informações básicas por meio de ícones sobre a coleta, armazenamento e o compartilhamento de dados pessoais por dispositivos.

Modelo de selo adotado pela iniciativa "Digital Standard", que visa criar padrão na indústria para a disponibilização de informações sobre as características de software e hardware do dispositivo, descrevendo indicadores e procedimentos de operação.[134]

Test Name	Criteria	Indicators	Procedure Overview
Security (Is it safe?)			
Build Quality			
Best Build Practices	The software was built and developed according to the industry's best practices for security.	The product was built with effectively implemented safety features.	Run static analysis software to determine what application armoring features are present. Are there Stack Guards, and if so, are they effectively implemented? Are all safety features available in the pertinent OS enabled? (e.g., ASLR, CFI, RELRO, DEP, etc.) Are those safety features well implemented and/or enabled with optimal settings? (E.g., High Entropy ASLR, rather than just Dynamic Base on Windows 10) Are the binaries 32 or 64 bit?

Em momento oportuno, com a consolidação do modelo de certificação voluntária, contudo, o arranjo de autorregulação poderia evoluir para corregulação ou regulação híbrida, com participação de um conselho multissetorial ou agência pública focada em segurança da informação, caso um destes órgãos seja, eventualmente, criado no âmbito do Poder Público. Nesse modelo, o órgão estatal pode confiar a certificação de dispositivos à iniciativa privada, mas mantém a possibilidade de determinar diretrizes e requisitos.

A atuação do conselho ou agência se daria, dessa forma, por meio da elaboração de diretrizes para a avaliação de conformidade de produtos e emissão de certificado e para o compartilhamento de informações sobre vulnerabilidades infra e intersetorial.[135] Outro

[134] Disponível em https://www.thedigitalstandard.org/the-standard.

[135] Há modelos bem estabelecidos de programas de compartilhamento de informações infra e inter-setoriais. Por um lado, como exemplo de modelos infra-setoriais, cita-se os programas específicos para energia (Distributed Energy Security Knowledge – DENSEK), transporte público (Transport Sector Information Exchange – TSIE), saúde (Zorg ISAC), serviços financeiros e bancários (European Financial Institutes – Information Sharing and Analysis Centre) e provimento de acesso à internet (UK Network Security Information Exchange). Por outro lado, modelos inter-setoriais

ponto da atuação do órgão público, em parceria com a iniciativa privada, academia e sociedade civil, é a adoção de medidas de estímulo para educação e conscientização sobre segurança da informação, como pela organização de *workshops* e a realização de programas de pesquisas e desenvolvimento. O órgão poderia, ainda, firmar acordos com agências estrangeiras, com a finalidade de simplificar procedimentos e compartilhar informações sobres riscos e vulnerabilidades.

2.3.4 Segurança da informação em infraestruturas críticas

Um dos aspectos importantes na temática da segurança da informação é o grau de segurança de infraestruturas consideradas críticas, como redes de saneamento básico e energia elétrica.[136] Isso porque, no contexto do desenvolvimento de IoT, há uma tendência de aumento da conectividade desses sistemas essenciais, o que aumenta, igualmente, a exigência de segurança da informação nestes setores, considerando o potencial impacto social causado por um possível ataque ou falha de segurança.

Já há atualmente no Brasil uma estrutura destinada à segurança de infraestruturas críticas. O Decreto nº 7.009/2009 tornou o tema uma atribuição da Câmara de Relações Exteriores e Defesa Nacional ("CREDEN"), presidida pelo Ministro-Chefe do GSI/PR.[137] Já no âmbito da Administração Pública Federal, o Departamento de Segurança da Informação e Comunicações ("DSIC"), também ligado ao GSI/PR, publicou o Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação ainda em 2010, que se mantém como referência para modelo institucional no tema.[138]

Sugere-se, desta forma, o fortalecimento da estrutura institucional dedicada à segurança de infraestruturas críticas no âmbito da Administração Pública Federal, com a manutenção do GSI/PR na coordenação de esforços e o estabelecimento de parcerias com centros técnicos especializados no tema. Há benefícios na estrutura atual, vide a competência já delimitada ao GSI/PR para a edição de normas sobre a segurança da Administração Pública. O objetivo imediato deve ser fomentar o compartilhamento já existente de informações sobre vulnerabilidades e experiências entre órgãos e entidades da Administração, bem como prestar assistência em caso de incidentes de segurança e

foram implementados em uma série de países, como Reino Unido (Cyber Security Coalition), Áustria (The Austrian Trust Circle), Alemanha (Cyber Threat Intellingente Sharing Reseach Project) e na União Europeia (Network and Information Security Platform e European Advanced Cyber Defense Centre).

136 Segundo a Portaria nº 2/2008 do GSI/PR, são infraestruturas críticas as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Destas, são infraestruturas críticas prioritárias as áreas de energia, água, transporte, telecomunicações e finanças. Disponível em http://contadores.cnt.br/legislacoes/portaria-gsipr-no-2-de-8-de-fevereiro-de-2008.html.

137 Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D7009.htm.

138 Disponível em http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf.

conscientizar servidores, como sugere o Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação do DSIC.

A atuação do CREDEN pode ser pautada por atividades de conscientização, com interação entre o GSI/PR com órgãos e entidades da APF (e.g., Ministérios), centros técnicos (e.g., CTIR Gov) e parcerias com a iniciativa privada e academia. Uma vez mais, a interface e coordenação entre os diversos setores, permitindo a comunicação e troca de informações permanente entre eles, mediada sempre de forma institucional, pode contribuir em muito na eficácia dessa política.

Em paralelo, CREDEN e GSI/PR, Ministérios responsáveis por setores específicos de infraestrutura crítica podem ser incumbidos da responsabilidade de elaboração de "guia de melhores práticas". Estas diretrizes devem servir de referência para a iniciativa privada e abordar metodologia para implementação de medidas de segurança e critérios de certificação. Os setores energético e de saneamento básico, em específico, são sintomáticos da necessidade de definição de critérios mínimos de segurança da informação a concessionárias.[139]

Em relação ao setor energético, nota-se que a geração, transmissão e distribuição de energia são, em larga medida, dependentes de sistemas de informação seguros.[140] Nota-se, entretanto, que não há definição de quadro de requisitos mínimos de segurança pela Agência Nacional de Energia Elétrica ("ANEEL") ou no âmbito do Operador Nacional do Sistema Elétrico ("ONS"). Como forma de mitigar vulnerabilidades no setor energético, sugere-se que a ANEEL crie *roadmap* para a prevenção de incidentes de segurança, detecção, reposta e gestão de crises. Sugere-se, ainda, a adoção de *framework* de segurança pela ANEEL, como forma de exigir o respeito a aspectos mínimos de segurança da informação por concessionárias, tais como a definição de arquitetura funcional de segurança, análise de riscos, definição de maturidade da rede e capacitação interna. Esses são passos mínimos e basilares para tratar da questão, sem prejuízo da adoção de outras medidas.

Sobre o setor de saneamento básico, por sua vez, há preocupação com ataques que permitam o acesso à infraestrutura, o que permitiria ofensivas como a modificação de sistemas de monitoramento e tratamento de água, afetando a prestação de serviço essencial. Em paralelo à adoção de sistemas informatizados deve haver emparelhamento

139 Para contexto sobre problemáticas de segurança no setor energético, ver FORMIGONI FILHO, José Reinaldo. Cibersegurança no Setor Elétrico: Ações internacionais e proposta para mitigar o problema no Brasil, 2016. Disponível em https://pt.slideshare.net/JoseynaldoFormigoniF/ciberseguranа-setor-eltrico-brasileiro-utcal-summit-2016-v3.

140 Para visão abrangente das vulnerabilidades envolvidas no setor elétrico, ver ANTUNES SOUZA, P. BRANQUINHO, M., KIEFER, SANTOS, C., VIDEIRA, E. Cyber Security para Sistemas de Automação de Energia – Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas, disponível em https://w3.siemens.com.br/home/br/automacao-energia/artigo-tec/Documents/Cyber-Security.pdf.

das estruturas de proteção à segurança da informação. Para tal, sugerimos a adoção de políticas de segurança da informação pelos titulares do serviço, como agências municiais.

Esse mesmo protocolo mínimo de definição de um *roadmap* e do apontamento de responsabilidades essenciais, atribuições, interfaces institucionais no âmbito do governo e com outros atores da sociedade deve ser repetido para todo e qualquer setor crítico do país, sem prejuízo de outras medidas a serem posteriormente adotadas.

2.3.5 Tecnologia blockchain para a certificação de dispositivos e garantia de identidade digital

Em adição às medidas já abordadas em segurança da informação na IoT, entendemos que um recurso promissor para salvaguardar a segurança de soluções e redes IoT pode estar no uso de tecnologia blockchain.

A blockchain pode ser visualizada, grosso modo, como um livro-razão público ou privado, com distribuição e permissão de acesso flexíveis e amplamente customizáveis. Cada evento é agregado na blockchain com identificação única por código *hash* criptografado, criando uma sequência "em blocos" que é imutável. Se qualquer intromissão ou fraude for detectada, não haverá "consenso" na rede, de forma que a violação de segurança será identificada.

Os benefícios possíveis para IoT decorrem de dois atributos fundamentais da tecnologia. Primeiro, a blockchain pode permitir a autenticação da identidade e origem de um dispositivo, indivíduo ou entidade ligado à IoT. Segundo, pode vir a asseverar a integridade dos dados coletados a partir dos dispositivos certificados.

A autenticação de eventos e objetos na blockchain é feita por meio de assinatura digital, usualmente constituída por um código *hash* criptografado, mediante o uso de certificação digital. Na prática, essa certificação digital possibilita a catalogação imutável de informações necessárias para a garantia da segurança da rede, como a identidade do objeto e do desenvolvedor, lista de atualizações de *software* disponíveis e as vulnerabilidades de segurança conhecidas.[141]

O mecanismo atribui "carimbo de hora" (*time stamp*) aos dados coletados por dispositivos e sensores autenticados, o que viabiliza a identificação de origem de qualquer inserção no livro-razão.[142] Como resultado, é possível reconhecer qualquer modificação da informação *após* a coleta, o que confere alto grau de transparência à rede, com redução

141 MANNING, J, Factom receives second DHS grant for blockchain IoT project. Disponível em https://www.ethnews.com/factom-receives-second-dhs-grant-for-blockchain-iot-project. Acesso em 27 de setembro de 2017.

142 SIGNORINI, M et al. Towards an internet of trust: issues and solutions for identification and authentication in the internet of things. 2015. Disponível em http://www.tdx.cat/bitstream/handle/10803/350029/tms.pdf?sequence=1. Acesso em 01 de outubro de 2017.

do risco de falsificações e intrusões. Nesse sentido, há iniciativas que permitem verificar a integridade de gravações em vídeo, obtidas a partir de câmeras de vigilância conectadas a uma rede. Cada gravação armazenada é ligada a um *hash* específico, imediatamente registrado no livro-razão da blockchain. Como resultado, qualquer tentativa de manipular o arquivo será em vão, já que o *hash* do arquivo modificado não encontrará paralelo com o *hash* registrado na blockchain.[143]

A certificação de dispositivos para garantia da segurança da rede é estudada e implementada em outras jurisdições. Nos EUA, o Departamento de Segurança Interna (*Department of Homeland Security)* financiou em 2016 uma prova de conceito de solução blockchain para a IoT, com foco justamente na detecção de componentes (i.e., a habilidade de associar dispositivos a uma determinada rede), autenticação (i.e., capacidade de verificar a origem de dispositivos e prevenir falsificações), e controle de atualizações (i.e., habilidade de controlar e programar *updates* de *software* de dispositivos).[144] Em outra prova de conceito relevante, o Departamento de Energia (*Department of Energy*), nos EUA, subsidiou solução para o uso de blockchain com o fim de segurar redes de *smart grids*, por meio da detecção automática de tentativas de invasão ao sistema e de anomalias nos dados coletados.[145]

A análise das possibilidades de uso da blockchain avança gradativamente no Brasil. Exemplos disso podem ser identificados nos estudos do BACEN e testes da FEBRABAN para utilização pelo setor bancário,[146] e no "*White Paper*" produzido pelo CPqD, analisando justamente as capacidades de verificação de autoria e auditoria que integram a blockchain.[147] Desse modo, notamos a formação de um crescente ecossistema técnico no Brasil capaz de implementar a tecnologia.

Para a consecução desse objetivo, há, entretanto, limitações na certificação digital unificada segundo o modelo de Infraestrutura de Chaves Públicas (ICP-Brasil), instituído pela Medida Provisória nº 2.201, de 27 de julho de 2001. A norma atrela a validade jurídica da declaração de autoria, autenticidade e integridade de documentos eletrônicos

143 GIPP, B; KOSTI, J; BREITINGER, C. Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain. MCIS. 2016. p. 51. Disponível em http://aisel.aisnet.org/mcis2016/51/. Acesso em 03 de outubro de 2017.

144 Departament of Homeland Security, DHS S&T Awards $199K to Austin Based Factom Inc. for Internet of Things Systems Security. Disponível em https://www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security. Acesso em 28 de setembro de 2017.

145 REESE, A. DoE Selects Guardtime to Develop Blockchain-Based Cybersecurity for Energy Grids. Disponível em https://www.ethnews.com/doe-selects-guardtime-to-develop-blockchain-based-cybersecurity-for-energy-grids. Acesso em 28 de setembro de 2017.

146 Disponível em: http://www.ciab.org.br/publicacoes/edicao/69/ciab-febraban-apresenta-testes-com-blockchain

147 CPqD, Blockchain Whitepaper, 2017. Disponível em https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf. Acesso em 27 de setembro de 2017.

à autenticação por meio dos certificados digitais emitidos de acordo com o padrão da ICP-Brasil.[148] O modelo padece de desafios práticos e estruturais, abordados a seguir.

Primeiro, certificados digitais são comercializados a alto custo, o que impossibilita a sua adoção pela maioria absoluta da população. Atualmente, um certificado digital custa entre R$ 180 a R$ 460 e é válido por 1 a 3 anos. Apenas cerca de 4 milhões de certificados foram emitidos até o momento, não obstante os mais de 16 anos de existência do sistema. O dado é sintomático: somente 1,3 milhão destes estão atrelados a pessoas físicas, o que corresponde a uma parcela mínima da população brasileira.[149]

Segundo, a chancela do Estado à estrutura ICP-Brasil cria reserva de mercado, em detrimento da inovação e de repercussões positivas, como o uso de blockchain para a certificação digital de objetos em IoT. Esse modelo vai contra as boas práticas internacionais, em que se permite maior flexibilidade na contratação de entidade certificadora e há menos risco de abusos e engessamento do mercado. Nesse sentido, entendemos que o mais coerente é o modelo no qual o mercado é mantido aberto, de modo em que a certificação pode ser feita tanto por entidades públicas ou pela iniciativa privada.

A blockchain pode ser utilizada para reverter esse cenário e democratizar o acesso à certificação digital, o que permitiria ganhos significativos em segurança da informação em IoT. A tecnologia pode servir para a criação de modelos de certificação digital independentes, mais baratos, confiáveis, auditáveis e transparentes, com segurança maior do que a certificação baseada no modelo ICP-Brasil.[150]

Por tais motivos, faz-se necessário, refletir sobre o aprimoramento do modelo ICP-Brasil implementado pela MP nº 2.200-1, de 27 de julho de 2001. O objetivo é possibilitar a criação de modelos em que qualquer interessado possa certificar dispositivos na IoT com confiabilidade jurídica, sem a necessária vinculação ao ICP-Brasil.

[148] O modelo permite alternativa de certificação digital ao processo adotado pela ICP-Brasil. Permite-se que outras entidades emitam seus próprios modelos de certificação, distintos do padrão ICP-Brasil, que produzirá efeitos legais desde que aceitos pelas partes envolvidas. Ocorre que essa alternativa possui eficácia limitada, já que só produz efeitos às partes em uma relação.

[149] Para visão geral, ver LEMOS, R. 'Certificação digital é futuro de serviços públicos, mas ainda é cara no Brasil'. Disponível em: www1.folha.uol.com.br/colunas/ronaldolemos/2017/07/1899775-certificacao-digital-e-futuro-de-servicos-publicos-mas-ainda-e-cara-no-brasil.shtml. Acesso em 02 de outubro de 2017.

[150] Para panorama dos benefícios da autenticação na blockchain, em detrimento do método unificado de infra-estrutura de chaves públicas, ver "Can Blockchain Save the Internet of Things?". Disponível em https://securityledger.com/2016/04/can-blockchain-save-the-internet-of-things/. Acesso em 28 de setembro de 2017. Para análise da redução de custos propiciada pela certificação de dispotivos IoT na blockchain, ver BALDI, M et al. 'Certificate Validation Through Public Ledgers and Blockchains'. ITASEC. 2017. p. 156-165, disponível em http://ceur-ws.org/Vol-1816/paper-16.pdf. Acesso em 02 de outubro de 2017.

Em um ambiente em que se espera a conexão de bilhões de dispositivos à IoT, com graus variados de observância a medidas de segurança, a abertura de caminho para novas tecnologias, como blockchain, poderá vir a permitir que fabricantes certifiquem e validem os seus dispositivos, autenticando objetos, indivíduos e entidades na IoT. A consequência seria o amadurecimento da segurança e proteção face a ataques e falsificações em de redes ligadas à IoT.

3 Análise dos ambientes priorizados

3.1 Cidades Inteligentes

3.1.1 Introdução

a) Noção de "cidades inteligentes"

Atualmente, mais de 50% da população mundial reside em cidades e projeta-se que em 2050 esse número será elevado para até 60%, sendo que o número de indivíduos vivendo nas áreas urbanas terá acréscimo de 2,5 bilhões.[151] É neste contexto de altos índices de urbanização que a introdução de soluções de IoT nas diversas modalidades apoiará substancialmente estratégias destinadas a tornar cada vez mais eficientes os serviços em centros urbanos.

A noção de *cidade inteligente* tem sido vinculada à utilização de novas tecnologias de informação e comunicação (TIC) para a otimização do planejamento e da gestão de políticas públicas no ambiente urbano. Ainda que seja considerado tema crucial nas discussões globais sobre desenvolvimento econômico e social, **não existe consenso sobre o seu conceito**, visto que a ideia de *cidade inteligente* é relativamente nova e se encontra em constante transformação. Isso porque experiências urbanas com serviços *inteligentes* seguem diferentes caminhos conforme os tipos de políticas, objetivos almejados e até mesmo formas de financiamento existentes em cada municipalidade.[152]

As definições mais restritivas de *cidades inteligentes* encontram-se focadas na instalação de sistemas de tecnologia da informação junto aos componentes de infraestrutura e serviços públicos de uma cidade, tornando-os conectados e passíveis de coletar e analisar diferentes tipos de dados. Definições mais amplas, por sua vez, entendem *cidades inteligentes* como aquelas nas quais investimentos em estruturas tecnológicas servem ao crescimento econômico sustentável.[153] Além disso, vale dizer que **o próprio emprego do termo *inteligente* é questionado** quando utilizado para referenciar as relações entre cidade e tecnologia. Argumenta-se que o uso de tal vocábulo levaria a um discurso

[151] Conforme o relatório *World Urbanization Prospects*, publicado pela Organização das Nações Unidas em 2014. Disponível em: https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.Pdf. Acesso em: 09.10.2017.

[152] Como apontado no relatório *Mapping smart cities in the EU*, publicado pelo Parlamento Europeu em 2014. Disponível em: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf. Acesso em: 09.10.2017.

[153] Nesse sentido, o relatório *Mapping smart cities in the EU* indica que "the concept of a Smart City can be viewed as recognising the growing and indeed critical importance of technologies (especially ICT) for improving a city's competitiveness, as well as ensuring a more sustainable future, across networks of people, businesses, technologies, infrastructures, consumption, energy and spaces" (p. 23).

tecnocrático, com a promoção da virtualização das relações interpessoais no ambiente urbano e a desconsideração das limitações inerentes às tecnologias.[154]

Todavia, não há dúvidas de que o **uso de tecnologias de comunicação e informação exercem papel relevante no processo de modernização dos sistemas urbanos**. Isso porque sua utilização possui o condão de aprimorar as relações entre governo, setor privado e cidadãos, por intermédio, por exemplo, do oferecimento de informações em tempo real sobre a circulação da frota de transporte público municipal ou para a aplicação de tarifas diferenciadas de energia elétrica quando da instalação de medidores inteligentes nas unidades residenciais. Assim, **o objetivo dos melhoramentos tecnológicos que descrevemos ao longo deste capítulo do Estudo está relacionado com a oferta de melhores serviços às pessoas que residem nas zonas urbanas**.

Ainda que TIC consista em componente essencial nesse percurso, *cidades inteligentes* não significam simplesmente a aparelhagem tecnológica das estruturas públicas, de modo que os **esforços de inovação por parte do Poder Público devem ter como ponto de partida o cidadão**.[155] Sendo assim, nas diferentes descrições regulatórias que descrevemos ao longo do trabalho indicamos preocupações concernentes aos usuários dos serviços públicos municipais, entre elas, a aproximação entre cidadãos e Administração pública por meio de maior transparência governamental[156]; e questões de privacidade e de segurança das informações geradas e armazenadas por dispositivos IoT.

Nesse cenário, dentre as possíveis compreensões do significado de *cidades inteligentes*, há um sem número de áreas que poderiam ser incrementadas pela utilização de tecnologia IoT. A título de exemplo, têm-se projetos que visam:

- A melhoria na **governança de instituições**, que conta também com ações de abertura de dados públicos e educação cidadã destinada a capacitar ainda mais indivíduos para a leitura e análise dos dados disponibilizados, além de mecanismos de participação popular na gestão pública;

[154] Para uma análise entre a interligação entre o conceito de cidades inteligentes e políticas públicas urbanas, ver: FERRAZ, Fábio. As cidades inteligentes devem ser reflexo de uma sociedade inteligente. **Nexo**, 22 ago. 2017. Disponível em: https://www.nexojornal.com.br/ensaio/2017/As-cidades-inteligentes-devem-ser-reflexo-de-uma-sociedade-inteligente?utm_campaign=a_nexo_2017823&utm_medium=email&utm_source=RD+Station. Acesso em: 09.10.2017.

[155] Tendo em vista o escopo do presente capítulo, consistente na avaliação do ambiente regulatório para que municipalidades possam implementar ou fomentar o desenvolvimento local de soluções de IoT, as análises serão centradas em iniciativas públicas ou na cooperação entre governo e iniciativa privada. Não obstante isso, deve-se ter em mente que soluções de IoT muitas vezes são idealizadas e implementadas exclusivamente por agentes privados.

[156] Argumenta-se, no relatório *Mapping smart cities in the EU* (p. 24), que a "inteligência" de uma cidade não pode ser dirigida apenas por controles centrais advindos de computadores do governo, que tentarão prever e guiar decisões dos cidadãos. Em verdade, cidades de fato inteligentes levarão em conta as contribuições de seus cidadãos, que poderão encontrar novas formas de interligar e imputar sentido aos dados e informações coletadas.

- A sustentabilidade e colaboração com a proteção ao **meio ambiente**, por meio da introdução de mecanismos automatizados de coleta de lixo e de produção de energia limpa;
- A implementação de sistema de redes de energia elétrica inteligentes (***smart grids***), capazes de reduzir perdas energéticas, aprimorar o direcionamento de investimentos na rede elétrica, diminuir tarifas cobradas de consumidores, dentre outros;
- A automação da rede de **fornecimento de água e de saneamento básico** que, tal como nas *smart grids*, viabiliza o incremento no sistema de medição e a redução de perdas comerciais e não comerciais; e
- E, ainda, aprimorar a experiência do cidadão no **trânsito e transporte público**, por meio de ações como a coleta e análise instantânea de dados sobre fluxo de veículos, bicicletas e pedestres.

b) Coleta de dados como ponto- chave das "cidades inteligentes".

Como se verifica pelos exemplos apresentados, a promoção uma cidade dita inteligente está intimamente relacionada à implementação de novas tecnologias pelo Poder Público. Isso porque, dentre os possíveis benefícios decorrentes da utilização de IoT em cidades, capazes de melhorar a qualidade de vida e a experiência dos cidadãos na cidade, diversos devem ser executados em parceria ou exclusivamente por órgão governamental. Mais que isso, determinados ambientes das cidades inteligentes são setores regulados e demandam da respectiva Agência ou órgão regulador estudos e modernização de normas setoriais destinadas a viabilizar a implementação de novas tecnologias na prestação do serviço público e a promover segurança aos gestores na adoção de inovadoras políticas.

Conforme se verá adiante, essa característica das cidades inteligentes levanta particular preocupação, visto que **a prestação de serviços públicos importa cada vez mais na coleta, armazenamento e compartilhamento de dados pessoais**. Como vastamente demonstrado nos produtos desse Estudo, a coleta e utilização de dados coletados por meio de tecnologia IoT promovem incontáveis benefícios para a prestação dos serviços pelas municipalidades. Esses dados podem ser coletados no âmbito de políticas locais,

mas também são de grande valia os dados coletados e disponibilizados por órgãos federais.[157-158]

Em razão disso, é **crucial a adoção de medidas capazes de inibir a utilização ilegal de dados e a vigilância do indivíduo por parte do Estado e agentes privados**. Dentre as medidas possíveis está a edição de legislação específica sobre proteção de dados pessoais e a implementação de autoridade de proteção de dados pessoais com competência para editar normativos e proferir opiniões orientadoras de gestores públicos e agentes privados sobre o tema.

Há também incertezas relacionadas ao armazenamento desses dados por órgãos públicos, relacionadas à segurança da informação e à regulação de serviços de computação em nuvem. No cenário atual, normativos federais regulamentam a contratação de serviços de TI pela Administração Pública Federal, estabelecendo qualificações mínimas para os contratados,[159] diretrizes de segurança da informação[160] e a necessidade serviços de comunicação de dados[161] serem prestados por órgãos ou entidades da administração pública federal.[162] Existem também normativos do Ministério do Planejamento (MPDG) e pelo Gabinete de Segurança Institucional[163] sobre contratação

[157] Pesquisa elaborada nos Estados Unidos aponta formas como os dados federais são relevantes para a elaboração e desenvolvimento de políticas em âmbito municipal: https://sunlightfoundation.com/cities-need-federal-data/. Acesso em 14.11.2017.

[158] Novamente, não se desconsidera a relevância da iniciativa privada para a idealização e implementação de soluções de IoT em Cidades Inteligentes. A restrição à análise de soluções implementadas diretamente pela administração pública ou em cooperação com a iniciativa privada se deve ao escopo do presente capítulo, consistente na análise do ambiente regulatório para que gestores municiapais fomentem ou implementem soluções de IoT.

[159] De acordo com o Decreto Federal nº 7.174/2010, o contratado deve possuir certificações emitidas por instituições públicas ou privadas credenciadas pelo Inmetro, que atestem, conforme regulamentação específica, a adequação dos seguintes requisitos: a) segurança para o usuário e instalações; b) compatibilidade eletromagnética; e c) consumo de energia. Além disso, a Portaria Interministerial nº 141/2014, exige ainda que os provedores privados de TI a) adotem os padrões definidos na arquitetura e-PING, b) usem criptografia para informações classificadas, c) usem ferramentas de controle de acesso e gerenciamento de identidade, e d) no caso de serviços de TI relacionados ao provimento de E-mail, usem ferramenta de prevenção de envio de mensagens em massa e de detecção de códigos maliciosos.

[160] O Gabinete de Segurança Institucional da Presidência da República publicou até essa data, 22 Normas Complementares sobre temas relacionados à segurança da informação na Administração Pública Federal.

[161] O Decreto Federal nº 8.135/2013 não define claramente os serviços de TI classificados como de "comunicação de dados", indicando uma interpretação ampla do conceito. A Portaria Interministerial nº 141/2014, que regulamentou o referido Decreto, indicou, de forma não exaustiva, os serviços abrangidos no conceito: "Art. 11. Para fins desta Portaria, serviços de tecnologia da informação abrangem os serviços de: I - correio eletrônico; II - compartilhamento e sincronização de arquivos; III - mensageria instantânea; IV - conferência (teleconferência, telepresença e webconferência); e V - comunicação de voz sobre protocolo de internet (VoIP)".

[162] Exigência estabelecida pelo Decreto Federal nº 8.135/2013. Essa regra possui como exceção a hipótese prevista no artigo 7º da Portaria Interministerial nº 141/2014, aplicável aos casos em que não houver oferta da prestação de serviços por órgãos ou entidades públicas fornecedores.

[163] Portaria MP/STI nº 20/2016 e Norma Complementar nº 14/IN01/DSIC/GSIPR. Citamos também o Acórdão nº 1739/2015 do Tribunal de Contas da União, que analisa o panorama de contratação de serviços de computação em nuvem na Administração Pública Federal e apresenta recomendações de boas práticas.

de serviços de nuvem, que estabelecem parâmetros de contratação e diretrizes de segurança da informação. Em especial, o normativo do MPDG estabelece a necessidade de dados e informações da Administração Pública Federal serem armazenados exclusivamente em território nacional.[164]

Assim, **há legislação mais detalhada sobre o tema apenas em relação à Administração Pública Federal, mas que não se estende a particulares ou aos órgãos públicos de outros poderes ou esferas federativas**. Tendo em vista essa lacuna de legislação e considerando que a execução de políticas públicas para cidades inteligentes é desenvolvida principalmente pelos Municípios, as regras para contratações da Administração Pública Federal poderão ser utilizadas pelas instâncias locais como modelo para as contratações de serviço de nuvem em aplicações de IoT.

c) Drones e cidades inteligentes.

Outra perspectiva no ambiente de cidades envolve a utilização de *drones*[165] para soluções de IoT e outras aplicações.[166] A comercialização e utilização dessas aeronaves no Brasil possui regras específicas definidas pela ANATEL[167], pela ANAC[168] e pelo DECEA.[169] Segundo os normativos pertinentes, a utilização segura de drones com peso máximo de decolagem acima de 250 gramas na área urbana requer, dentre outros: (a) a realização da

164 Conforme disposto no item 8 das "Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem" editadas pelo MPDG: "8. Os órgãos deverão exigir, por meio de cláusulas contratuais, em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, que os dados e informações do contratante residam exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem".

165 "Drone" é a expressão coloquial comumente utilizada para designar as "Aeronaves Remotamente Pilotadas" ou em inglês "*Remotely Piloted Aircraft*". Os órgãos técnicos utilizam a abreviação da designação em inglês como termo técnico para denominar drones: *RPA*. A designação técnica mais completa e adequada para designar todo o complexo (aeronave - RPA, Estação de Pilotagem Remota, o enlace de pilotagem e qualquer outro componente do projeto) é "*Remotely Piloted Aircraft System" (RPAS).*

166 A regulação referente ao cadastro, utilização e fiscalização de drones está mais detidamente abordada no capítulo referente ao ambiente rural.

167 Disponível em: http://www.anatel.gov.br/institucional/ultimas-noticiass/2-uncategorised/1485-drones-devem-ser-homologados-para-evitar-interferencias

168 Regulamento Brasileiro da Aviação Civil Especial – RBAC-E nº 94 (RBAC-E nº 94). Disponível em: http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@@display-file/arquivo_norma/RBACE94EMD00.pdf. Acesso em: 01.10.2017.

169 O DECEA é o órgão do Comando da Aeronáutica com competência para "planejar, gerenciar e controlar as atividades relacionadas ao controle do espaço aéreo, à proteção ao voo, ao serviço de busca e salvamento e às telecomunicações do Comando da Aeronáutica". Disponível em: http://www.decea.gov.br/drone/. São aplicáveis os seguintes normativos: Instrução Comando da Aeronáutica ("ICA") 100-40; Circular de Informações Aeronáuticas ("AIC") - N 17, AIC-N 23 e AIC-N 24.

operação com distância de pelo menos 30 metros horizontais em relação a edificações e instalações[170] e a pessoas não envolvidas e não anuentes com a operação;[171-172] b) a contratação de seguro com cobertura de danos a terceiros;[173] c) a não utilização de drones autônomos;[174] d) que cada piloto de *drone* opere apenas um equipamento por vez; e e) cumprir com os requisitos estabelecidos pelo DECEA para uso do espaço aéreo.[175] Especificamente em relação ao poder público, observados os requisitos regulamentares aplicáveis, há previsão expressa que afasta a necessidade de contratação de seguro com cobertura de danos a terceiros e a necessidade de cumprir com o requisito de distância mínima em face de terceiros.

Para além desses exemplos, é de suma importância que a operação de *drones* cumpra com todos os demais requisitos e obrigações aplicáveis a cada caso de utilização, conforme disposto nos normativos indicados.[176-177]

d) Escopo do presente capítulo.

Mais adiante, conforme mencionado nos demais produtos deste Estudo, a vastidão de possibilidades no tema tornou necessário ao consórcio restringir o objeto de estudo em cidades inteligentes para os seguintes casos, que serão mais detidamente abordados nos tópicos que seguem:

170 Essa distância pode ser flexibilizada com a anuência do proprietário do edifício ou instalação.

171 Exceção feita para os casos em que haja "uma barreira mecânica suficientemente forte para isolar e proteger as pessoas não envolvidas e não anuentes na eventualidade de um acidente".

172 Conforme será descrito a seguir, essa disposição não se aplica ao poder público.

173 Exceção feita aos drones pertencentes a entidades controladas pelo Estado.

174 A vedação a operações autônomas não implica uma vedação de voos totalmente automatizados, que podem ser feitos desde que haja a possibilidade de intervenção, a qualquer momento, do piloto remoto.

175 O DECEA, em seu site institucional, possui um exemplo simples da importância da observância das regras de uso do espaço aéreo por operadores de drones: "O operador de drone quer realizar um voo em área desabitada até 400ft AGL (aproximadamente 120 metros de altura). Pela ICA 100-4, que trata das operações de helicópteros, a altura mínima para voos de helicópteros em áreas desabitadas é de 200ft (aproximadamente 60 metros). Só por essa questão podemos perceber que o voo do drone sem coordenação poderá causar conflito no caso de um tráfego de helicóptero convergente com a área de voo, colocando em risco a operação do helicóptero". Disponível em: http://www.decea.gov.br/drone/. Acesso em: 01.10.2017.

176 O descumprimento da regulação incidente sobre o manusei de drones no ambiente de cidades poderá provocar consideráveis prejuízos, como a paralização das atividades de aeroporto por determinado período. Em novembro de 2017 o aeroporto de Congonhas, em São Paulo, cancelou as atividades de pouso de aeronaves por 2 horas, ocasionando o atraso de inúmeros voos. Sobre o tema, vide: https://oglobo.globo.com/brasil/falta-de-fiscalizacao-sobre-drones-coloca-em-risco-seguranca-de-avioes-dizem-especialistas-22067331 Acesso em 30.01.2018

177 Entre os responsáveis pela fiscalização da utilização de drones estão a ANAC, DECEA, ANATEL e os órgãos de segurança pública. Todavia, essa fiscalização tem sofrido dificuldades por fatores como a (i) dificuldade de individualizar o drone em situação irregular e identificar seu proprietário; ou (ii) falta de pessoal nos órgãos competentes para implementar as práticas necessárias a identificar a prática de ilicitudes.

- **Iluminação pública inteligente:** Utilização de sensores de monitoramento e de queima de lâmpadas para otimizar o uso e a substituição de ativos de iluminação pública;
- **Medidores inteligentes de energia elétrica:** Redução de custos operacionais de leitura de medidores e prevenção de roubos;
- **Controles tráfego e transporte público:** Uso de dados obtidos por meio de câmeras, celulares e sensores para monitorar o tráfego e otimizar a circulação de veículos, pedestres e bicicletas; e
- **Monitoramento de crime por vídeo/sensores:** Uso de circuito fechado de TV e sistema de monitoramento de áudio para viabilizar resposta e coordenação em tempo real, assim como *analytics* preditiva por meio de dados históricos.

Além disso, tendo em vista que o desenvolvimento de IoT no ambiente de cidades inteligentes envolve a contratação e implementação pela administração pública de dispositivos específicos, as possíveis formas de contratação de TIC também serão brevemente problematizadas.

Nesse sentido, para além desta introdução, e tendo em vista a delimitação realizada pelo consórcio, o estudo regulatório sobre cidades inteligentes apresentará o estado da arte e desafios legislativos sobre privacidade nas cidades e sobre cada uma das aplicações selecionadas (*e.g.* iluminação pública inteligente, energia elétrica inteligente, mobilidade e segurança pública), além de debate sobre formas de contratação pública de TIC.[178]

3.1.2 Privacidade em cidades inteligentes

A crescente utilização de dispositivos tecnológicos dispersos pelo espaço urbano, capazes de coletar dados sobre os cidadãos, monitorar suas atividades e até mesmo identificá-los, traz à tona diversas questões referentes à proteção da privacidade e dos dados pessoais dos indivíduos.[179] Para que o planejamento público das cidades inteligentes seja uma realidade bem-sucedida, é imprescindível que a privacidade dos cidadãos seja garantida primeiro na implementação das cidades inteligentes. Para tal, além de boas práticas de gestão a serem adotadas pelo Poder Público, que levem em conta as determinações da atual legislação difusa sobre o tema - em especial, pelo Marco Civil da Internet e o Decreto nº 8.771/2016 -, entendemos ser importante para a

[178] O presente estudo não teve como objetivo avaliar o mérito e resultados dos projetos referenciados. O escopo é realizar análise do ambiente regulatório para a implementação de IoT no ambiente das cidades, de modo que a referência a projetos conduzidos ou em andamento possui finalidade exclusivamente ilustrativa.

[179] Conforme o art. 14, I, do Decreto nº 8.771, de 2016, será qualificado como pessoal o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".

preservação de direitos fundamentais a aprovação de lei específica para a proteção de dados pessoais – como já destacado anteriormente.[180]

Levando em conta as diversas possibilidades de uso de dados pessoais em cidades inteligentes, descreveremos abaixo alguns dos principais desafios quanto à proteção da privacidade, atualmente potencializados pelo uso crescente de dispositivos IoT e, em seguida, indicaremos possíveis alternativas para minimizá-los.

a. Coleta de dados pessoais

Como primeiro passo da análise das obrigações legais em proteção de dados incidentes em soluções IoT em cidades inteligentes, é necessário identificar qual a expectativa de privacidade de cidadãos em ambientes públicos, como ruas, parques, praças e demais áreas abertas e em ambientes privados.[181]

Em relação a ambientes privados, a doutrina assume a aplicação integral da proteção legal à privacidade de forma inconteste, mediante a expectativa de controle integral por indivíduos sobre seus dados pessoais em locais privados.[182] Por sua vez, em relação a locais públicos, o debate possui diversas nuances.[183] Por um lado, parte da doutrina entende não haver expectativa razoável de privacidade do cidadão em espaços públicos.[184] Por outro, a posição mais garantista defende o respeito integral à privacidade também nestes ambientes. Como o cidadão deve poder determinar quais informações pessoais serão acessíveis a terceiros, e em que medida, há expectativa legítima de proteção e respeito à sua vida privada, ainda que em locais de acesso público.

A partir dessa premissa, a implementação de projetos ligados à Internet das Coisas em ambientes públicos situados em cidades inteligentes perpassa tanto cenários em que há coleta de dados considerados como "pessoais", já que identificam ou permitem a

180 A depender dos desdobramentos do tema, a jurisprudência também tem lançado mão de dispositivos do Código de Defesa do Consumidor, em especial, em casos de compartilhamento de bases de dados cadastrais sem consentimento prévio.

181 Uma primeira distinção se faz necessária entre espaços "públicos" e "privados". Para os fins desta análise, considera-se ambiente público como o local que pode ser acessado por qualquer membro do público, em qualquer tempo e circunstância.

182 A concepção de privacidade como o controle do indivíduo sobre suas informações pessoais é fundamental para a formação do direito à autodeterminação no contexto de proteção de dados pessoais.

183 The Constitution Project, Guidelines for Public Video Surveillance: a Guide to Protecting Communities and Preserving Civil Liberties. Disponível em https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf. Acesso em 16 de outubro de 2017, p. 24.

184 Para análise abrangente das posições doutrinárias e de casos seminais na jurisprudência sobre a expectativa de privacidade em ambientes públicos, ver MOREHAM, N.A. , Privacy in Public Places, 65 Cambridge Law Journal, 2006, p. 606-635.

identificação do titular de dados, quanto hipóteses nas quais as informações coletadas por dispositivos e sensores não permitem assinalar a identidade do cidadão. Esse é um caso clássico tratado na doutrina civilista com relação ao direito de imagem. Fotografias "da multidão", em que não é possível identificar nenhum dos indivíduos que a integram, são permissíveis. No entanto, fotografias que individualizem um indivíduo que caminha na rua da cidade não são permissíveis, exceto quando há conflito com outro interesse público bem definido (como é o caso de investigação criminal ou instrução processual penal, por exemplo).

No caso de soluções em que não há coleta de dados pessoais - como a "fotografia da multidão", onde os dados sejam anonimizados e agregados - seja pelo Poder Público ou pela iniciativa privada, a exigência de conformidade com o regime legal de proteção de dados pessoais é afastada. Nessas hipóteses, não há necessidade de se obter a autorização prévia do titular para a coleta, processamento, armazenamento e compartilhamento de dados, desde que haja uma anonimização e agregação efetiva dos dados coletados.

É o caso, por exemplo, de sensores voltados à obtenção de informações para fins de análise de mobilidade urbana, que monitoram a circulação e o comportamento de pedestres meramente por meio de mapas de calor. Nesse caso, não há identificação de cada indivíduo, mas apenas o registro das informações calorimétricas. Outras circunstâncias em que não há por princípio coleta de dados pessoais envolvem a coleta de dados técnicos objetivos, como dados como humidade do ar, índices de poluição, volume de ruídos, temperatura, pressão atmosférica, radiação, dentre outros.

Em outras situações, entretanto, soluções IoT em cidades inteligentes implicam a coleta de dados pessoais. Nesses casos, um rol distinto de normas e práticas aplica-se com relação ao setor público e ao setor privado.

Em cenário no qual é a iniciativa privada que implementa dispositivos de IoT, há a incidência integral das obrigações legais em vigor decorrentes do Marco Civil, Decreto nº 8.771/16 e outras normas setoriais. Como resultado, deve haver obtenção de consentimento válido para a coleta, tratamento, uso e transferência de dados pessoais, com a prestação de informações sobre a finalidade do tratamento, armazenamento e compartilhamento dos dados. A alternativa é que os dados sejam coletados de forma anonimizada e agregada, o que desconfiguraria sua natureza de dados pessoais. No entanto, nesses casos, é preciso haver segurança objetiva de que os dados não são passíveis de desanonimização, isto é, a possibilidade de que com o emprego de meios técnicos, ou ainda, o cruzamento daqueles dados com outros bancos de dados, eles possam então identificar indivíduos, voltando a se configurar como dados pessoais.

Por sua vez, em relação ao uso de dispositivos IoT em cidades inteligentes pelo Poder Público, o órgão ou entidade pública que colete dados pessoais deverá respeitar o quadro

legal de proteção de dados pessoais, salvo quando a coleta de dados seja necessária e inerente à prestação de serviço público essencial, em atenção ao interesse público.[185]

De imediato, nota-se que, no âmbito da prestação de serviços públicos, haverá muitos casos em que será necessária a identificação do titular de dados como requisito inerente à prestação de um serviço público essencial. Nesses casos, dada a essencialidade dos serviços, os cidadãos que dele se utilizam não possuem a possibilidade de "não utilizar" o serviço embarcado com soluções de IoT. Por exemplo, um morador de uma grande cidade como São Paulo não pode simplesmente "optar" por não usar o serviço de transporte público municipal, justamente porque depende do uso desse serviço para seu deslocamento cotidiano e, como resultado, para sua sobrevivência econômica. Nesses casos, mesmo que venha a "consentir" sobre a coleta de dados atrelada ao uso do serviço, esse consentimento não é livre, expresso e informado, haja vista a dependência do usuário para com aquele serviço. Nesses casos, há uma responsabilidade adicional do Poder Público, uma vez que o dado pessoal precisará ser coletado de qualquer forma, independentemente da manifestação de vontade do usuário do serviço público. Como visto acima, o dado poderá ser coletado, mas o Poder Público deverá assegurar a segurança daquele dado, bem como deverá se ater à finalidade específica para a qual o dado foi obtido, ficando vedada a transferência dos dados para terceiros alheios à prestação do serviço.

A dispensa da obrigação de obter o consentimento do titular sobre a coleta de dados pessoais para possibilitar a prestação de serviços públicos encontra paralelo em modelos implementados por jurisdições consideradas avançadas com relação à privacidade de cidadãos, como União Europeia e, no contexto Latino Americano, países como a Argentina e o Uruguai. O caso uruguaio é de interesse por se tratar de país em desenvolvimento inserido no mesmo contexto regional que o Brasil. O Uruguai permite o tratamento de dados pessoais pela Administração Pública sem a obtenção prévia de consentimento quando o processamento for necessário para a prestação de "funções de Estado"[186], tal como a prestação de serviços públicos essenciais, como visto acima. Em

185 A ressalva nesses casos é de que o dado coletado deve ser utilizado apenas para a finalidade em que foi obtido. Por exemplo, o Poder Público pode coletar dados pessoais necessários para a gestão de um sistema de bilhetagem eletrônica (como o "Bilhete Único" da cidade de São Paulo) no âmbito do transporte público municipal. Como esses dados são essenciais para a boa prestação do serviço, o consentimento ficaria dispensado. No entanto, os dados devem ser usados apenas para a finalidade específica de gestão do serviço e devem ser guardados com elevados níveis de segurança, não podendo ser cedidos a terceiros alheios à própria gestão do serviço. Outros dados que porventura possam vir a ser coletados que não são necessários para a prestação do serviço em si devem ser objeto de consentimento prévio, livre, expresso e informado por parte dos titulares dos dados.

186 O modelo é, ainda, implementado por jurisdições como o Uruguai. Segundo o guia "Manejo de datos personales em la Administración Pública", permite-se o tratamento de dados pela Administração Pública sem a obtenção prévia de consentimento pelo titular quando (i) o processamento for necessário para a prestação de "funções de Estado", e (ii) quando o dado pessoal for coletado mediante procedimento de anonimização, sem que haja identificação do titular. Disponível em http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-

relação à União Europeia, o Regulamento (EU) 2016/679 (Regulamento Geral sobre a Proteção de Dados ou *General Data Protection Regulation*), que entrará em vigor em maio de 2018, estabelece que órgãos e entidades públicas podem tratar dados pessoais coletados sem consentimento caso o processamento seja necessário, de acordo com o interesse público ou no exercício das atribuições da autoridade pública.[187]

Uma questão concreta é o uso de soluções IoT para o monitoramento por câmeras de vigilância, nas quais a identificação do cidadão está alinhada com a finalidade de garantir a segurança pública, a exemplo dos centros de monitoramento implementados no Rio de Janeiro e São Paulo.[188-189] Nesses casos, conforme expresso acima, justifica-se a coleta de dados sem a obtenção de consentimento prévio e expresso, com a condição de que a coleta desses dados pessoais seja utilizada estritamente para a finalidade a que se destina (garantia da segurança pública), seja necessária e proporcional e realizada apenas por autoridades que componham o sistema de segurança pública.[190]

Com base nas considerações feitas acima, fica claro que a responsabilidade por assegurar a privacidade dos cidadãos como primeira etapa da implementação de qualquer modalidade de cidade inteligente materializa-se no âmbito da União, dos Estados e dos Municípios. Nesse sentido, é necessário adotar legislação precisa que seja capaz de abranger todos os âmbitos da federação, garantindo a privacidade dos cidadãos (por meio de uma série de garantias, que incluem o princípio de legítimo interesse, da finalidade, da transparência, o direito de retificação, o princípio da necessidade e

d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756. Acesso em 26 de setembro de 2017.

187 Parlamento Europeu e Conselho, Regulamento (EU) 2016/679, de 27 de abril de 2016. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em 27 de setembro de 2017.

188 O projeto City Câmera, em São Paulo, tem o objetivo de instalar e permitir o monitoramento urbano a partir de mais de 10.000 câmeras de vigilância. Disponível em https://www.citycameras.prefeitura.sp.gov.br/howworks.Acesso em 22 de agosto de 2017.

189 No Rio de Janeiro, o Centro Integrado de Comando e Controle ("CICC") tem acesso à transmissão de mais de 3.000 câmeras de vigilância, utilizadas para segurança pública. Disponível em https://goo.gl/zpTeRc e http://www1.folha.uol.com.br/cotidiano/2013/05/1277131-bbb-da-favela-da-rocinha-monitora-moradores-24-horas.shtmlMARTINEZ-BALLESTÉ, Antoni; PÉREZ-MARTINEZ, Pablo; SOLANAS, Agosti. The Pursuit of Citizens' Privacy: a Privacy-Aware Smart City is Possible. Disponível em https://crises-deim.urv.cat/web/docs/publications/journals/794.pdf. Acesso em: 22 de agosto de 2017. A prefeitura do Rio de Janeiro possui um histórico de parceria com empresas de *big data*. À época das Olimpíadas, contratou com empresas de telefonia, como a TIM, para que essas fornecessem dados sobre a localização de seus clientes. Disponível em: http://www.inova.jor.br/2016/07/22/tim-big-data/. Acesso em 22 de agosto de 2017.

190 A sugestão reflete o mecanismo adotado para defesa nacional e segurança pública no modelo uruguaio. A Lei nº 18.331, de 18 de agosto de 2008, estabelece que o tratamento de dados para estes fins, por parte das forças armadas e órgãos policiais ou de inteligência é permitido, ainda que não prescindido do consentimento do titular, na medida em que os dados sejam necessários para o estrito cumprimento do objeto. Disponível em http://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/f085d1b8-0a24-4070-9dad-adc87b7595f2/18.331_con_modificaciones_de_la_19.355..pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=f085d1b8-0a24-4070-9dad-adc87b7595f2. Acesso em 26 de setembro de 2017.

proporcionalidade, dentre outros), autorizando a coleta de dados pela Administração Pública desde que circunscritos a finalidades específicas inerentes à prestação do serviço em questão. Vale lembrar que no plano da Constituição, a privacidade está definida no mesmo patamar que outros direitos fundamentais.

Para além do cenário descrito, o Poder Público pode também coletar dados pessoais por meio de soluções IoT em cidades inteligentes que não estejam ligadas à prestação de serviços públicos. Nessas hipóteses, é necessário autorização legal para tanto, bem como a aplicação do quadro legal usual da proteção de dados pessoais. Nesses casos, é necessário haver consentimento válido para a coleta por órgãos e entidades públicas, bem como autorização legal para a coleta, que determine os limites e finalidades para sua coleta.

Um outro problema é a Administração Pública receber dados que foram coletados por terceiros, tais como entidades privadas. Nesses casos, atenção especial deve ser dada à avaliação de conformidade (*compliance*) da recepção desses dados, bem como à cadeia de custódia dos mesmos e às autorizações inerentes para o seu uso, inclusive por parte da Administração Pública.

É o caso da solução de realidade aumentada implementada na cidade de Santander, Espanha, no contexto do projeto SmartSantander, com o fim de incentivar turismo e entretenimento.[191] A solução envolve a disponibilização de informações sobre pontos turísticos e experiências interativas e customizadas a cidadãos por meio de aplicativo *mobile*. A coleta de dados a partir de sensores distribuídos no município, inclusive com o uso de códigos QR, e o cruzamento de bases de dados entre a Prefeitura e a iniciativa privada permitiram apontar pontos de interesse ao usuário, enquanto a coleta de dados de geolocalização e a identificação dos hábitos de navegação do usuário permitem customização caso-a-caso, de acordo com o perfil do cidadão. Tais usos são bem-vindos, mas impõem a necessidade de cautela da parte do Administrador Público, que deverá verificar se a empresa que obteve os dados possui as necessárias autorizações para sua coleta, obtidas por meio de consentimento livre, expresso e informado, e se esse consentimento abrangeu também a transferência ou uso dos dados especificamente pelo Poder Público e para quais finalidades.

Outra questão relevante nas cidades inteligentes diz respeito à qualificação dos dados coletados ou obtidos, seja por soluções disponibilizadas pelo Poder Público, como pela iniciativa privada. Embora o Marco Civil e seu Decreto regulamentador não façam

191 Smart Santander, Evaluation report on potentials of IoT for enhancing cityservices, 2014. Disponível em http://www.smartsantander.eu/downloads/Deliverables/D4.3_%20Final_version.pdf. https://www.fed4fire.eu/fileadmin/documents/public_deliverables/D4-3_Report_on_first_cycle_developments_of_the_services_and_applications_communityFed4FIRE_318389.pdf. Acesso em 25 de setembro de 2017.

distinções entre os tipos de dados pessoais, os três Projetos de Lei em tramitação no Congresso Nacional sobre proteção de dados pessoais - PLs nº 5.276, de 2016, 330, de 2013 e 4.060, de 2012 -, distinguem "dados pessoais" de "dados pessoais sensíveis". Os últimos envolveriam, em geral, os dados pessoais sobre a origem racial ou étnica, convicções religiosas e políticas, além de dados referentes à saúde e à vida sexual. Tal distinção é de grande relevância, visto que a coleta do "dado pessoal sensível" deverá respeitar critérios mais rigorosos em relação ao consentimento obtido, como a prestação de informações prévias e específicas ao indivíduo e a manifestação própria para a coleta de dados sensíveis, caso um dentre os Projetos de Lei mencionados seja aprovado.[192]

Dessa forma, caso haja coleta de dados pessoais sensíveis por soluções em IoT em cidades inteligentes, tem-se cenário de maior complexidade em relação à coleta de consentimento válido, com aumento do risco de violação ao quadro legal em privacidade e proteção de dados. Um exemplo diz respeito ao reconhecimento facial, tecnologia cada vez mais disseminada. Estudo recente da universidade de Stanford demonstrou que é possível inferir um dado como a orientação sexual de um indivíduo (um dado considerado sensível por todas as principais legislações de privacidade globais) apenas analisando sua face.[193] O caso ilustra a problemática envolvida na coleta e uso de "dados pessoais sensíveis", que deve ser cercada por amplas cautelas, freios e contrapesos. Uma vez mais, uma legislação que permita assegurar os direitos constitucionais à privacidade dos cidadãos é fundamental e um passo prévio e necessário à implementação do uso de tecnologias que coletem "dados pessoais sensíveis", como o reconhecimento facial.[194]

Tendo em vista as problemáticas descritas em referência à coleta de dados pessoais no ambiente urbano, **aconselha-se, em primeiro lugar, que a coleta de dados pessoais por soluções IoT pelo Poder Público seja feita de forma anonimizada e agregada, por meio de critérios robustos de criptografia e emprego de práticas como privacidade diferencial, dentre outras**.[195] O objetivo é impossibilitar que as informações coletadas sem consentimento permitam a identificação de um usuário especificamente, com o fim de evitar a violação, por parte do Estado, dos princípios constitucionais de proteção à

192 Note-se que o Projeto de Lei nº 4.060/2012 traz critério mais brando para a coleta de dados pessoais sensíveis, quando comparado aos Projetos de Lei nº 5.276/2016 e nº 330/2013. Ele não considera dados genéticos ou biométricos como dados sensíveis, além de ser silente em relação aos critérios classificadores do consentimento válido.

193 KOSINSKI, Michal. WANG, Yilun. Deep neutral networks are more accurate than humans at detecting sexual orientation from facial images, Journal of Personality and Social Psychology. Disponível em https://osf.io/zn79k/. Acesso em 29 de agosto de 2017.

194 Nesses casos, o princípio da finalidade é também essencial. Um dado facial pode ser coletado para fins de segurança pública, mas jamais poderia ser tratador para analisar a orientação sexual do titular do dado, o que seria desnecessário, desproporcional e, tão importante, extrapolaria a finalidade que justifica a coleta do dado.

195 Como referência sobre mecanismos de criptografia, cabe menção a https://cartilha.cert.br/criptografia/ e https://cartilha.cert.br/mecanismos/. Acesso em 29 de agosto de 2017.

privacidade e à vida privada, bem como o disposto e normas infraconstitucionais como o Marco Civil da Internet (art. 7º, IX c/c arts. 10 e 11).

Em outras palavras, a coleta de dados deve ser pensada tendo sempre em mente o conceito de "privacidade por desenho" (*privacy by design*), isto é, o próprio desenho do serviço público deverá considerar desde o início de sua concepção a dimensão de proteção à privacidade. Nesse sentido, uma solução é que os dados sejam anonimizados e agregados desde o momento da sua coleta. Outras técnicas como o uso da chamada "privacidade diferencial" devem também ser empregados como forma de oferecer garantias técnicas ainda mais robustas para o indivíduo com relação a sua vida privada.

Como visto acima, para além da coleta de dados inerente e necessária à prestação de serviços públicos essenciais, órgãos e entidades públicas que desejam coletar dados que extrapolam a necessidades do serviço devem implementar mecanismos de obtenção do consentimento válido para a coleta desses dados, mediante a prestação de informações claras e específicas.

Nessa hipótese, como primeira possibilidade, poder-se-ia disponibilizar publicamente uma Política de Privacidade pública para cada solução IoT, com a criação de ferramenta *opt-in* em *website* ou aplicativo móvel, através da qual o usuário concorda com os termos propostos para a coleta de dados. Além do *opt-in* é fundamental o oferecimento também da ferramenta de *opt-out*, em que o indivíduo possa fazer cessar a qualquer momento a coleta ou tratamento de dados individualmente sobre ele. Nenhuma dessas soluções elide, no entanto, a necessidade que esses temas sejam regulados de forma ampla e geral por meio de lei. A própria política de privacidade do município pode ser definida por meio de lei municipal, na medida em que restrinja-se a matéria de "interesse local", como a organização institucional dos órgãos da Administração Pública em relação à proteção de dados de indivíduos.[196] Isso daria ao mesmo tempo a necessária proteção aos cidadãos, ao mesmo tempo em que autoriza o município a seguirem em frente na implementação de serviços inteligentes de IoT que coletam dados pessoais. Em suma, a proteção da privacidade e a autorização para implementação de serviços inteligente baseados em dados são "lados da mesma moeda".

A Política de Privacidade deve ser ainda publicamente acessível e capaz de informar com clareza aos cidadãos a respeito das práticas de coleta, anonimização, tratamento,

196 Compete privativamente à União legislar sobre matérias referentes ao direito civil (art. 22, I, Constituição Federal), o que inclui a temática de proteção de dados. Qualquer lei municipal sobre proteção de dados deve versar apenas sobre "assuntos de interesse local" (art. 30, I, Constituição Federal), de forma suplementar ao quadro legal federal, a fim de evitar inconstitucionalidade por vício de competência. Dessa forma, a lei municipal deve ater-se a tratar da matéria no âmbito institucional ou funcional da Administração Municipal. Para visão geral sobre o conceito de "interesse local", ver SILVA, José Afonso da. Comentário Contextual à Constituição, 9ª ed., São Paulo: ed. Malheiros, pp. 314-315.

armazenamento e compartilhamento de dados.[197] Especificamente, a Política de Privacidade deverá incluir necessariamente informações sobre: (i) o órgão da Administração responsável pelo tratamento dos dados coletados; (ii) qual informação é coletada; (iii) os fins para os quais as informações estão sendo coletadas; (v) de forma geral, quais os destinatários do compartilhamento das informações; (iv) como o titular pode se opor ou requerer a exclusão dos dados para fins de tratamento, processamento e outras atividades; (v) qual o meio de contato com a entidade pública responsável pelo tratamento dos dados.

Outra possibilidade é a prestação de informações por meio da identificação visual sobre a coleta de dados pessoais no local do sensor, com a disponibilização de meio de contato. Nota-se, entretanto, que o baixo grau de formalização da implementação de soluções IoT – sem que normalmente haja lei, norma infralegal ou instrumento de contratação pública formalizado – cria desafio na publicização de práticas de proteção de dados.[198]

Recomenda-se, ainda, que o Poder Público evite, por completo, coletar dados pessoais considerados "sensíveis". Caso uma lei geral específica para a proteção de dados pessoais seja aprovada, a coleta - ou a inferência -, desses dados representaria riscos exacerbados aos municípios, haja vista a mencionada dificuldade para a obtenção de consentimento prévio em cidades inteligentes.

b. Processamento de dados pessoais

No âmbito do processamento de dados pessoais, por sua vez, um dos problemas emergentes é o uso de dados para finalidade diversa da consentida pelo indivíduo.[199] Muito embora a coleta de dados pessoais possa permitir ao Poder Público obter padrões de consumo de água e eletricidade, tornar a segurança pública mais eficaz, ou até mesmo alavancar a transparência das ações governamentais e a aproximação entre os indivíduos e o Estado, é necessário que cada uso atenda especificamente à finalidade daquele serviço. Caso os dados sejam utilizados para outra finalidade que não aquela do serviço (ou informada ao cidadão quando do seu consentimento original), entende-se que seria necessário obter novo consentimento do cidadão ou a anonimização, agregação e utilização de técnicas como privacidade diferencial, sempre de forma tecnicamente segura e à prova de desanonimização.

197 Trata-se, por exemplo, do modelo adotado pela solução de WiFi (LinkNYC) da cidade de Nova Iorque, EUA. A Prefeitura disponibilizou Política de Privacidade em website dedicado à solução, com a descrição das práticas de coleta, uso, armazenamento, compartilhamento e exclusão de dados. Disponível em https://www.link.nyc/privacy-policy.html. Acesso em 22 de agosto de 2017.

198 PACHECO DA SILVA, A., CAMELO, A., LIGUORI FILHO, C., *et al*, *Um novo mundo de dados – relatório final*, GEPI – Grupo de Estudos em Pesquisa e Inovação (FGV), 2017, p. 38 - 40.

199 Pode ser o caso do uso de dados pessoais para investigação forense ou fins comerciais por parte do Poder Público, por exemplo.

Desta forma, como dito, para mitigar riscos de utilização dos dados coletados para finalidade diversa da informada, sugerimos a implementação de mecanismos técnicos baseados no princípio de *privacy by design*, segundo o qual o desenho da solução IoT já implementa mecanismos de proteção à privacidade desde sua concepção, como a utilização de privacidade diferencial e técnicas de anonimização, que podem protegem a privacidade dos usuários sem, entretanto, inviabilizar a possibilidade de utilização da base de dados para a prestação de serviços públicos.[200]

Além disso, o processamento de dados traz à tona a questão da vigilância do indivíduo por autoridades e órgãos públicos, sem que haja previsão legal expressa para tal. Engajamento e debate sobre os usos possíveis dos dados coletados pelo Poder Público são indispensáveis tanto para fomentar a transparência governamental quanto para evitar o mencionado "efeito panóptico", sob o qual o monitoramento sem controle supera os benefícios da obtenção de dados para a prestação de serviços públicos.[201]

Ao passo em que a Administração Pública disponibiliza vastas opções de soluções de IoT em diferentes segmentos, como na segurança pública, gestão de recursos hídricos e fornecimento de energia elétrica, outra preocupação emergente diz respeito à possível perda do controle sobre o fluxo de dados derivados dessas tecnologias pelo Poder Público. Faz-se necessária gestão apropriada dos dados coletados individualmente em cada solução em IoT, a fim de que a Administração tenha pleno controle das finalidades de processamento dos dados pessoais coletados.

Importante notar, por fim, que todo o uso de dados pelo Poder Público deve respeitar os princípios da legalidade e o interesse público. Em outras palavras, as finalidades para as quais o governo utiliza dados de seus cidadãos devem possuir previsão legal, ou seja, devem constituir finalidade lícita.

c. Armazenamento de dados pessoais

Quanto ao armazenamento, é recorrente a preocupação com a segurança tanto dos dispositivos tecnológicos utilizados nas soluções de IoT, pois estes são comumente compostos de *hardware* e *software* vulneráveis, quanto dos dados coletados. Sendo assim, fica patente a necessidade de adoção de medidas de privacidade e segurança da informação no armazenamento de dados pessoais.

Como forma de mitigar riscos, recomenda-se a adoção de medidas de *privacy by design* para o armazenamento de dados obtidos por soluções IoT em cidades inteligentes, bem como para o referido processamento e até mesmo compartilhamento de dados. Entre tais

[200] Os conceitos de privacidade diferencial e anonimização são tratados em detalhes no sub-tópico "Armazenamento de dados pessoais".

[201] NEWCOMBE, Tod. Santander: The smartest smart city. Disponível em http://www.governing.com/topics/urban/gov-santander-spain-smart-city.html. Acesso em 22 de agosto de 2017.

ferramentas, estão a já mencionada privacidade diferencial, agregação e anonimização de dados coletados por dispositivos IoT.[202]

A técnica de privacidade diferencial permite que o responsável pelo tratamento e armazenamento dos dados seja capaz de disponibilizar, de forma anonimizada, estatísticas e consultas a partir da base de dados original, que, contudo, permanece inalterada.

A anonimização, por sua vez, caracteriza-se por ser a forma mais rígida de proteção de dados pessoais. Através de "chave" criptográfica, os dados são anonimizados, e, por consequência, podem perder sua característica de "dados pessoais" e, desse modo, ser processados, armazenados e compartilhados sem risco de identificação de seus titulares. *O objetivo imediato é, portanto, assegurar que os dados armazenados não permitam a identificação dos cidadãos, escondendo de forma permanente informações que os individualizem.* Ainda, o uso de criptografia para a codificação de dados evitaria que atores mal-intencionados tenham acesso a informações coletadas por meio de soluções IoT, de forma a resguardar a identidade do titular de dados.

Há ainda outras medidas que podem ser implementadas para mitigar riscos no armazenamento de dados pessoais, como sua manutenção de forma "agregada" ou "agrupada". Essa técnica prescreve que os dados podem ser armazenados "em conjunto" com outros dados que se enquadrem em um mesmo critério.[203]

d. Compartilhamento dos dados pessoais

Outro aspecto central no debate sobre privacidade nas cidades inteligentes é o compartilhamento de dados coletados nas soluções desenvolvidas pelo Poder Público a outros órgãos da Administração Pública e autoridades policiais.

Ressaltamos, de imediato, que o próprio compartilhamento de bancos de dados por parte do Poder Público gera questionamentos. Podem os dados de mobilidade de um indivíduo ser utilizados para fins de segurança pública, sendo compartilhados com a polícia? É necessária uma ordem judicial para esse compartilhamento? Ou ainda, podem os dados dos cidadãos relativos a mobilidade serem utilizados pela fazenda pública municipal para fins de fiscalização de cobrança dos impostos sobre propriedade e sobre

[202] A Estônia tem histórico de armazenamento de dados sensíveis utilizando a tecnologia *blockchain*, sistema que também configura alternativa de interesse para a proteção de dados pessoais. No caso em questão, o país utiliza do mecanismo para registrar informações médicas dos cidadãos do país de forma segura. Disponível em: https://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers. Acesso em 22 de agosto de 2017.

[203] Ver Parecer nº 50/2014 sobre anonimização, do "Grupo de Trabalho de Proteção de Dados do Artigo 29", no âmbito da Comissão Europeia.
Disponível em http://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf, p. 18-19. Acesso em 27 de setembro de 2017.

serviços? Seria necessária ordem judicial prévia para esse fim? Em nosso entendimento a resposta é afirmativa. O Poder Público só pode efetuar o cruzamento de dados em que foram coletados para o fim de "*enforcement*" que vá além das finalidades para as quais o dado foi coletado se autorizado pelo Poder Judiciário. Esse é o corolário da proteção constitucional à privacidade. De outra forma, o indivíduo passaria a estar sob vigilância permanente, eliminando o princípio da presunção de inocência, o princípio da boa-fé, bem como desequilibrando a relação entre Estado e as liberdades públicas dos cidadãos. Em outras palavras, as cidades converter-se-iam em um "panóptico", no sentido da famosa prisão concebida por Jeremy Bentham, na qual os internos estão sujeitos à vigilância permanente em todos os seus atos, até mesmo os mais privados. A publicização das práticas de proteção de dados pela Administração Pública poderia resolver o desafio e prevenir esse problema no âmbito local.

Além disso, deve ser vedado ao Poder Público oferecer os dados coletados pela Administração Pública às entidades privadas, exceto em casos em que haja a obtenção do consentimento livre, expresso e informado dos cidadãos (sem detrimento de serviços públicos essenciais, como já abordado), ou, alternativamente, os dados sejam anonimizados de forma definitiva e segura, bem como agregados, sujeitos a técnicas como a privacidade diferencial, e mesmo assim, respeitados princípios gerais, como a questão da finalidade. Note-se que o mecanismo não impede que a Administração Pública utilize bancos de dados resultantes de soluções IoT em cidades inteligentes como fonte de recursos, mas exige que qualquer exploração comercial se atenha aos dados anonimizados, como por meio da elaboração de estatísticas e padrões.

Deve ainda haver a exigência de que o parceiro adote padrões elevados de proteção aos dados, vedado o compartilhamento com outros terceiros e também qualquer tentativa de desanonimização. Dessa forma, sempre que houver acesso por parte de terceiros a esses dados, mesmo que anonimizados, este deverá se comprometer a proteger aqueles dados com elevados padrões de segurança e a não os compartilhar com outros terceiros, ou a tentar empregar qualquer processo que vise obter a identidade do titular.

Ainda, a Administração Pública pode adotar medidas diligentes por meio da definição de critérios definidos na contratação pública de soluções em IoT.[204] É recomendado garantir que os parceiros observem exigências legais sobre dados pessoais, ofereçam nível mínimo de proteção gerencial e também adotem técnicas para a proteção de dados e segurança.

[204] Em contratações de serviço de computação em nuvem, por exemplo, a Administração Pública Federal faz uso de cláusulas que exigem do parceiro respeito a técnicas de segurança da informação. Cita-se o Termo de Referência publicado em 16/05/2017 para a contratação de serviço de infraestrutura como serviço (IaaS) e plataforma como serviço (PaaS): http://www.participa.br/contratacao-de-servicos-de-computacao-em-nuvem/servicos-de-computacao-em-nuvem-consulta-publica/consulta-publica-termo-de-referencia/termo-de-referencia-servicos-de-computacao-em-nuvem.

O Poder Público pode, ainda, exigir que seu parceiro empregue providências como disponibilizar aos seus usuários uma Política de Privacidade. Trata-se, de forma ilustrativa, ainda que desprendida da temática da Internet das Coisas, do programa "Wi-Fi Livre SP", conforme identificado pelo estudo "Um Novo Mundo de Dados", do GEPI-FGV.[205] O Apêndice I ao Edital (Termo de Referência) de contratação impede, ainda que timidamente, que o parceiro ceda ou compartilhe dados pessoais identificáveis de maneira individualizada.

Também é possível que as informações coletadas por soluções em IoT permitam a cooperação entre autoridades policiais, com compartilhamento de dados entre diferentes esferas. Não obstante os evidentes benefícios e as oportunidades criadas a partir da coleta de informações para a realização de investigações policiais, como já abordado, há grande preocupação sobre a possibilidade de acesso irrestrito dessas informações por autoridades policiais.[206] No compartilhamento de dados com outros órgãos públicos ou com autoridades investigativas, recomenda-se sempre a obtenção de ordem judicial prévia, nos termos do Marco Civil da Internet, que concretiza a proteção constitucional. Além disso, devem ser adotados limites, freios e contrapesos, respeito ao princípio da finalidade e níveis de proteção elevados pela autoridade recipiente do dado, após autorizada pela ordem judicial em questão. Para tal, pode ser medida eficaz a implementação de programas de capacitação gerencial e técnica dos servidores públicos da Administração direta e indireta e das autoridades policiais sobre as obrigações relacionadas à proteção de dados.[207]

Em síntese, sobre esse ponto, o Marco Civil da Internet estabelece ser necessária ordem judicial prévia para a disponibilização de dados pessoais de usuários de aplicação de internet, salvo nos casos nos casos previstos em Lei. Autoridades administrativas somente poderão ter acesso a informações pessoais de usuários independentemente de

205 PACHECO DA SILVA, A., CAMELO, A., LIGUORI FILHO, C., *et al*, *Um novo mundo de dados – relatório final*, GEPI – Grupo de Estudos em Pesquisa e Inovação (FGV), 2017, p. 46 - 47. De acordo com o item 7.2.1 do Termo de Referência, o "Parceiro somente poderá compartilhar informações de maneira genérica, ou seja, sem identificar quem são os usuários relacionados a tais informações, individualmente considerados".

206 Nesse ponto, cabe ressaltar o exemplo da prestação de informações pelo serviço de WiFi da Prefeitura de Nova York, nos Estados Unidos, que contará com cerca de dez mil quiosques de acesso distribuídos pela cidade. Embora não se trate solução em IoT, o serviço coleta dados pessoais, tais como as informações cadastrais e o histórico de navegação do usuário. Representantes do programa alegam que as informações coletadas somente podem ser acessadas pelo Departamento de Polícia mediante ordem judicial. Ver Política de Privacidade do programa LinkNYC em: https://www.link.nyc/privacy-policy.html. Mais informações sobre o programa e as possibilidades de acesso a dados pessoais por autoridades policiais em: https://www.fastcompany.com/3057980/privacy-concerns-raised-about-new-york-citys-free-wi-fi.

207 Essa prática já é adotada em determinados âmbitos da Administração Pública. Como exemplo, o Gabinete de Segurança Institucional - GSI editou a Instrução Normativa nº 1, de 13 de junho de 2008, na qual esboça diretrizes para a segurança da informação, entre elas, a implementação de programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações (art. 3º, IV).

autorização judicial quando expressamente previsto em Lei, como se dá em casos de investigação de crimes de lavagem ou ocultação de bens, direitos e valores (art. 17-B, da Lei nº 9.613/1998, "Lei de Lavagem de Dinheiro") e de organização criminosa (art. 14, § 3º da Lei nº 12.850/2013) ou nos termos da Lei de Acesso à Informação (Lei nº 12.527/2011 ou LAI), sempre respeitados os limites definidos por essas legislações e o princípio da necessidade e proporcionalidade.

e. Acesso aos dados coletados pelos titulares

Órgãos e entidades estão sujeitos ao dever de publicidade, previsto no art. 37 da Constituição Federal, e devem observar o regime de transparência disposto na Lei de Acesso à Informação. A LAI atribui a órgãos públicos a obrigação de fornecer aos cidadãos informações de interesse público, seja independente de solicitação (transparência ativa) ou após demanda apresentada por cidadão (transparência passiva).

A LAI inclui entre as informações de interesse público aquela "produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado". Exclui-se, entretanto, as informações de "cunho pessoal", referentes à pessoa natural identificada ou identificável. Estas informações serão de acesso restrito, sendo necessário consentimento para a sua disponibilização.

Como resultado, verifica-se que os dados que identifiquem ou permitam a identificação de cidadãos, coletados por órgãos e entidades públicas por meio de soluções em IoT em cidades inteligentes, não poderão ser acessados e divulgados publicamente, senão na ocasião de consentimento do titular do dado, quando esse consentimento for válido (como mencionado acima, o consentimento poderá não ser válido quando tomado no âmbito ou como requisito para a utilização de serviço público essencial).

Não obstante o cenário disposto pela Lei de Acesso à Informação, **recomendamos que o Poder Público disponibilize informações anonimizadas a respeito dos dados coletados por soluções IoT à população**. Esta prestação de informações pode ocorrer por meio de formulários estatísticos, sem que haja a possibilidade de identificação do titular de dados. É o caso, por exemplo, da iniciativa Open Data NY, lançada pela cidade de Nova Iorque, nos EUA e considerada líder no uso de *big data* para acesso à informação.[208] Por meio de website, o público pode ter acesso a dados catalogados a partir de mais de 1.400 fontes, sobre temas como educação, energia e meio ambiente, saúde, transporte público e segurança pública. As informações são prestadas de forma anonimizada, sem a identificação de indivíduos.

f. Mecanismos para a exclusão e retificação de dados pessoais

[208] Disponível em https://data.ny.gov. Acesso em 27 de setembro de 2017.

De acordo com o Marco Civil da Internet, garante-se ao titular de dados pessoais o direito de requerer a exclusão dos dados que tenha fornecido a alguma aplicação de internet, a seu requerimento, quando terminada a relação entre as partes ou quando os dados não sejam mais necessários para a consecução da finalidade indicada ao cidadão. Na ausência de legislação específica para a proteção de dados pessoais, entende-se que a disposição do Marco Civil se mantém também como a obrigação legal aplicável para a coleta de dados realizada por soluções IoT.

Face ao cenário de aplicação do Marco Civil para soluções IoT em cidades inteligentes, abre-se um leque de questionamentos, como qual a possibilidade de averiguação sobre o tempo de armazenamento do dado pelo Poder Público e como viabilizar o requerimento de exclusão de dados pelo titular.

Isso porque pode não haver, a partir das soluções IoT implementadas e das bases de dados criadas, ferramentas aptas a identificar quais dados pessoais devem ser excluídos, ou mesmo aptas a permitir a exclusão após requerimento do titular. Como problemática adicional, é possível vislumbrar cenário em que os dados pessoais coletados por sensores em cidades inteligentes são compartilhados com outros órgãos da Administração Pública, sem que haja controle de acesso apropriado.

Sugere-se, portanto, que o Poder Público estabeleça que os dados sejam excluídos após determinado período de tempo, inclusive com a manutenção de ferramenta que possibilite exclusão dos dados de forma automatizada. É o caso, por exemplo, do programa LinkNYC, nos quais as imagens coletadas por câmeras de monitoramento são excluídas após 7 dias, com exceção das imagens mantidas para a investigação de incidentes.[209]

Para garantir segurança jurídica de forma definitiva e evitar margens interpretativas, entendemos ser necessário aprovar lei geral específica para proteção de dados pessoais no Brasil, que verse sobre a questão da exclusão de dados coletados pelo Poder Público e traga definições sobre as obrigações que recaem ao órgãos e entidades da Administração Pública na exclusão de dados pessoais. Mais do que isso, entendemos como fundamental a definição e publicização de estratégias sobre o tema da privacidade por outros planos da federação, como estados e municípios.

3.1.3 Rede de energia elétrica inteligente

A lógica operativa do setor elétrico é tradicionalmente baseada em geração centralizada e em fluxo unidirecional de energia nas linhas de transmissão e nas redes de distribuição. Todavia, com a adoção de novas tecnologias, algumas das quais contam com

[209] Disponível em https://www.link.nyc/privacy-policy.html, item "Cameras". Acesso em 27 de setembro de 2017.

comunicação máquina-a-máquina, o **modelo de prestação desse serviço tem passado por significativas transformações** e permitem a composição das denominadas redes elétricas inteligentes (ou *smart grids*).[210]

As redes elétricas inteligentes distinguem-se do modelo clássico de distribuição de energia elétrica ao passo em que **incorporam à rede dispositivos tecnológicos de informação, medição e monitoramento**.[211] A introdução dessas novas tecnologias à infraestrutura da rede elétrica assegura, entre outros, a expansão da rede com serviços multidirecionais, a transmissão de dados em maior velocidade e quantidade, a utilização de mecanismos de medição inteligente e a integração do sistema de energia elétrica a outros serviços públicos.[212]

Assim, é possível indicar que as *smart grids* englobam, entre outros arranjos, estruturas de transmissão de energia controladas por sensores aptos a detectar flutuações e distúrbios, permitem direcionar o armazenamento de energia não consumida para baterias, e processadores capazes de controlar e responder à demanda.[213] Referido sistema requer a implementação de infraestrutura com capacidade de processamento e análise de grandes volumes de informação, o que permite a melhor gestão dos recursos energéticos, com aumento da eficiência operacional da rede pela redução de perdas e falhas na transmissão e pela diminuição do consumo por parte da concessionária.[214-215]

Tamanha a relevância atribuída às Redes Elétricas Inteligentes que desde 2010 diversos órgãos governamentais vêm conduzindo estudos e editando normativos relacionados ao

[210] Cf. MARTINI, José Sidnei Colombo. A gestão da infraestrutura urbana na cidade do futuro: Energia elétrica. In CASTRO, Nivaldo de J. (Org.). **Visão 2030**. Cenários, tendências e novos paradigmas do setor elétrico. Rio de Janeiro: Babilônia Cultural Editorial, 2015, p. 23.

[211] Cf. ANTUNES, Vitor Amuri. **Parcerias público-privadas para *smart cities***. 2ª ed. Rio de Janeiro: Lumen Juris, 2017, p. 19.

[212] Como demonstrado ao longo do relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

[213] Mais informações em: http://gizmodo.uol.com.br/infografico-o-que-e-como-funciona-e-quais-os-beneficios-do-smart-grid/; https://www.cpfl.com.br/energias-sustentaveis/sites-tematicos/smart-grid/Paginas/default.aspx; e http://www.cemig.com.br/pt-br/A_Cemig_e_o_Futuro/sustentabilidade/nossos_programas/Redes_Inteligentes/Paginas/as_redes_inteligentes.aspx . Acesso em: 11.09.2017.

[214] Para uma análise da utilização de tecnologias da comunicação em medidores inteligentes, ver relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017, p. 19.

[215] MONZONI, Mario; NICOLETTI, Mariana. A cidade para os cidadãos: Mobilidade, energia e agricultura urbana. **Caderno FGV Projetos**, jun./jul. 2014, ano 9, nº 24, p. 63. Disponível em: http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf. Acesso em: 05.092.017.

tema.[216] Em especial, a Agência Nacional de Energia Elétrica - ANEEL conduziu diversas audiências públicas que culminaram em resoluções sobre temas relacionados às tecnologias de *smart grids*, como a geração distribuída de pequeno porte ou a possibilidade de implementar sistemas de variação tarifária. Igualmente, foram debatidas no Congresso Nacional propostas legislativas sobre o tema, a exemplo do Projeto de Lei do Senado nº 84/2012 e dos Projetos de Lei da Câmara dos Deputados nº 3.337/2012, nº 3.138/2015 e nº 2.932/2015.[217] De forma geral, as propostas determinam a substituição dos medidores eletromecânicos por medidores inteligentes, a implantação de sistema integrado de comunicação entre os medidores e uma central de gestão da rede, o estabelecimento de padrões mínimos para os medidores e a possibilidade de estabelecer tarifas variáveis.

A despeito desse cenário e da constatação de que o setor de energia elétrica poderá se beneficiar de amplas formas da implementação de tecnologias máquina-a-máquina, a **avaliação do ambiente regulatório em *smart grids* se restringirá à aplicação selecionada pelo consórcio, consistente nos medidores inteligentes**.[218] Essa aplicação está relacionada à etapa de controle e resposta à demanda por energia elétrica e permite, com o uso de *analytics*, a precificação dinâmica em função da disponibilidade energética e demanda instantâneas, o monitoramento da qualidade da transmissão e a identificação de anomalias.[219]

3.1.3.1. Oportunidades decorrentes da utilização de medidores inteligentes

A implementação de medidores elétricos com tecnologia IoT **influencia diretamente as formas de medição e fornecimento de energia elétrica**, uma vez que permitem acesso ao consumo de energia em tempo real e produzem dados capazes de substanciar políticas de variação tarifária destinadas a modificar padrões de consumo e reduzir investimento em infraestrutura.

Os benefícios e funcionalidades da substituição dos medidores eletromecânicos por eletrônicos inteligentes, detentores de tecnologia de medição avançada (*Advanced*

216 A título de exemplo, o Ministério de Minas e Energia criou em 2010 grupo de trabalho para analisar e identificar ações capazes de fomentar a implementação de políticas públicas no tema. Mais sobre o tema, vide: BANDEIRA, Fausto de Paula Menezes. **Redes de Energia Elétrica Inteligentes (Smart Grids)**. Nota Técnica da Consultoria Legislativa da Câmara dos Deputados. Abril de 2012. Disponível em http://www2.camara.leg.br/a-camara/documentos-e-pesquisa/estudos-e-notas-tecnicas/areas-da-conle/tema16/2012_7872.pdf Acesso em 13.09.2017.

217 Para acompanhar a tramitação dos mencionados Projetos de Lei, vide: https://www25.senado.leg.br/web/atividade/materias/-/materia/104860, http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=535991, http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1805590 e http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1713431 Acesso em 13.09.2017

218 Vide relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

219 Como observado no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

Metering Infrastructure - AMI)[220], alcançam tanto os consumidores quanto os agentes do mercado de fornecimento de energia elétrica. Do ponto de vista dos consumidores, medidores inteligentes asseguram maior transparência em relação ao faturamento e permitem o **controle informado do consumo**. Esse benefício pode ser potencializado se associado à tecnologia *blockchain*, que pode armazenar de forma segura e a longo prazo informações detalhadas sobre preferências de consumo e geração dos consumidores (como variações de preço e de fluxos e estoque de energia).[221]

Os mecanismos de medição inteligente permitem também a **aferição da qualidade da energia ofertada pelas concessionárias** e permitem que a ANEEL determine a redução do valor cobrado pela energia caso os indicadores fiquem fora do padrão de qualidade estabelecido. Outro benefício consiste em, por meio de fluxo bidirecional de energia, viabilizar a **geração e a injeção de energia na rede elétrica pelo próprio consumidor**.[222]

Por sua vez, as concessionárias que se utilizarem desses dispositivos terão mais controle sobre o consumo de energia individual e coletivo, que **permitem a cobrança de tarifas diferenciadas por horário de uso** (horo sazonal), mecanismo denominado "tarifa branca".[223] Em especial, a capacidade de reunir dados que viabilizem a implementação de variação tarifária permitirá a adoção de políticas indutoras de consumo de energia em horários em que a rede elétrica está menos carregada, de modo a haver menos horários de sobrecarga do sistema e a consequente redução de custos operacionais.[224] Além disso, os medidores eletrônicos inteligentes também possibilitam às concessionárias o **oferecimento pré-pago de energia elétrica**, sistema mais flexível de oferta de energia,

220 Conforme relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

221 ROMEIRO. Diogo Lisboa. **Do *bitcoin* à geração distribuída** - A revolução da blockchain rumo à descentralização. Acesso em: https://infopetro.wordpress.com/2017/05/10/do-bitcoin-a-geracao-distribuida-a-revolucao-da-blockchain-rumo-a-descentralizacao/. Acesso em 13.09.2017.

222 Conforme se verá adiante, essa funcionalidade já está regulamentada pela ANEEL desde 2012, por meio da Resolução nº 482, que instaurou o sistema de compensação de energia elétrica por micro ou minigeração. Sobre o tema, vide ADAMI, Mateus Piva; CAMARGO, Manuela; KRAFT, Amanda Moreira. Geração distribuída: avanços encorajados pela ANEEL. **Jota**, São Paulo, 15 ago. 2017. Disponível em: https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017. Acesso em: 12.09.2017. A ANEEL promoveu, através da Resolução nº 687/2015, alterações nesse modelo, entre as quais, a ampliação de fontes permitidas (incluindo aquelas renováveis); a redefinição dos limites máximos de geração; a previsão de novas modalidades (condomínios); e a estipulação de um procedimento mais simplificado e informatizado.

223 RIVERA, Ricardo et al. **Redes elétricas inteligentes (smart grid)**: Oportunidade para adensamento produtivo e tecnológico local. Disponível em: https://web.bndes.gov.br/bib/jspui/bitstream/1408/2927/1/RB%2040%20Redes%20el%C3%A9tricas%20inteligentes_P.pdf. Acesso em: 05.09.2017.

224 Essa possibilidade também já está regulamentada pela Resolução nº 502/2012 da ANEEL e poderá ser implementada pelas concessionárias a partir de janeiro de 2018. O tema será abordado mais detalhadamente em seguida. De todo modo, vide: http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel Acesso em 13.09.2017.

adaptando o consumo à renda do consumidor, podendo ser mecanismo interessante para mitigar a inadimplência.[225]

Todavia, a despeito dos benefícios que medidores inteligentes podem fornecer para a qualidade e eficiência dos sistemas elétricos, sua implementação enfrenta **desafio relacionado aos elevados custos dos novos aparelhos**, pois chegam a ser quase dez vezes mais caros que os aparelhos atualmente empregados no sistema de energia elétrica.[226] Acredita-se que diminuição do custo decorrente da adoção dessa tecnologia depende especialmente do ganho razoável de escala em sua produção e distribuição.

3.1.3.2. Competência e regulação sobre medidores de energia elétrica

3.1.3.2.1. Competência e descentralização federativa

Diferentemente do cenário das demais aplicações selecionadas para compor o estudo sobre cidades inteligentes, **compete à União legislar e administrar, diretamente ou mediante concessão, permissão ou autorização, a prestação dos serviços de energia elétrica** (arts. 21, XII, "b" e 22, da Constituição Federal). Há, sobre esse respeito, precedentes do Supremo Tribunal Federal que declaram a inconstitucionalidade de legislação estadual que impõe às concessionárias de energia elétrica a instalação de medidores de consumo.[227]

Diante da competência federal sobre o tema, foi instituída em 1996, pela Lei nº 9.427, a Agência Nacional de Energia Elétrica, dotada de competência para regular, fiscalizar e implementar políticas relacionadas às etapas da prestação do serviço de fornecimento de energia elétrica. Dentre as faculdades da Agência está a possibilidade de descentralizar algumas de suas atividades por meio do estabelecimento de parcerias com Agências Reguladoras dos Estados e do Distrito Federal[228], com vistas a viabilizar e aproximar suas ações dos consumidores de energia elétrica – notadamente no que se refere à fiscalização

[225] O ambiente de pré-pagamento e pós-pagamento eletrônico de energia elétrica consiste em mais dos temas já regulamentados pela ANEEL por intermédio da Resolução nº 610/2014.

[226] Segundo Maria Tereza Vellano, diretora de planejamento, engenharia e obras de distribuição da AES Eletropaulo, o medidor inteligente usado num *smart grid* custa R$ 800, enquanto o convencional sai por R$ 70. Mais informações em: http://redesinteligentesbrasil.org.br/component/content/article/13-ultimas-noticias/57-rede-eletrica-inteligente-ajuda-a-reduzir-perdas-o-estado-de-s-paulo.html. Acesso em: 11.09.2017.

[227] ADI 3.558, voto da rel. min. Cármen Lúcia, j. 17-3-2011, P, DJE de 6-5-2011.

[228] Sobre mais informações sobre o tema, vide: http://www2.aneel.gov.br/biblioteca/downloads/livros/caderno-tematico-descentralizacao.pdf. Acesso em: 08.09.2017.

dos serviços.[229] Dentre os Estados em que houve a descentralização ou o estabelecimento de convênio estão o Acre, Tocantins, Ceará, Rio Grande do Norte, Goiás, São Paulo e Rio Grande do Sul.[230]

3.1.3.2.2. Regulamentação sobre medidores inteligentes

Com vistas a regulamentar sistemas de medição de energia das unidades consumidoras, a ANEEL editou em 2010 a Resolução nº 414[231], na qual reafirmou a **competência das distribuidoras de energia em fornecer e instalar os equipamentos de medição**. O custeio dos referidos equipamentos também está entre as obrigações das distribuidoras, salvo em hipóteses expressamente previstas em lei[232], como na situação em que o consumidor solicita a instalação de medidores para cargas distintas à do seu perfil. Nesses casos, o consumidor será responsável pelo custeio da diferença do preço do medidor e demais materiais e equipamentos de medição relacionados. Igualmente, a Resolução nº 414/2010 determina que a escolha dos medidores de energia ficará a cargo da distribuidora, desde que cumpra os requisitos constantes da legislação e obtenha a **devida homologação pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO**.[233]

Em relação ao processo de leitura dos medidores, a Resolução determina que a distribuidora deverá efetuá-las em intervalos não inferiores a 27 dias e não superiores a 33 dias.[234] A realização de leitura em prazos distintos deverá ser acompanhada de prévia concordância do consumidor, de autorização da ANEEL e em outras hipóteses mais específicas, como o impedimento de acesso, situações de emergência ou de calamidade pública.

229 As atividades descentralizadas estão a fiscalização, o apoio à regulação dos serviços e instalações de energia elétrica e a mediação de problemas entre os agentes de mercado. Para mais informações sobre o tema, vide: http://www.aneel.gov.br/descentralizacao-de-atividades

230 De forma exemplificativa, vide o convênio de Cooperação entre a ANEEL e a Arsep: http://www.aneel.gov.br/documents/656877/15015002/ARSESP_19.2011.pdf/cce6347d-9361-4f8b-8145-85ae51029364

231 Diante das competências que lhe foram atribuídas pela Lei nº 9.427/1996 e regulamentadas pelo Decreto nº 2.335/1997. Referida Resolução é fruto de Audiência Pública nº 08/2008 e da Consulta Pública nº 02/2009 e resultou na revogação integral de inúmeras resoluções anteriores da Agência. Texto disponível em: http://www2.aneel.gov.br/cedoc/ren2010414.pdf. Acesso em: 05.09.2017.

232 Vide art. 73 e seguintes.

233 A homologação dos medidores não faz parte das competências da ANEEL, de forma que essa atividade é desempenhada pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO. Ver legislação em: http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001931.pdf. Acesso em: 05.09.2017.

234 Vide art. 84 e seguintes.

Diante da constatação da existência de novos medidores eletrônicos com a capacidade de modernizar a prestação do serviço de energia elétrica, inclusive com a possibilidade de incluir consumidores entre os fornecedores de insumos à rede de energia, a ANEEL convocou a Audiência Pública nº 43/2010, visando à elaboração de proposta normativa para regular os requisitos mínimos dos inovadores aparelhos.[235] Como resultado desse processo participativo, foi editada a Resolução ANEEL nº 502/2012[236], que regulamenta o sistema de medição eletrônica de energia para os consumidores de perfil residencial, rural e demais classes, exceto baixa renda e iluminação pública.

Em seu texto original, essa Resolução determinava às distribuidoras a adoção do sistema de medição eletrônico em até 18 meses da publicação da norma. Essa data foi modificada pela Resolução nº 732/2016[237], que prorrogou a implementação do novo sistema de medição para 1º de janeiro de 2018, salvo no caso de distribuidoras que celebrarem contrato de concessão após a edição da Resolução. Para esses casos, o prazo estabelecido é de 18 meses do início da vigência do contrato de permissão ou 1º de janeiro de 2018, devendo prevalecer a data que ocorrer por último.[238]

Nesse sentido, a partir do começo de 2018 as distribuidoras de energia elétrica deverão instalar gratuitamente medidores capazes de mensurar energia ativa em quatro diferentes postos tarifários, aos usuários que solicitarem a migração.[239] Para os consumidores que não aderirem a essa nova modalidade de tarifa a instalação dos novos aparelhos não é obrigatória.[240] A instalação dos novos medidores deverá ocorrer em até 30 dias da solicitação e o consumidor será autorizado a regressar à modalidade tarifária convencional, que deverá ser implementada dentro do mesmo prazo (cf. Resolução ANEEL nº 733/2016).

235 A proposta de regulamentação dos requisitos mínimos para os medidores eletrônicos foi debatida na Audiência Pública 43/2010, que colheu contribuições da sociedade entre 1º de outubro de 2010 a 28 de janeiro de 2011, e contou com uma sessão presencial realizada em Brasília em 26 de janeiro de 2011. Ao fim desse período, a ANEEL recebeu 212 contribuições de 57 agentes, com sugestões de consumidores, distribuidoras, indústrias, associações setoriais e outros segmentos da sociedade. Durante a sessão presencial foram realizadas 19 manifestações, com apresentação de comentários e contribuições. Vide: http://www2.aneel.gov.br/aplicacoes/noticias/Output_Noticias.cfm?Identidade=5903&id_area=90. Acesso em: 10.09.2017.

236 Disponível em: http://www2.aneel.gov.br/cedoc/ren2012502.pdf. Acesso em: 05.09.2017.

237 Disponível em: http://www2.aneel.gov.br/cedoc/ren2016732.pdf. Acesso em: 08.09.2017.

238 Vide art. 1º da Resolução nº 502/2012.

239 Fonte: http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel. Acesso em: 13.09.2017.

240 A opção é uma garantia ao consumidor que não consegue promover mudanças de hábito para consumir menos nos horários de pico.

Além dos medidores inteligentes, os consumidores aderentes da tarifa branca terão direito de visualizar informações em mostrador no próprio medidor ou em outro dispositivo dentro da residência. Modelos de medidor com funcionalidades mais avançadas, como a disponibilização de acesso a informações específicas individualizadas sobre o serviço, poderão ser requeridas pelos consumidores, contudo a instalação poderá ser cobrada pela distribuidora.[241]

Dentre as preocupações expressadas em relação à execução do determinado pela Resolução estava a homologação de medidores pelo INMETRO. Todavia, **tem-se notícia da existência de medidores eletrônicos inteligentes já homologados pelo INMETRO**, como é o caso do equipamento desenvolvido pela empresa *Weg* em parceria com a concessionária AES Eletropaulo, para ser implantado no projeto-piloto de *smart city* em Barueri/SP.[242-243] Esse fato indica que o processo de homologação dos aparelhos pelo Instituto não representa um obstáculo à implementação das disposições da referida Resolução e à competitividade capaz de reduzir o preço dos aparelhos.

Verifica-se, portanto, que desde 2010 a ANEEL vem enfrentando os desafios regulatórios relacionados à implementação de medidores adequados às novas demandas do mercado de energia elétrica. Todavia, os medidores eletrônicos previstos na Resolução nº 502/2012 são destinados à tarifa branca e não dispõem de sistema avançado de comunicação que permita a leitura, corte e coleta instantânea de informações – que são importantes para a implementação de *smart grids*.

Isso significa que as concessionárias deverão instalar, mediante solicitação do consumidor, a partir de janeiro de 2018, medidores eletrônicos com funcionalidades específicas para a tarifa branca. No entanto, a demanda por novas funcionalidades e expansão das *smart grids* poderão demandar uma nova substituição, em período inferior à vida útil dos equipamentos, o que denota a necessidade de a ANEEL seguir nos seus esforços de modernização do setor.[244]

241 Mais informações em: http://www2.aneel.gov.br/aplicacoes/noticias/Output_Noticias.cfm?Identidade=5912&id_area=90. Acesso em: 05.09.2017.

242 A primeira distribuidora a ter medidores inteligentes homologados pelo INMETRO foi a AES Eletropaulo, no ano de 2016, através das portarias n° 586/2012, n° 587/2012 e n° 520/2014. Mais informações em: https://www.weg.net/institutional/BR/pt/news/produtos-e-solucoes/weg-tem-o-primeiro-medidor-de-energia-do-brasil-certificado-pelo-inmetro e http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=43137&sid=3. Acesso em: 05.09.2017.

243 Outro exemplo é o da Ecil Energia, empresa que também homologou modelos de medidores eletrônicos inteligentes no INMETRO nos últimos anos. Mais informações em: http://www.ecilenergia.com.br/download/Medidores.pdf. Acesso em: 11.09.2017.

244 Há que se avaliar a viabilidade e estímulos financeiros para a troca, especialmente tendo em vista que a forma de remuneração das concessionárias pelos investimentos realizados leva em consideração cota de depreciação dos

Em paralelo aos esforços da Agência, tramitam no Congresso Nacional propostas normativas que visam regulamentar a implementação de medidores elétricos inteligentes, mas que apresentam relativa inovação aos normativos da Agência Regulatória competente. Dentre as propostas existentes, destacam-se o Projeto de Lei do Senado nº 84/2012[245], e os Projetos de Lei da Câmara nº 3.337/2012[246] e nº 2.932/2015[247], ao qual foi apensado o Projeto de Lei nº 3.138/2015. Seus principais objetivos relacionados à medição são a extensão do prazo para a substituição dos medidores de energia para 10 a 15 anos da sanção da Lei, a obrigação de implementar sistema confiável de comunicação entre todos os dispositivos e a autorização e regulamentação da geração distribuída de energia.

Dentre as mudanças propostas nos referidos Projetos de Lei, considera-se que sua inovação em relação ao estado da arte regulatório reside apenas na exigência de implementação de sistema de comunicação entre todos os dispositivos de automação do sistema. Nesse sentido, considera-se que a ANEEL vem enfrentando os principais **desafios regulatórios relacionados à implementação de medidores inteligentes**[248], mas que avanços ainda são necessários, especialmente em relação à obrigatoriedade de novos medidores instalados possuírem mecanismos avançados e confiáveis de comunicação.

3.1.3.2.3. Regulamentação sobre geração distribuída

Com a preocupação em desenvolver redes elétricas inteligentes, a ANEEL editou a Resolução nº 482/2012 para inaugurar **sistema de compensação de energia elétrica por**

aparelhos, que são calculados com base na idade, vida útil, estado de manutenção, conservação e obsolescência (Anexo V da Resolução nº 493/2002). Com parque tecnológico atualizado, sem aparelhos próximos da obsolescência, o ônus para a modernização de aparelhos de medição recairá essencialmente sobre as concessionárias. Resolução disponível aqui: http://www2.aneel.gov.br/cedoc/res2002493.pdf%20Acesso%20em%2003.10.2017. Acesso em: 10.09.2017.

245 A proposta estabelece que as concessionárias de energia elétrica deverão ajustar seu sistema de distribuição para implantar todos os requisitos necessários à sua transformação em Redes Elétricas Inteligentes (art. 1º). Entre as diretrizes para a implantação dessas Redes está o provimento de sensores de medição, dispositivos de automação, sistema confiável de comunicação entre todos os dispositivos de automação e a possibilidade de transferência instantânea e bidirecional de informações entre os dispositivos (art. 3º).

246 O PL nº 3.337, de forma mais específica, determina que as concessionárias deverão providenciar a substituição integral de medidores de consumo de energia eletromecânicos por medidores eletrônicos, no prazo de até dez anos (art. 1º). Regulamenta também, nos arts. 2º e 3º, a venda de energia excedente produzida pelos consumidores.

247 Por sua vez, o PL nº 2.932 dispõe sobre o Plano Nacional de Redes Elétricas Inteligentes. De forma semelhante ao PL anterior, determina-se que as concessionárias deverão providenciar a substituição de medidores tradicionais por medidores eletrônicos inteligentes, contudo com prazo mais extenso, de até quinze anos após a publicação desta lei (art. 3º). Também, prescreve a venda de energia excedente (art. 6º). Tramitando em conjunto encontra-se o PL nº 3.138, que possui disposições semelhantes.

248 Para mais informações sobre a regulamentação vigente sobre medidores, vide: http://www.aneel.gov.br/documents/656827/14866914/Modulo5_Revisao5/4d9e298e-cbf6-4b09-a01a-2e55f05dc9c7 Acesso em 18.09.2017.

micro ou minigeração e estabelecer condições para seu acesso.[249] Referido normativo removeu obstáculos para que consumidores conectados em baixa tensão passem a injetar energia à rede de energia elétrica, tendo determinado às distribuidoras, entre outros, adequar seus sistemas para viabilizar referida modalidade de geração energética e permitiu que sejam remunerados à medida em que contribuam com energia excedente.[250]

A despeito das modificações promovidas pela Resolução nº 482/2012, não houve adesão massiva ao programa, o que estimulou a edição pela ANEEL da Resolução nº 687 em 2015.[251]-[252] Dentre as mudanças promovidas estão a redefinição dos limites máximos para a micro e minigeração distribuída, a previsão de novos formatos de geração distribuída (como o empreendimento com múltiplas unidades e a geração compartilhada), a possibilidade de o sistema incorporar fontes renováveis de energia e o estabelecimento de procedimento mais simplificado e informatizado.[253]

Também com vistas a angariar ainda maior número de aderentes à geração distribuída, a Agência expediu em 2017 o Ofício Circular nº 10/2017 para realizar esclarecimento de dúvidas sobre o sistema, especialmente em virtude do surgimento de novos modelos de negócios cujo enquadramento nas resoluções anteriores restava incerto.[254]

Segundo Nota Técnica divulgada pela ANEEL em maio de 2017 as alterações regulatórias promovidas pela Agência, em especial após a edição da Resolução nº 687/2015, resultaram em aumento de 4,4 vezes o número de consumidores com micro ou minigeração distribuída até o final de 2017. Referido relatório também indicou que a principal fonte de geração distribuída está na energia solar fotovoltaica produzida por consumidores residenciais. A perspectiva da ANEEL é que o número de consumidores aderentes ao programa, que atualmente está em 26.834, aumente para 886.700.[255]

[249] Ainda que seja passível de ser instrumentalizada independentemente da utilização de medidores inteligentes, a geração distribuída de energia elétrica pode ser potencializada com esse advento tecnológico. Para usuários de baixo consumo é possível aderir à política de micro e minigeração distribuída mediante o uso de medidores unidirecionais, cf. http://www2.aneel.gov.br/arquivos/PDF/FAQ_GD_Atualizado.pdf. Acesso em: 13.09.2017.

[250] Para o faturamento da unidade consumidora que participe do sistema de compensação, deve ser considerada a energia consumida, sendo deste valor deduzida a energia injetada (cf. art. 7º).

[251] Disponível em: http://www2.aneel.gov.br/cedoc/ren2015687.pdf. Acesso em: 14.09.2017.

[252] Após a edição da resolução houve aumento mais significativo na adesão ao programa. Conforme: http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica_0056_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9. Acesso em: 14.09.2017.

[253] ADAMI, Mateus Piva; CAMARGO, Manuela; KRAFT, Amanda Moreira. Geração distribuída: avanços encorajados pela ANEEL. **Jota**, São Paulo, 15 ago. 2017. Disponível em: https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017. Acesso em: 12.09.2017.

[254] Fonte: https://jota.info/artigos/geracao-distribuida-avancos-encorajados-pela-aneel-15082017#_ftn2. Acesso em: 13.09.2017.

[255] Vide

Nesse sentido, considera-se que **há regulação hoje que já permite o desenvolvimento de geração distribuída**. Um possível desafio diz respeito à incidência do ICMS, de competência dos Estados, sobre atividades e **micro** ou **minigeração**, dentre outras. Seria importante que se estabelecesse, em coordenação com os Estados, a disseminação de leis estaduais que criem isenções a respeito dessas atividades, no mínimo enquanto as mesmas ainda forem incipientes.[256]

Dito isso, desde 2010 a ANEEL vem realizando estudos e editando normativos ou opiniões técnicas aptas a estimular a modernização da rede elétrica e, mais específica, do estímulo à geração distribuída. Além disso, a larga instalação dos novos modelos de medidores até 2020 possui a capacidade de colaborar com o sistema pela qualidade de medição dos dados enviados à rede e por independer da instalação de medidor adicional para a micro ou minigeração.

3.1.3.2.4. Regulamentação sobre novas modalidades tarifárias

Outro aspecto relacionado à implementação de medidores inteligentes consiste em **implementar diversas formas de tarifação pelo consumo do serviço**, dentre as quais estão a tarifa branca e o pré-pagamento.

A **tarifa branca** foi originalmente inserida na Resolução Aneel nº 414/2010 pela Resolução nº 502/2012, sendo qualificada como de adesão voluntária pelo consumidor e contendo tarifas diferenciadas de consumo de energia elétrica a depender do horário de utilização. As condições de implementação foram posteriormente regulamentadas pela Agência por meio da Resolução nº 733/2016. Segundo a regulamentação vigente, a tarifa branca será destinada aos consumidores residenciais e comerciais (Grupo B), salvo a iluminação pública e as unidades consumidoras de baixa renda. Conforme mencionado anteriormente, o consumidor com consumo acima de 250 kWh por mês poderá solicitar a adesão à tarifa branca a partir de janeiro de 2018, os consumidores com consumo superior a 250kWh mensais poderão migrar em janeiro de 2019 e os demais consumidores poderão aderir a partir de 2020.[257]

http://www.aneel.gov.br/documents/656827/15234696/Nota+T%25C3%25A9cnica_0056_PROJE%25C3%2587%25C3%2595ES+GD+2017/38cad9ae-71f6-8788-0429-d097409a0ba9 Acesso em 18.09.2017.

256 Movimentação nesse sentido é encontrada no recente Convênio Confaz 16/2015, que autorizou os Estados de Goiás, Pernambuco e São Paulo a concederem isenção do ICMS incidente sobre a energia elétrica fornecida pela distribuidora à unidade consumidora através de micro e minigeração distribuída. In: FREITAS, Bruno M. R. e HOLLANDA, Lavínia. **Micro e minigeração no Brasil**: Viabilidade econômica e entraves do setor. *White Paper* nº 1, maio 2015, Fundação Getúlio Vargas – FGV. Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13853/micro.pdf?sequence=1. Acesso em: 14.11.2017.

257 Fonte: http://atarde.uol.com.br/economia/noticias/1894067-tarifa-branca-comeca-em-janeiro-de-2018-diz-aneel. Acesso em: 13.09.2017.

A tarifa branca será válida apenas em dias de semana e o valor será variável em três grupos de horários (ponta, intermediário e fora de ponta). O horário de ponta será entre 19 e 21h e possuirá valores mais elevados, o horário intermediário será das 18 às 19h e das 21 às 22h e possuirá valores intermediários, e os demais horários terão tarifa mais reduzida.[258] Os valores de tarifa cobrados aos aderentes dessa modalidade tarifária deverão ser discriminados na fatura.

Por sua vez, a **modalidade de pré-pagamento** eletrônico de energia elétrica está regulamentada pela Resolução ANEEL nº 610/2014[259], sendo sua adesão voluntária e podendo ser cancelada a qualquer momento pelo consumidor. A adesão não será autorizada aos consumidores aderentes à micro ou minigeração distribuída ou que se enquadre na modalidade tarifária horária branca.

Os medidores inteligentes colaboram para a implementação dessa modalidade tarifária, uma vez que sua cobrança é dependente da existência de visor com informações atualizadas sobre a quantidade de créditos disponíveis. A regulamentação também exige que o aparelho tenha alarme visual e sonoro que informe o usuário 15 dias antes da proximidade do encerramento dos créditos e da suspensão do fornecimento de energia.[260] Encerrado o crédito do consumidor, o fornecimento de energia elétrica poderá ser suspenso, sendo autorizado à distribuidora disponibilizar a qualquer momento ao consumidor crédito de 20kWh. A restituição da energia elétrica deverá ocorrer imediatamente após a quitação do crédito pelo consumidor.

A despeito da existência de regulação pela Agência, ressalta-se a existência de divergência jurisprudencial acerca da legalidade de cortes de energia elétrica por inadimplemento, o que poderá gerar alguma complicação na implementação do modelo de energia pré-paga. Isso porque, muito embora a Lei nº 9.247/1996 possibilita expressamente a suspensão sem aviso prévio do serviço na ausência de pagamento, o Código de Defesa do Consumidor determina que as empresas prestadoras de serviços essenciais devem fornecer seus produtos de forma eficiente e contínua, sendo vedadas quaisquer interrupções. De todo modo, a modernização proposta pela ANEEL se mostra viável em razão do posicionamento que o Superior Tribunal de Justiça vem adotando

258 Vide: http://www.aneel.gov.br/sala-de-imprensa-exibicao/-/asset_publisher/XGPXSqdMFHrE/content/aneel-aprova-tarifa-branca-nova-opcao-para-os-consumidores-a-partir-de-2018/656877?inheritRedirect=false Acesso em 18.09.2017.

259 Vide: http://www2.aneel.gov.br/cedoc/ren2014610.pdf Acesso em 18.09.2017.

260 Por isso, nessa modalidade a o demonstrativo de faturamento de energia com informações consolidadas deverá ser solicitado pelo consumidor à distribuidora.

desde 2003, de modo a reconhecer a licitude do corte de energia elétrica por inadimplemento, desde que observados os requisitos legais.[261]

Vale ressaltar também que na modalidade pré-paga o esgotamento do crédito, a rigor, sequer pode ser considerado inadimplemento porque que o consumidor simplesmente não adquiriu créditos adicionais. Assim, a discussão se afastaria da possibilidade de interrupção por inadimplemento, vez que a suspensão do serviço até a aquisição novos créditos é pressuposto da modalidade pré-paga.

Finalmente, **atualmente estão sendo estudados os benefícios decorrentes da implementação de tarifa binômia no faturamento da eletricidade consumida por consumidores da categoria de baixa tensão**. A tarifa binômia consiste na separação da fatura de eletricidade entre pagamento pelo consumo e uso da rede elétrica, e sua implementação para esse grupo de consumidores visa à remuneração das concessionárias pela disponibilização da rede para os consumidores aderentes à geração distribuída. A proposta foi debatida quando da tramitação no Congresso Nacional da Medida Provisória nº 735/2016, que promoveu alterações no marco legal de energia elétrica, mas não foi inserida ao texto da Lei nº 13.360/2016. A sua implementação, todavia, depende da realização de estudos adicionais, especialmente em virtude dos potenciais efeitos negativos que poderá promover ao avanço da geração distribuída.[262]

Assim sendo, também **em relação às novas possibilidades de modalidade tarifária não há considerável desafio regulatório**. As recentes modificações em resoluções da ANEEL, realizadas mediante a condução de prévios estudos e consultas públicas, se mostram alinhados às novas demandas de modernização do sistema de fornecimento de energia elétrica.

261 STJ, 1ª Turma, REsp 1270339/SC, Min. Rel. Gurgel de Faria, d.j. 15.12.2016. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/87/edicao-1/principio-da-continuidade-do-servico-publico-e-interrupcao. Acesso em: 14.09.2017. A Corte já havia uniformizado seu entendimento pela legalidade do corte de energia elétrica por inadimplemento em 2003, no REsp 363.943/MG. A 1ª Turma do Tribunal, até a uniformização, reprimia de forma veemente a interrupção do bem essencial, enquanto a Segunda Turma pendia sua orientação pela legalidade do procedimento. Mais informações em: SUZIN, Juliana Bonella. **Suspensão do fornecimento de energia elétrica por inadimplemento**. Disponível em: http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2012_2/juliana_suzin.pdf. Acesso em: 14.09.2017.

262 Segundo relata a Associação Nacional dos Consumidores de Energia, a implementação da tarifa binômia para consumidores do segmento de baixa tensão, visto que poderá aumentar em até 30% o tempo de retorno dos projetos de geração distribuída. Vide: http://www.anacebrasil.org.br/noticias/tarifa-binomia-aumentara-tempo-de-retorno-dos-projetos-de-gd/ Acesso em 11.10.2017.

3.1.3.3. Privacidade de dados pessoais e segurança da informação

Conforme mencionado, a medição avançada proporciona significativos benefícios aos três elos da cadeia do serviço de fornecimento de energia elétrica: aferição da qualidade do serviço por parte do órgão regulador, controle do faturamento pelo consumidor e redução de custos operacionais e de investimento em infraestrutura pelos concessionários. Todavia, a incorporação à rede elétrica de dispositivos tecnológicos de informação e monitoramento potencializa a capacidade dessa rede de reunir dados, levantando a **preocupação com a privacidade dos usuários do sistema de distribuição de energia e com a segurança desse aparato**.

O acesso, em tempo real, às informações de consumo de energia elétrica de indivíduos, residências e corporativos, por intermédio de dispositivos equipados com endereços de protocolo de Internet e aplicação de rede *wireless*, levanta preocupações relacionadas à privacidade. A título de exemplo, citamos a possibilidade de monitoramento de padrões comportamentais[263], identificação do grau de suscetibilidade do local a crimes[264], a prática de vigilância em tempo real, a determinação de equipamentos eletrodomésticos utilizados, o envio de publicidade não desejada, entre outras.[265]

Além disso, a própria rede de energia elétrica está propensa a falhas de segurança. Como ilustração desse tipo de risco, que afeta de forma global a estrutura operacional do sistema de distribuição, grupo de *hackers* vêm direcionando, desde 2011, ataques a redes de companhias do ramo de energia localizadas nos Estados Unidos e na Europa.[266] Em relatório disponibilizado pela empresa *Symantec*, os *hackers* atuam em campanha de cyber-espionagem que, em alguns casos, já foi capaz de penetrar com sucesso os âmbitos mais centrais dos sistemas pertencentes a essas corporações. Isso significa que os *hackers*

[263] Como exemplo, há relatos de que dados de uso de eletricidade já foram utilizados por autoridades policiais nos estados do Texas e da Califórnia para identificar possíveis plantações residenciais de *cannabis* e, consequentemente, obter mandados de busca e apreensão. Fonte: Balancing access to electricity data and privacy concerns, **PV Magazine**, 11 mai. 2017. Disponível em: https://pv-magazine-usa.com/2017/05/11/guest-column-balancing-access-to-electricity-data-and-privacy-concerns/. Acesso em: 14.09.2017.

[264] Como observado no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017, informações sobre o consumo instantâneo podem indicar se determinada residência encontra-se sem ninguém presente no momento, estando assim mais propensa a invasões.

[265] Listagem de práticas veiculada pelo *Electronic Privacy Information Center*, disponíveis em: https://epic.org/privacy/smartgrid/smartgrid.html. Acesso em: 18.09.2017.

[266] GOODIN, Dan. **Hackers lie in wait after penetrating US and Europe power grid networks**. 6 set. 2017. Disponível em: https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1. Acesso em: 18.09.2017. Como exemplo, em dezembro de 2015, um ataque no centro de distribuição de energia próximo à cidade de Kiev, na Ucrânia, fez com que por volta de 225.000 pessoas ficassem sem energia por 6 horas. Essa foi a primeira ocorrência conhecida de *hacking* voltado a gerar interrupção de energia em larga escala.

podem exercer influência sobre a estabilidade de matriz de energia ofertada diariamente a milhões de pessoas.[267]

Entre as implicações da ruptura de segurança de redes de distribuição de energia (em especial, aquelas passíveis de monitorar o consumo em tempo real, das quais tratamos neste relatório), temos o corte repentino de energia em determinadas localidades, potenciais alterações na qualidade da rede[268], a divulgação de dados sobre localização e níveis de consumo dos indivíduos[269], e, inclusive, a possibilidade de fraude nos valores da fatura do usuário.[270] Foi, a propósito, o que ocorreu em Porto Rico, quando, em 2009, medidores inteligentes foram alvo de *hackeamento* em massa, situação que teria gerado fraude generalizada no faturamento de energia.[271]

Para que o planejamento de redes elétricas inteligentes seja uma prática bem-sucedida – tendo em vista, notadamente, a instalação e emprego de medidores inteligentes –, **reiteramos as recomendações previamente veiculadas no tópico sobre privacidade em Cidades**. Nele, apontamos, para além do perfilhamento de boas práticas organizacionais pelo Poder Público que levem em consideração a atual legislação difusa sobre a questão da privacidade, a necessidade de que seja promulgada lei específica para a proteção de dados pessoais.

Em um contexto de legislação ainda esparsa sobre o tema, sugere-se que à coleta de dados realizada por equipamentos com solução IoT (entre eles, medidores avançados) sejam empregados métodos de anonimização de dados, por intermédio de medidas de criptografia e de tecnologia *blockchain*, cujas vantagens já foram elencadas acima. Desse

[267] VOLZ, Dustin. **Hackers gain entry into U.S., European energy sector, Symantec warns**. 6 set. 2017. Disponível em: http://www.reuters.com/article/us-usa-cyber-energy/hackers-gain-entry-into-u-s-european-energy-sector-symantec-warns-idUSKCN1BH171. Acesso em: 18.09.2017. ALEEM, Zeeshan. **Russia-linked hackers are infiltrating the US power grid: report**. 6 set. 2017. Disponível em: https://www.vox.com/world/2017/9/6/16262198/hackers-us-power-grid-russia. Acesso em: 18.09.2017.

[268] Nesse sentido, Goodin observa que hackers no controle do sistema operacional teriam a habilidade de abrir a rede para outros invasores e também se apropriar do sistema que monitora a qualidade da rede. In: **Hackers lie in wait after penetrating US and Europe power grid networks**. 6 set. 2017. Disponível em: https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1. Acesso em: 18.09.2017.

[269] No ataque de 2015 na Ucrânia, descrito acima, houve coleta de senhas de acesso e outros tipos de dados que permitiriam aos invasores acessar os níveis de supervisionamento da rede. Dessa maneira, ficam desprotegidos os dados dos consumidores e patente a possibilidade de acesso a eles. In: GOODIN, Dan. **Hackers lie in wait after penetrating US and Europe power grid networks**. 6 set. 2017. Disponível em: https://arstechnica.com/information-technology/2017/09/hackers-lie-in-wait-after-penetrating-us-and-europe-power-grid-networks/?comments=1. Acesso em: 18.09.2017.

[270] HERN, Alex. **Smart electricity meters can be dangerously insecure, warns expert**. 29 dec. 2016. Disponível em: https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers. Acesso em: 18.09.2017.

[271] Fonte: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/. Acesso em: 18.09.2017.

modo, informações coletadas sem o consentimento do usuário da rede de energia não permitiriam sua identificação.

Além disso, é recomendável o desenvolvimento de modelos de segurança robustos para os medidores inteligentes. Por exemplo, certificando sua comunicação ponta-a-ponta, valendo-se inclusive de criptografia e permitindo a comunicando apenas com partes pré-certificadas. **Recomenda-se como diretriz geral que a coleta de dados por medidores inteligentes ou qualquer outro dispositivo de IoT na rede elétrica seja feita apenas para a finalidade de medição do consumo e gestão da rede**.

A exceção a essa regra geral deve ocorrer mediante a obtenção do consentimento válido do usuário do serviço, cumprindo no mínimo com as determinações elencadas pelo Marco Civil da Internet quando ocorrer coleta de dados pessoais (arts. 3º, III c/c 7º, VIII e IX). Mais que isso, deve sempre haver a opção de "opt-out" para o usuário do serviço, que poderá optar por não ter seus dados coletados ou utilizados para outras finalidades, não podendo ser penalizado por essa opção.

Além disso, **os dados coletados não podem ser compartilhados com terceiros** (exceto se houver consentimento livre, expresso e informado) ou com outras entidades governamentais (como por exemplo, para fins de investigação criminal), salvo na hipótese de ordem judicial prévia autorizando esse compartilhamento.

Em suma, os usos dos dados para finalidades outras que não a prestação do próprio serviço e a gestão da rede devem ser exceções, sujeitas ao escrutínio do poder judiciário e ao consentimento livre, expresso e informado dos usuários do serviço. É essencial, nesse sentido, que a coleta de dados pessoais seja objeto de salvaguardas regulatórios, que serão essenciais para a concretização do preceito constitucional da privacidade nesse âmbito específico.

3.1.4 Iluminação pública inteligente

3.1.4.1. Oportunidades decorrentes da implementação de aplicações de IoT

Atualmente a rede de iluminação pública passa por importantes transformações, seja em função do **deslocamento de sua exploração para os municípios**, seja pela possibilidade **de adoção de novas tecnologias** – em especial a substituição das lâmpadas a vapor metálico por placas de LED (*Light-Emitting Diode*).[272] A migração para luminárias com menor consumo pode ser um indutor importante para o desenvolvimento de IoT, pois

[272] MARTINI, José Sidnei Colombo. A gestão da infraestrutura urbana na cidade do futuro: energia elétrica. In CASTRO, Nivaldo de J. (Org.). **Visão 2030**. Cenários, tendências e novos paradigmas do setor elétrico. Rio de Janeiro: Babilônia Cultural Editorial, 2015, p. 49-51.

permite a introdução de mecanismos que viabilizam a comunicação sem fio com dispositivos de controle e de comunicação.

A nova luminária será, portanto, utilizada como ponto de rede de comunicação de dados conectada à Internet, inteligente à medida que cada ponto é individualmente controlável através do uso de *software*.[273] Isso permite, na prática, a comunicação com central controladora e de transferir, de forma bidirecional, dados e informações.

Isso viabiliza, entre outras funções, a identificação da situação da luminária em tempo real, o monitoramento de seu consumo energético e também sua dimerização[274], consistente na modulação de luminescência de acordo com luminosidade do ambiente e a ocupação do espaço, maximizando o uso de energia. Desse modo, a implementação de aplicações de IoT proporciona a gestão inteligente do parque de iluminação pública dos municípios, com a possibilidade de redução não só do consumo de energia na cidade como também do custo de manutenção da rede.

Ainda, é possível **a integração desse serviço com outras aplicações de utilidade pública**, tais como as câmeras de segurança instaladas nas vias públicas, semáforos de controle de tráfego nas vias públicas e análises de localização capazes de oferecer informações importantes para, por exemplo, gestores de aeroportos. Também é possível a integração de outros sensores, em que informações de diversas naturezas são coletadas a partir da infraestrutura de iluminação pública. Essa rede municipal *inteligente* pode, assim, se tornar fonte de informações do Poder Público para tomada de decisões mais eficientes em relação aos serviços públicos oferecidos.[275]-[276] No entanto, as mesmas cautelas com relação à privacidade que apontamos na parte em que tratamos de cidades inteligentes aplicam-se também para a iluminação pública.

[273] Mais informações em: https://www.voltimum.pt/artigos/noticias-do-sector/smart-city-iluminacao-conectada-atraves-de-software-de-gestao-de-luz. Acesso em: 04.09.2017.

[274] As luminárias LED possuem tecnologia que possibilita o ajustamento do seu brilho e intensidade (de 0 a 100%), com o auxílio de um dispositivo chamado *dimmer*. A dimerização aumenta a durabilidade da lâmpada e permite redução drástica no consumo. Mais informações em: http://www.g20brasil.com.br/o-conforto-e-a-economia-na-dimerizacao-com-lampadas-de-led/. Acesso em: 04.08.2017.

[275] ANTUNES, Vitor Amuri. **Parcerias público-privadas para cidades inteligentes**. Disponível em: http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5. Acesso em: 24.08.2017.

[276] A iluminação *inteligente*, conectada à Internet das Coisas, poderia funcionar como plataforma para uma série de tecnologias de sensoriamento que coletam dados sobre movimento de tráfego e de pessoas, segurança pública, estacionamento, qualidade do ar, clima, poluição, sonora, atividade sísmica, entre outras funções. Mais informações em: http://www.archdaily.com.br/br/785682/iluminacao-conectada-da-ethernet-a-internet-li-fi e http://ofuturodascoisas.com/uma-iluminacao-publica-inteligente-e-que-gera-receita-para-cidade/. Acesso em: 04.09.2017.

3.1.4.2. Competências para gestão da iluminação pública

Inicialmente, é importante consignar que esse cenário de adaptação do sistema de iluminação pública às novas tecnologias deve levar em consideração que a **gestão do serviço de iluminação pública é de competência dos Municípios, conforme determinação constitucional** (art. 30, V). Assim, mesmo que a atividade possua evidente relação com os serviços de distribuição de energia elétrica, cuja competência é do governo federal (art. 21, XII, "b"), a competência para sua exploração e regulação é municipal.

Inclusive, por essa razão, a **ANEEL editou Resolução determinando a transferência para os municípios dos ativos de iluminação pública** (Resolução ANEEL nº 414/2010)[277]. Essa transferência de ativos enfrentou barreiras, relacionadas em especial aos custos para a prestação direta do serviço e ao estado de conservação dos ativos transferidos, que resultou na realização de audiência pública[278] em 2013 para renegociar os prazos da transferência, dando origem à Resolução ANEEL nº 587/2013.[279]

Assim, com o reconhecimento da municipalização da prestação do serviço de iluminação pública, **as prefeituras passaram a se responsabilizar por exercer atividades relacionadas à operação, manutenção, melhoria e modernização das redes de iluminação**.

3.1.4.3. Postes de iluminação pública e de energia elétrica

3.1.4.3.1. Competências para regulação e gestão dos postes

Os postes são infraestrutura central em tema de iluminação pública, uma vez que consistem no suporte para a instalação das luminárias e poderão igualmente ser utilizados para a instalação de dispositivos de IoT. **Os postes podem compor os ativos de iluminação pública ou os ativos de energia elétrica, caso em que são utilizados também como suporte para cabos de energia elétrica e de serviços de telecomunicações**[280]. Conforme mencionado previamente, a gestão dos postes de iluminação pública é de competência dos municípios (art. 30, V da CF) e a gestão dos postes de energia elétrica é de competência da União (art. 21, XII, b).

277 Disponível em: http://www.aneel.gov.br/documents/656877/14486448/bren2010414.pdf/3bd33297-26f9-4ddf-94c3-f01d76d6f14a?version=1.0. Acesso em: 15.08.2017.

278 Vide voto do relator sobre o resultado da audiência pública, disponível aqui: http://www2.aneel.gov.br/aplicacoes/audiencia/arquivo/2013/107/resultado/voto_do_diretor_relator.pdf. Acesso em: 15.08.2017.

279 Disponível em: http://www2.aneel.gov.br/cedoc/ren2013587.pdf. Acesso em: 15.08.2017.

280 Em regra, a maioria dos postes constitui ativo do setor elétrico, mas existem situações em que são instalados por empresas de telecomunicações ou detidos pelas municipalidades. Aqui trataremos dessa situação, que parece ser a mais complexa e comum.

Nesse sentido, a instalação de dispositivos de IoT em **postes ou braços de iluminação pública** deverá observar a regulamentação específica do município e os eventuais contratos de concessão estabelecidos. Isso poderá significar a necessidade de remoção ou observação de eventuais limitações à instalação nos postes de câmeras, sensores e demais equipamentos para soluções de IoT. Também poderá ser necessário verificar a existência de regulamentação específica sobre a quantidade de pontos que poderão ser instalados nos postes e braços de Iluminação Pública do Município e os valores cobrados para o compartilhamento de infraestrutura.

Esse cenário já vem sendo enfrentado pelas empresas de telefonia que, ao buscar aumentar a oferta de internet móvel por meio da implementação de antenas em postes de iluminação pública, tem lidado com restrições impostas por legislação municipal urbanística.[281] A título de exemplo, na cidade de São Paulo atualmente tramita Projeto de Lei nº 751/2013[282] que visa remover obstáculos às instalações de Estação Rádio Base - ERB no município. Entre outros objetivos, a proposta autoriza cessões não exclusivas de uso de áreas públicas a prestadores serviços de transmissão de radiofrequência e simplifica procedimentos de licença para a instalação da infraestrutura suporte necessária. A despeito de a proposta estar com a tramitação suspensa, há notícias de que a prefeitura vem estudando a possibilidade de editar decreto ou enviar novo texto normativo sobre o tema para a Câmara dos Vereadores.[283]

Por sua vez, os **postes de energia elétrica** são de propriedade da União e geridos pela distribuidora de energia elétrica, que possui obrigação legal de zelar pela integridade desses bens públicos (art. 31, VII da Lei nº 8.987/1995). Em razão disso, **a transferência dos ativos de iluminação pública prevista pela Resolução Aneel nº 414/2010 não incluiu a transferência dos postes que servem de suporte ao serviço de distribuição de energia elétrica**, os quais permanecem como ativo do serviço público federal.

Sua infraestrutura é compartilhada com outros serviços, dentre os quais se destaca o serviço de telecomunicações[284], motivo pelo qual a utilização dos postes de energia elétrica observa também regras sobre telecomunicações, como a Lei nº 9.472/1997 (Lei Geral de Telecomunicações, LGT) e a Lei nº 13.116/2015 (Lei Geral de Antenas). Em

281 Sobre o tema, vide: https://oglobo.globo.com/sociedade/tecnologia/operadoras-apostam-nas-antenas-em-postes-de-luz-para-melhorar-cobertura-9815112 Acesso em 19.09.2017.

282 Proposta original disponível aqui: http://documentacao.camara.sp.gov.br/iah/fulltext/projeto/PL0751-2013.pdf Acesso em 20.09.2017.

283 http://www.telesintese.com.br/nova-proposta-de-lei-das-antenas-em-sao-paulo-reve-conceito-de-erb/ Acesso em 20.09.2017.

284 Esse compartilhamento de infraestrutura permite a potencialização de estrutura já existente, a redução de custos de instalação e manutenção dos postes e, por vezes, viabiliza a expansão da estrutura onde sua instalação não seria viável isoladamente. SUNDFELD, Carlos Ari. Estudo Jurídico sobre o preço de compartilhamento de infra-estrutura de energia elétrica. Revista Eletrônica de Direito Administrativo Econômico, nº 4, nov/dez de 2006. Disponível em http://www.direitodoestado.com/revista/REDAE-4-NOVEMBRO-2005-CARLOS%20ARI%20SUNDFELD.pdf Acesso em 19.09.2017.

especial, referidas normas determinam que os valores e condições exigidos das empresas de telecomunicações pelo compartilhamento de infraestrutura sejam justos e razoáveis (art. 73, LGT), e que as respectivas Agências Reguladoras serão responsáveis por estabelecer parâmetros relacionados à instalação, operação, manutenção e remoção dessa infraestrutura de suporte (art. 13, I da Lei de Antenas).

3.1.4.3.2. Cenário regulatório sobre postes de energia elétrica

Tendo em vista sua competência compartilhada para regular o tema, a ANEEL, a ANATEL e a ANP[285] editaram a Resolução Conjunta nº 01/1999, que estabelece regras gerais para o compartilhamento de postes de energia elétrica. Em especial, referida resolução prevê (i) liberdade para o estabelecimento de preço a ser pago por empresas de telecomunicações pela ocupação de pontos de fixação de poste; (ii) o papel do detentor da infraestrutura em determinar e gerir sua capacidade de compartilhamento; e (iii) a obrigatoriedade de homologação do contrato de compartilhamento pela Agência competente.

Em 2001, a ANATEL editou a Resolução nº 274 para regulamentar certos dispositivos da Resolução Conjunta nº 01/1999, reforçando a competência da concessionária em determinar e gerir a capacidade de compartilhamento de sua infraestrutura e estabelecendo regras para o compartilhamento da capacidade excedente. Referida resolução foi revogada pela Resolução nº 683, publicada em 09 de outubro de 2017, que estabelece a obrigatoriedade da concessionária em compartilhar a capacidade excedente da infraestrutura de suporte quando solicitado pela prestadora dos serviços de telecomunicações. Igualmente, a ANEEL editou a Resolução nº 581/2002 que estabeleceu requisitos mínimos de qualidade, segurança e proteção ao meio ambiente e às obrigações das concessionárias envolvidas no compartilhamento dos postes.

A ausência de parâmetros balizadores dos valores de contratação entre as concessionárias permitiu a ocorrência de impasses negociais que, por sua vez, estimulou a aprovação da Resolução Conjunta nº 04/2014[286], que aprova o preço de referência em R$ 3,19 por ponto de fixação e estabelece regras adicionais ao compartilhamento de postes entre distribuidoras de energia elétrica e prestadoras de serviços de telecomunicações. A resolução também determina que uma mesma empresa de telecomunicações, individualmente ou conjuntamente com empresas do mesmo grupo, somente poderá ocupar um ponto de fixação por poste, salvo situações excepcionais e mediante autorização da ANEEL. Não há, todavia, vedação à utilização de um mesmo

[285] A ANP assina em conjunto porque a Resolução trata também de dutos.

[286] Resultante da Consulta Pública Anatel nº 30/2013 e da Audiência Pública ANEEL nº 07/2007.

ponto de fixação por mais de uma prestadora de serviços, caso em que o valor será pago apenas pela empresa contratualmente responsável (art. 3º, parágrafo único).

Também incidem sobre compartilhamento de postes normas técnicas da ABNT, em especial ABNT NBR 5434/1982 – Redes de distribuição aérea urbana de energia elétrica e a ABNT NBR 15214/2004 – Compartilhamento de infraestrutura com redes de telecomunicações. Referidos normativos apresentam critérios técnicos para a instalação de pontos de fixação em postes, tendo em vista o espaço da faixa de fixação de 50 centímetros. A quantidade exata de pontos de fixação por postes será fixada pela concessionária[287], que deverá considerar custos e a obrigação de segurança e zelo pela infraestrutura do poste.

3.1.4.3.3. Reflexos da regulação de postes de energia sobre serviços de IoT

A regulamentação brevemente apresentada se mostra relevante às políticas de fomento à implementação de tecnologias máquina-a-máquina no país por dois principais motivos: (i) sustentabilidade do sistema para novos atores de mercado que precisem utilizar espaços em postes; e (ii) restrições à quantidade de pontos de fixação em postes poderá, por sua vez, restringir a implementação de dispositivos de IoT.

Em relação ao primeiro ponto, a utilização do valor referência estabelecido pela Resolução Conjunta nº 04/2014 para outros segmentos de mercado poderá prejudicar a capilaridade da instalação de dispositivos de IoT ou a expansão de pequenos provedores de internet.[288] Alternativas podem ser adotadas, como o compartilhamento de um mesmo ponto de fixação por mais de um serviço ou por diversas empresas prestadoras de um mesmo serviço, a exemplo do *Ran Sharing* praticado notadamente em torres de telecomunicações.[289-290]

[287] Vide, por exemplo: https://www.aeseletropaulo.com.br/padroes-e-normas-tecnicas/manuais-normas-tecnicas-e-de-seguranca/Documents/Padr%C3%B5es%20e%20Normas%20T%C3%A9cnicas/ID-4.044-Compartilhamento%20de%20Infraestrutura%20de%20RDA%20com%20Redes%20de%20Telecomunica%C3%A7%C3%B5es.pdf , http://www.celesc.com.br/portal/images/arquivos/normas/AnexoII-I3130015-Compartilhamento_Postes-23-11-09.pdf e http://www.eneldistribuicao.com.br/rj/documentos/PE2012_R-02.pdf Acesso em 20.09.2017

[288] Sobre o tema, vide: http://www.abranet.org.br/Noticias/Provedores-alertam-que-acordo-Anatel%7CAneel-por-postes-nao-funciona-na-pratica-1515.html?UserActiveTemplate=site#.WcEoWrKGO01 Acesso em 19.09.2017.

[289] Em síntese, *ran sharing* é um tipo de compartilhamento utilizado por operadoras brasileiras, que pode assumir diversos modelos, e que permite o compartilhamento de rede de acesso e de frequência por duas ou mais empresas de telecomunicações. A alternativa tem sido amplamente utilizada por empresas de telecom brasileiras, conforme se verifica: http://www.telesintese.com.br/projeto-de-ran-sharing-entre-tim-oi-e-accenture-ganha-premio-em-barcelona/ Todavia, a iniciativa tem sido questionada pelas detentoras de torres, uma vez que o compartilhamento reduziria sua receita, dado que valor dos pontos são atualmente remunerados por espaço ocupado – e não pela quantidade de operadoras que efetivamente ocupa a torre.

[290] Vide, por exemplo, conflito estabelecido entre a Nextel e a SBA Torres relacionado ao contrato de ran sharing estabelecido entre a Vivo e a Nextel foi encaminhado à Anatel (ANATEL, Processo nº 53504.011048/2016-12, interessados: NEXTEL TELECOMUNICAÇÕES LTDA., SBA TORRES BRASIL, julgado em 21/12/2016).

Há também a possibilidade de exercer pressão para a redução do valor referência estabelecido pela Resolução nº 04/2014, que segue sendo objeto de acirrado debate entre distribuidoras de energia elétrica e empresas de telecomunicações. Existiram propostas anteriores nesse sentido, como a apresentação de Proposta de Decreto Legislativo nº 49/2016 perante a Câmara dos Deputados, destinada a sustar os efeitos da Resolução, mas cuja tramitação foi encerrada por solicitação do próprio autor da proposta.[291]

A quantidade de pontos em postes, por sua vez, poderá obstaculizar a instalação de novos dispositivos de IoT ou de difusão de internet. Será necessário, para tanto, incentivar o compartilhamento de dispositivos de IoT entre serviços, públicos ou privados, e investir em alternativas como a instalação de antenas em topos de edifícios, a implementação de Estações Rádio Base subterrâneas[292], implantação de infraestrutura passiva subterrânea, entre outras. A despeito, é de relevância a observância do limite de pontos em postes, visto que a instalação de dispositivos e cabos em peso superior ao comportado pelo poste poderia provocar riscos à segurança dos serviços por ele suportados e dos próprios cidadãos.

3.1.4.4. Financiamento da iluminação pública

A insuficiência financeira e organizacional de municípios para expandir, modernizar e gerir o sistema de iluminação pública justificou a instituição de taxas de iluminação pública, que foram declaradas inconstitucionais pelo Supremo Tribunal Federal.[293] Também estimulou a instituição de autarquias ou empresas públicas próprias ou a contratação de parcerias público-privadas de longo prazo.[294] Outra externalidade dessa carência de recursos municipais foi a aprovação da Emenda Constitucional nº 39/2002[295], que incluiu o art. 149-A ao texto da Constituição Federal, autorizando Municípios e o

291 Vide: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2093587 Acesso em 19.09.2017.

292 Sobre o tema, vide: http://economia.estadao.com.br/blogs/radar-imobiliario/nos-edificios-topo-e-subsolo-podem-ser-fontes-de-renda/ e http://www.ebc.com.br/noticias/economia/2013/12/operadoras-de-celular-buscam-alternativas-para-instalacao-de-antenas-e Acesso em 21.09.2017.

293 Vide argumentos e deliberações em torno da aprovação da Súmula Vinculante nº 41, que determina "o serviço de iluminação pública não pode ser remunerado mediante taxa", disponível aqui: http://www.stf.jus.br/portal/jurisprudencia/menuSumario.asp?sumula=2218 Acesso em: 04.09.2017.

294 ANTUNES, Vitor Amuri. **Parcerias público-privadas para cidades inteligentes**. Disponível em: http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5.

295 Nesse sentido, vide parecer do relator da Comissão Especial da Câmara dos Deputados sobre a PEC nº 559/2002 do Senado Federal, disponível aqui: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=85426&filename=PRL+1+PEC50402+%3D%3E+PEC+559/2002 Acesso em: 04.09.2017.

Distrito Federal a instituírem a "contribuição para o custeio do serviço de iluminação pública".

Não obstante a referida emenda à Constituição, Leis Municipais que instituíram contribuições com base no art. 149-A, em geral denominadas **Contribuição para o Serviço de Iluminação Pública (COSIP)**, tiveram sua constitucionalidade questionada perante o Supremo Tribunal Federal. Esse foi o caso do Recurso Extraordinário nº 573.675, em que o Ministério Público de Santa Catarina questionou a instituição da COSIP pelo município de São José, julgado improcedente pelo STF para reconhecer a constitucionalidade da contribuição e diferenciá-la de impostos e taxas.[296]

Resta pendente, todavia, debate em torno da possibilidade de endereçar verbas da COSIP para o financiamento de PPPs que terão dentre seus objetivos a modernização de serviços de iluminação pública, ora entendida como investimento na rede e como implementação de dispositivos de IoT.[297] Trata-se de aspecto de grande relevância para a implantação de parcerias no segmento de iluminação pública, bem como para a própria difusão de soluções de IoT.

Uma questão particularmente delicada nesse sentido é acerca da **possibilidade de destinação da verba da COSIP para ações de melhoramento e expansão da rede**, o que certamente influencia na possibilidade de serem acopladas à infraestrutura de iluminação pública de tecnologias que poderão ser utilizadas de forma integrada para a prestação de serviços públicos de outra natureza, como transporte e segurança.

Especificamente sobre a destinação da verba da COSIP para o melhoramento e expansão da rede[298] - que não abrange a modernização com sensores e dispositivos dotados de conectividade -, há processo pendente de julgamento no Supremo Tribunal Federal, consistente no **Recurso Extraordinário nº 666404 com Repercussão Geral reconhecida** em novembro de 2013. A Procuradoria Geral da República apresentou manifestação no processo, tendo opinado que o termo *custeio do serviço de iluminação pública* "não é empregado de forma restritiva ou técnica que obrigue excluir de seu comando os serviços de melhoramento e expansão da rede, admitindo a destinação dos recursos advindos da

296 Notícia sobre o caso pode ser verificada em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=105304 Acesso em: 04.09.2017.

297 A Frente Parlamentar Mista em Apoio às Cidades Inteligentes e Humanas propõe entre suas prioridades a alteração da lei da COSIP, permitindo que os recursos da mesma sejam utilizados também para instalação de tecnologias eficientes e integradas, voltadas à implementação das cidades inteligentes. Mais informações em: http://fpcidadesinteligentes.com.br/index.php/5-prioridades-iniciais/. Acesso em: 24.08.2017.

298 Melhoria e expansão da rede envolve atividades como a elaboração de projeto, aquisição de materiais e equipamentos e execução das obras.

contribuição não apenas para remunerar o serviço de iluminação em sentido estrito, mas todas as ações que o processo de seu fornecimento implica".[299]

Referido debate se torna relevante na medida em que a COSIP tem se constituído como a principal fonte de financiamento dos serviços relacionados à iluminação pública e poderá ser utilizada também para a implementação nos postes de iluminação novas tecnologias com suporte máquina-a-máquina. A solução do referido debate poderá respaldar o entendimento de que é igualmente possível a utilização da verba da COSIP para implementar sistema de iluminação pública inteligente, de modo a garantir maior segurança jurídica na publicação de editais de PPP de iluminação pública. Isso porque poderá embasar a redução de casos de suspensão de certames por decisão de Tribunais de Contas locais em virtude de divergência a respeito da destinação da COSIP.

Diante do cenário exposto e com vistas a evitar a obstrução de projetos de iluminação inteligente, avalia-se a possibilidade de ser **apresentada nova Proposta de Emenda à Constituição (PEC) com o objetivo de adicionar o artigo 149-B à Constituição Federal**, para expressamente autorizar a destinação da COSIP à implementação de rede de iluminação pública inteligente.[300] Outra possibilidade seria a apresentação **perante o STF,** seja por parte do Governo Federal, seja por partes privadas com competência para apresentação de *amicus curiae*, de manifestação explicitando as questões listadas acima.

3.1.4.5. Financiamento das PPPs em iluminação pública

Na medida em que inúmeros municípios sequer possuem capacidade financeira e organizacional para prestar o serviço tradicional de iluminação pública, o **estabelecimento de Parcerias Público-Privadas** se mostra opção bastante interessante.[301] Primeiro porque a parceria público-privada consiste em **alternativa viável do ponto de vista jurídico**, pois é espécie de concessão administrativa (art. 2º, § 2º, da Lei nº 11.079/2004), principal opção para a contratação em longo prazo de serviços públicos que não podem ser remunerados por tarifa.[302]

299 Adicionalmente, o PGR afirmou que "Verifica-se, ainda, que a inclusão do melhoramento e expansão da rede dentre as ações a serem custeadas pela contribuição em tela é medida necessária para que o serviço de iluminação pública possa ser prestado em toda a potencialidade, pois não há outra maneira menos gravosa, que não contribuir nos termos estabelecidos constitucionalmente, para se ter o serviço prestado com isonomia, eficiência e qualidade." Disponível em: http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4179476. Acesso em: 24.08.2017.

300 Proposta da Rede Cidades Inteligentes, disponível em: http://fpcidadesinteligentes.com.br/index.php/5-prioridades-iniciais/. Acesso em: 04.09.2017.

301 Cumpre ressalvar que outros aspectos da regulação de PPP demandam aprofundamento e reflexão. Todavia, neste relatório serão abordadas somente questões extitamente relacionadas à implementação de rede de iluminação pública inteligente pelos municípios.

302 ANTUNES, Vitor Amuri. Parcerias público-privadas para smart cities. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 40-41.

De forma distinta das tradicionais concessões para serviços públicos (regidas pela Lei nº 8.987/1995), o concessionário presta serviço diretamente à própria Administração. Desse modo, a remuneração do concessionário não envolveria a cobrança de tarifa, mas a contraprestação paga pela entidade pública.[303] Daí a importância de solucionar as dúvidas sobre o uso da COSIP – uma vez que tais receitas configuram fonte importante para as parcerias.

Nesse sentido, é relevante ressaltar a possibilidade de os projetos de PPPs de iluminação poderem contar com outras fontes de receita para além de verbas oriundas da COSIP, de modo que **eventual interpretação restritiva a respeito da utilização da COSIP não inviabiliza financeiramente, por si só, a implementação de rede de iluminação pública inteligente**.

Com efeito, a escassez de recursos públicos resulta em dificuldade por parte de municípios brasileiros em implantar projetos de expansão, manutenção e modernização de serviços públicos. Todavia, a legislação já prevê a possibilidade de contratos de concessão preverem receitas alternativas, acessórias[304] e a implementação de receitas diversificadas. Além disso, é possível agregar receita ao contrato de PPP de iluminação pública por meio da cobrança pelo compartilhamento da infraestrutura das luminárias para o desempenho de outros serviços públicos mediante tecnologias de IoT. Conforme mencionado anteriormente, a instalação, nas luminárias e em seus braços, de sensores, câmaras e demais dispositivos destinados à prestação de serviços públicos, como a segurança pública e a mobilidade, poderá ser desempenhada de forma remunerada. [305-306]

Nesse sentido, compreender a extensão do alcance da COSIP poderá colaborar para assegurar segurança jurídica aos editais e contratos de PPP, dado que restringirá as possibilidades de a parceria ser questionada perante Tribunais de Contas ou Judiciário. A despeito disso, eventual cenário de restrição do escopo COSIP, embora seja uma fonte relevante de receita, não inviabiliza por si só a implementação de projetos de iluminação pública inteligente porque a legislação vigente já prevê rendas alternativas que viabilizam similares empreendimentos.

303 Cf. ANTUNES, Vitor Amuri. **Parcerias público-privadas para smart cities**. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 43.

304 Embora o texto expresso do artigo 11 da Lei nº 11.079/2004 determine que as verbas acessórias deverão ser destinadas à promoção da modicidade tarifária, há precedente do TCU que autoriza sua utilização para promover a viabilidade econômica do contrato em contraprestação do governo (Acórdão 2886/2008, Rel. Min. Ubiratan Aguiar, j. 03.12.2008).

305 A título de exemplo, o desempenho pelas lâmpadas LED de funções adicionais à simples iluminação do espaço público, colaborando com o fornecimento de dados para os serviços de transporte e segurança pública, permite a celebração de contratos de parceria que prevejam compensação financeira do concessionário.

306 Referidas receitas não substituem a utilização da COSIP e seriam facultativamente auferidas pela concessionária como consequência da prestação de serviços relacionados ao objeto da contratação.

3.1.4.6. Capacidades e experiências de PPPs de iluminação Pública

A contratação com entes privados - aptos a investir em infraestrutura e possuidores da *expertise* técnica para a operação do serviço -, possui o **condão de viabilizar arranjos contratuais inovadores**. Isso possibilitaria a modernização desse serviço, entre outros, pela instalação de lâmpadas tipo LED e pela a implantação de centros de controle automatizados para a manutenção eficiente da rede.

Ainda, a remuneração do concessionário tem sido atrelada ao seu desempenho na prestação dos serviços e assume uma parte dos riscos, previstos em contrato, nos termos do art. 6º, § 1º da Lei nº 11.079/2004.[307] Isto é, de alguma maneira o contrato de PPP detém o **potencial de permitir que o Poder Público dilua determinados riscos operacionais** na implantação das redes inteligentes de iluminação pública, já que a responsabilidade por financiar, equipar e manter em perfeito estado de funcionamento esse sistema será de um parceiro privado, que fará jus às contraprestações baseadas em seu desempenho, conforme padrões de qualidade pré-fixados no contrato.[308]

Até início de 2017, já existiam mais de uma centena de projetos de PPP iniciados pelas municipalidades com o objetivo de implantar sistemas de iluminação pública inteligente. Todos eles foram modelados a partir da espécie de concessão administrativa, sendo o investimento médio de um contrato de PPP para a gestão inteligente da iluminação pública de aproximadamente 273 milhões de reais.[309]

Interessante notar que **três projetos constituem iniciativas consorciadas**, isto é, um único contrato de PPP para servir mais de um município, conforme previsto no art. 241 da Constituição Federal e na Lei nº 11.107/2005.[310] Esse arranjo contratual desvela-se útil (i) a tornar o projeto de iluminação pública inteligente mais barato aos municípios, tendo em vista que as despesas e investimentos feitos pela concessionária são diluídos entre as municipalidades participantes; e (ii) a maximizar a eficiência do contrato de PPP, já que os diversos municípios estarão convergidos em único ponto contratual.[311] Outrossim, a contratação de PPP para o setor de iluminação pública não consiste em tarefa simples para municípios de médio ou pequeno porte, visto que tais contratos possuem

[307] TUROLLA, Frederico; ALLAIN, Marcelo; ANKER, Thomas. Iluminação pública para cidades inteligentes. **Valor Econômico**. São Paulo, 28 de agosto de 2014. Disponível em: http://www.provedor.nuca.ie.ufrj.br/eletrobras/estudos/turolla1.pdf. Acesso em: 15.08.2017.

[308] ANTUNES, Vitor Amuri. **Parcerias público-privadas para smart cities**. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 48.

[309] Ibid., p. 51.

[310] Consórcio Intermunicipal de Iluminação Pública de Alagoas, Consórcio Público Intermunicipal do Agreste Pernambucano e Consórcio Complexo Nascentes do Pantanal, no Maranhão.

[311] Cf. ANTUNES, Vitor Amuri. **Parcerias público-privadas para smart cities**. 2 ed. Rio de Janeiro: Lumen Juris, 2017, p. 52.

complexidades e suas cláusulas e condições criam vínculo pelo período de até 35 anos (art. 5º, II, da Lei nº 11.079/2004).

Dentre os projetos de PPP de iluminação pública inteligente, destaca-se o intentado pelo Município de São Paulo por estar entre os mais vultosos da área e por ter enfrentado inúmeros obstáculos que resultaram na sua paralização. Com vistas à modernização, otimização e expansão de toda a rede de iluminação da cidade de São Paulo, o edital previa como fonte de recurso verbas provenientes da COSIP, e possuía como principais objetivos a substituição das lâmpadas da cidade por luminárias LED dotadas de controlador (dispositivo responsável pela comunicação entre a luminária e o Centro de Controle Operacional) e a criação de novos pontos de luz.[312]

O prosseguimento da contratação foi impedido por reiteradas decisões do Tribunal de Contas do Município, com o respaldo do Tribunal de Justiça do Estado de São Paulo.[313] A primeira paralização estava relacionada a inconsistências técnicas do edital, como a divergência do seu texto com o da minuta enviada para audiência pública.[314] A segunda paralização se deu no momento de abertura dos envelopes das propostas apresentadas pelas empresas concorrentes. O consórcio vencedor apresentou recurso ao TCM devido à não aceitação pela comissão de avaliação das garantias oferecidas. Note que os motivos que obstaculizaram o prosseguimento da PPP não são específicos ao setor de iluminação pública e tampouco estão relacionados ao financiamento com verbas da COSIP.[315]

Assim, a experiência de São Paulo aponta para a relevância das garantias financeiras apresentadas pelo município aos potenciais consorciados quando da publicação do edital e no estabelecimento de contrato de concessão.[316]

A despeito disso, a tendência de implementação de PPPs de iluminação pública se mostra adequada às limitações orçamentárias e organizacionais dos municípios e aproveita a expertise do mercado privado na área. De todo modo, a implementação deverá observar

312 Cf. ANTUNES, Vitor Amuri. **Parcerias público-privadas para cidades inteligentes**. Disponível em: http://www.pppbrasil.com.br/portal/content/artigo-parcerias-p%C3%BAblico-privadas-para-cidades-inteligentes?page=5.

313 De início, o tribunal afirmou que o edital não tinha "condições de prosseguimento". Depois, decidiu que, para prosseguir, o edital terá que passar por "adequações". Mais informações em: http://g1.globo.com/sao-paulo/noticia/2015/10/tcm-autoriza-retomada-de-licitacao-da-ppp-da-iluminacao-publica-em-sp.html; https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2016/10/14/mais-uma-vez-justica-suspende-ppp-da-iluminacao-de-sao-paulo.htm; e http://g1.globo.com/sao-paulo/noticia/2016/10/gestao-haddad-retoma-ppp-da-iluminacao-publica.html. Acesso em: 24.08.2017.

314 Vide http://sao-paulo.estadao.com.br/noticias/geral,mais-uma-vez-justica-suspende-ppp-da-iluminacao-de-sp,10000082137Acesso em 21.09.2017.

315 Vide: http://www.pppbrasil.com.br/portal/content/tcm-suspende-sess%C3%A3o-de-abertura-de-propostas-comerciais-na-ppp-de-ilumina%C3%A7%C3%A3o-p%C3%BAblica-de-s%C3%A3o- Acesso em 21.09.2017.

316 A integra do edital e suas modificações pode ser encontrado em: http://www.prefeitura.sp.gov.br/cidade/secretarias/obras/ilume/noticias/?p=206645

com cautela os requisitos da legislação específica, de modo a evitar sua inviabilização por decisões dos respectivos Tribunais de Contas e Tribunais.

3.1.4.7. Privacidade em Iluminação Pública Inteligente

A iluminação pública está entre os principais segmentos da infraestrutura municipal e vêm sendo modernizada através da instalação de lâmpadas LED, que tem por característica a eficiência energética. Em breve, a essa moderna infraestrutura de iluminação pública serão adicionados mecanismos tecnológicos, como sensores e dispositivos audiovisuais, os quais, para exercerem suas funções, realizam coleta de dados. É o caso, por exemplo, de sensores de luminosidade, câmeras de monitoramento e sensores de captação de ruídos, muitas vezes utilizados por autoridades para a constatação de atividades suspeitas na localidade.[317_318]

Não obstante as oportunidades oferecidas por tais ferramentas acopladas à rede, dentre as quais apontamos a redução do uso de energia elétrica[319] e a gestão eficiente do tráfego urbano, sua potencialidade de coletar dados levanta preocupação com a privacidade dos indivíduos. Já em 2014, o periódico *The New York Times* apontava problemas de privacidade relacionados à captura de dados por sensores e câmeras instalados na iluminação inteligente do aeroporto internacional *Newark Liberty*, nas proximidades da cidade de Nova York. Esses dados, de posse da administradora *Port Authority*, seriam capazes de sistematizar os padrões de comportamentos dos indivíduos que passam pelo local.[320]

Ademais, tal interconexão entre iluminação pública e variados dispositivos conectados à Internet poderá tornar a infraestrutura de iluminação pública vulnerável a ataques cibernéticos, da mesma forma que ocorre com o sistema de medidores elétricos.[321] **Assim, é importante que o Poder Público, com vistas à segurança da informação veiculada nessa estrutura de serviço público, atue de forma colaborativa, incentivando as entidades privadas que fabricam e circulam esses novos dispositivos a adotarem**

317 Conforme: http://www.ul.com/inside-ul/street-smart-security-for-connected-lighting-infrastructure-2/. Acesso em: 20.09.2017. Em Doncaster, no Reino Unido, postes de iluminação pública ganharam 33 mil pontos LED que fazem uso de tecnologia de banda larga sem fio capaz de transformar cada lâmpada em um roteador. Fonte: http://www.techradar.com/news/world-of-tech/why-you-should-be-worried-about-connected-street-lights-1327834. Acesso em: 20.09.2017.

318 Tratamos desses equipamentos de forma mais detalhada no tópico sobre segurança em Cidades.

319 Através da implementação de dispositivos de monitoramento da intensidade luminosa, a cidade de Nice, na França, espera reduzir os valores gastos com energia elétrica em por volta de 8 milhões de dólares. In: CHAMBERS, John; ELFRINK, Wim. The future of cities: The internet of everything will change how we live. **Foreign Affairs**. 31 out. 2014. Disponível em: https://www.foreignaffairs.com/articles/2014-10-31/future-cities. Acesso em: 20.09.2017.

320 Fonte: https://www.nytimes.com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you.html. Acesso em: 20.09.2017.

321 Fonte: http://www.ul.com/inside-ul/street-smart-security-for-connected-lighting-infrastructure-2/. Acesso em: 20.09.2017.

padrões de conduta adequados ao quadro legislativo sobre privacidade e proteção de dados pessoais.[322]

Por fim, indica-se para contexto de iluminação pública inteligente as mesmas resoluções acima apontadas para os medidores elétricos, entre elas, (i) a necessidade de edição de lei específica para a proteção de dados pessoais, capaz de consolidar os entendimentos jurídicos ainda esparsos sobre o tema e determinando que a proteção alcance os dados coletados pelo setor público; (ii) desnecessidade de obtenção de consentimento prévio para dados pessoais indispensáveis à prestação de serviços públicos essenciais; (iii) respeito ao princípio da finalidade na coleta do dado, que só poderá ser usado para aqueles fins específicos; (iv) existência de mecanismos de "opt-out" para o usuário do serviço, que poderá optar por não ter seus dados pessoais utilizados para finalidade distinta da estrita prestação do serviço público essencial, e não poderá ser penalizado por essa opção; e (v) adoção de variadas técnicas de anonimização e agregação de dados, inclusive quanto a dados coletados no espaço público – quando não incompatível com sua finalidade originária; (v) determinação normativa de que os dados não possam ser compartilhados com terceiros, exceto se anonimizados ou no caso de consentimento prévio livre, expresso e informado; (vi) determinação de que os dados não possam ser compartilhados com nenhum outro órgão governamental (como Receita Federal, autoridades policiais, dentre outros) exceto no caso de ordem judicial prévia e circunscrita autorizando esse compartilhamento.

3.1.5 Mobilidade urbana

A mobilidade, consistente na facilidade em que pessoas e bens deslocam no ambiente urbano, é elemento crucial para a qualidade de vida e para a acessibilidade a serviços essenciais nas cidades, além de produzir efeitos imediatos no desenvolvimento social e econômico. A qualidade da mobilidade reflete diretamente na forma como o cidadão experiência a cidade, visto que a segurança e os períodos de trajeto importam em barreiras ou facilidade de acesso a trabalho, a centros de lazer e aos serviços públicos em geral.

Atualmente a mobilidade nos centros urbanos brasileiros possui muitos congestionamentos, falta de oferta de transporte público e elevados índices de acidentes

[322] A empresa responsável pela tecnologia *Sensity Systems*, voltada à instalação de luminárias LED e sensores acoplados, declara que pretende endereçar as questões de privacidade advindas de sua atividade através de atuação conjunta com a *American Civil Liberties Union* (ACLU) e da implementação de cargo responsável por lidar com o assunto (*chief privacy officer*). Manifestação disponível em: https://atelier.bnpparibas/en/smart-city/article/turning-street-lighting-system-gathering-big-data. Acesso em: 20.09.2017.

de trânsito. Dentre os desafios ao aprimoramento da circulação de bens e pessoas no espaço urbano, que serão mais detidamente abordados a seguir, estão[323]:

- Redução no tempo de deslocamento e melhoria na experiência do cidadão no trânsito,
- Aprimoramento da gestão do transporte público, com especial enfoque à promoção de eficiência, segurança e qualidade do serviço;
- Priorização do transporte público em detrimento do automóvel particular;
- Integração entre diferentes modais de transporte;
- Estímulo à locomoção não motorizada (pedestres e bicicletas); e
- Adoção de medidas para assegurar a acessibilidade universal.

Conforme será apresentado a seguir, a adoção de dispositivos de IoT nos equipamentos e infraestrutura de trânsito e transporte público poderão colaborar com a consecução dos mencionados objetivos e, consequentemente, com o aprimoramento da experiência do cidadão nas cidades.[324] São inúmeras as possíveis soluções de IoT em mobilidade, como a utilização de câmeras e sensores para a coleta de informações que permitam a modulação do trânsito em tempo real. Todavia, a avaliação do ambiente regulatório de mobilidade se restringirá a dois aspectos, consistentes em: (a) controle centralizado e adaptável de trânsito; e (b) monitoramento da circulação de transporte público.

3.1.5.1. Competências em mobilidade urbana

O desenho e a implementação de políticas de **trânsito e transporte** que contem com tecnologias de IoT devem ter em mente que a **competência legislativa sobre o tema é privativa da União**, sendo autorizado a Estados legislar sobre o tema mediante autorização expressa em Lei Complementar (art. 22, inciso XI e parágrafo único, da Constituição Federal).[325]

323 Nesse sentido, aponta-se, no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017. Nesse mesmo sentido, vide: http://sengeba.org.br/wp-content/uploads/2015/09/merged.pdf. Acesso em: 15.09.2017.

324 Agradecimentos a Pedro do Carmo Baumgratz de Paula pelas contribuições sobre IoT em questões de mobilidade. A seguir apresentamos obras de sua autoria ou participação relacionadas a mobilidade em cidades inteligentes: http://sengeba.org.br/wp-content/uploads/2015/09/merged.pdf e http://www.ibdu.org.br/eficiente/sites/ibdu.org.br/pt-br/site.php?secao=noticias&pub=62. Acesso em: 14.11.2017.

325 O Supremo Tribunal Federal possui entendimento reiterado pela competência privativa da União para legislar sobre trânsito e transporte. Nesse sentido se manifestou o STF: "O disciplinamento da colocação de barreiras eletrônicas para aferir a velocidade de veículos, por inserir-se na matéria trânsito, é de competência exclusiva da União (art. 22, XI, da CF/1988). [ADI 2.718, rel. min. Joaquim Barbosa, j. 6-4-2005, P, DJ de 24-6-2005.] = ADI 3.897, rel. min.

Em relação ao **trânsito**, é autorizado aos demais entes federados estabelecer políticas públicas desde que relacionadas à segurança no trânsito, que compreende ações de educação, engenharia, fiscalização de trânsito e demais atividades previstas em lei que promovam o direito à mobilidade urbana eficiente (arts. 23, XII e 144, § 10, I e II da CF).[326]

O **transporte**, por sua vez, possui maiores especificidades na distribuição de competências. À União compete privativamente instituir diretrizes básicas para o desenvolvimento urbano e para legislar sobre política nacional de transportes (art. 22, IX e XX da CF). Aos Estados compete a regulação dos serviços intermunicipais de transporte[327]-[328] e aos Municípios recai a competência para organizar e prestar o serviço público de transporte coletivo dentro dos limites urbanos (art. 30, V). Assim, a regulamentação e fiscalização dos serviços de **transporte** são exercidas conjuntamente por todas as esferas federativas, a depender da área territorial na qual o transporte será realizado.

Portanto, **regulação sobre a utilização de dispositivos de IoT destinados à promoção de mobilidade inteligente** deve observar tanto leis federais como legislação estadual e municipal relacionada à segurança no trânsito e transporte. Destaca-se nesse cenário o Código de Trânsito Brasileiro (Lei nº 9.503/1997), as normas regulamentares editadas pelo Conselho Nacional de Trânsito - CONTRAN, a Política Nacional de Mobilidade Urbana (Lei nº 12.587/2012) e normas municipais sobre mobilidade e transporte (em regra contidas no Plano Diretor ou em Plano de Mobilidade).

3.1.5.2. Trânsito: controle centralizado e adaptável

3.1.5.2.1. Oportunidades decorrentes do uso de soluções IoT

Gilmar Mendes, j. 4-3-2009, P, DJE de 24-4-2009". Veja também a ADI 3.671 MC, rel. min. Cezar Peluso, j. 28-8-2008, P, DJE de 28-11-2008."

326 Nesse sentido já se manifestou o Supremo Tribunal Federal: "O art. 1º da Lei catarinense contempla matéria afeita à competência administrativa comum da União, dos Estados-membros, do Distrito Federal e dos Municípios, conforme previsto no inciso XII do art. 23 da CR, pelo que nele podem estar fixadas obrigações, desde que tenham pertinência com as competências que são próprias do Estado federado e que digam respeito à segurança pública e à educação para o trânsito" (ADI 2.407, rel. min. Carmen Lúcia, j. 31-5-2007, P, DJ de 29-6-2007).

327 Caberá à União permitir, mediante autorização, concessão ou permissão, que entes privados explorem os serviços de **transporte rodoviário interestadual** (art. 21, XII, CF).

328 O Supremo Tribunal Federal decidiu que "**os Estados-membros são competentes para explorar e regulamentar a prestação de serviços de transporte intermunicipal**. (...) A prestação de transporte urbano, consubstanciando serviço público de interesse local, é matéria albergada pela competência legislativa dos Municípios, não cabendo aos Estados-membros dispor a seu respeito (ADI 2.349, rel. min. Eros Grau, j. 31-8-2005, P, DJ de 14-10-2005).

Os sistemas já amplamente utilizados pela Administração Pública no controle do trânsito urbano, tais como os de monitoramento por vídeo[329] e de radares, poderão ter suas funcionalidades potencializadas com a adição de novas tecnologias, como é o caso da OCR (*Optical Character Recognition*), capaz reconhecer automaticamente placas de veículos[330], e sensores instalados em ciclovias e calçadas para quantificar o fluxo de pedestres ou para produzir energia.[331] Para oferecer suporte adicional ao controle de tráfego, as **soluções de IoT deverão estar interconectadas a uma central de processamento de dados, possibilitando a identificação das condições do trânsito e a promoção de ações para melhorias do fluxo de veículos, ciclistas e pedestres**.[332]

Entre as oportunidades viabilizadas pela utilização desses dispositivos para a coleta e processamento de dados está a **melhor configuração de temporização dos semáforos**, através de **práticas de redirecionamento do tráfego em tempo real**, o que propiciará a **otimização da circulação de pedestres, carros e ciclistas**. Com base em um simples comando na central de controle, será possível alterar o tempo de espera em um cruzamento em razão do fluxo de tráfego.[333-334]

329 Para uma análise pormenorizada do uso de câmeras de vigilância pelo Poder Público, ver observações veiculadas no tópico sobre segurança em Cidades. Nele, descrevemos os avanços experimentados pelos tradicionais sistemas de CCTV e as implicações que isto pode trazer à privacidade dos cidadãos.

330 Nesse sentido, aponta-se, no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017, que "radares instalados em pontos estratégicos são utilizados não apenas para o controle de velocidade mas para a identificação de todos os veículos que passam por este trajeto".

331 Em Londres foi inaugurada calçada capaz de gerar energia a partir da pressão feita por pedestres quando caminham. Vide: http://ciclovivo.com.br/noticia/rua-inteligente-que-gera-energia-e-inaugurada-em-londres/ e http://www.techtudo.com.br/artigos/noticia/2011/03/conceito-uma-calcada-que-transforma-passos-de-pedestres-em-energia.html Acesso em: 14.11.2017.

332 Como observado ao longo do relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

333 Em 08 de maior de 2017 a cidade de Salvador inaugurou o funcionamento de sistema de semáforos inteligentes, interligados entre si e permitindo a comunicação e ajuste do fluxo do trânsito em tempo real. Vide: http://atarde.uol.com.br/transito/noticias/1859571-semaforos-inteligentes-comecam-a-funcionar-em-salvador Acesso em 14.11.2017. Esse também é o objetivo da Prefeitura de São Paulo que, em conjunto com a CET, prepara-se para lançar Parceria Público-Privada (PPP) para modernizar a rede de semáforos da cidade, implementando tecnologia para estes sejam operados à distância. Fonte: Dória vai lançar PPP para modernizar semáforos de SP. **O Estado de São Paulo, São Paulo**, 26 jul. 2017. Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,doria-deve-lancar-ppp-para-modernizar-semaforos-de-sp,70001906369. Acesso em: 12.09.2017.

334 Desde 2011, encontra-se em tramitação no Congresso Nacional o Projeto de Lei nº 1.542, cujo objetivo é determinar, no Código Brasileiro de Trânsito (CTB), obrigação para que o Poder Público instale temporizadores (cronômetros) nos semáforos que contarem com radares detectores de avanço do sinal vermelho. Texto disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=507344. Acesso em: 21.09.2017.

Também poderão ser oferecidas em tempo real informações à população sobre o trânsito em cada localidade.[335] A oferta desse serviço pode ser aprimorada através de dados provenientes de mídias sociais e plataformas que permitem o monitoramento de condições pelos usuários. É o caso da parceria celebrada entre a aplicação *Waze* e a Prefeitura de São Paulo, a fim de repassar ao Poder Público informações disponíveis em seu sistema sobre a existência de semáforos quebrados na cidade. Segundo a Companhia de Engenharia de Tráfego - CET, esse programa de cooperação público-privada tem o condão de reduzir o tempo de resposta às falhas detectadas no sistema de controle do tráfego.[336] De forma similar, o Centro de Operações Rio - COR, instituído na cidade do Rio de Janeiro, utiliza a plataforma da aplicação para avisar os cidadãos sobre intervenções programas ou outros tipos de ocorrência de possam impactar o tráfego.[337]

3.1.5.2.2. Regulação dos equipamentos de controle de trânsito

Em vista da **competência privativa da União** para legislar sobre trânsito, em 1997 foi editado a Lei nº 9.503/1997 (Código de Trânsito Brasileiro - CTB), que dispõe sobre o Sistema Nacional de Trânsito, as regras de conduta no trânsito e as infrações ao seu descumprimento. A incorporação de novas tecnologias ao sistema de gestão do tráfego deverá, portanto, levar em consideração as normas e competências estabelecidas pelo CTB.

A regulamentação do disposto no CTB compete ao **Conselho Nacional de Trânsito - CONTRAN**, entidade normativa e consultiva do Sistema Nacional de Trânsito (art. 12), de modo que a modernização da infraestrutura de trânsito deverá contar com seu apoio e normatização. Em especial, o CTB veda a utilização de mecanismos de sinalização que não estejam previstos em legislação de trânsito, sendo autorizado ao CONTRAN permitir o uso experimental e temporário de diferentes modalidades de sinalização (art. 80, *caput* e § 2º).

Ao CONTRAN incumbe também **a organização e elaboração de manuais e normas referentes à implementação dos equipamentos** de trânsito por ele aprovados (art. 12, XIX do CTB). Em virtude disso, o órgão vem emitindo normativas para regulamentar a

335 Tais oportunidades advindas da aplicação de tecnologia IoT ao trânsito encontram-se devidamente descritas no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

336 Fonte: Dória anuncia parceria com aplicativos de trânsito para monitorar semáforos. **Folha de São Paulo**. 20 set. 2017. Disponível em: http://www1.folha.uol.com.br/cotidiano/2017/09/1920134-doria-anuncia-parceria-com-aplicativo-de-transito-para-monitorar-semaforos.shtml. Acesso em: 21.09.2017.

337 Conforme matéria disponibilizada pela Prefeitura do Rio de Janeiro em maio de 2017: http://prefeitura.rio/web/guest/exibeconteudo?id=6993721. Acesso em: 28.09.2017.

utilização de determinados dispositivos, tais como os sistemas de videomonitoramento, os medidores de velocidade e os instrumentos de identificação de veículos.

A modernização e integração dos dispositivos tecnológicos que monitoram o fluxo do tráfego urbano também encontra respaldo na Lei Federal nº 12.587/2012 (Política Nacional de Mobilidade), que regulamenta o art. 182 da Constituição Federal e estabelece normas gerais sobre mobilidade urbana. Dentre outros, referida norma determina a integração das redes de transporte das cidades (art. 1º), a eficiência e segurança no deslocamento de pessoas (art. 5º, IV, VI e XI) e o incentivo ao desenvolvimento científico-tecnológico (art. 6º, V). [338] Estabelece também a priorização da utilização de transportes não motorizados e dos serviços de transporte público em relação ao transporte individual motorizado (art. 6º, II), que poderão ser potencializados mediante a utilização de dispositivos de IoT.

Não obstante a regulação federal sobre trânsito, os **Municípios** assumem relevância no tema, visto que seus órgãos e entidades de trânsito serão responsáveis pela **implantação, manutenção e operação** de equipamentos de controle viário (art. 24, III do CTB). [339] Conforme será mais detalhadamente descrito, referida atividade municipal deverá ser prevista em normativo específico, como o plano diretor e a política de mobilidade municipal. A título de exemplo, o plano diretor da cidade de São Paulo (Lei nº 16.050/2014)[340] prevê ações e diretrizes como o aumento no tempo semafórico nas travessias em locais de grande fluxo de pedestres (art. 222, VIII) e a elaboração de planos semafóricos e de comunicação com controladores para viabilizar a fluidez no trânsito com priorização para o transporte coletivo (art. 245, I, "c"). Em virtude disso, editou recentemente o Estatuto do Pedestre (Lei Municipal nº 16.673/2017)[341], que assegura ao pedestre a possibilidade de usufruir de sinais de trânsito luminosos de tecnologia inteligente, dotados de temporizadores.

Em relação à utilização de **aparelhos eletrônicos**, incluindo os **equipamentos audiovisuais** para a comprovação de infrações de trânsito, está disposta no art. 280, § 2º, do CTB e foi regulamentada pelas **Resoluções CONTRAN nº 471/2013 e 532/2015**.[342] Aos

[338] Compete à União o fomento ao desenvolvimento tecnológico e científico com vistas à persecução dos objetivos dessa Política (art. 16, VI)

[339] Nas situações em que o trânsito não esteja circunscrito ao território do Município, o art. 21 prescreve a competência dos órgãos e entidades executivos rodoviários da União, dos Estados e do Distrito Federal, conforme suas devidas circunscrições, para a realização de tais atividades.

[340] Disponível aqui: http://legislacao.prefeitura.sp.gov.br/leis/lei-16050-de-31-de-julho-de-2014/ Acesso em 04.10.2017.

[341] Disponível em: https://diariodotransporte.com.br/2017/06/14/confira-na-integra-o-estatuto-do-pedestre-sancionado-por-doria/. Acesso em: 29.09.2017.

[342] Disponíveis respectivamente em: http://www.denatran.gov.br/download/Resolucoes/Resolucao4712013.pdf e http://www.denatran.gov.br/images/Resolucoes/Resolucao5322015.pdf. Acesso em: 29.09.2017.

agentes de trânsito caberá a autuação de condutores e veículos cujas infrações tenham sido detectadas de forma *online* por meio desses sistemas, com a ressalva de que a fiscalização do trânsito mediante câmeras de monitoramento somente poderá ser realizada nas vias públicas devidamente sinalizadas para esse fim (art. 2 e 3º, da Resolução nº 471). Ao permitir que as prefeituras utilizem imagens geradas por câmeras para comprovar infrações, tais Resoluções viabilizaram a consecução de diversas iniciativas municipais, como o projeto "Cidade Inteligente" do município carioca de Nova Friburgo, que instalou câmeras de segurança no perímetro urbano, com o objetivo de tornar mais eficaz o sistema de multas.[343]

Por sua vez, os **radares**, dispositivos destinados à medição de velocidade de circulação dos veículos automotores, são regulados pela **Resolução CONTRAN nº 396/2011**. [344] Referido normativo determina a **competência do Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO** para aprovar e averiguar periodicamente modelos de radares que estejam em conforme a legislação metrológica em vigor (art. 3º, I a III). A implementação desses dispositivos cabe à autoridade com circunscrição sobre a via onde ele estará localizado (art. 4º), de modo que nas vias circunscritas ao Municípios, **caberá às entidades municipais estipular sua localização, instalação e operação**.

No que concerne à identificação dos veículos, o CONTRAN gerencia o **Sistema Nacional de Identificação Automática de Veículos - SINIAV**, baseado em tecnologia de radiofrequência, conforme o art. 1º, da Resolução nº 412/2012.[345] Segundo a última regulamentação sobre o tema, todos os veículos que circulam pelo país deverão possuir *chip* de identificação eletrônica (arts. 1º e 2º, da Resolução nº 537/2015).[346-347] As informações obtidas por meio desses dispositivos são de uso dos órgãos e entidades públicas que integram o SINIAV, para as finalidades e competências a eles atribuídas, devendo ser observado o sigilo das informações (art. 7º, da Resolução nº 412/2012).

343 Conforme matéria veiculada em: http://g1.globo.com/rj/regiao-serrana/noticia/2015/08/motoristas-de-nova-friburgo-rj-sao-multados-atraves-de-cameras.html. Acesso em: 29.09.2017.

344 Disponível em: http://www.denatran.gov.br/download/Resolucoes/RESOLUCAO_CONTRAN_396_11.pdf. Acesso em: 29.09.2017.

345 Disponível em: http://www.denatran.gov.br/download/Resolucoes/(Resolu%C3%A7%C3%A3o%20412.2012).pdf. Acesso em: 29.09.2017.

346 Disponível em: http://www.denatran.gov.br/images/Resolucoes/Resolucao5372015.pdf. Acesso em: 29.09.2017.

347 Em outubro de 2017, o deputado federal Eduardo Barbosa (PSDB/MG) propôs o Projeto de Lei nº 8.988/2017, cujo o objeto principal é estipular obrigação às empresas concessionárias de rodovias para manter sistema de segurança das instalações, em integração com o Sistema Nacional de Identificação Automática de Veículos (SINIAV). Ainda, o PL define que os órgãos de segurança pública poderão requisitar às empresas concessionárias de rodovias os dados e informações necessárias às diligências policiais. Texto disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2159920. Acesso em: 14.11.2017.

Todavia, o sistema tem **encontrado entrave de consecução nas formas de financiamento**, visto que as Resoluções não dispõem sobre quem são os responsáveis para arcar com tais custos e atores do sistema de trânsito apontam a inexistência de orçamento específico para a persecução da meta.[348] Embora as tentativas de implantação do SINIAV tenham sido inauguradas com a promulgação da Resolução CONTRAN nº 212/2006, o sistema segue inativo pois apenas o Estado de Roraima conduziu licitação para a aquisição dos equipamentos.[349]

Nesse sentido, a modernização de equipamentos de trânsito com soluções de IoT deverá observar a legislação federal, regulamentada por Resoluções do CONTRAN, e legislação municipal, em especial possíveis planos diretores e de mobilidade. As resoluções do CONTRAN se mostram alinhadas às novas tendências tecnológicas, sendo o maior desafio na implementação de IoT em mobilidade a incorporação de mudanças tecnológicas na legislação local.

3.1.5.3. Transporte: monitoramento da circulação e manutenção baseada em condições

3.1.5.3.1. Oportunidades decorrentes do uso de soluções IoT

O transporte urbano foi recentemente incluído entre os direitos constitucionais do cidadão brasileiro (pela Emenda Constitucional nº 90/2015) e representa um dos mais importantes pilares em índices de qualidade de vida do indivíduo.[350] **No entanto, o oferecimento desse serviço público tem representado significativo desafio à Administração Pública e ainda depende de melhorias em qualidade e segurança**. Dentre os fatores responsáveis pela situação de tráfego intenso observado nas grandes cidades brasileiras[351] estão a infraestrutura insuficiente para atingir de modo satisfatório

348 Conforme matéria veiculada em: http://g1.globo.com/carros/noticia/2015/04/exigencia-de-chip-em-veiculos-comeca-valer-daqui-2-meses.html. Acesso em: 29.09.2017.

349 Conforme informações disponíveis em: http://g1.globo.com/carros/noticia/2015/04/exigencia-de-chip-em-veiculos-comeca-valer-daqui-2-meses.html. Acesso em: 29.09.2017.

350 Compilação de estudos realizada pela Organização Mundial da Saúde demonstra que uma rede transporte público eficiente ajuda a combater problemas de saúde, como acidentes de trânsito, sedentarismo, obesidade e estresse. Disponível em: http://www1.folha.uol.com.br/cotidiano/2013/08/1328474-transporte-publico-de-qualidade-reduz-doencas-e-mortes-diz-membro-da-oms.shtml. Acesso em: 26.09.2017.

351 Em levantamento realizado em 2016, aponta-se que três cidades brasileiras, Rio de Janeiro, Salvador e Recife, estão entre as dez cidades mundiais com maior congestionamento. Disponível em: http://brasil.estadao.com.br/noticias/geral,tres-cidades-do-brasil-estao-no-top-10-de-congestionamentos,10000022561. Acesso em: 26.09.2017.

o território da cidade[352], a priorização de modelo de transporte que privilegia o carro e a escassa manutenção dos serviços públicos de transporte.

À vista disso, **o uso de tecnologias de IoT possui potencial de colaborar para o melhor planejamento do sistema urbano de transporte público**, por meio da utilização de conjunto de sensores conectados às unidades de transporte, capazes de monitorar o fluxo de usuários, as condições de tráfego nas vias públicas, bem como a localização de veículos de transporte público - esta última função realizada especialmente pelo uso de sensores de localização via GPS (*Global Positioning System*). [353]-[354] Este é o caso, por exemplo, da cidade de Curitiba, que vêm avançando no desenvolvimento de soluções tecnológicas para conexão e acompanhamento, em tempo real, dos equipamentos públicos, como a frota municipal de ônibus e até mesmo daqueles da rede pública de saúde. [355]

Tendo em vista que esses sensores captam quantidade monumental de dados, o uso de *big data* e *analytics* representa importante ferramenta para **otimizar a experiência do usuário**, gerando ganhos referentes à **confiabilidade no sistema**. [356] Isto porque o processamento e cruzamento dos dados coletados por estes sensores auxiliam na disponibilização de informações sobre, por exemplo: (i) horários de chegada e partidas das unidades e das rotas por elas percorridas; (ii) qual rota é a melhor opção em determinado período do dia; (iii) qual momento do dia é mais movimentando para cada tipo de transporte; e (iv) qual unidade ou combinação de transportes é ideal para

[352] Conforme pesquisa publicada pelo Instituto de Políticas de Transporte & Desenvolvimento e WRI Brasil Cidades Sustentáveis, apesar de a cidade de São Paulo possuir a maior rede de transporte público da cidade, apenas 25% de sua população vive próxima à uma estação de transporte. Argumenta-se que essa porcentagem é muito baixa se comparada com a de outras cidades, como Rio de Janeiro (47%), Cidade do México (48%), Pequim (60%), Nova Iorque (77%) e Paris (100%). Disponível em: http://2rps5v3y8o843iokettbxnya.wpengine.netdna-cdn.com/wp-content/uploads/2016/09/2016-09-ITDP-PNT-SP.pdf. Acesso em: 26.09.2017.

[353] Conforme descrição da solução IoT para mobilidade feita no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

[354] Nesse sentido, notícia veiculada no periódico indiano *The Economic Times* aponta que soluções voltadas ao rastreamento de veículos (*GPS-based tracking system*) possibilitam o aprimoramento das operações do serviço de transporte público, o que gera maior confiabilidade no sistema, dado que ao usuário é fornecida ferramenta para localizar as unidades e planejar, de forma otimizada, sua viagem. Disponível em: http://economictimes.indiatimes.com/news/economy/infrastructure/smart-transportation-for-smart-cities/articleshow/48772473.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Acesso em: 25.09.2017.

[355] Cidades inteligentes e mobilidade urbana. **Caderno FGV Projetos**, jun./jul. 2014, ano 9, nº 24, p. 59-60. Disponível em: http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf. Acesso em: 12.09.2017.

[356] Estudo indica que indivíduos que possuem acesso a informações esperam 7 minutos a menos - uma redução de espera de cerca de 13% -, nas paradas de ônibus. Disponível em: http://www.sciencedirect.com/science/article/pii/S0965856411001030. Acesso em: 04.10.2017.

determinado trajeto.[357] Além da experiência do usuário, o Poder Público poderia utilizar os dados coletados para **atividades de planejamento** mais efetivas, reconhecendo mais rapidamente mudanças no comportamento do descolamento populacional e antecipando a realização de obras e disponibilização de recursos materiais e humanos para atende-la.

Os dados gerados a partir da circulação das unidades de transporte **facilitam também a execução de auditorias dos contratos** de concessão do serviço de transporte público, já que permitiriam verificar, de forma mais acertada, se as velocidades contratadas estão sendo cumpridas pelo ente concessionário.[358]-[359] Por exemplo, seria possível ainda acompanhar a efetiva disponibilidade de material rodante aos usuários pelas empresas em horários de baixa demanda. Ainda, o uso de sensores em ônibus e trens **viabilizam manutenção e renovação mais eficiente da infraestrutura de transporte**, feita sob demanda em períodos que não afetam a sua utilização pelos cidadãos. [360]

3.1.5.3.2. Regulação do serviço de transporte urbano

Tal como o trânsito, o **transporte** também possui regulação pelo CTB, mas é abordado de forma mais contundente no Estatuto da Cidade (Lei nº 10.257/2001) e na Política Nacional de Mobilidade Urbana (Lei nº 12.587/2012). O Estatuto da Cidade estabelece como diretrizes da política urbana a oferta e garantia de acesso a transportes (art. 2º, I e V), e estabelece que a obrigatoriedade de o plano diretor das cidades com mais de quinhentos mil habitantes possuir plano de transporte urbano integrado (art. 41, §2º). Estabelece

[357] Exemplo do processamento de dados no âmbito do transporte coletivo urbano é a aplicação israelita *Moovit*, que atualmente conta com mais de 200 mil editores e vêm ganhando espaço nas cidades brasileiras. Vide: https://smartcitiesworld.net/news/news/public-transport-stops-reaches-mapped-milestone-2259. Acesso em: 14.11.2017.

[358] Em 2016, a Prefeitura de São Paulo determinou a ampliação do Sistema Integrado de Monitoramento (SIM), com a introdução de modelos de veículos com tecnologia GPS integrada a fim de verificar o cumprimento dos horários de partidas e chegadas. Notícia veiculada em: http://sao-paulo.estadao.com.br/noticias/geral,prefeitura-vai-ampliar-fiscalizacao-de-onibus-em-sp,10000024859. Acesso em: 04.10.2017.

[359] Atualmente o cruzamento de informações é realizada pelos cronotacógrafos presentes nos veículos que realizam o serviço público. Todavia, referido dispositivo não conta com inteligência IoT e requer leitura manual dos dados coletados. Os cronotacógrafos são equipamentos destinados a indicar e registrar a velocidade e a distância percorrida pelo veículo. Conforme a legislação de trânsito, são dispositivos obrigatórios para os veículos de passageiros com mais de 10 lugares (ônibus municipais e de viagem); veículos de transporte e de condução escolar; e veículos de carga com peso bruto acima de 4.536 quilogramas (Resoluções CONTRAN nº 14/1998, 87/1999 e 92/1999). Cabe ao INMETRO aprovar os modelos existentes e realizar verificação periódica, segundo diretivas emitidas pelo órgão e disponíveis em: https://cronotacografo.rbmlq.gov.br/legislacao.

[360] Aponta-se que as manutenções programadas evitam que o tráfego de mais de 800 mil pessoas seja interrompido em Londres. A análise de *big data* vem sendo utilizada para responder, de forma rápida, quando é necessário fazer intervenções no sistema *Transport for London*, serviço que integra a gestão de ônibus, trens, táxis, estradas, ciclovias e balsas da cidade. Disponível em: http://www.bigdatabusiness.com.br/iot-big-data-e-as-cidades-inteligentes-revolucionando-o-transporte-publico/. Acesso em: 26.09.2017.

também que à União compete instituir diretrizes sobre transporte e mobilidade urbana, que fundamentou a edição da Política Nacional de Mobilidade Urbana.

A edição da legislação referida consiste em avanço do ponto de vista institucional, visto que compõem o marco regulatório para a formulação e execução de políticas públicas para o ambiente urbano e destinadas à melhoria do trânsito e dos serviços de transporte público. Sua consecução deverá ser, todavia, complementada pela gestão integrada com Estados e Municípios e por investimentos em infraestrutura. [361]

Nesse contexto, a Política Nacional de Mobilidade Urbana atribui à **União o papel de assistência técnica e financeira** aos demais entes federados e **de fomento ao desenvolvimento tecnológico e científico** em mobilidade (art. 16, I e VI, da Política). Também lhe atribui a **prerrogativa de editar normas que facilitem a cooperação entre os entes da federação**, papel este que assume relevo em cenário de compartilhamento de funções regulamentares e administrativas.

Aos **Estados foram designadas atribuições relacionadas à proposição de política tributária** específica para a implantação da Política Nacional de Mobilidade (art. 17, II), e **aos Municípios a execução propriamente dita da Política de Mobilidade**, através do planejamento e prestação dos serviços de transporte público coletivo, de forma direta, indireta ou por gestão associada (art. 18). Assim, os Municípios **exercem função relevante na regulação e execução dos serviços de transporte, especialmente por meio dos planos diretores**, quando de implementação obrigatória. [362] Assim, Planos Diretores como os de Curitiba, Rio de Janeiro, Salvador e São Paulo[363] possuem capítulos que versam especificamente sobre política de mobilidade, sendo determinada, em todos eles, a constituição de rede de mobilidade que priorize o transporte público e os

361 **Caderno FGV Projetos**, jun./jul. 2014, ano 9, nº 24. Disponível em: http://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernos_fgvprojetos_smart_cities_gwa_0.pdf. Acesso em: 12.09.2017.)

362 Obrigatório para as cidades: (i) com mais de vinte mil habitantes; (ii) integrantes de regiões metropolitanas e aglomerações urbanas; (iii) que desejem implementar instrumentos de política urbana como o IPTU progressivo; (iv) integrantes de áreas de especial interesse turístico; (v) inseridas na área de influência de empreendimentos ou atividades com significativo impacto ambiental de âmbito regional ou nacional; e (v) incluídas no cadastro nacional de Municípios com áreas suscetíveis à ocorrência de deslizamentos de grande impacto, inundações bruscas ou processos geológicos ou hidrológicos correlatos (art. 41, Estatuto das Cidades). Para as cidades com mais de vinte mil habitantes, decorre a obrigação de editar Plano de Mobilidade Urbana, que tenha por foco o transporte não motorizado e infraestrutura que facilite os deslocamentos a pé ou por bicicleta (art. 24, § 1º e § 2º, da Política Nacional de Mobilidade). Ainda, nas cidades com mais de quinhentos mil habitantes, é igualmente dever do Município elaborar um plano de transporte urbano integrado, que esteja compatível com o plano diretor existente (art. 41, § 2º).

363 Textos dos Planos Diretores disponíveis, respectivamente, em: http://multimidia.curitiba.pr.gov.br/2015/00175701.pdf; http://www.rio.rj.gov.br/dlstatic/10112/139339/DLFE-229591.pdf/LeiComplementar1112011PlanoDiretor.pdf; http://www.ibdi-ba.com.br/plano-diretor-de-desenvolvimento-urbano-de-salvadorba/; e http://gestaourbana.prefeitura.sp.gov.br/arquivos/PDE_lei_final_aprovada/TEXTO/2014-07-31%20-%20LEI%2016050%20-%20PLANO%20DIRETOR%20ESTRAT%C3%89GICO.pdf. Acesso em: 06.10.2017.

deslocamentos não motorizados. Da mesma forma, tais textos legais contêm dispositivos que incentivam a elevação do patamar tecnológico tanto da gestão dos sistemas de transporte público coletivo - no art. 217 do Plano Diretor do Rio de Janeiro preconiza-se a implantação de tecnologias inteligentes para a rede integrada de transportes da cidade -, quanto do controle do trânsito, como é feito no art. 243 do Plano de Salvador, que determina a utilização de estratégias tecnológicas nos dispositivos de sinalização e segurança do trânsito.

A Política de Mobilidade também determina ser direito dos usuários de sistemas de transporte público a possibilidade de obter informações gratuitas e acessíveis sobre itinerários, horários, tarifas de serviços e modos de interação com outros modais de locomoção (art. 14), de modo que as soluções IoT descritas nesta seção podem servir como instrumento eficaz para a realização de direitos de mobilidade.

Mais que isso, a introdução de novas camadas tecnológicas ao serviço público de transporte, tais como radares identificadores do fluxo e da localização de usuários e veículos, poderá **auxiliar na consecução dos princípios da política urbana**.[364] Isso porque fornecem mecanismos para aperfeiçoar os níveis de eficiência da prestação do serviço, através de informação aos usuários da localização de determinado veículo, e também permitem otimizar a oferta de equipamentos de transporte público de qualidade (art. 2º, I e II, do Estatuto da Cidade) e a melhora na mobilidade de pessoas e cargas dentro do território do Município (art. 1º, *caput*, da Política de Mobilidade).

Nesse cenário de implementação de tecnologia IoT, deve-se levar em consideração que compete à **União oferecer aos municípios assistência financeira** para a melhora tecnológica das estruturas de mobilidade (art. 16, I, da Política de Mobilidade), o que pode ser feito através de linhas de financiamento federal para custear a instalação de diversos tipos de sensores passíveis de serem acoplados às unidades de transporte e locais de circulação. **Os Estados podem igualmente contribuir para tal sistema de financiamento**, vez que lhes são facultados a implementação de mudanças tributárias e de incentivos fiscais que possibilitem a adoção dessas tecnologias (art. 17, II, da Política).

Por fim, indica-se a necessidade de cooperação entre os diferentes âmbitos da federação na gestão conjunta do adimplemento do contrato de serviço de transporte público. À medida em que União, Estados e Municípios possuem atribuições relativas ao fornecimento de transporte urbano e gestão da mobilidade, faz-se fundamental atuação normativa federal destinada a coordenar e fomentar essa cooperação.

Nesse sentido, a modernização dos serviços de transporte urbano deve igualmente observar diretrizes nacionais, mas ter em mente as especificidades da legislação

364 Texto legislativo disponível em: http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10257.htm. Acesso em: 29.09.2017.

municipal. Igualmente, projetos de IoT em transporte público podem ser estimulados mediante fomento financeiro por parte da União e dos Estados.

3.1.5.4. Breve apontamentos sobre privacidade, segurança da informação e uso de dados

A instalação de dispositivos tecnológicos de informação e monitoramento junto aos tradicionais sistemas de controle de tráfego e à infraestrutura de mobilidade urbana resulta em aumento significativo na coleta e análise de dados pessoais. Conforme já mencionado, a coleta e análise de dados se mostra relevante para a melhoria na prestação do serviço de transporte público e nas ações destinadas à melhoria na qualidade da circulação de bens e pessoas na cidade. Essa melhoria é proporcionada pela imediata agregação e análise de dados capazes de fomentar a melhor destinação de recursos tecnológicos, pessoais e financeiros. Mais que isso, as bases de dados de órgãos de trânsito poderão ser integradas com *databases* de outros serviços públicos ou de particulares, potencializando ainda mais as soluções existentes. Por exemplo, conjuntos de dados sobre o trânsito podem ser combinados com aqueles coletados através de dispositivos acoplados à infraestrutura de iluminação pública, servindo como fonte de informações do Poder Público para a tomada de decisões mais eficientes em relação aos serviços públicos oferecidos.

Essa composição de atualizadas e robustas bases de dados origina **alta criticidade em relação à segurança da informação e à privacidade de dados pessoais** de cidadãos. [365] Ao passo em que sensores, câmeras e outros dispositivos utilizados no trânsito podem se valer de conectividade cabeada e sem-fio, o sistema de coleta de dados de mobilidade pode estar sujeito a falhas de segurança. Situações do tipo tornaram-se recorrentes no noticiário, tais como o ataque ocorrido em 2016 às redes de computadores do sistema de transporte em São Francisco, na Califórnia[366], e no recente alcance do *ransomware Wanna Cry* às redes de trens da Alemanha. [367] Desse modo, assinala-se, consoante as indicações do relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017, a importância da **implementação de mecanismos de segurança** contra interferência proposital no sinal (*anti-jamming*) a fim de evitar ataques cibernéticos.

Ainda, **a utilização de tais dispositivos pode ocasionar a identificação de indivíduos**, tanto através da coleta direta de dados pessoais quanto do intercruzamento entre

[365] Conforme indicado no relatório parcial **Produto 8: Aprofundamento de Verticais - Cidade**, de setembro de 2017.

[366] Notícia veiculada em: https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/. Acesso em: 04.10.2017.

[367] Notícia veiculada em: http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/. Acesso em: 04.10.2017.

determinados dados com outros advindos de fontes externas. Como exemplo de base de dados composta por órgãos de trânsito, podem ser mencionadas *databases* dos sistemas e subsistemas do Denatran, que agregam dados como a CNH de motoristas, infrações cometidas e regularidade de automóveis perante os órgãos de trânsito. O acesso à base de dados está regulamentado pela Portaria Denatran nº 15/2016[368] e é dado a restritos órgãos públicos e entidades privadas, embora os dados sejam oferecidos remuneradamente por intermédio de serviço prestado pela empresa pública Serviço Federal de Processamento de Dados - Serpro.[369]

Nesse contexto, reiteramos as recomendações previamente veiculadas no tópico sobre privacidade em Cidades. Acima de tudo, apontamos a **necessidade de edição de lei específica para a proteção de dados pessoais** que estabeleça parâmetros para a coleta, tratamento e compartilhamento dos dados pessoais coletados no âmbito de ações de modernização da gestão pública. Note-se que a recomendação reside sobre legislação ainda pendente de aprovação pelo Congresso Nacional, de modo que as disposições do Marco Civil da Internet atendem às finalidades propostas.

Todavia, no atual contexto de legislação ainda esparsa sobre a temática, faz-se extremamente relevante a **adoção de medidas capazes de minimizar os riscos atinentes à identificação dos indivíduos e consequente violação de sua privacidade**, dentre as quais ressaltamos:

- Observância ao princípio da finalidade na utilização do dado coletado;
- Obtenção do consentimento livre, expresso e informado dos usuários – especialmente quando os dados não passarão por processos de anonimização –, para quaisquer outros usos atribuídos aos dados pessoais coletados distintos da finalidade originária de prestação de serviço público essencial, nos termos do Marco Civil da Internet;
- Disponibilização de mecanismos de *opt-out* aos usuários, que poderão escolher não ter seus dados pessoais utilizados para finalidades distintas da estrita prestação do serviço público essencial, de modo a viabilizar o controle sobre possíveis usos de seus dados;

[368] Disponível em: http://www.denatran.gov.br/images/Portarias/2016/Portaria0152016_nova.pdf Acesso em 06.10.2017

[369] Vide: http://www.serpro.gov.br/menu/nosso-portfolio/por-publico/portfolio-para-empresas

- Solicitar consentimento prévio, livre, expresso e informado para o compartilhamento de dados a terceiros, salvo em hipóteses de interesse público previstas em legislação ou por determinação judicial[370];
- Utilização de diferentes técnicas de anonimização e agregação de dados, como a criptografia e a tecnologia *blockchain*[371], especialmente quando o do dado pessoal for distinto de sua finalidade originária.

A observância das medidas apontadas é de grande relevância, especialmente tendo em vista que a coleta de dados ocorre no escopo da prestação de serviços públicos, muitos deles considerados direito fundamental do cidadão. Por esse motivo, **parcerias estabelecidas por órgãos governamentais que resultem na coleta ou transferência de dados pessoais para particulares devem respeitar legislação específica sobre contratação pública**, de modo a privilegiar a livre concorrência e estipular regras rígidas de proteção de dados pessoais. Ainda, a recusa em consentir ou a utilização de mecanismos de *opt-out* não devem inviabilizar a utilização pelo cidadão do respectivo serviço público.

Para além da segurança da informação e da privacidade de dados coletados no âmbito de políticas de trânsito e transporte público, a **boa prática é que soluções de IoT sejam realizadas sempre que possível baseadas em padrões abertos, em *software* livre ou *open source*, e com API para dados abertos**. O *software* livre ou *open source*, em primeiro lugar, consiste em programa de computador construído de forma gratuita e colaborativa, podendo ser utilizado, copiado, modificado e redistribuído sem a necessidade de permissões do criador original.[372] Também é essencial ao *software* livre que seu próprio

370 No Uruguai, as exceções à obtenção de consentimento para a divulgação de dados pessoais com terceiros são: (i) determinação expressa em lei; (ii) dados provenientes de fontes acessíveis ao público; (iii) quando a divulgação for essencial ao desempenho de funções governamentais; (iv) se apenas forem divulgados dados como, nome, sobrenome, documento de identidade, nacionalidade, domicílio e data de nascimento; (v) os dados sejam provenientes de relação contratual, científica ou profissional do titular dos dados e sejam necessários para o desempenho do contrato; (vi) por motivos de saúde e higiene públicas, de emergência ou necessários para a realização de estudos epidemiológicos, desde que preservada a identidade dos indivíduos mediante mecanismo de dissociação; (vii) se forem aplicados procedimentos de dissociação de modo que os titulares não possam ser identificados. Fonte: https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/e23f0f93-1004-4b65-833f-d1f74c347756/guia-4-web.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=e23f0f93-1004-4b65-833f-d1f74c347756 Acesso em 04.10.2017.

371 As vantagens do uso de *blockchain* em tecnologias de transporte são elencadas por Yong Yuan e Fei-Yue Wang no texto **Towards Blockchain-based Intelligent Transportation Systems**, disponível em: https://www.researchgate.net/publication/311919998_Towards_blockchain-based_intelligent_transportation_systems.

372 Sobre o tema, vide: MIZUKAMI, Pedro Nicoletti; LEMOS, Ronaldo. From free software to free culture: The emergence of open business. **Access to knowledge in Brazil: New research on intellectual property, innovation and development**, p. 13-39, 2010. Disponível em: http://klangable.com/uploads/books/A2KBrazil.pdf#page=27 Acesso em 09.10.2017.

código-fonte seja livre, ou seja, revelado a terceiros e não mantido em exclusividade pelos seus autores e proprietários.[373]

A adoção dessa modalidade de *software* pela Administração Pública atende ao princípio constitucional da eficiência no setor público (art. 37 da CF) e possui a capacidade de evitar o monopólio na contratação de *softwares* para uso governamental. Além disso, evita a emergência do efeito *lock in*, decorrente de dificuldades técnicas decorrentes da migração para outros *softwares* ou da transferência de dados previamente coletados e armazenados em *software* de determinado fornecedor.

Dentre as vantagens da adoção de *software* livre por órgãos governamentais, podem ser mencionadas também (i) a gratuidade na sua obtenção pelo governo e no uso pelo cidadão; (ii) a possibilidade de personalizar o *software* conforme necessidade do serviço público prestado; (iii) autonomia do órgão público e do usuário em relação à contratação de *software* produzido por determinado fornecedor, de modo a democratizar o acesso à informação pública; e (iv) a maior segurança do sistema, visto que seu formato colaborativo permite a constante contribuição de terceiros na identificação e melhorias de falhas.

Há municipalidades que já empregam o *software* livre em seus programas e sistemas de computador, como é o caso do Município de São Carlos, que já em 2001 editou a Lei nº 12.883 para determinar que a Prefeitura deverá utilizar preferencialmente programas com códigos abertos, livres de restrição de propriedade.[374] Igualmente, a Secretaria Municipal de Transportes do Município de São Paulo lançou em 2015 edital destinado a contratar projetos de tecnologia em *software* livre visando, entre outros objetivos, a automação de *back office* do sistema de processamento de infrações e multas e da visualização do nível de serviço do transporte público.[375] Todavia, a adoção desse tipo de *software* dependerá de iniciativa do gestor público, quando não houver legislação local sobre o tema, visto que o estímulo à política de *software* livre pela Administração Pública Federal está arrefecido nos últimos anos.[376]

O API (*Application Programming Interface*) consiste em conjunto de padrões de programação que permite a criação de novas aplicações, e sua adoção por órgãos públicos permite a colaboração de programadores externos com o desenvolvimento ou

[373] Vide **Estudo sobre software livre**, comissionado pelo Instituto Nacional da Tecnologia da Informação (ITI): http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2673/FGV-CTS%20-%20Software%20livre.pdf?sequence=1 Acesso em 09.10.2017.

[374] Disponível em: https://leismunicipais.com.br/SP/SAO.CARLOS/LEI-12883-2001-SAO-CARLOS-SP.pdf. Acesso em 09.10.2017.

[375] Disponível em: http://mobilab.prefeitura.sp.gov.br/projetos/. Acesso em 09.10.2017.

[376] Para mais informações sobre o tema, ver: https://www.nexojornal.com.br/expresso/2016/11/03/Por-que-o-software-livre-vai-perder-espa%C3%A7o-no-governo-federal. Acesso em: 06.10.2017.

aprimoramento de aplicações capazes de se comunicar com bases de dados governamentais.[377] Dados abertos, por sua vez, são divulgados por meio da Internet, de maneira atualizada e em formato não proprietário e reutilizável. Nesse sentido, a utilização de API para dados governamentais abertos permite que terceiros utilizem dados públicos atualizados para criar novas soluções tecnológicas em colaboração com serviços públicos.

Ainda que exija investimento por parte dos órgãos públicos para o processo de divulgação de suas bases de dados em formato não proprietário e legível por máquina, referida solução tem o potencial de viabilizar o desenvolvimento de aplicações de IoT com base em dados públicos atualizados. Como exemplo, dados coletados por sensores de trânsito ou GPS instalados em ônibus e disponibilizados em bases de dados públicas podem ser transportados para aplicações de dispositivos móveis, como celulares, que permitem ao passageiro reduzir o tempo de espera no transporte público. A maior previsibilidade sobre os horários de modais de transporte público pode, inclusive, fundamentar a escolha de passageiros em privilegiar o transporte coletivo ou a integração de modais de trânsito em detrimento do automóvel individual.[378]

Em vista dos benefícios decorrentes da disponibilização de API para dados abertos, o governo federal disponibiliza plataforma com dados abertos de distintos órgãos da Administração Pública Federal[379], assim como o Município de São Paulo possui plataforma destinada a desenvolvedores, na qual são divulgadas bases de dados sobre áreas diversas da cidade.[380] Contudo, a adoção de padrões abertos ainda não está amplamente difundida nos órgãos públicos, o que dificulta sensivelmente a complementação dos serviços públicos de trânsito e transporte com API em dados abertos.

Por fim, uma nota importante sobre inteligência artificial e decisões automatizadas feitas por algoritmos. Na medida em que aplicações de cidades inteligentes e de IoT vão se tornando corriqueiras, elas passam também a serem "cognificadas". Em outras palavras, passam a ter suas operações integradas a sistemas "inteligentes" de tomada de decisão, baseados em algoritmos ou mesmo em aplicações de inteligência artificial.

No setor público, esse tipo de integração entre IoT, algoritmos e inteligência artificial merece especial atenção do ponto de vista regulatório e de políticas públicas. Como

[377] Para mais informações, ver: https://www.pcmag.com/encyclopedia/term/37856/api. Acesso em: 04.10.2017.

[378] Vide: http://thecityfixbrasil.com/2016/02/12/dados-de-transito-em-tempo-real-sao-bons-para-as-pessoas-e-para-as-cidades-o-que-esta-atrasando-esse-tecnologia/

[379] Vide: http://kit.dados.gov.br/

[380] Sobre o tema, vide: http://dados.prefeitura.sp.gov.br/pt_PT/

afirmou o professor da universidade de Harvard, Lawrence Lessig, em seu livro de 1999 chamado "O Código e Outras Leis do Ciberespaço": "o código é a lei".

Lessig chamava a atenção para o fato de que programas de computador ("códigos") serão cada vez mais responsáveis por embutir neles regras que regulam decisões sobre um grande número de pessoas, todos os dias.

Para ter certeza de que um algoritmo utilizando pelo setor público está sendo aplicado como deveria, sem interferências externas e em atendimento aos princípios que regem a administração pública, é fundamental que tanto seu código quanto seu hardware sejam conhecidos, transparentes e auditáveis.

Note-se que essa preocupação sinaliza um novo paradigma para a transparência pública. Toda e qualquer função pública que seja mediada por "código" precisa atender a requisitos de transparência e auditabilidade, quando empregados pelo poder público. Por exemplo, o hardware e o código embarcado precisa ser transparente, auditável, com código e hardware preferencialmente abertos à análise de qualquer cidadão, inclusive quanto a seus processos de manutenção e atualização.

Em seu livro paradigmático, Lessig apontou que um dos desafios de embarcar normas em códigos é que eles são escritos em linguagem que não é compreensível para a maioria das pessoas. Essa opacidade poderia ser chamariz para a corrupção. Por essa razão, é fundamental que o uso de decisões automatizadas no âmbito da administração pública, seja por algoritmos, inteligência artificial ou outros modelos de análise, atendam aos princípios gerais que a governam. Dentre eles a impessoalidade (rejeição a análise baseadas em estereótipos ou preconceitos), publicidade (transparência e auditabilidade), eficiência, bem como direito de recurso com relação a decisões tomadas no âmbito da administração pública.

Essa preocupação já foi incorporada no âmbito do Congresso Nacional e está em tramitação um projeto de lei que trata especificamente desse assunto. Trata-se do Projeto de Lei nº 8.503 de 2017[381], cujo texto entendemos como positivo e adequado, segue transcrito abaixo para referência:

> *PL 8.503/2017*
>
> *Altera a Lei nº 12.527, de 18 de Novembro de 2011 (Lei de Acesso à Informação), para tornar expresso o direito de obter informações relativas à aquisição e funcionamento de softwares, hardwares e códigos mediadores de funções públicas e tornar obrigatória a disponibilização dos códigos-fonte dos algoritmos utilizados para a distribuição de processos nos órgãos do Poder Judiciário. O Congresso Nacional decreta: Art.1º A Lei 12.527, de 18 de Novembro de 2011, passa a vigorar com os acréscimos:*

[381] Texto disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2150508. Acesso em: 14.11.2017.

"Art.7º.....
.....

VIII – informação e detalhamento técnico relativos à criação, aquisição, configuração, manutenção e funcionamento de softwares, hardwares e códigos mediadores de quaisquer funções públicas" (NR)

"Art.8º.....
.....
§3º.....
.....

IX – No caso dos órgãos do Poder Judiciário, disponibilizar os códigos-fontes auditáveis de quaisquer algoritmos ou sistema automatizado empregado, inclusive para distribuição de processos, bem como dos parâmetros e estatísticas que informam seus funcionamentos." (NR) Art. 2º Esta Lei entre em vigor na data de sua publicação.

3.1.6 Segurança Pública inteligente

As aplicações IoT no ambiente de cidades também serão utilizadas na **construção e aperfeiçoamento dos atuais sistemas de suporte a ações de segurança pública**, através da utilização de novas tecnologias de sensoriamento e de câmeras conectadas de alta definição[382], mecanismos que trazem consigo preocupações acerca dos limites e controles necessários para evitar abusos por parte do Estado.[383]

Essas preocupações não são novas, e refletem muitas dos receios já existentes com os atuais sistemas de câmeras de vigilância. Entretanto, elas ganham novos contornos em virtude da expansão do tipo e do volume de dados passíveis de serem tratados, além do desenvolvimento de tecnologias capazes de tratá-los automaticamente.[384]

[382] Como parte do progressivo desenvolvimento das possibilidades do sistema de vigilância pública, estão sendo integrados aos já existentes sistemas de CCTV equipamentos de alta resolução de vídeo; microfones de alta sensibilidade; câmeras com tecnologia OCR e de reconhecimento facial; e sensores dos mais variados tipos. Para uma descrição técnica das soluções, consultar seção descritiva das aplicações em (indicar referência).

[383] Em reportagem para o periódico *The Guardian*, o Comissário de Segurança do Reino Unido apresenta preocupação semelhante em relação ao desenvolvimento das tecnologias de monitoramento nas cidades do país: "The increasing use of surveillance technology – including body-worn video, drones and number plate recognition systems – risks changing the 'psyche of the community' by reducing individuals to trackable numbers in a database, the government's CCTV watchdog has warned." Disponível em: https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent. Acesso em: 15.09.2017. No Estado da Califórnia, residentes mostram preocupação com a existência do *Domain Awareness Center* (DAC), central de vigilância voltada a monitorar o porto e o aeroporto da cidade de Oakland. O Conselho Municipal propôs uma expansão do sistema, para que esse se utilizasse de streaming contínuo de imagens veiculadas por circuito fechado de câmeras de tráfego; de técnicas de leitura de placas de veículos; de detectores de tiros de arma de fogo; e, ainda, de outras tecnologias capazes de contemplar toda a cidade. Disponível em: http://edition.cnn.com/2014/05/26/tech/city-of-tomorrow-video-data-surveillance/index.html. Acesso em: 15.09.2017.

[384] Conforme relatório publicado pelo *Berkman Center for Internet & Society* da Universidade de Harvard, os dispositivos de tecnologia IoT são projetadas para crescer progressivamente, e eles possuem o condão de mudar

De início, é importante destacar que é permissível ao Estado implementar mecanismos de vigilância com aplicações IoT. Assim como no caso das câmeras de vigilância atualmente disponíveis, essas **novas ações de monitoramento por parte do Poder Público encontram-se juridicamente respaldadas na sistemática constitucional**, que confere, no art. 144, ao Estado o dever de garantir aos cidadãos brasileiros segurança através da execução de políticas de segurança pública[385] eficientes. A própria jurisprudência constitucional compreende o direito à segurança como "prerrogativa constitucional indisponível", que deve ser garantido mediante a implementação de políticas públicas, o que impõe ao Estado, portanto, a obrigação de criar condições objetivas que possibilitem o efetivo acesso a tal serviço.[386]

Nesse contexto, como já foi bem destacado no capítulo de Privacidade do Relatório de Cidades Inteligentes, justifica-se o tratamento de dados pessoais sem a obtenção de consentimento prévio e expresso, **com a condição de que o tratamento desses dados seja estritamente necessário e proporcional à finalidade a que se destina (garantia da segurança pública), bem como seja realizado apenas por autoridades que componham o sistema de segurança pública.**

Entretanto, é importante ter ciência de que **o aprimoramento das capacidades dos sistemas de monitoramento,** em conjunção com a maior integração desses sistemas com uma variedade de sensores[387], **desafiam os limites da prerrogativa constitucional do Estado estabelecida no mencionado art. 144 e os condicionantes acima expostos**. A progressiva integração de novas tecnologias aos mecanismos já existentes de vigilância tem o potencial de atingir significativamente direitos fundamentais, tais como o direito à privacidade e a liberdade de expressão, igualmente garantidos pela Constituição.

Desse modo, preconiza-se a **utilização desse novo complexo de tecnologias pela Administração de forma responsável, com a aplicação de freios e contrapesos e tendo em vista as noções de necessidade e proporcionalidade**. Ainda que o poder de polícia represente uma faculdade da qual dispõe a Administração Pública para condicionar e

drasticamente o cenário da vigilância. As imagens, vídeos e áudios coletados por esses objetos podem propiciar interceptações em tempo real e checagens de fatos depois de sua ocorrência (p. 3). Disponível em:

https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Acesso em: 06.09.2017.

385 José Afonso da Silva caracteriza "segurança pública" como "atividade de vigilância, prevenção e repressão de condutas delituosas". In: SILVA, José Afonso da. **Curso de direito constitucional positivo**. 34 ed. São Paulo: Malheiros, 2011, p. 779.

386 Supremo Tribunal Federal, RE 559.646 AgR, rel. min. Ellen Gracie, j. 7-6-2011, 2ª T, DJE de 24-6-2011.

387 "The integration of a variety of sensors (audio sensors and chemical, biological and radiological sensors) with CCTV technology has been categorized in Europe as "Massively Integrated Multiple Sensor Installations" (MIMSI). In the US, the term for MIMSI is "Domain Awareness System" (DAS)." In: KLITOU, Demetrius. **Privacy-invading technologies and privacy by design**: Safeguarding privacy, liberty and security in the 21st century. The Hague: Asser Press, 2014, p. 116.

restringir direitos individuais[388], as medidas não devem ser utilizadas para além do estritamente necessário. A segurança pública consiste, conforme o texto constitucional, em ação estatal com vistas à preservação ou restauração da ordem pública, circunstância na qual os indivíduos possuem a prerrogativa de gozar de todos os seus direitos[389], inclusive aquele referente à intimidade.

Nessa perspectiva, **as atividades de segurança pública devem ser demarcadas pela proibição do excesso e pela limitação específica com relação à finalidade à qual os dados são coletados.** É fundamental o estabelecimento desses limites como forma de se resguardar liberdades individuais.[390] Desse modo, os direitos fundamentais dos cidadãos – entre eles aqueles referentes à inviolabilidade da privacidade e as liberdades civis –, devem ser encarados como um limite à atuação do Estado na esfera da segurança pública. Uma vez mais, isso não implica na proibição da coleta ou monitoramento de dados para fins de segurança pública. No entanto, implica a proibição de abusos. Fica vedado, por exemplo, o uso dos dados para finalidades outras que não aquelas que justificaram sua coleta. Além disso, os dados não utilizados deverão ser descartados. Não pode haver qualquer tipo de arbitrariedade na prática de coleta de dados. Fica vedada também qualquer possibilidade de discriminação, por exemplo, com base em raça e ou outras características socioeconômicas. Além disso, os dados devem ser mantidos em regime de segurança. O acesso a eles para outras finalidades que não sejam diretamente relacionadas à segurança pública dependerá de ordem judicial. Deve ser também vedado o acesso dos dados por terceiros ou a cessão dos dados para outras entidades.

Ainda, **faz-se necessário avaliar também os níveis de efetividade do uso dessas novas soluções de monitoramento**, já que falhas de efetividade em tais aplicações podem gerar questionamentos sobre a necessidade da implementação do sistema, de treinamento dos agentes públicos envolvidos, bem como sobre a proporcionalidade do tratamento de dados realizado.

388 Conforme Hely Lopes Meirelles, "tradicionalmente, a polícia em sentido material é conceituada a partir da posição de supremacia do Poder Público em impor limites à atuação dos particulares, a fim de preservar a ordem pública". MEIRELLES, Hely Lopes. Estudos e pareceres de direito público, v. II, São Paulo: RT, 1979/1995, p. 6. In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. **Constituição Federal comentada e legislação constitucional**. 6 ed. São Paulo: Editora Tribunal dos Tribunais, 2017, p. 1022.

389 "A segurança pública consiste numa situação de preservação ou restabelecimento dessa convivência social que permite que todos gozem de seus direitos e que exerçam suas atividades sem perturbação de outrem". In: SILVA, José Afonso da. **Curso de direito constitucional positivo**. 34 ed. São Paulo: Malheiros, 2011, p. 779.

390 Segundo Pedro Machete, "toda atividade policial deve ser balizada pelo princípio da proibição do excesso, cuja existência é fundamental para o controle da atuação dos poderes públicos no Estado Constitucional, assumindo, notadamente no que se refere aos direitos fundamentais, o papel de principal instrumento de controle da atuação restritiva da liberdade individual". In: NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. **Constituição Federal comentada e legislação constitucional**. 6 ed. São Paulo: Editora Tribunal dos Tribunais, 2017, p. 1023.

No Brasil, o sistema "Detecta"[391], já teve sua eficiência contestada no âmbito do Tribunal de Contas do Estado de São Paulo ("TCE-SP").[392] O Tribunal questionou, entre outros aspectos, as capacidades do sistema de reduzir a quantidade de pessoal envolvido no monitoramento e de garantir a confiabilidade e a segurança das informações. De modo geral, entendeu-se que havia (i) falhas de planejamento na contratação do serviço; (ii) o serviço é pouco utilizado pelas unidades policiais; (iii) e existem desacertos na segurança de acesso à informação.

No exterior, a utilização de técnicas de reconhecimento facial para a identificação de suspeitos no atentado ocorrido em 2013 na cidade de *Boston*, Estados Unidos também despertou problemas. Imagens de dois suspeitos encontravam-se disponíveis em banco de dados públicos, contudo os computadores não foram capazes de indentificá-los.[393]

A título de exemplo, vale também demonstrar como os novos sistemas com sensores de captação sonora nas câmeras e com a possibilidade de identificação automatizada de indivíduos através de reconhecimento facial, podem ser abusivos no que tange a garantia de direitos fundamentais como a privacidade e a liberdade de expressão.

Um sistema de câmeras com captação sonora ininterrupta, pode gerar gravações das conversas de indivíduos em geral nas ruas em tempo real e em série histórica, o que além de ser uma intrusão abusiva na intimidade desses indivíduos ainda poderia gerar um efeito de desestimular manifestações públicas de indivíduos, acarretando em um *chilling effect* ("efeito apaziguador" ou "efeito resfriador").[394] Do mesmo modo, um sistema de câmeras com reconhecimento facial automatizado, poderia ser utilizado para monitorar em tempo real e em série histórica, o deslocamento e hábitos de indivíduos em geral, criando uma base de dados precisa de cada cidadão preventivamente.

Assim, embora a utilização de câmeras de vigilância pelos órgãos de segurança pública já seja um elemento importante na atual estratégia de garantia da segurança pública, será

391 O Detecta é um sistema de identificação de veículos e atividades *suspeitas* (como roubo e furtos) por meio de câmeras de monitoramento e câmeras com tecnologia OCR, implementado em 2014 pela Secretaria de Segurança Pública do Estado de São Paulo.

392 Tribunal de Contas do Estado de São Paulo. Relatório de Fiscalização de Natureza Operacional, Solução de Consciência Situacional - TCA nº 17.941/026/2015, Conselheiro Rel. Sidney Estanislau Beraldo. Disponível em: https://www4.tce.sp.gov.br/sites/tcesp/files/downloads/detecta.pdf. Acesso em: 15.09.2017. O relatório possui o objetivo de "verificar se a aquisição do Detecta atendeu a demanda quanto a ser um software inteligente que automatiza o processo de videomonitoramento dos espaços públicos e reduz o contingente de pessoas dedicadas à função de monitoramento das câmeras; se está operando com as funcionalidades previstas em contrato; bem como se é garantida a confiabilidade e a segurança das informações, além de avaliar os resultados nas atividades de planejamento, prevenção e investigação policial" (fls. 7-8).

393 Fonte: http://edition.cnn.com/2014/05/26/tech/city-of-tomorrow-video-data-surveillance/index.html. Acesso em: 15.09.2017.

394 KLITOU, Demetrius. **Privacy-invading technologies and privacy by design**: Safeguarding privacy, liberty and security in the 21st century. The Hague: Asser Press, 2014, p. 119.

necessário **aprimorar as salvaguardas e mecanismos de controle**, de modo a evitar práticas abusivas de vigilância com a modernização dos sistemas e aplicações sendo utilizados. Em todos os casos, os benefícios deverão sempre superar os ônus. Um sistema de vigilância que demonstrar ter pouca ou nenhuma eficácia positiva, ao mesmo tempo em que seus efeitos negativos são comprovados (tais como como redução de direitos fundamentais), deve ser descontinuado.

Com vistas a esse sistema de freios e contrapesos, o **Fórum Europeu para a Segurança Urbana[395] publicou a Carta de Uso Democrático da Videovigilância**.[396] Nesse texto, são apresentados princípios gerais para a concepção e funcionamento de sistemas de vigilância por vídeo, entre eles, os de legalidade, necessidade e proporcionalidade. A Carta sugere que o emprego de soluções de vigilância deve, em primeiro lugar, respeitar as leis locais e os tratados internacionais que tratem da proteção da privacidade, do monitoramento das comunicações e do uso de dados pessoais. Em segundo lugar, a decisão pública sobre a instalação desses dispositivos deve ser baseada na necessidade. O documento identifica tal termo como o balanço adequado entre, de um lado, circunstâncias e urgência, e, de outro, o tipo de resposta – no caso, o uso de equipamentos de vigilância. Ainda, a ação da Administração deve ser proporcional ao problema que pretende resolver. Em outras palavras, deve haver adequação entre os objetivos da atividade estatal e os meios utilizados para alcançá-los.

Na mesma direção de garantir um equilíbrio entre a garantia da segurança pública e os direitos individuais, foi publicada recentemente a **Diretiva 2016/680 do Parlamento Europeu**, "relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados".[397] No considerando nº 26 da referida Diretiva é possível identificar as mesmas balizas de uma atuação dentro dos limites legais, através de medidas necessárias e proporcionais.[398]

[395] O Fórum Europeu para a Segurança Urbana (*European Forum for Urban Security*) foi fundado em 1987 sob os auspícios do Conselho da Europa, constituíndo-se na única rede europeia de autoridades locais e regionais dedicadas à segurança urbana, incluíndo cerca de 250 autoridades locais e regionais de 16 países. Disponível em: https://efus.eu/en/about-us/about-efus/public/1450/. Acesso em: 15.09.2017.

[396] Disponível em: https://issuu.com/efus/docs/cctv_charter_pt. Acesso em: 15.09.2017.

[397] Disponível em português em: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN. Acesso em: 09.10.2017.

[398] (26) "O tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares em causa, e exclusivamente para os efeitos específicos previstos na lei. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância. Tais atividades podem ser executadas para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular em causa. A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal imparcial, tal como definido

No Brasil, é importante que essa agenda também avance, pois nesse cenário de novas soluções voltadas à segurança pública que envolverão a coleta de dados pessoais, o estabelecimento de balizas e diretrizes de boas práticas para o seu tratamento se torna crucial para evitar abusos por parte dos órgãos de segurança pública ou outros. Como já indicado em outros documentos do Estudo, a aprovação de lei específica acerca da proteção de dados pessoais e a criação ou designação de uma autoridade de proteção de dados pessoais são medidas essenciais nesse sentido.[399]

Adicionalmente a essa iniciativa, é importante que se avance no **desenvolvimento de um arcabouço de boas práticas por parte do Poder Público**. Dentre as iniciativas possíveis está a adoção de documento de avaliação do impacto na proteção de dados (em inglês, *Data Protection Impact Assessment* - DPIA), a fim de identificar problemas de privacidade e decidir quais procedimentos seguir para garantir que os riscos sejam gerenciados. Outra possibilidade interessante é a concepção de um código de conduta que estabeleça diretrizes sobre como os órgãos de segurança pública deveriam implementar e operar os atuais e futuros sistemas de monitoramento por câmeras e sensores. Dentre as questões que podem ser endereçadas, ressaltamos as seguintes:

a) Estabelecimento das funcionalidades, e seus respectivos parâmetros, a serem adotados como melhores práticas no monitoramento por câmeras e sensores em atividades de segurança pública;

b) Estabelecimento de informações claras e de instrumentos de comunicação ao público acerca do monitoramento por câmeras e sensores, com exceção de monitoramento secreto autorizado[400];

no artigo 47.o da Carta e no artigo 6.o da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). As pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais. Os dados pessoais deverão ser adequados e relevantes para os efeitos para os quais são tratados. É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica. Os Estados-Membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos."

399 Como observado no relatório da Horizontal de Regulação, a proliferação desses novos dispositivos conectados à Internet capazes de tratar os mais diversos tipos de dados, aumenta a preocupação quanto ao uso indevido de dados pessoais de cidadãos, bem como aos riscos de vazamento desses dados. Para mais informações, ver relatório da Horizontal de Regulação.

400 As operações específicas de monitoramento secreto, devem ser autorizadas e dentro da lei.

c) Definição de parâmetros para o tempo de guarda de dados, para cada tipo de monitoramento. Em algumas hipóteses pode não ser necessário nem mesmo reter dados, como nos casos de sensores de captação de áudio em logradouros públicos;

d) Definição de políticas de compartilhamento de dados entre os órgãos de segurança pública, não permitindo o compartilhamento fora das finalidades de segurança pública.

3.1.7 Aspectos regulatórios da contratação de soluções de Tecnologia da Informação e Comunicação pela Administração Pública

3.1.7.1. Introdução

Nesse momento trataremos dos aspectos gerais relativos ao processo de contratação de bens e serviços de Tecnologia da Informação e Comunicação ("TIC") pelo Poder Público, entre os quais apontamos as máquinas, equipamentos e dispositivos baseados em tecnologia digital (*hardware*); componentes eletrônicos diversos; programas para máquinas, equipamentos e dispositivos (*software*); e os serviços de cunho técnico associados a tais bens.

Para tanto, identificamos as normas aplicáveis à contratação de soluções de TIC pela Administração Pública Federal, mas que podem servir como parâmetros pelos entes municipais na ausência de regramento local. Em seguida, apresentamos exemplo de contratação de TIC no âmbito da Administração Pública Federal, consistente na contratação de serviço de computação em nuvem. Finalmente, abordamos os principais impasses na contratação de soluções de TIC pelos entes públicos e mapeamos os debates existentes sobre a possibilidade de flexibilização e aprimoramento das normas vigentes.

3.1.7.2. Panorama regulatório da contratação de TIC pela Administração Pública

A contratação de TIC deve ser pautada pelos procedimentos gerais de licitação estipulados nas Leis nº 8.666/1993 (Lei de Licitações) e nº 10.520/2002 (Lei do Pregão) e em seus Decretos regulamentadores, de nº 5.450/2005 e nº 7.892/2013.[401]

401 Igualmente deve observar a Lei nº 8.248/1991 (Lei de Informática), que trata de medidas de capacitação e competitividade do setor de informática e automação. Entre as disposições, o regramento cria orientações para que a Administração dê **preferência às aquisições de produtos e serviços desenvolvidos com tecnologia nacional** (art. 3º). Interessante observar que a Lei apresenta rol de bens e serviços considerados de Tecnologia da Informação e Comunicação, tais como componentes eletrônicos; máquinas, equipamentos e dispositivos baseados em técnica digital; programas para computadores, equipamentos e dispositivos; e os serviços técnicos relacionados a estes bens (art. 16-A). Esse regramento foi modificado pela Medida Provisória nº 810/2017, que incluiu as empresas de desenvolvimento ou produção de bens e serviços de TIC que investirem em atividades de pesquisa, desenvolvimento e inovação deste setor no regime de benefícios fiscais previsto na Lei nº 8.191/1991, instituidora de isenção sobre o Imposto sobre Produtos Industrializados - IPI.

No âmbito federal essa contratação deve seguir também regras específicas para a aquisição de soluções de TIC, que serão descritas em detalhe a seguir.

- **Decreto nº 8.135/2013 e Portaria Interministerial nº 141/2014**

O Decreto Federal nº 8.135/2013 estabelece que toda comunicação de dados da Administração Pública Federal deverá ser realizada por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da própria administração pública federal. Entretanto, a Portaria Interministerial nº 141/2014, regulamentadora do Decreto, cria exceção à tal regra, estabelecendo que **nos casos em que a instituição pública não é capaz de prover adequadamente o serviço de TI, este pode ser oferecido por entidades privadas** (art. 7º). Nestas situações a licitação será obrigatória, enquanto nas circunstâncias em que as soluções sejam providas diretamente pelo Poder Público o processo licitatório é dispensado (art. 2º do Decreto nº 8.135).[402]

Ações adotadas pelo MPDG e pelo Tribunal de Contas da União ("TCU")[403] sobre o tema indicam que **ambos vêm aplicando uma interpretação ampla sobre o art. 7º da Portaria, de modo a flexibilizar a contratação de entidades privadas para fornecimento de soluções de TIC**. Tal entendimento pode ser motivado pela atual ausência de capacidade adequada por parte de órgãos da Administração Pública Federal para oferecer soluções de TIC requeridas pelo governo.

- **Decreto nº 7.174/2010**

Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública federal. Para tanto, determina que a aquisição seja precedida de **elaboração de planejamento**, o que pode ser feito através de **projeto básico ou termo de referência**, não devendo tais documentos favorecerem a contratação de um fornecedor específico (art. 2º). Contudo, as regras do Decreto permitem que seja dada a preferência, no momento da contratação, para produtos e serviços com tecnologia de origem nacional (art. 5º), nos moldes do que determina a mencionada Lei nº 8.248/1991.[404]

402 A Portaria nº 141/2014 também estipula que a Administração deve requerer dos entes privados que oferecem serviços de TIC a adoção dos Padrões de Intergovernabilidade do Governo Eletrônico (e-PING), além de utilizarem técnicas de encriptação para informação confidencial e ferramentas para controle de acesso e identificação. Disponível em:

https://www.governoeletronico.gov.br/documentos-e-arquivos/e-PING_v2017_20161221.pdf/at_download/file.

403 Importante consignar, contudo, que há dificuldade em mapear o exato entendimento de MPDG e TCU, dado que estes órgãos não referenciam o Decreto nº 8.135 ou a Portaria nº 141 em suas publicações ou comunicações à imprensa. Entre as recentes movimentações desses atores governamentais em relação à contratação de soluções tecnológicas estão ações voltadas aos serviços de nuvem, que serão descritas abaixo.

404 A Administração deverá também requerer que os participantes de processos licitatórios para contratação de soluções de TI demonstrem, na fase de qualificação, estarem certificados por uma entidade pública ou privada

O Decreto determina também que na contratação de bens e serviços de informática e automação a Administração deve **adotar os tipos de licitação "menor preço" ou "técnica e preço"** (arts. 9 e 10) – conforme autorização do art. 45, § 4º, da Lei nº 8.666/1993. A licitação "menor preço" é exclusiva para a aquisição de bens e serviços de informática e automação considerados comuns, ou seja, passíveis de serem oferecidos por vários fornecedores, e será realizada na modalidade "pregão". Por sua vez, aquela do tipo "técnica e preço" é utilizada para bens e serviços de informática e automação de natureza predominantemente intelectual, isto porque as características dos bens ou serviços demandados requerem sua individualização.

- **Instrução Normativa SLTI/MPOG nº 04/2014**

Editada pelo Ministério do Planejamento, Desenvolvimento e Gestão ("MPDG"), visa regular especificamente as contratações de soluções de TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação ("SISP"), sistema criado com o objetivo de gerenciar os recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal.[405]

Em linhas gerais, a Instrução veda expressamente que (i) as contratações lidem com mais de uma solução de TIC para cada contrato e que (ii) sejam tratados aspectos de gestão de segurança da informação (art. 5º). Em todas as contratações, as entidades integrantes do SISP devem seguir três fases, as de planejamento da contratação,[406] de seleção de fornecedor,[407] e de gestão do contrato, durante a qual a Administração deverá acompanhar e garantir a adequada prestação de serviços e o fornecimento de bens (art. 8º).

- **Normas sobre segurança da informação editados pelo GSI**

acreditada pelo INMETRO em três diferentes aspectos: (i) segurança para os usuários e nas instalações; (ii) compatibilidade eletromagnética; e (iii) consumo de energia (art. 3º).

405 A atribuição primordial do órgão central do SISP é a elaboração da Estratégia Geral de Tecnologia da Informação e Comunicação - EGTIC, publicada anualmente e deverá servir de subsídio à elaboração de planos diretores de tecnologia da informação (PDTI) pelos órgãos e entidades integrantes do SISP (art. 3º). Conforme Decretos nº 1.048/1994 e 7.579/2011.

406 Válido observar que durante o momento inicial de planejamento, para além da celebração de termo de referência ou projeto básico, deve ser instituída equipe de planejamento da contratação e realizados estudo preliminar técnico e análise de riscos sobre a contratação (art. 9º).

407 A Instrução especifica que a seleção deverá ser na modalidade de licitação do tipo "pregão", preferencialmente realizada na forma eletrônica, para a seleção de soluções de TI que sejam enquadradas como bens ou serviços comuns (art. 26, parágrafo único).

Conforme o Decreto nº 3.505/2000, o Gabinete de Segurança Institucional da Presidência da República ("GSI/PR") têm competência para regular questões de segurança da informação no âmbito da Administração Pública Federal.[408]

O GSI já editou instruções normativas e dezenas de normas suplementares estabelecendo obrigações à segurança da informação em serviços de TIC oferecidos nas entidades federais.[409] As normas emitidas pelo GSI/PR são, aliás, consideradas pelo TCU como obrigatórias para a Administração Pública Federal.[410]

Por fim, ainda que o panorama regulatório apresentado acima tenha sido promulgado com vistas à contratação de bens e serviços de TIC pela Administração Pública Federal, tais regras devem ser também observadas pelos municípios brasileiros, juntamente com eventuais regramentos locais. **As normas federais poderão ser utilizadas como parâmetro para a contratação quando inexistentes normas específicas no âmbito municipal**, desde que considerado o posicionamento do Tribunal de Contas *competente* - isso porque pode haver divergências entre o entendimento dos Tribunais de Contas dos Estados e Municípios (no caso das cidades de São Paulo e Rio de Janeiro) e eventuais decisões do TCU.

3.1.7.2.1. Aspectos da contratação de serviços de nuvem

Entre as movimentações recentes de órgãos públicos relativas à contratação de soluções de TIC, destaca-se a **licitação realizada pelo TCU em 2017 para contratação de serviços de computação em nuvem**.[411] Nos Termos de Referência adotados, o Tribunal acolheu

408 A primeira movimentação para regulamentação de aspectos da segurança da informação remonta ao ano 2000, com a promulgação do referido Decreto nº 3.505, que institui a Política de Segurança da Informação para as instituições da Administração Pública em âmbito federal.

409 Conforme dados do Ministério das Comunicações veiculados em 2014, o GSI havia até o momento editado 4 Decretos, 3 Instruções normativas, 21 Normas complementares à IN 01 – SIC, e 1 Norma complementar à IN 02 – Credenciamento de Segurança.

410 No relatório sobre segurança da informação do Produto 8, tratamos da atuação do GSI/PR em segurança da informação no âmbito exclusivo da Administração Pública Federal e, especificamente, da gestão de segurança de infraestruturas críticas, da qual participa o GSI/PR. O Decreto nº 7.009/2009 tornou este tema uma atribuição da Câmara de Relações Exteriores e Defesa Nacional ("CREDEN"), presidida pelo Ministro-Chefe do GSI/PR. Em 2010, o Departamento de Segurança da Informação e Comunicações ("DSIC"), também ligado ao GSI/PR, publicou o Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação, atual referência para reflexão sobre modelos institucionais no tema. Disponível em http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf.

411 Disponível em:

http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15CC7BCB8015CEA6BFBA152F8. Embora a contratação desse certame esteja suspensa, em decorrência do Mandado de Segurança nº 1011543-07.2017.4.01.3400, a controvérsia não versa sobre o objeto da contratação, mas sim sobre possível violação do devido processo em uma das fases da contratação (utilização de robôs na fase competitiva do pregão, com violação do intervalo mínimo de segundos previsto na Instrução Normativa nº 03, de 04.10.2013 entre lances).

um tipo específico de contratação de serviços de nuvem, o de *cloud broker* (ou integrador de serviço de nuvem).[412]

Mesmo que tais Termos de Referência não sejam vinculantes para outros órgãos da Administração Pública, eles podem servir de referências para futuras licitações. O próprio MPDG, ao realizar em 2017[413] Consulta Pública sobre o "Termo de Referência - Serviços de Computação em Nuvem", adotou o método de contratação por meio de integrador empreendido pelo TCU.[414]

Além do conjunto de normas relativo à contratação de soluções de TIC descritos anteriormente, a Administração Pública deve também observar no momento da contratação de serviços de TIC: (i) as **normas suplementares nº 4 a 19 do GSI**; (ii) a **Portaria MP/STI nº 20/2016 do MPOG**,[415] com foco em seu documento anexo que contém orientações gerais e boas práticas;[416] e (iii) a **decisão nº 1.739, de 2015**, proferida pelo Tribunal de Contas da União[417], além de seu Anexo I.[418]

Entre as recomendações e requerimentos veiculados por essas normativas, estão, *primeiro*, a preferência pela implementação de serviços *hybrid cloud*[419] nas contratações feitas pelo MPDG, desde que seu objeto não coloque em risco a segurança nacional, conforme a Portaria nº 20/2016.

412 De acordo com a NIST SP 500-292 definition, *cloud broker* é uma entidade que gerencia o uso, execução e fornecimento de serviços de nuvem, e, ainda, negocia as relações entre provedores de serviço de nuvem e consumidores. Disponível em: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505. Acesso em: 15.01.2018.

413 Disponíveis em: http://www.participa.br/contratacao-de-servicos-de-computacao-em-nuvem/consulta-publica-servicos-de-computacao-em-nuvem/termo-de-referencia/termo-de-referencia-servicos-de-computacao-em-nuvem e http://www.participa.br/contratacao-de-servicos-de-computacao-em-nuvem/servicos-de-computacao-em-nuvem-consulta-publica/consulta-publica-termo-de-referencia/termo-de-referencia-servicos-de-computacao-em-nuvem.

414 Os Termos do MPDG, entretanto, trazem como requisito tanto operadores de serviços de nuvem quanto os integradores devem possuir seus servidores fisicamente localizados no Brasil.

415 Disponível em:

https://www.governoeletronico.gov.br/documentos-e-arquivos/Portaria%20MP-STI%20no%2020%20de%2014%20de%20junho%20de%202016.pdf.

416 Disponível em:

https://www.governoeletronico.gov.br/documentos-e-arquivos/Orientacao%20servicos%20em%20nuvem.pdf.

417 Devido à adoção progressiva de serviços de computação em nuvem pela Administração Pública federal, o TCU realizou, entre outubro de 2014 e fevereiro de 2015, uma pesquisa a fim de saber de forma mais clara os riscos e benefícios relativos a esse tipo de contratação. A análise desenvolvida pelo Tribunal inclui uma tabela na qual são indicados possíveis padrões de controle e boas práticas associadas com os 43 (quarenta e três) riscos identificados pela corte. Disponível em: http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20150720/AC_1739_24_15_P.doc.

418 Disponível em:

http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A15005860201501E7CDF5B41AC.

419 Conforme definição adotada pelo MPDG no anexo a Portaria nº 20/2016, com orientações gerais e boas práticas na contratação de serviços de nuvem, nuvem híbrida "é uma composição de duas infraestruturas de nuvem (privada e pública), interligadas por tecnologias apropriadas que permitem portabilidade de aplicações e de dados entre as nuvens".

Segundo, tal Portaria requer que a Administração exija em seus contratos de serviços de computação em nuvem que os dados ou informações, inclusive as cópias de segurança (*backup*) de arquivos, sejam armazenados em servidores localizados no Brasil.

Terceiro, as orientações gerais da Portaria estabelecem que os órgãos públicos deverão assegurar por meio de cláusulas contratuais que o serviço de nuvem a ser contratado permita a portabilidade de dados e aplicativos e que as informações do órgão contratante estejam disponíveis para transferência de localização, em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar a transição contratual (item 11).[420]

Quarto, a Portaria também determina que a Administração deve assegurar em suas contratações o sigilo das informações ou dados sob custódia do provedor de serviços de nuvem, devendo ser proibido ao provedor fazer deles qualquer uso ou transferi-los a terceiros sem que haja autorização dos órgãos públicos (item 12).[421]

Quinto, conforme a Norma Complementar nº 14/2012 do GSI, a Administração deve exigir que o provedor de serviços de nuvem garanta a prevalência da legislação brasileira durante a prestação de seu serviço (item 5.2.2.).[422] Quanto a esse aspecto, na opinião do TCU, embora esta norma não proíba de forma expressa a contratação de serviços de nuvem com servidores localizados no exterior, ela pode restringir "em termos práticos" as contratações feitas pela Administração a apenas aqueles serviços de nuvem com servidores localizados fisicamente no Brasil.[423]

Por fim, o TCU possui recomendação no sentido de que seja exigido dos provedores de serviços de nuvem a implementação de métodos de segurança no armazenamento e transferência de dados, tais como o uso de encriptação (que seja compatível com o nível de sigilo dado à informação armazenada) e de *Virtual Private Networks* - VPN. Além disso, entendeu-se que a *Application Programming Interface* - API dos serviços de nuvem devem ser desenvolvidos de acordo com os padrões de segurança adotados no mercado, incluindo mecanismos rigorosos de autenticação de usuários e controle de acesso.

420 Nesse sentido, a decisão nº 1.739/2015 do TCU frisa a necessidade de procedimentos adequados de portabilidade de dados, com vistas à eventual necessidade de se trocar o provedor do serviço. Ainda, o Tribunal recomenda uso de pacotes modulares, padrões abertos para serviços e uso de dados e transparência em relação aos procedimentos e custos referentes aos processos de portabilidade.

421 Corrobora a referida decisão nº 1.739/2015, visto que o TCU recomendou a existência de limites claros em relação aos direitos do provedor de serviço de nuvem em acessar e fazer uso de dados governamentais.

422 NC GSI/PR nº 14, item 5.2.2. A legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem.

423 O TCU entendeu que nem todos os serviços de nuvem com servidores fora do Brasil seriam capazes de garantir que eventual legislação estrangeira não prevalecesse sobre a nacional durante a execução de seus serviços. O Tribunal chega a sugerir que os contratos para a prestação desse tipo de serviço devem definir, de forma clara, em quais países os dados de seus consumidores estarão armazenados. Tribunal de Contas da União (TCU), Decisão nº 1739, de 2015, e seu Anexo I.

3.1.7.3. Mapeamento do debate atual em contratação de soluções de TIC pela Administração Pública

3.1.7.3.1. Competência legislativa em matéria de licitações

Realizado panorama a respeito da legislação incidente sobre a contratação de Tecnologias da Informação e Comunicação por órgãos públicos, apresentamos nessa seção mapeamento não exaustivo de entraves enfrentados pelo gestor público na condução dos referidos procedimentos.[424]

Em um primeiro momento, as principais dificuldades enfrentadas no âmbito local para contratar soluções de TIC estão intimamente relacionadas à distribuição de competência legislativa em matéria de licitações. Conforme determina o art. 22, XXVII, da Constituição Federal, a **União possui competência para editar *normas gerais* sobre contratações públicas, restando aos demais entes federados abordar aspectos de alcance local**.

Como se sabe, regras gerais versam sobre interesses não restritos ao âmbito local de entes federativos, isto é, versam sobre interesses *gerais* de todos eles. Um delineamento possível é o de que as modalidades (ex., pregão e convite) e tipos (ex., "menor preço" ou "técnica e preço") de licitação[425] não devem ser editados por Estados ou Municípios, porque as normas editadas por esses entes não devem tratar de interesses gerais (apenas locais) e não podem esbarrar em diretivas constitucionais como a de isonomia entre licitantes (artigo 37, XXI, da CF).

Em decisão recente o Supremo Tribunal federal ("STF") confirmou a constitucionalidade de lei estadual que estabelece preferência abstrata para a aquisição de *software* livre, dado que a matéria é de competência legislativa "regular" e não enseja exclusão de potenciais licitantes do universo de contratação com o Poder Público.[426] Diferentemente, decidiu-se em caso anterior pela inconstitucionalidade de lei estadual que ocasionava restrições competitivas em processos licitatórios às empresas. Ao conflitar com as previsões gerais de isonomia entre os competidores, a lei extrapolaria a competência suplementar conferida aos Estados em matéria legislativa.[427]-[428]

424 Portanto, não se objetiva apresentar encaminhamentos para a atuação de gestores públicos ou de potenciais contratados, e tampouco se pretende indicar encaminhamentos normativos para os órgãos dotados da respectiva competência normativa.

425 Modalidades e tipos não são sinônimos. Modalidades são as espécies de procedimento licitatório e tipos, por sua vez, são os critérios de decisão para a contratação.

426 Supremo Tribunal Federal, Tribunal Pleno, ADI 3059/RS. Rel. Min. Luiz Fux, d.j., 09/04/2015.

427 Supremo Tribunal Federal, Tribunal Pleno, ADI 3670/DF, Rel. Min. Sepúlveda Pertence, d.j. 02.04.2007.

428 Outro caso de relevância é o julgamento da lei paulista de licitações (Supremo Tribunal Federal, Decisão Monocrática, ADI 4116/SP, Rel. Min. Gilmar Mendes, d.j. 20.07.2012), que inverte as fases de julgamento de propostas e habilitação de proponentes previstas na lei federal (Lei 8.666/1993). Tal lei estadual, bem como a baiana, a paranaense e uma lei municipal de São Paulo, seguem a tendência estabelecida pelo modelo licitatório do pregão, inicialmente desenvolvido no âmbito da Agência Nacional de Telecomunicações - ANATEL. Questionou-se se a inversão dos

Em suma, pode-se afirmar que o estabelecimento de procedimentos licitatórios, delimitando a forma como será executado, é autorizado aos Municípios, Estados e Distrito Federal (art. 24, XI, da CF). Todavia, isso não significa que será autorizado à norma local estabelecer novas modalidades de preferência na seleção ou suprimir fases do processo de licitação. Afinal, os procedimentos de compras públicas são em grande medida definidos no âmbito federal, como observado em item anterior, e pouco maleáveis a mudanças de acordo com as particularidades locais. Esse cenário limita demasiadamente as possibilidades de flexibilização e adequação dos processos de licitação às especificidades das TIC.

Não obstante, algumas das dificuldades enfrentadas serão mais detidamente abordadas a seguir. Por ora, destacamos que, dentre os possíveis aspectos passíveis de regulação local, há: (i) a inclusão de aspectos adicionais em relação ao conteúdo mínimo de editais de licitação, e (ii) a definição de valores e prazos constantes dos editais.

3.1.7.3.2. Capacidade institucional e técnica dos municípios

Dentre as dificuldades enfrentadas pelos municípios em desenvolver processo de contratação de TIC está a ausência de capacidade institucional para (i) **identificar a demanda pelos referidos produtos**; e (ii) **elaborar projeto e edital de licitação específicos para sua demanda**.[429] Diferentemente de outros produtos essenciais à gestão pública, novas tecnologias são disponibilizadas no mercado a todo momento ou podem ser desenhadas especificamente para necessidades de determinado órgão ou entidade pública.

A projeção de demanda requer capacidade técnica para avaliar o lançamento de novos produtos e as especificidades técnicas do que se deseja adquirir. Igualmente, a elaboração de processo licitatório requer conhecimento pelo gestor para identificar e justificar a necessidade por determinado produto, bem como desenhar edital capaz de selecionar o melhor produto disponível para suas necessidades.[430] Por vezes, contudo, gestores e corpo técnico da Administração não se encontram familiarizados com conceitos técnicos básicos e características de produtos tecnológicos.

procedimentos licitatórios poderia ser considerada nova modalidade licitatória e, portanto, impossível de deliberação em âmbito local. O mérito da ação não chegou a ser julgado e a dúvida persiste até os dias de hoje.

429 VOJVODIC, Adriana et al. **Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação**: Análise de Entraves e Propostas para Aquisição. São Paulo: Iniciativa para Inovação na Educação Brasileira e Internet Lab, 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf. Acesso em 17.01.2018.

430 Uma alternativa existente para problemas de eficiência e capacidade técnica do gestor público seria a instituição de órgão central de compras, com *know how* e estrutura institucional para a contratação de TIC. Este órgão possuiria melhores condições de identificar os produtos disponíveis no mercado e coordenar as compras de forma a aumentar sua capacidade de negociação com fornecedores. FIUZA, Eduardo P. S.; MEDEIROS, Bernardo de A. **A Agenda Perdida das Compras Públicas**: Rumo a uma Reforma Abrangente da Lei de Licitações e do Arcabouço Institucional. Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada - IPEA, ago. 2014, p. 91-92. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/3362/1/td_1990.pdf. Acesso em 17.01.2018.

Entre os desafios enfrentados no desenho de edital para a contratação de TIC está a forma de **especificar a tecnologia ou rede de comunicação específica**, de modo a não inviabilizar ou direcionar a contração a um determinado fornecedor.[431]

Para aprimorar as capacidades dos membros da Administração Pública, em especial no âmbito municipal, interessante que seja realizada **formação continuada do corpo técnico dos entes públicos, em conjunto com a elaboração e distribuição de guias de referência** para orientação nos procedimentos de compra. Essas medidas poderão auxiliar os funcionários da Administração na identificação mais ágil e fácil de demanda por produtos e na execução adequada à demanda de projetos e editais de licitação.[432]

3.1.7.3.3. Falta de critérios adequados para a seleção da melhor solução técnica

Outro grande desafio à efetiva contratação de TIC pela Administração Pública consiste na **inexistência de procedimentos céleres e flexíveis que permitam a seleção com base na qualidade do produto** e após processo competitivo.[433] Ao contrário, as modalidades mais simples de licitação geralmente objetivam a aquisição de produtos amplamente disponibilizados no mercado e que podem ser adquiridos pelo tipo licitatório de "menor preço". Além disso, o tempo dispensado para o percurso das etapas da licitação por vezes se mostra incompatível com o tempo de desenvolvimento de novas soluções tecnológicas.[434]

Ao lado da legislação pouco flexível às peculiaridades da contratação de soluções tecnológicas, os órgãos de controle têm reforçado a rigidez e formalismo do processo licitatório. Em algumas oportunidades os Tribunais de Contas, por ausência de

431 Em sua manifestação na Consulta Pública realizada pelo estudo, a Telefônica Brasil apontou como possível solução ao desafio na elaboração do edital: "Seria interessante a existência de Editais "referência", gerados pela Câmara IoT, que poderiam ser adotados pelo poder público, garantindo qualidade dos serviços contratados. Desta forma, reduz-se o risco para o governo de não trazer a melhor solução (tecnicamente e economicamente) para a sociedade."

432 Preocupação semelhante foi demonstrada na Consulta Pública IoT, em que atores como a Unitec indicaram o conhecimento insuficiente dos membros da Administração sobre conceitos técnicos e benefícios inerentes ao emprego de dispositivos IoT como uma das barreiras a ser enfrentada pelos entes públicos na adoção de soluções baseadas em tecnologias de comunicação M2M e IoT. Disponível em: http://www.participa.br/portal/blog/consulta-publica-iot. Acesso em: 19.01.2018.

433 VOJVODIC, Adriana et al. **Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação**: Análise de Entraves e Propostas para Aquisição. São Paulo: Iniciativa para Inovação na Educação Brasileira e Internet Lab, 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf Acesso em 17.01.2018.

434 Segundo verificado em pesquisa sobre a contratação de TIC para a educação, conforme se verifica: "As entrevistas destacaram uma estimativa de 18 a 24 meses para vender um produto ao governo. Mesmo nos procedimentos viabilizados pelas atas de registro de preços do FNDE, que são mais eficientes, foram apontados como insuficientes para garantir a compra de produtos não defasados pelo tempo da inovação tecnológica". VOJVODIC, Adriana et al. **Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação**: Análise de Entraves e Propostas para Aquisição. São Paulo: Iniciativa para Inovação na Educação Brasileira e Internet Lab, 2015, p. 35. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf Acesso em 17.01.2018.

procedimentos internos capazes de lidar com a especificidade da contratação de novas tecnologias, acabam por reforçar parâmetros tradicionais de licitação.[435]

Mais que isso, não há uniformidade no entendimento dos diversos Tribunais de Conta sobre procedimentos, requisitos e dispensas de licitação. Essa combinação de fatores estimula cenário de incertezas e desestímulo à inovação do setor público. Gestores passam a ativamente adotar procedimentos burocratizados para evitar fiscalização e sanção pelos diversos órgãos de controle.

3.1.7.3.3.1. Impasses na modalidade de pregão: termo de referência e menor preço

Embora o pregão conte com procedimento mais célere, em razão da inversão das fases de habilitação e análise das propostas, requer a formulação de detalhado Termo de Referência e somente admite a contratação pelo menor preço.

Em relação ao Termo, documento base para a formulação dessa modalidade de licitação, deverá conter informações precisas sobre o produto, estratégia de suprimento, valor estimado baseado no preço de mercado, cronograma de entrega, entre outros (art. 9º, Decreto nº 5.450/2005). Na contratação de TIC, porém, nem sempre é possível apresentar semelhante detalhamento, visto que se tratam muitas vezes de novos produtos e sem qualquer equivalente no mercado. Mesmo que referido detalhamento seja palpável, ainda assim o procedimento poderá ser inadequado porque **a especificação exigida ao Termo de Referência pode restringir os fornecedores e excluir diferentes e inovadoras tecnologias** das possíveis soluções contratadas.[436-437]

435 Nesse sentido se posiciona relatório sobre contratação de TIC para a educação: "Além disso, foi mencionado em algumas entrevistas a necessidade de comprovar que o preço praticado para o objeto da contratação estava dentro dos parâmetros de mercado. Isso sugere que não há uma rotina adequada para contratar produtos únicos, impondo os mesmos critérios de formalização de contrato para casos de mercados competitivos." VOJVODIC, Adriana et al. **Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação**: Análise de Entraves e Propostas para Aquisição. São Paulo: Iniciativa para Inovação na Educação Brasileira e Internet Lab, 2015, p. 35. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf Acesso em 17.01.2018.

436 **Aquisição de Tecnologia Educacional pelo Setor Público**: Entraves e Caminhos para Estimular o Ecossistema de Inovação no Brasil. Iniciativa da Inovação na Educação Brasileira - IIEB, 2015, p. 39. Disponível em: http://www.cieb.net.br/wp-content/uploads/2016/06/082015_IIEB-Relatorio-Compras-Executivo_WEB_AFF.pdf. Acesso em 18.01.2018.

437 Em pesquisa realizada pelo InternetLab, aponta-se que a modalidade pregão tem sido utilizada pelo MEC para a contratação de hardware. Assim, as TIC com maior disponibilidade no mercado e menor potencial de inovação são mais facilmente licitados por pregão se comparado com outras modalidades de TIC, como o *software*. "Desde 2008, o MEC concluiu 41 licitações ligadas à informática, tecnologia e inovação. A maioria dessas licitações foram para consumo interno e, para as poucas compras de tecnologia observadas, elas são normalmente de hardware e feitas via pregão eletrônico". VOJVODIC, Adriana et al. **Compras de Tecnologia e Inovação pelos Órgãos Públicos de Educação**: Análise de Entraves e Propostas para Aquisição. São Paulo: Iniciativa para Inovação na Educação Brasileira e Internet Lab, 2015, p. 14. http://www.internetlab.org.br/wp-content/uploads/2015/12/ILAB_CompraseInovacaoEduc_v6-1.pdf. Acesso em 17.01.2018.

Outro desafio relacionado à contratação de TIC por pregão reside na **exigência de contratação por menor preço,**[438] **visto que restringe a possibilidade de avaliação sobre a qualidade técnica das TIC** em relação às necessidades específicas do órgão público contratante. Essa dificuldade se apresenta mais comumente na aquisição de *softwares*, visto que muitas vezes são dotados de peculiaridades e especificidades, enquanto a aquisição de *hardware* poderá ser realizada de forma mais descomplicada por pregão.

Em relação aos TIC mais difundidos, certos órgãos de controle entendem que seus protocolos, método e padrões de desempenho e qualidade são estabelecidos e conhecidos pelo mercado. Em razão disso, estabeleceram que sua aquisição seria melhor materializada por meio de licitação na modalidade pregão.[439]-[440]

3.1.7.3.3.2. Contratação direta: possibilidades e insegurança jurídica

Uma das alternativas à aquisição de TIC com características únicas e inovadoras, em que a aquisição por pregão não se mostre adequada, consiste na contratação direta por dispensa (art. 24) ou inexigibilidade de licitação (art. 25, Lei nº 8.666/1993).

Primeiro, a dispensa de licitação poderá ocorrer para a contratação de *software* e outras soluções tecnológicas pela Administração Pública, mesmo quando há outros produtos e fornecedores aptos a constituir concorrência, **quando é possível a aquisição de bens produzidos ou prestados por próprio órgão da Administração Pública** (art. 24, III, da Lei 8.666/1993). Este é o caso da Serpro (Serviço Federal de Processamento de Dados), empresa pública federal destinada à prestação de serviços em tecnologia da informação.

A Lei nº 5.615/1970, que regulamenta a atuação do Serpro, dispensa licitação para a sua contratação pela União para a prestação de serviços de tecnologia da informação considerados estratégicos (art. 2º). Igualmente, o Decreto nº 8.135/2013 determina que (i) comunicações de dados por órgãos federais deverão ser realizadas por serviços de TI fornecidos por órgãos ou entidades do próprio governo federal; e (ii) dispensa a licitação para contratação de órgãos ou entidades federais voltadas a preservar a segurança nacional.

438 COSTA, Gustavo Vidigal. Pregão para contratação de bens e serviços em Tecnologia da Informação – Sistema (Software) em Gestão Pública. **Revista do TCU**, n. 119, p. 13-22, 2010.

439 Esse posicionamento é adotado pelo Tribunal de Contas da União. Vide Acórdão nº 2.471/2008-TCU-Plenário, item 9.2.2.

440 Conforme o entendimento do TCU, aqueles bens e serviços de TIC detentores de padrões de desempenho e qualidade objetivamente definidos em edital devem ser licitados via pregão. Como vários desses produtos vêm apresentado natureza cada vez mais padronizada, em oposição a produtos de natureza intelectual e artística, espera-se que a modalidade de pregão se expanda na contratação de TIC. Segundo o Tribunal, nem a complexidade desses produtos e nem sua essencialidade à Administração poderiam ser usados como fundamentos para a descaracterização de sua padronização. Em Nota Técnica SEFTI/TCU nº 02/2008, disponível em:http://revista.tcu.gov.br/ojs/index.php/RTCU/article/download/284/297. Acesso em: 19.01.2018.

Segundo, soluções de TIC também poderão ser contratadas diretamente, por inexigibilidade de licitação caso comprovada a **exclusividade do produto oferecido e a existência de somente um fornecedor habilitado a prestar o serviço**. Essa possibilidade, todavia, tem provocado incertezas ao gestor público após diversas decisões proferidas por Tribunais de Contas afastando a excepcionalidade no caso. A título de exemplo, em 2004 Tribunal de Contas da União rejeitou contratação direta pela Agência Nacional do Petróleo - ANP - de licenças do *software Oracle* em razão da existência no mercado de outros *softwares* de bancos de dados.[441]-[442]

Finalmente, quando realizada a opção por contratação direta, por dispensa ou inexigibilidade de licitação, é importante que sejam disponibilizados canais para que fornecedores possam apresentar seus novos produtos que poderão ser de interesse da Administração. Isso porque a tendência será a contratação de fornecedores previamente conhecidos pelo gestor.

3.1.7.3.3.3. Impasses na contratação de software livre: eficiência versus isonomia

O "*software* livre" consiste em programa de computador construído de forma gratuita e colaborativa, podendo ser utilizado, copiado, modificado e redistribuído sem a necessidade de permissões do criador original.[443] Ainda, é essencial ao *software* livre que seu próprio código-fonte seja livre, isto é, de amplo conhecimento e não mantido em exclusividade por seus proprietários.[444]

441 Tribunal de Contas da União, TC 010.123/2003-9, julgada em 29/06/2004. Disponível em: https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjQ7sOzgeLYAhVBDpAKHR3CCOQQFggoMAA&url=http%3A%2F%2Fwww.tcu.gov.br%2FConsultas%2FJuris%2FDocs%2Fjudoc%2FAcord%2F20041215%2FTC-020-353-2003-2.doc&usg=AOvVaw2b8i3_di7MaBWiG8XyxDoN. Acesso em 18.01.2018.

442 O Projetos de Lei nº 4432/2008, de autoria do Deputado Carlos Zarattini, visa incluir entre as hipóteses de dispensa de licitação os bens e serviços de média baixa complexidade tecnológica que sejam essenciais a atividades estratégias para a defesa nacional. A proposta foi apensado ao Projeto de Lei nº 1.292/1995, que propõe alterar a lei de licitações. A proposta poderá ser verificada em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=418926. Acesso em 18/01/2018.

443 Sobre o tema, vide: MIZUKAMI, Pedro Nicoletti; LEMOS, Ronaldo. From free software to free culture: The emergence of open business. In: **Access to knowledge in Brazil: New research on intellectual property, innovation and development**, p. 13-39, 2010. Disponível em: http://klangable.com/uploads/books/A2KBrazil.pdf#page=27 Acesso em 18.01.2018.

444 Vide estudo sobre *software livre* comissionado pelo Instituto Nacional da Tecnologia da Informação (ITI): http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2673/FGV-CTS%20-%20Software%20livre.pdf?sequence=1 Acesso em 09.10.2017.

No capítulo sobre mobilidade urbana no Produto 8, defendemos que a adoção do *software* livre pelos órgãos públicos garantiria mais eficiência na gestão pública.[445-446] Isso porque o *software* livre detém capacidade de evitar o monopólio na contratação de *softwares* para uso governamental, assim como o efeito *lock-in*, decorrente de dificuldades técnicas decorrentes da migração entre *softwares* e transferência de dados.

Todavia, diretivas no sentido de que a Administração privilegie a contratação de *software* livre[447] geram incertezas do ponto de vista constitucional e desafiam as determinações da legislação sobre licitações.[448] **Questiona-se se os poderes públicos podem fazer uma opção prévia e geral por esse regime de *software*, visto que esta opção, segundo uma corrente jurisprudencial já sustentada pelo STF[449], não observaria o princípio de isonomia da licitação**, ao discriminar *ex ante* os ofertantes de *software* em regime proprietário da licitação.[450-451]

Em sentido oposto, **defende-se que a opção de *software* livre pela Administração, além de estar de acordo com o princípio constitucional da eficiência**[452] - cabendo ao Poder Público se utilizar de seu poder de compra para coibir o estabelecimento e preservação de monopólios privados -, não vai contra o princípio da isonomia. Isso porque a opção

445 Já em 2000 o Governo Federal havia se movimentado para racionalizar gastos com contratação de *software*, promulgando o Decreto Presidencial nº 18/00, que instituiu o Comitê Executivo do Governo Eletrônico.

446 Nesse sentido, ver: TEIXEIRA, Raphael L. C. J. A Contratação de Licenciamento de Software na Administração Pública. **Quaestio Juris**, v. 4, n. 01, 2011, p. 619. Disponível em: http://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/10201 Acesso em: 18.01.2018.

447 Exemplo disso é a Lei nº 12.883, de 2001, promulgada no município paulista de São Carlos para determinar que a Prefeitura deverá utilizar preferencialmente programas com códigos abertos e livres de restrição de propriedade. Disponível em: https://leismunicipais.com.br/SP/SAO.CARLOS/LEI-12883-2001-SAO-CARLOS-SP.pdf. Acesso em 17.01.2018.

448 Vide art. 37, XXI, da Constituição Federal e art. 3º da Lei nº 8.666/1993.

449 STF, Medida Cautelar em Ação Direta de Inconstitucionalidade 3.059-1-RS, Rel. Min. Carlos Ayres Britto, d.j. 15.04.2004.

450 O raciocínio empregado pelo Tribunal foi utilizado no exame de constitucionalidade de lei do Rio Grande do Sul que estabelecia a preferência por software livre nas contratações dos órgãos públicos estaduais. Lei do Estado do Rio Grande do Sul nº 11.871/2002, art. 1º, caput. "(...) Utilizarão preferencialmente em seus sistemas e equipamentos de informática programas abertos, livres de restrições proprietárias quanto a sua cessão, alteração e distribuição". Cf. FERRAZ JÚNIOR, Tércio Sampaio. Software Livre: a Administração Pública e a Comunhão do Conhecimento Informático. **Revista de Direito Público da Economia - RDPE**, Belo Horizonte, ano 3, n. 11, jul./set. 2005, p. 190.

451 Projetos de Lei já buscaram assegurar a isonomia de oportunidades entre fornecedores na situação de compras concomitantes de diversas soluções tecnológicas, entre eles, PL nº 167/2007 e PL nº 1739/2003, ambos arquivados.

452 Cf. FERRAZ JÚNIOR, Tércio Sampaio. Software Livre: a Administração Pública e a Comunhão do Conhecimento Informático. **Revista de Direito Público da Economia - RDPE**, Belo Horizonte, ano 3, n. 11, jul./set. 2005, p. 186.

da Administração por software livre tem por fundamento a própria definição do objeto da licitação ou a finalidade e não uma qualificação técnica esperada do software.[453]-[454]

Finalmente, conforme indicado anteriormente, recente decisão do STF considerou constitucional de lei estadual que estabelece preferência abstrata para a aquisição de *software* livre, dado que a matéria é de competência legislativa "regular" e não enseja exclusão de potenciais licitantes do universo de contratação com o Poder Público.[455]

3.2 Saúde

O objeto dessa parte da análise é identificar os aspectos regulatórios relacionados à Internet das Coisas (IoT) no ambiente da saúde e mapear eventuais barreiras regulatórias que impactem o desenvolvimento dessa tecnologia no setor, notadamente em relação às seguintes aplicações priorizadas[456]: *(i)* monitoramento remoto das condições dos pacientes com diabetes; *(ii)* localização de ativos dentro de unidades de saúde; *(iii)* apoio ao diagnóstico de Sepse; *(iv)* diagnóstico descentralizado; e *(v)* identificação e controle de epidemias.

Importante esclarecer que a presente análise regulatória não se concentrará em cada aplicação específica, na medida em que, primeiramente, é importante traçar um diagnóstico geral da legislação do setor. Em seguida, caso necessário, serão analisados eventuais aspectos específicos relacionados às aplicações selecionadas.

Para se atingir o objetivo proposto, a metodologia utilizada para a elaboração do diagnóstico regulatório de IoT no ambiente de saúde envolveu *(i)* o mapeamento das normas que impactam o setor, especialmente as normas e diretrizes estabelecidas pelo Ministério da Saúde (MS), pela Agência Nacional de Vigilância Sanitária (ANVISA) e pelo Conselho Federal de Medicina (CFM); *(ii)* entrevistas com técnicos da ANVISA; e *(iii)* contribuições dos agentes do setor de saúde que participaram dos *workshops* conduzidos pelo BNDES e pelo MCTIC.

[453] Para melhor entendimento, faz-se a analogia com as obrigações de compra de casa ou aluguel de casa: a escolha pela compra ou pelo aluguel diz respeito ao fim esperado pelo contratante e ao desígnio da contratação e não às características do imóvel. O mesmo acontece com a opção pelo software 'livre' ou 'proprietário': a contratação não está relacionada às qualificações técnicas do software, mas sim à definição do objeto da licitação e ao propósito perseguido pela Administração.

[454] Essa preocupação alude à previsão legal existente na política nacional de informática de "proibição à criação de situações monopolísticas, de direito ou de fato" (art. 2º, IV, da Lei nº 7.232/1984). O mercado de *software*, baseado em alta tecnologia e inovação, tende ao monopólio por ser capaz de criar ciclo virtuoso em "rede": quanto mais pessoas usam determinado produto ou serviço, mais pessoas passam a utilizá-los. Por causa disso, os produtos inovadores líderes acabam concentrando em suas mãos grossa fatia do mercado (*winner-takes-most*).

455 Supremo Tribunal Federal, Tribunal Pleno, ADI 3059/RS. Rel. Min. Luiz Fux, d.j., 09/04/2015.

[456] Aplicações priorizadas no "*7-B Relatório de aprofundamento das verticais – Saúde*".

3.2.1 Regulação da Agência Nacional de Vigilância Sanitária – ANVISA

Conforme explicado no Produto 2 – *Roadmap* tecnológico[457], os elementos comuns aos casos de uso de Internet das Coisas são: *(i)* recebimento de dados digitais vindos de sensores e/ou indo para atuadores; *(ii)* conexão a uma rede fora do objeto; e *(iii)* capacidade de processamento de dados de forma automática.

A partir dessa definição buscou-se identificar quais normas da legislação do setor de saúde teriam incidência sobre as aplicações envolvendo a tecnologia descrita, notadamente sobre *produtos* e *serviços* para saúde – que recebem atenção do *sistema de vigilância sanitária*.

Nesse sentido, analisando-se a legislação setorial, verificou-se que a Lei nº 6.360, de 23 de setembro de 1976 ("Lei nº 6.360/76"), dispõe que nenhum **produto de interesse à saúde**, seja nacional ou importado, poderá ser industrializado, exposto à venda ou entregue ao consumo no mercado brasileiro antes de registrado no Ministério da Saúde[458]. Mesmo nas hipóteses de exceção ao regime de registro, é necessário o cadastro do produto (§ 1º do art. 25 dessa lei[459]).

Importante esclarecer que a referida lei foi regulamentada pelo Decreto nº 79.094, de 5 de janeiro de 1977 ("Decreto nº 79.094/77"), posteriormente revogado pelo Decreto nº 8.077, de 14 de agosto de 2013 ("Decreto nº 8.077/13"), que atribuiu à ANVISA a competência para registro dos produtos sujeitos ao regime de vigilância sanitária.

A Lei nº 9.782, de 26 de janeiro de 1999 ("Lei nº 9.782/99") que, por sua vez, criou a Agência e instituiu o Sistema Nacional de Vigilância Sanitária, atribuiu à ANVISA a

457 Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/1970e8af-33d4-48a5-9522-d6335c931e26/170614_Produto_Parcial_Frente+2_Sumario_Executivo_Roadmap_Final.pdf?MOD=AJPERES&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz&CVID=lOOitOz. P. 7. Acesso em 28.09.2017.

458 "Art. 12 - Nenhum dos produtos de que trata esta Lei, inclusive os importados, poderá ser industrializado, exposto à venda ou entregue ao consumo antes de registrado no Ministério da Saúde. (...)"

459 "Art. 25 - Os aparelhos, instrumentos e acessórios usados em medicina, odontologia e atividades afins, bem como nas de educação física, embelezamento ou correção estética, somente poderão ser fabricados, ou importados, para entrega ao consumo e exposição à venda, depois que o Ministério da Saúde se pronunciar sobre a obrigatoriedade ou não do registro.

§ 1º - Estarão dispensados do registro os aparelhos, instrumentos ou acessórios de que trata este artigo, que figurem em relações para tal fim elaboradas pelo Ministério da Saúde, ficando, porém, sujeitos, para os demais efeitos desta Lei e de seu Regulamento, a regime de vigilância sanitária.

§ 2º - O regulamento desta Lei prescreverá as condições, as exigências e os procedimentos concernentes ao registro dos aparelhos, instrumentos ou acessórios de que trata este artigo."

competência para regulamentar, controlar e fiscalizar os produtos[460] e serviços que envolvam risco à saúde pública[461].

Esse mesmo diploma legal traz a lista de produtos e serviços submetidos à fiscalização sanitária da ANVISA. Entre os produtos listados no art. 8º, § 1º da Lei nº 9.782/99, encontram-se: *(i)* medicamentos de uso humano, suas substâncias ativas e demais insumos, processos e tecnologias; *(ii)* conjuntos, reagentes e insumos destinados a diagnóstico; *(iii)* equipamentos e materiais médico-hospitalares, odontológicos e hemoterápicos e de diagnóstico laboratorial e por imagem; *(vi)* radioisótopos para uso diagnóstico *in vivo* e radiofármacos e produtos radioativos utilizados em diagnóstico e terapia; *(vii)* quaisquer produtos que envolvam a possibilidade de risco à saúde, obtidos por engenharia genética, por outro procedimento ou ainda submetidos a fontes de radiação.

Os **serviços para a saúde**, por sua vez, são definidos no parágrafo seguinte do dispositivo acima citado como aqueles voltados para a atenção ambulatorial, seja de rotina ou de emergência, os realizados em regime de internação, os serviços de apoio diagnóstico e terapêutico, bem como aqueles que impliquem a incorporação de novas tecnologias. Tendo em vista que a tecnologia IoT é desenvolvida por meio de dispositivos, por mais que eles possam ter impacto sobre os serviços de saúde, não haverá incidência das regras que regulamentam os serviços de saúde sobre IoT.

Por fim, importante ressaltar que o conceito de **vigilância sanitária** relaciona-se a um conjunto de ações capazes de eliminar, diminuir ou prevenir riscos à saúde e de intervir nos problemas sanitários decorrentes do meio ambiente, da produção e circulação de bens e da prestação de serviços de interesse da saúde, podendo abranger: *(i)* o controle de bens de consumo que, direta ou indiretamente, se relacionem com a saúde, compreendidas todas as etapas e processos, da produção ao consumo; e *(ii)* o controle da prestação de serviços que se relacionem direta ou indiretamente com a saúde[462].

Feita essa descrição inicial da legislação do setor e compreendido o papel central da ANVISA, enquanto o órgão federal responsável pela vigilância sanitária, segue-se ao aprofundamento da análise das normas regulamentares da agência.

460 "Art. 7º Compete à Agência proceder à implementação e à execução do disposto nos incisos II a VII do art. 2º desta Lei, devendo: (...)

IX - conceder registros de produtos, segundo as normas de sua área de atuação;"

461 "Art. 8º Incumbe à Agência, respeitada a legislação em vigor, regulamentar, controlar e fiscalizar os produtos e serviços que envolvam risco à saúde pública".

462 Conforme art. 6º, § 1º, da Lei nº 8.080 de 19 de setembro de 1990.

3.2.2 Produtos para a Saúde

a) Caracterização

Conforme explicado acima, os produtos para a saúde somente poderão ser industrializados, expostos à venda ou entregues ao consumo no mercado brasileiro após registrados ou cadastrados perante a ANVISA.

A Resolução da Diretoria Colegiada nº 185, de 2001 ("RDC 185/01") definiu produto para a saúde como o "*equipamento, aparelho, material, artigo ou sistema de uso ou aplicação médica, odontológica ou laboratorial, destinado à prevenção, diagnóstico, tratamento, reabilitação ou anticoncepção e que não utiliza meio farmacológico, imunológico ou metabólico para realizar sua principal função em seres humanos, podendo, entretanto, ser auxiliado em suas funções por tais meios*".

Da definição acima extrai-se que o aspecto determinante para o enquadramento de um produto como "produto para a saúde" está relacionado à sua finalidade terapêutica ou de diagnóstico. Tal definição gera insegurança em relação ao objeto do presente estudo, quando o produto envolve alguma solução tecnológica, como já ocorreu no caso do enquadramento do *software* para a saúde, cujo procedimento pode ser utilizado como parâmetro para aplicações IoT.

Para tentar tornar mais claro o regramento do *software* para saúde foi publicada a Nota Técnica nº 04/2012/GQUIP/GGTPS/ANVISA ("Nota Técnica nº 04/2012"), que buscou esclarecer as hipóteses de registro ou cadastro dos *softwares*.

Considerando que as aplicações de IoT sempre conterão algum dispositivo de *software* em um dos elos de sua cadeia de valor, e que não existe uma norma específica relacionada aos produtos operados com IoT, importante entender quais foram as conclusões da referida nota orientativa, pois elas poderão servir para a análise do enquadramento das soluções de IoT como produtos para a saúde.

No âmbito da Nota Técnica, a ANVISA concluiu que os *softwares* podem ser enquadrados de três formas:

	Definição	**Disciplina da ANVISA**	**Exemplo**
***Software* produto para a saúde**	Não precisa de *hardware* classificado como produto para saúde para ser executado	Só pode ser industrializado, exposto à venda ou entregue ao consumo no mercado após	*Softwares* usados para o processamento de dados médicos; para posicionamentos

		registro ou cadastro perante a ANVISA.	cirúrgicos e para diagnosticar uma doença, como o *Software Match It! DNA* e o Sistema de Captura de Imagens e Gestão de Laudos ZSCAN.
***Software* parte ou acessório de um produto para saúde**	É parte integrante do *hardware*, precisando dele para funcionar	Deve ser registrado em conjunto com o *hardware* (salvo alguns casos previstos na Nota Técnica Nº 04/2012[463])	*Software* que controla as funções de um dispositivo médico ou que transfere informações de equipamentos médicos, como o *Picture Archiving and Communication System* (PACS)
***Software* não produto para saúde**	São destinados a finalidades diferentes da prevenção, diagnóstico, tratamento, reabilitação ou anticoncepção de seres humanos.	Não são passíveis de registro ou cadastro junto à ANVISA.	Aplicativos para dispositivos móveis indicados especificamente para fins de prática esportiva e para o lazer, como o *Apple Watch* e o *Fit Bit*

463 Entre essas hipóteses, está o caso de o *software* ter classificação de risco superior ao do equipamento ao qual se destina ou quando for comercializado por terceiros, que não o fabricante do equipamento médico ao qual se destina.

Diante do exposto, é possível **concluir que quando o equipamento que envolver tecnologia IoT tiver finalidade terapêutica ou de diagnóstico, ele será enquadrado como produto para a saúde, estando, portanto, sujeito à vigilância sanitária**.

b) Processo de registro / cadastro

A compreensão do processo de registro e cadastro junto à ANVISA é relevante para a identificação de eventuais barreiras ao desenvolvimento de IoT na área da saúde.

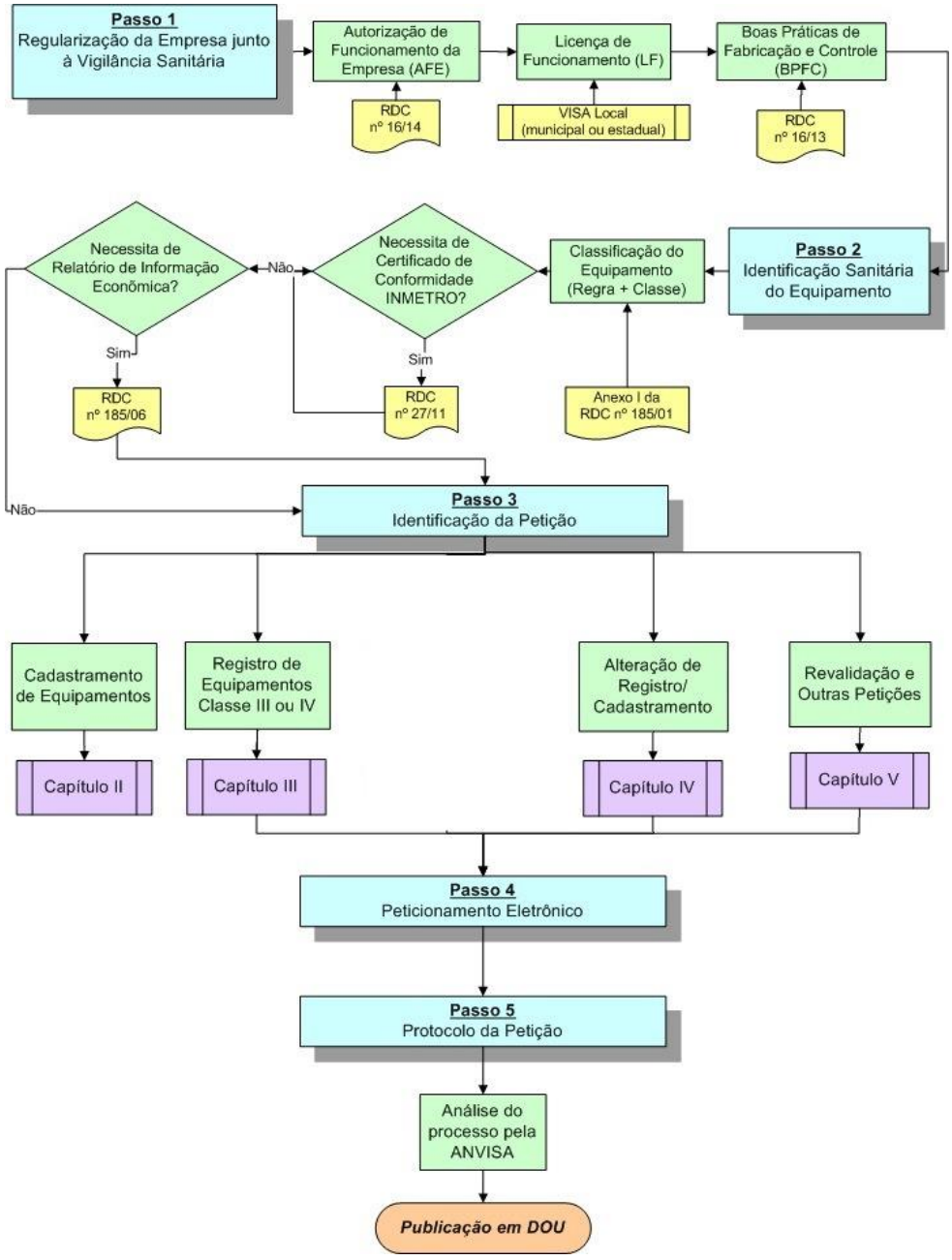
O procedimento para registro é disciplinado pela RDC 185/01 e, nos termos do Decreto nº 8077, de 2014, deverá ser concedido em 90 dias[464]. Já o procedimento para cadastro é mais simples e encontra-se regulamentado pela Resolução da Diretoria Colegiada nº 40 de 2015 ("RDC 40/2015"). Na imagem abaixo, retirada do *"Manual para regularização de equipamentos médicos da ANVISA"*, é possível visualizar o fluxograma com todo o procedimento para solicitação de Registro ou Cadastro perante a ANVISA[465].

464 Decreto nº 8077/2013:

Art. 7º Os produtos de que trata o art. 1º somente poderão ser objeto das atividades a eles relacionadas se registrados junto a Anvisa, observados seus regulamentos específicos.

§ 1º O registro será concedido no prazo de noventa dias, contado da data de entrega do requerimento, salvo nos casos de inobservância da Lei nº 6.360, de 1976, deste Decreto ou de outras normas pertinentes.

465 Página 6 do "Manual para regularização de equipamentos médicos da ANVISA".



Do fluxograma acima verifica-se que antes da solicitação do registo ou cadastro perante a ANVISA, existem passos prévios que devem ser cuidadosamente cumpridos, pois a insuficiência da documentação técnica exigida poderá ensejar o indeferimento sumário da petição[466], o que tornará o processo mais moroso.

Diante disso, a primeira etapa para a solicitação do registro ou cadastro de equipamentos médicos perante a ANVISA é a regularização da empresa junto à vigilância sanitária por meio da obtenção *(i)* da Autorização de Funcionamento da Empresa ("AFE"), *(ii)* da

466 Conforme o inciso II do § 2º do art. 2º da RDC nº 204, de 06 de julho de 2005 e § 2º do art. 4º da RDC nº 40/2015 para os casos de cadastro.

Licença da Funcionamento local ("LF") e *(iii)* do Certificado de Boas Práticas de Fabricação e Controle ("CBPF").

A AFE deve ser obtida nos termos da Resolução da Diretoria Colegiada nº 16, de 1º de abril de 2014, sendo que apenas as empresas legalmente constituídas em território brasileiro podem pleitear essa autorização perante a ANVISA.

Importante destacar que, de acordo com o referido manual, uma empresa estrangeira que tenha interesse em comercializar os seus produtos no mercado brasileiro deve possuir um acordo comercial com uma empresa no Brasil.

Esta empresa, por sua vez, não necessita ser uma filial ou subsidiária de empresa estrangeira, sendo possível que a empresa brasileira seja apenas uma importadora, a qual assumirá a responsabilidade técnica e legal da empresa estrangeira em território brasileiro.

Além da AFE, é necessária a emissão de uma Licença de Funcionamento Local ("LF") perante a agência de vigilância sanitária local, seja ela estadual ou municipal.

Em seguida, é necessário que a empresa atenda aos requisitos de Boas Práticas de Fabricação e Controle ("BPFC"), o que é uma obrigação de toda empresa que pretenda fabricar, importar ou comercializar produtos médicos, conforme dispõe o Decreto nº 8.077, de 14 de agosto de 2013.

Após essa comprovação, é emitido o certificado de boas práticas de fabricação e controle, cuja apresentação é obrigatória para o registro de produtos das classes III e IV. Para os produtos das classes I e II, sujeitos à cadastro, não é obrigatória a sua apresentação, contudo, devem ser cumpridos os requisitos de BPFC estabelecidos na Resolução da Diretoria Colegiada nº 16/2013.

É possível que a evolução tecnológica representada pela tecnologia IoT requeira a atualização das BPFC, mas até o presente momento não se tem indicação de que as exigências atualmente postas representem uma barreira para as atuais aplicações.

Passada essa etapa, segue-se à identificação sanitária do equipamento. Para tanto, deve-se identificar em qual classe de risco de I a IV o equipamento está enquadrado.

Além da classificação de risco, é necessário enquadrar o produto por regras, as quais obedecem à indicação e finalidade de uso do equipamento. São as seguintes: *(i)* produtos não invasivos – regras 1 a 4; *(ii)* produtos invasivos – regras 5 a 8; *(iii)* produtos ativos – regras 9 a 12; e *(iv)* regras especiais – regras 13 a 18. Tais regras de classificação podem ser identificadas no Anexo II do Regulamento Técnico aprovado pela RDC 185/01.

Da leitura da Resolução observa-se que existem diversas regras, que por vezes podem apresentar critérios complexos de classificação, o que poderá representar dificuldade para enquadramento dos produtos por parte dos agentes e consequente acréscimo de tempo ao processo.

Em seguida, é necessário identificar se o equipamento estará sujeito a registro ou cadastro[467]. O Cadastro de produtos médicos tem fundamento legal no § 1º do art. 25 da Lei nº 6.360/76 e é regido pela RDC nº 40, de 26 de agosto de 2015[468], aplicando-se aos produtos para saúde classificados nas classes de risco I e II, com exceção dos produtos para diagnóstico *in vitro*.

O procedimento para solicitação do cadastro junto à ANVISA encontra-se previsto no art. 4º da RDC nº 40/2015, entre eles *(i)* formulário de petição para cadastro com informações do produto; *(ii)* comprovante de pagamento de taxa de fiscalização de vigilância sanitária; *(iii)* cópia autenticada do certificado de conformidade, aplicável aos produtos médicos com certificação compulsória; *(iv)* declaração apostilada acompanhada de tradução juramentada para os produtos médicos importados.

O preenchimento do formulário requer a apresentação detalhada de dados do produto. Diante do nível de detalhamento das informações, é possível que surjam dúvidas por parte dos interessados, as quais buscam ser endereçadas pelo *Manual para regularização de equipamentos médicos na ANVISA*.

Importante ressaltar que o cadastro de *software* requer o preenchimento de formulário próprio. Nesse ponto, pode surgir a dúvida sobre a necessidade de utilização desse formulário para o cadastramento de produtos IoT já que, no geral, aplicações com essa tecnologia terão dispositivo de *software* em algum elo de sua cadeia.

O detalhamento das informações que devem ser apresentadas também se encontra no Manual referido acima e envolvem informações como arquitetura do *software*, compatibilidade (interoperabilidade e comunicação) com outros produtos médicos, requisitos de infraestrutura, entre outros.

Ainda, imporante ressaltar que o fabricante ou importador do produto deverá manter dossiê técnico[469] atualizado, para fins de fiscalização do Sistema Nacional de Vigilância Sanitária, que descreva os elementos que compõem o produto com a indicação das características, finalidade, modo de uso, conteúdo, cuidados especiais, potenciais riscos, processo produtivo e informações adicionais do produto.

467 Equipamentos médicos sujeitos tanto ao registro como ao cadastro podem figurar em qualquer uma daquelas dezoito regras de classificação, conforme sua indicação e finalidade de uso.

468 Na justificativa à consulta pública nº 24/2014, cujo assunto era a proposta de Resolução nº 40/2015 em substituição à RDC nº 24/2009, foi explicado que a proposta tinha como um de seus pontos centrais a simplificação do processo de análise para os produtos considerados de baixo risco, considerando-se que ao simplificar o processo pré-mercado, seria dado maior ênfase no controle das etapas pós-mercado dos produtos.

469 Anexo II – Dossiê Técnico de Produtos Médicos: "1. O Dossiê Técnico não precisa corresponder a um arquivo físico ou eletrônico contendo todas as informações abaixo descritas, podendo ser composto por referências a documentos e informações que compõem outros arquivos ou registros do Sistema de Qualidade da empresa, os quais deverão estar disponíveis para fiscalização do Sistema Nacional de Vigilância Sanitária".

Por fim, cumpre dizer que não é necessária a revalidação do cadastro, ficando sua manutenção vinculada ao cumprimento dos requisitos das Boas Práticas de Fabricação.

Os equipamentos classes III e IV, por sua vez, estão sujeitos a registro, devendo ser apresentados à ANVISA uma quantidade maior de documentos, previstos na RDC 185/2001, que no caso do cadastro. São eles: *(i)* formulário do fabricante ou importador de produtos médicos preenchido; *(ii)* comprovante de pagamento da taxa de vigilância sanitária; *(iii)* dados da empresa – cópia da AFE; *(iv)* rótulo; *(v)* etiqueta indelével; *(vi)* instruções de uso; *(vii)* relatório técnico; *(viii)* comprovante de cumprimento dos requisitos estabelecidos em regulamentos técnicos; *(ix)* Certificado de Boas Práticas de Fabricação e Controle.

Para os produtos importados ainda deverá ser apresentado *(i)* carta de autorização de representação no Brasil, emitido pelo fabricante no exterior; e *(ii)* Certificado de Livre Comércio.

O registro de *software* também exige requisitos específicos, que podem ser sumarizados da seguinte forma: *(i)* arquitetura de *software*; *(ii)* arquitetura de *hardware*; *(iii)* requisitos técnicos mínimos e recomendáveis; *(iv)* plataforma; *(v)* compatibilidade; *(vi)* características de segurança; *(vii)* requisitos de infraestrutura; *(viii)* verificação (lista de testes realizados, seus critérios de falha ou sucesso e o percentual de aprovação obtido neles).

Ainda, imporante ressaltar que o relatório técnico referido como um dos documentos que devem ser apresentados para efetivação do registro deverá descrever a eficácia e segurança do produto médico, cujos requisitos estão indicados na Resolução da Diretoria Colegiada nº 56, de 2001 ("RDC 56/2001").

Tais requisitos orientam o fabricante a respeito de possíveis riscos, que necessitam ser controlados, sendo responsabilidade exclusiva do fabricante analisar, avaliar e controlar os riscos associados ao seu produto.

Estes serão verificados pela autoridade de vigilância sanitária por ocasião da inspeção das Boas Práticas de Fabricação, do registro na ANVISA ou da fiscalização sanitária dos produtos.

Caso a descrição constante do relatório técnico não comprove a eficácia e segurança do produto, a ANVISA solicitará pesquisa clínica do mesmo, a qual se caracteriza como investigação utilizando seres humanos, destinada a verificar o desempenho e segurança e eficácia do produto, nos termos do disposto na Resolução da Diretoria Colegiada nº 10, de 2015 ("RDC 10/2015").

Por fim, quanto ao prazo de validade, o registro valerá por 10 anos, podendo ser revalidado sucessivamente por igual período[470]. Importante ressaltar que o equipamento está autorizado a ser comercializado apenas após a concessão do registro ou cadastro. O produto comercializado deve necessariamente corresponder ao que foi autorizado pela ANVISA e qualquer alteração nesses equipamentos deverão ser endereçadas à Agência por meio de petições de alteração.

c) Necessidade de atualização regulatória

Descrita a regulamentação que rege o enquadramento sanitário de produtos perante a ANVISA, verifica-se que as aplicações analisadas nesse relatório provavelmente estarão sujeitas a cadastro ou a registro, a depender do nível de risco da aplicação.

Contudo, considerando que existem inúmeras aplicações possíveis para IoT e que a tecnologia está em constante e rápida evolução, uma preocupação que se coloca diz respeito à capacidade de a regulação acompanhar os avanços da tecnologia. Exemplo desse desafio refere-se ao enquadramento dos produtos combinados (*drug-device combination products*[471]), que são produtos terapêuticos e diagnósticos que combinam remédio com dispositivos.

Tendo em vista que a definição de produto para a saúde presente na RDC 185 excluiu dessa classificação os produtos que utilizem meio farmacológico, surge a dúvida acerca de qual seria o enquadramento sanitário desse tipo de produto, bem como sobre como a Agência regulamentará outros produtos complexos que venham a surgir a partir do avanço tecnológico.

Além da necessidade de constante atualização das normas que regulam um setor em crescente desenvolvimento, outro desafio que se coloca é a dificuldade de a regulação setorial conseguir traduzir ou endereçar os riscos à saúde pública relacionados aos *softwares* enquanto dispositivos médicos, ou à soluções de IoT especificamente, bem

[470] Resolução RDC nº 185, de 2001:
"13. O registro de produtos para saúde terá validade por 10 (dez) anos, contados a partir do dia da sua publicação no Diário Oficial da União, podendo ser revalidado sucessivamente por igual período. (Redação dada pela Resolução – RDC nº 211, de 22 de janeiro de 2018)."

[471] Nos Estados Unidos, já existe regulamentação para os produtos combinados pela U.S Food & Drug Administration – FDA. "*Combination products are therapeutic and diagnostic products that combine drugs, devices, and/or biological products. FDA expects to receive large numbers of combination products for review as technological advances continue to merge product types and blur the historical lines of separation between FDA's medical product centers, which are made up of the Center for Biologics Evaluation and Research (CBER), the Center for Drug Evaluation and Research (CDER), and the Center for Devices and Radiological Health (CDRH). Because combination products involve components that would normally be regulated under different types of regulatory authorities, and frequently by different FDA Centers, they raise challenging regulatory, policy, and review management challenges. Differences in regulatory pathways for each component can impact the regulatory processes for all aspects of product development and management, including preclinical testing, clinical investigation, marketing applications, manufacturing and quality control, adverse event reporting, promotion and advertising, and post-approval modifications.*" Disponível em https://www.fda.gov/CombinationProducts/AboutCombinationProducts/default.htm

como garantir o apropriado equilíbrio entre proteção ao paciente/consumidor e promoção da saúde pública por meio do incentivo à inovação.

É nesse sentido que o *International Medical Device Regulators Forum ("IMDRF")*, fórum internacional de reguladores de diversos países, está regularmente atualizando as normas que dispõem sobre *software* como dispositivo médico, de forma a garantir convergência regulatória entre os órgãos reguladores dos diversos países que o compõem.

Sobre esse aspecto, a Gerência-Geral de Tecnologia de Produtos para a Saúde da ANVISA sinalizou em entrevistas com técnicos da área e no Seminário Internacional de Dispositivos Médicos 2017, que a agenda regulatória 2018/2019 da Agência irá prever a elaboração de Resolução específica para regulamentação e controle de *software* como dispositivo médico[472].

A atualização desse regramento levará em consideração as diretrizes do IMDRF. Entre elas estariam: *(i)* a N10, que estabelece as definições e terminologias aplicadas a *software* enquanto dispositivo médico[473]; *(ii)* a N12, que dispõe sobre classificação de risco[474], *(iii)* a N23, que trata de sistema de gerenciamento de qualidade[475]; e *(iv)* a N41R3, que normatiza a avaliação clínica de *software*[476]. Além disso, a Agência também avalia a internalização do Guia sobre cibersegurança do U.S Food & Drug Administration – FDA[477], o que será aprofundado abaixo no capítulo sobre proteção de dados.

Diante disso, observa-se que a disciplina de *software* como produto para saúde sofrerá atualizações em breve, o que modificará o cenário explicado nos itens anteriores. Tal atualização, no entanto, parece convergir com as mais avançadas práticas e normas internacionais do setor.

472 Disponível em:

http://portal.anvisa.gov.br/documents/33912/264673/Software+as+a+Medical+Device.pdf/df5e4fa8-4d45-4f7d-ba67-bfd49c1f3bcd. Acesso em 16.11.2017.

473 Disponível em "IMDRF/SaMD WG/N10FINAL:2013, *Title: Software as a medical device: key definitions"*. Acesso em 16.11.2017.

474 Disponível em "IMDRF/SaMD WG/N12FINAL: 2014, *Title: Software as a medical device: possible framework for risk categorization and corresponding considerations"*. Acesso em 16.11.2017.

475 Disponível em "IMDRF/SaMD WG/N23 FINAL:2015. *Title: Software as a Medical Device: application of quality management system."* Acesso em 16.11.2017.

476 Disponível em IMDRF/SaMD WG/N41FINAL:2017. *Title: Software as a Medical Device: clinical evaluation*. Acesso em 16.11.2017.

477 Disponível em:

https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. Acesso em 16.11.2017.

3.2.3 Regulação dos Conselhos de Medicina

O Conselho Federal e os Conselhos Regionais de Medicina, constituídos sob a forma de autarquias, têm como principal atribuição a supervisão da ética médica[478].

Por mais que suas normas não constituam obstáculos ao desenvolvimento de soluções de IoT na área da saúde, importante ressaltar que o código de ética médica deverá ser sempre seguido pelos médicos no exercício da sua profissão independentemente do meio tecnológico utilizado na sua atuação.

O Conselho Federal de Medicina, buscando adequar o exercício da profissão médica aos avanços tecnológicos na área da saúde, já regulamentou a utilização dos prontuários digitais[479] (Resolução nº 1.821/07) e a telemedicina[480] (Resolução nº 1.643/02).

Com relação aos prontuários digitais, a Resolução nº 1.821/07 tem como objeto a guarda e o manuseio digitais dos prontuários dos pacientes. Ela equipara em certos aspectos o prontuário digital ao físico, apontando para a necessidade de se manter o sigilo profissional e a privacidade do indivíduo, nos termos do Código de Ética Médica. Em seguida, a resolução ainda levanta algumas regras específicas para a digitalização de prontuários, como os parâmetros que os sistemas de gerenciamento eletrônico especializados devem possuir, os quais incluem garantias de segurança.

Cabe destacar que a Resolução prevê também a assinatura de um convênio entre o Conselho Federal de Medicina e a Sociedade Brasileira de Informática em saúde para

478 Lei nº 3.268, de 30 de setembro de 1957:

"Art. 2º O conselho Federal e os Conselhos Regionais de Medicina são os órgãos supervisores da ética profissional em toda a República e ao mesmo tempo, julgadores e disciplinadores da classe médica, cabendo-lhes zelar e trabalhar por todos os meios ao seu alcance, pelo perfeito desempenho ético da medicina e pelo prestígio e bom conceito da profissão e dos que a exerçam legalmente".

479 Exposição de Motivos da Resolução CFM nº 1.821/2007: "O prontuário do paciente, em qualquer meio de armazenamento, é propriedade física da instituição onde o mesmo é assistido, quer seja uma unidade de saúde quer seja um consultório, a quem cabe o dever da guarda do documento. Assim, ao paciente pertencem os dados ali contidos, os quais só podem ser divulgados com a sua autorização ou a de seu responsável, ou por dever legal ou justa causa. Estes dados devem estar permanentemente disponíveis, de modo que, quando solicitados por ele ou seu representante legal, permitam o fornecimento de cópias autênticas das informações a ele pertinentes (...)

Com isso, o Conselho Federal de Medicina reconhece a importância do uso de sistemas informatizados para a guarda e manuseio de prontuários de pacientes e para a troca de informação identificada em saúde, bem como a digitalização dos prontuários em papel, como instrumento de modernização, com consequente melhoria no atendimento ao paciente. É dever do CFM garantir ao médico amplo respaldo legal na utilização desses sistemas, motivo pelo qual publica esta Resolução."

480 A resolução, em seu artigo 1.º, define a telemedicina como *"o exercício da medicina mediante a utilização de metodologias interativas de comunicação audiovisual e de dados, com o objetivo de assistência, educação e pesquisa em saúde"*. Face à interpretação de que se trata de ato médico, os serviços prestados através da telemedicina deverão oferecer infraestrutura tecnológica apropriada e obedecer as normas técnicas do CFM, no que se refere à guarda, manuseio, transmissão de dados, confidencialidade, privacidade e garantia do sigilo profissional.

Disponível em: http://portal.cfm.org.br/index.php?option=com_content&view=article&id=1087:&catid=3. Acesso em: 25.09.2017.

expedir um selo de qualidade dos sistemas informatizados. Isto, aliado ao reconhecimento dos impactos positivos que a tecnologia pode ter no atendimento dos pacientes, demonstra a preocupação do CFM em absorver e regular os avanços tecnológicos na área da saúde, podendo vir a regular o impacto de tecnologias IoT no futuro.

Quanto à telemedicina, a Resolução 1.643/02 busca disciplinar "o exercício da Medicina através da utilização de metodologias interativas de comunicação audiovisual e de dados, com o objetivo de assistência, educação e pesquisa em saúde".

A Resolução dá liberdade aos médicos de praticarem a telemedicina, aproximando essa prática ao exercício regular da medicina. Além disso, ela determina que a telemedicina deve se pautar também pela confidencialidade, privacidade e pelo sigilo profissional, que devem ser garantidos pela infraestrutura tecnológica usada para prestar o serviço.

Uma vez que a Resolução se justifica pelo surgimento de novas tecnologias e que a sua definição abrangente incide sobre "metodologias interativas de comunicação audiovisual e de dados", percebe-se que tal norma pode se aplicar a futuros equipamentos e tecnologias IoT que sejam usadas na área da saúde.

Diante disso, é possível que o avanço tecnológico proporcionado por IoT também resulte em inovações que demandem a atualização das normas dos referidos conselhos. É importante que essas normas harmonizem adequadamente a proteção à saúde e os interesses médicos, estimulando os avanços tecnológicos.

3.2.4 Debates sobre Privacidade

a. Privacidade e saúde

As aplicações de IoT na área de saúde podem ou não envolver a coleta de dados pessoais. Entre os casos de uso, ocorrerá a utilização de dados pessoais, por exemplo, no monitoramento remoto das condições dos pacientes com diabetes e no diagnóstico de Sepse.

Conforme descrito no item deste relatório dedicado à análise tecnológica das aplicações, **a garantia da confidencialidade e privacidade dos dados são aspectos críticos para o adequado desenvolvimento das aplicações de IoT na área da saúde**.

Assim, a proteção à privacidade e aos dados pessoais é questão que merece atenção especial em virtude da necessidade de, por um lado, resguardar a privacidade dos indivíduos e, por outro, permitir que o Estado, institutos de pesquisa e organizações privadas de saúde possam acessar dados relevantes para o auxílio na elaboração de políticas públicas ou para o desenvolvimento tecnológico do setor.

Diante disso, tendo em vista que a utilização de dispositivos IoT na área da saúde ampliará a capacidade de coleta de dados dos cidadãos, faremos a contextualização e análise do regramento relativo à privacidade e proteção de dados na área da saúde.

Conforme explicado no Produto 3,[481] ainda não há no Brasil uma lei geral de proteção de dados. É importante ressaltar que a ausência dessa norma geral impacta IoT, especialmente na área da saúde onde os dados coletados são sensíveis e devem receber atenção especial.

Em que pese a inexistência de uma lei geral de proteção de dados, há atualmente três projetos de lei em tramitação no Congresso Nacional para tratar desse tema. São eles os Projetos de Lei nº 4.060/2012[482], nº 330/2013[483], e nº 5.276/2016[484], os quais, entre outros aspectos, distinguem dados pessoais de dados pessoais sensíveis.

Importante ressaltar que nesses projetos de lei verificam-se uma gradação crescente quanto à proteção de dados pessoais na área da saúde. Enquanto no Projeto de Lei nº 4.060/2012 apenas os dados genéticos são considerados sensíveis, não havendo menção aos dados de saúde em geral, os demais projetos de lei incluem os dados de saúde entre os dados sensíveis.

No caso do Projeto de Lei nº 330/2013, o art. 5º estabelece requisitos para a coleta, o armazenamento, o processamento, a transmissão, a utilização, o fornecimento ou a divulgação de dados sensíveis.

Entre esses requisitos encontra-se o expresso, específico e inequívoco consentimento do titular do dado, bem como a existência de relevante interesse público, o qual estaria caracterizado para fins de medicina preventiva, de diagnóstico ou tratamento médico, e gestão de serviços para a saúde.

O referido dispositivo ainda determina que o tratamento desses dados sensíveis fundado em relevante interesse público somente poderá ocorrer por órgãos da administração pública direta, pessoas jurídicas de direito público ou pessoas jurídicas de direito privado no exercício da medicina ou proteção à saúde.

Por fim, o Projeto de Lei nº 5.276/2016 é ainda mais restritivo quanto à definição de dados sensíveis, incluindo nesse rol não apenas os dados de saúde, como também os dados

481 Disponível em: http://www.bndes.gov.br/wps/wcm/connect/site/e614e9a3-053b-42d4-853a-6b4aa406e31f/produto-3-analise-de-oferta-e-demanda-relatorio-horizontal-ambiente regulatorio.pdf?MOD=AJPERES&CVID=lWrmVIj&CVID=lWrmVIj&CVID=lWrmVIj, páginas 33 a 52. Acesso em 16.11.2017.

482 Projeto de Lei apresentado em 13.06.2012 pelo Deputado Milton Monti do PR/SP.

483 Projeto de Lei do Senado nº 330 apresentado em 13.08.2013 pelo Senador Antonio Carlos Valadares do PSB/SE.

484 Projeto de Lei nº 5.276 apresentado em 13.05.2016 pelo Poder Executivo e apensado ao PL nº 4060/2012.

biométricos. Ele também prevê a necessidade de consentimento para tratamento dos dados sensíveis e que o titular do dado tem direito à anonimização, ao bloqueio ou à eliminação de dados desnecessários ou excessivos.

Dito isso, diante da inexistência de uma lei específica de proteção de dados pessoais, são aplicáveis normas esparsas, em especial a Constituição Federal, o Marco Civil da Internet e o Código de Defesa do Consumidor, conforme detalhadamente explicado no Produto 3.

Outro aspecto relevante na análise desse tema, refere-se à cibersegurança. Considerando que os dispositivos médicos, principalmente quando conectados à *internet*, estão sujeitos à ataques, é imprescindível que sejam criadas estratégias para mitigação desses riscos.

Conforme já explicado no item referente à regulação da ANVISA, a agência, no Seminário Internacional de Dispositivos Médicos 2017[485], informou que será incorporado à agenda regulatória 2018/2019, o Guia sobre cibersegurança do U.S Food & Drug Administration – FDA[486]. De acordo a agência americana, deve ocorrer o adequado balanceamento entre a proteção dos pacientes e a promoção do desenvolvimento de inovações tecnológicas.

Assim, entre as principais diretrizes do FDA para mitigação das ameaças à cibersegurança, incluem-se a necessidade de os fabricantes de dispositivos médicos e os estabelecimentos de saúde adotarem medidas de salvaguarda. Nesse sentido, os fabricantes são responsáveis por se manterem vigilantes acerca da identificação dos riscos e perigos associados aos seus dispositivos médicos, incluindo os riscos relacionados à segurança cibernética. Os hospitais e instalações de saúde, por sua vez, são responsáveis por avaliar a segurança da sua rede e proteger seus sistemas hospitalares[487].

Feita essa breve introdução, segue-se à análise dos aspectos mais relevantes acerca da proteção de dados pessoais e privacidade na área da saúde que podem impactar IoT.

485 Sobre o Seminário Internacional 2017:

http://portal.anvisa.gov.br/documents/33912/264673/Software+as+a+Medical+Device.pdf/df5e4fa8-4d45-4f7d-ba67-bfd49c1f3bcd. Último acesso em 16.11.2017.

486 Sobre a política de cibersegurança do FDA:

https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm. Último acesso em 16.11.2017.

487 "FDA recommendations for mitigating and managing cybersecurity threats include:

- Medical device manufacturers and health care facilities should take steps to ensure appropriate safeguards. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

- Hospitals and health care facilities should evaluate their network security and protect their hospital systems.

b. Coleta de dados pessoais

No caso das aplicações que envolverão coleta de dados, o primeiro aspecto relevante refere-se à necessidade de obtenção de consentimento válido para essa coleta.

Quando um indivíduo anui com a realização de um serviço na rede pública ou privada de saúde que pressupõe a utilização de informações pessoais, a contratação desse serviço implicará no consentimento para coleta e utilização desses dados para a finalidade específica do serviço contratado. Tais dados, por sua vez, estarão resguardados pelo sigilo médico.

A questão sensível se coloca quando esses dados puderem ser utilizados para outras finalidades diversas da finalidade de tratamento. Nessa hipótese, o consentimento expresso do usuário será fundamental, bem como a prestação de informações sobre a finalidade para a qual o dado será utilizado.

Nesse sentido, quando a aplicação for operacionalizada por meio de dispositivos que possuam interface com o paciente, inclusive por meio de *smartphones*, como é o caso da aplicação desenvolvida para monitoramento de condições dos pacientes com diabetes, é relevante que haja uma política de privacidade com previsão de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, nos termos do art. 7º, inciso IX, da Lei nº 12.965, de 23 de abril de 2014[488] ("Marco Civil da Internet").

Ainda, assim como sugerido no capítulo dedicado a Cidades Inteligentes, é importante que a coleta de dados seja planejada a partir do conceito de "privacidade por desenho" (*privacy by design*)[489]. O que significa dizer que o próprio desenho do produto ou serviço que fará a coleta deverá considerar desde o início de sua concepção a dimensão de proteção à privacidade.

Nos casos em que as soluções de IoT tenham funcionamento restrito às unidades de saúde e devam ser operadas por um profissional de saúde, como é o caso da aplicação descrita para o diagnóstico descentralizado, também é importante que o paciente possa anuir com a política de coleta de dados relativa a essa aplicação.

Além disso, cumpre ressaltar que, dada a sensibilidade dos dados pessoais na área da saúde, a sua confidencialidade deve ser resguardada. Nesse sentido, as normas do

488 "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;"

489 *Privacy by design* é um conceito que designa uma abordagem para a elaboração de projetos, produtos e serviços que promova um cuidado com a privacidade e a proteção de dados pessoais dos usuários desde o momento inicial de elaboração. Para mais informações: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

próprio sistema de saúde estabelecem o dever de confidencialidade das informações pessoais dos usuários por meio da Portaria nº 1.820 de 2009 do Ministério da Saúde. Esta norma dispõe sobre os direitos e deveres dos usuários de saúde e preconiza que, nas consultas, procedimentos diagnósticos, preventivos, cirúrgicos, terapêuticos e internações, deve ser resguardada a confidencialidade de toda e qualquer informação pessoal[490].

Assim, embora não haja uma disciplina legal para a coleta e uso de dados pessoais, a normatização do Ministério da Saúde já é um claro indicativo quanto à necessidade de manutenção de seu sigilo e a necessidade de formalizar o consentimento do usuário dos serviços de saúde quanto a sua coleta.

c. Processamento de dados pessoais

Com relação ao processamento de dados pessoais, como já foi abordado no mesmo tópico relativo ao ambiente "Cidades Inteligentes", um dos problemas emergentes é o uso de dados para finalidade diversa da consentida pelo indivíduo.

Conforme explicado acima, o consentimento expresso do usuário é imprescindível para a coleta de dados pessoais para finalidades diversas da realização do serviço de saúde contratado.

Além disso, é necessário que o uso do dado respeite a finalidade informada ao cidadão na ocasião da obtenção do consentimento. Caso os dados sejam utilizados para outra finalidade que não aquela informada, entende-se que seria necessário obter novo consentimento ou a anonimização, agregação e utilização de técnicas como privacidade diferencial, sempre de forma tecnicamente segura e à prova de desanonimização.

No ambiente da saúde, ainda cumpre destacar que, diante da sensibilidade dos dados para fins de saúde pública, existem informações que devem ser obrigatoriamente prestadas ao poder público por dever legal, sem necessidade de consentimento.

490 "Art. 4º Toda pessoa tem direito ao atendimento humanizado e acolhedor, realizado por profissionais qualificados, em ambiente limpo, confortável e acessível a todos.

Parágrafo único. É direito da pessoa, na rede de serviços de saúde, ter atendimento humanizado, acolhedor, livre de qualquer discriminação, restrição ou negação em virtude de idade, raça, cor, etnia, religião, orientação sexual, identidade de gênero, condições econômicas ou sociais, estado de saúde, de anomalia, patologia ou deficiência, garantindo-lhe: (...)

III - nas consultas, nos procedimentos diagnósticos, preventivos, cirúrgicos, terapêuticos e internações, o seguinte:

(...)

e) a confidencialidade de toda e qualquer informação pessoal;"

É o caso, por exemplo, da notificação compulsória de doenças estabelecida pela Lei nº 6.259, de 1975, para investigação epidemiológica pelas autoridades sanitárias. Essa lei também prevê que a notificação tem caráter sigiloso, devendo ser anonimizado o dado do paciente, com exceção de casos excepcionais de grande risco à comunidade[491]. Nesse caso, por mais que não haja a necessidade de consentimento, a finalidade para utilização do dado deve ser respeitada.

Por fim, aproveita-se para destacar que, também no ambiente da saúde, o uso de dados pelo Poder Público deve respeitar os princípios da legalidade e do interesse público. O que significa dizer que as finalidades para as quais o Estado utiliza dados de seus cidadãos devem possuir previsão legal e constituir finalidade que atenda ao interesse público.

d. Armazenamento de dados pessoais

Com relação ao armazenamento, é comum a preocupação com a segurança tanto das informações processadas nos dispositivos tecnológicos, quanto dos dados coletados e armazenados na nuvem, ficando evidente a necessidade de adoção de medidas de privacidade e de segurança da informação no armazenamento de dados pessoais.

Diante disso, para garantir maior segurança ao armazenamento de dados é recomendável a utilização de ferramentas como agregação e anonimização das informações coletadas por dispositivos IoT.

Ainda quanto a esse tema, importante destacar que, neste ano, o Ministério da Saúde, atendendo recomendação do Tribunal de Contas da União[492], reforçou sua política de proteção de dados e segurança da informação por meio da publicação da Portaria nº 271, de 27 de janeiro de 2017[493].

491 "Art. 8º É dever de todo cidadão comunicar à autoridade sanitária local a ocorrência de fato, comprovado ou presumível, de caso de doença transmissível, sendo obrigatória a médicos e outros profissionais de saúde no exercício da profissão, bem como aos responsáveis por organizações e estabelecimentos públicos e particulares de saúde e ensino a notificação de casos suspeitos ou confirmados das doenças relacionadas em conformidade com o artigo 7º. (...)

Art. 10. A notificação compulsória de casos de doenças tem caráter sigiloso, obrigando nesse sentido as autoridades sanitárias que a tenham recebido.

Parágrafo único. A identificação do paciente de doenças referidas neste artigo, fora do âmbito médico sanitário, somente poderá efetivar-se, em caráter excepcional, em caso de grande risco à comunidade a juízo da autoridade sanitária e com conhecimento prévio do paciente ou do seu responsável."

492 A publicação da portaria considerou o Acórdão nº 1.233 - TCU/2012, que trata da adoção dos normativos de Segurança da Informação e Comunicações (SIC) e o Acórdão nº 3.051-TCU/2014, que prevê a estratégia geral de Segurança da Informação.

493 A Portaria estabelece as referências legais e normativas em segurança da informação do Ministério da Saúde:

O objetivo dessa política é promover maior segurança no processamento, armazenamento e comunicação de dados nos sistemas informatizados do Sistema Único de Saúde (SUS) e na rede do Ministério da Saúde. Assim, essa política de proteção de dados poderá impactar a segurança da informação de aplicações de IoT na rede pública de saúde.

Entre os princípios que devem reger a política encontra-se o princípio da privacidade, que determina que informações que firam o respeito à intimidade, à integridade e à honra dos cidadãos não podem ser divulgadas.

A norma também estabelece uma série de diretrizes para proteção de dados e informações com destaque para responsabilidades e deveres dos agentes públicos[494].Entre essas diretrizes encontra-se o regramento da propriedade e do tratamento da informação que, entre outras regras, estabelece o seguinte:

> *(i)* toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo Ministério da Saúde é de sua responsabilidade e são classificadas

"Art. 6º As ações de Segurança da Informação e Comunicações do Ministério da Saúde deverão observar os seguintes requisitos legais e normativos:

I - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

II - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III - Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

IV - Art. 1.016 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), que dispõe que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

V - Portaria nº 589, de 20 de maio de 2015, que Institui a Política Nacional de Informação e Informática em Saúde (PNIIS);

VI - Instrução Normativa nº 01, de 13 de junho de 2008, do Conselho de Defesa Nacional e suas respectivas Normas Complementares publicadas no Diário Oficial da União (DOU) pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

VII - Portaria nº 2072, de 31 de agosto de 2011, que redefine o Comitê de Informação e Informática em Saúde (CIINFO) no âmbito do Ministério da Saúde;

VIII - Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações;

IX - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

X - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

XI - Norma NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação; e

XII - ISO 31.000:2009 - Diretrizes para a implementação da gestão de riscos".

494 Art. 10 Todos os agentes públicos do MS são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede (Login), crachá, carimbo, endereço de correio eletrônico ou assinatura digital.

e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo; e

(ii) as informações produzidas, armazenadas e transportadas em meios eletrônicos, utilizará criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações.

A Portaria ainda avançou ao estabelecer mecanismos de controle da informação por meio de monitoramento e auditoria[495], bem como regras acerca da computação em nuvem que garantam disponibilidade, integridade, confidencialidade e autenticidade para as informações hospedadas em nuvem[496].

e. Compartilhamento dos dados pessoais

O compartilhamento de dados coletados é tema de extrema relevância que encontra alguns desafios, como a necessidade de proteção à privacidade, a garantia de interoperabilidade e o adequado intercâmbio de informações entre sistemas de informação de instituições de saúde.

495 "Art. 7º As ações relacionadas com a Segurança da Informação e Comunicações no MS são norteadas pelos seguintes princípios: (...)

VI - Auditoria e Conformidade:

a) o uso dos recursos de TIC disponibilizados pelo MS é passível de monitoramento e auditoria, conforme o previsto no item 9.1.4 do acórdão do Tribunal de Contas da União nº 461 de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos para monitoramento do uso dos sistemas, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso; e

(...)"

496 "Art. 13 - Esta política aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e rege-se pelas seguintes diretrizes:

(...)

XIII - Computação em Nuvem:

a) o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SIC, estabelecidas pelo MS, e às legislações vigentes;

b) o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço; e

c) o armazenamento de informação em nuvem deverá estar respaldado por um contrato entre o MS e o provedor de serviço em nuvem, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem. (...)"

Inúmeras finalidades poderiam ensejar o compartilhamento de dados na área da saúde, como a necessidade de compartilhamento de informações entre unidades de saúde, públicas ou privadas, para a condução do tratamento de um paciente específico, a realização de pesquisas, bem como finalidades comerciais.

Em qualquer caso, em regra, é imprescindível que seja obtido o consentimento livre, expresso e informado dos cidadãos.

Além disso, quando o compartilhamento de dados ocorrer para finalidades diversas do tratamento do próprio solicitante do dado, como para pesquisa ou finalidades comerciais, é necessário que os dados sejam anonimizados de forma definitiva e segura, bem como agregados e sujeitos a técnicas como a privacidade diferencial.

Ainda, sempre que houver acesso por parte de terceiros a esses dados, mesmo que anonimizados, ele deverá se comprometer a protegê-los com elevados padrões de segurança e a não os compartilhar, ou tentar empregar qualquer processo de desanonimização dos dados.

Além disso, no caso do compartilhamento de dados, outra barreira que se verifica é a questão da interoperabilidade e intercâmbio das informações no setor de saúde.

Nas reuniões do Grupo de Trabalho de IoT em Saúde conduzidas pelo BNDES e pelo MCTIC com representantes dos setores público e privado, esse tema foi levantado como uma barreira ao adequado desenvolvimento de IoT.

O incentivo à interoperabilidade no setor pode ocorrer por meio da normatização de critérios pelo poder público, ou pela autorregulação dos agentes do setor.

Atualmente, a Portaria do Ministério da Saúde nº 2.073, de 31 de agosto de 2011, regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar.

Entre os objetivos dessa política encontra-se a promoção da utilização de uma arquitetura de informação em saúde que contemple a representação de conceitos que permitam o compartilhamento de informações em saúde e a cooperação de todos os profissionais, estabelecimentos de saúde e demais envolvidos na atenção à saúde prestada ao usuário do SUS, em meio seguro e com respeito ao direito à privacidade.

Entendida a relevância da interoperabilidade dos dados na área da saúde, é importante que essas normas e práticas estejam em constante aperfeiçoamento e que a privacidade, por meio do respeito ao consentimento e à finalidade para a qual autorizou-se o compartilhamento do dado, seja sempre garantida.

f. Acesso aos dados coletados

Quanto ao acesso aos dados, estão sujeitos à Lei nº 12.527, de 18 de novembro de 2011, ("Lei de Acesso à Informação"), todos os órgãos públicos integrantes da administração direta, bem como as autarquias, fundações, empresas públicas e sociedades de economia mista de todos níveis da federação.

Nesse sentido, o acesso à informação dos órgãos e entidades públicos de saúde seria regido por essa lei e pelo Decreto nº 7.724, de 16 de maio de 2012, que a regulamenta. Além disso, a Portaria do Ministério da Saúde nº 1.583, de 19 de julho 2012, dispõe sobre a execução da Lei de Acesso à Informação no âmbito desse Ministério e de suas entidades vinculadas.

Como já explicado anteriormente, a referida Lei dispõe que o tratamento de informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

Tais informações terão seu acesso restrito à pessoa a que elas se referirem e aos agentes públicos legalmente autorizados, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção.

O acesso a esse tipo de informação por terceiros, por sua vez, só poderá ocorrer mediante previsão legal ou consentimento expresso do titular do dado.

Contudo, tal consentimento poderá ser excetuado quando a informação se destinar *(i)* à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização exclusivamente para o tratamento médico; *(ii)* à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, vedada a identificação da pessoa a que a informação se referir; *(iii)* ao cumprimento de decisão judicial; *(iv)* à defesa de direitos humanos de terceiros; ou *(v)* à proteção do interesse público geral e preponderante.

Ainda, o acesso à informação pessoal por terceiros estará condicionado à assinatura de termo de responsabilidade, que disporá sobre a finalidade e a destinação que fundamentaram a autorização, bem como sobre as obrigações a que se submeterá o requerente.

A Portaria também prevê que a utilização de informação pessoal por terceiros estará vinculada à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa.

Cumpre ressaltar que essa norma também se aplica às entidades privadas sem fins lucrativos que recebam recursos públicos.

Quanto às demais instituições privadas, entende-se que os padrões previstos na Lei de Acesso à Informação também deveriam nortear o acesso às informações pessoais no âmbito das instituições privadas de saúde. Isto é, o acesso a dados pessoais de saúde só poderia ocorrer pelo próprio indivíduo ou por agentes públicos legalmente autorizados,

sendo permitido o acesso aos dados por terceiros apenas quando expressamente autorizado pelo seu titular.

3.3 Rural

O ambiente rural possui um conjunto de características e questões que tornam sua análise particular em relação aos outros ambientes priorizados.

Dentre as preocupações regulatórias analisadas, três tópicos se destacaram: a) a disponibilidade de infraestrutura de conectividade, e as questões regulatórias correlatas; b) regulamentação para a utilização de *drones* em aplicações IoT rurais; e c) propriedade e proteção de dados no ambiente rural.

As questões envolvendo telecomunicações foram endereçadas no item 2.1 deste documento, enquanto as demais serão apresentadas a seguir.

3.3.1 Uso de Remotely Piloted Aircraft Systems ("RPAS") em aplicações de IoT

Algumas aplicações de IoT no campo podem se beneficiar da utilização de *Remotely Piloted Aircraft Systems (RPAS),* também conhecidos coloquialmente como *drones*.

a) *Quadro regulatório*

Essas aeronaves, em sua utilização geral, são **reguladas por três entes distintos no país**: a) **Agência Nacional de Telecomunicações (ANATEL), b) Agência Nacional de Aviação Civil (ANAC) e c) Departamento de Controle do Espaço Aéreo (DECEA)**. Para a utilização segura e dentro da lei dos *drones* é, portanto, necessário seguir os regulamentos desses três órgãos.

O primeiro elemento regulatório a se observar é o relacionado à **ANATEL**. A competência da ANATEL em relação aos *drones* está relacionada a necessidade de homologação dos módulos de conectividade presentes nessas aeronaves: para sua operação, os *drones* possuem transmissores de radiofrequência nas suas estações de pilotagem remota, bem como, em alguns casos, na própria aeronave para a transmissão de imagens.[497] Essa homologação visa evitar que módulos de conectividades de *drones* irregulares gerem interferências em outros serviços de telecomunicações.

A operação deve observar também o regulamento da **ANAC**. A ANAC, dentro de sua competência para regular e fiscalizar as atividades da aviação civil, publicou o

[497] Disponível em: http://www.anatel.gov.br/institucional/ultimas-noticiass/2-uncategorised/1485-drones-devem-ser-homologados-para-evitar-interferencias

Regulamento Brasileiro da Aviação Civil Especial nº 94 ("RBAC-E nº 94"),[498] estabelecendo regras para as operações civis de RPAS. Dentre as disposições do Regulamento, a utilização segura de *drones* com peso máximo de decolagem acima de 250 gramas requer, dentre outros requisitos: (a) a realização da operação com distância de pelo menos 30 metros horizontais em relação a edificações,[499] e a pessoas não envolvidas e não anuentes com a operação;[500]-[501] b) a contratação de seguro com cobertura de danos a terceiros;[502] c) a não utilização de *drones* autônomos;[503] e d) que cada piloto de *drone* opere apenas um equipamento por vez.

Cumpridos os requisitos regulatórios da ANATEL e da ANAC, o operador do *drone* deverá, então, cumprir com os requisitos do **DECEA**[504] para poder utilizar o espaço aéreo.

A regulação do DECEA é de suma importância para garantir a utilização segura do espaço aéreo, possibilitando a coordenação da sua utilização entre os mais diversos usuários (aeronaves comerciais, militares, ultraleves, helicópteros, drones, entre outros).[505] Com vistas a estabelecer as bases dessa utilização pelos operadores de *drones*, o DECEA publicou a Instrução do Comando da Aeronáutica 100-40 ("ICA 100-40").[506]

Adicionalmente, é importante que o desenvolvimento de aplicações de IoT no ambiente rural observe, ainda, disposições legais ou regulamentares relacionadas especificamente às atividades que estão sendo desempenhadas com a utilização de *drones*. Como

498 Disponível em: http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00/@@display-file/arquivo_norma/RBACE94EMD00.pdf

499 Essa distância pode ser flexibilizada com a anuência do proprietário do edifício ou instalação.

500 Exceção feita para os casos em que haja "uma barreira mecânica suficientemente forte para isolar e proteger as pessoas não envolvidas e não anuentes na eventualidade de um acidente".

501 Essa disposição não se aplica ao Poder Público.

502 Exceção feita aos drones pertencentes a entidades controladas pelo Estado.

503 A vedação a operações autônomas não implica uma vedação de voos totalmente automatizados, que podem ser feitos desde que haja a possibilidade de intervenção, a qualquer momento, do piloto remoto.

504 O DECEA é o órgão do Comando da Aeronáutica com competência para "planejar, gerenciar e controlar as atividades relacionadas ao controle do espaço aéreo, à proteção ao voo, ao serviço de busca e salvamento e às telecomunicações do Comando da Aeronáutica". Disponível em: http://www.decea.gov.br/drone/

505 O DECEA, em seu site institucional, possui um exemplo simples da importância dessa coordenação com a utilização de drones: "O operador de drone quer realizar um voo em área desabitada até 400ft AGL (aproximadamente 120 metros de altura). Bem, pela ICA 100-4, a qual trata das operações de helicópteros, é preconizado que a altura mínima para voos de helicópteros em áreas desabitadas é de 200ft (aproximadamente 60 metros). Só por essa questão podemos perceber que o voo do drone sem coordenação poderá causar conflito no caso de um tráfego de helicóptero convergente com a área de voo, colocando em risco a operação do helicóptero". Disponível em: http://www.decea.gov.br/drone/

506 Disponível em: http://publicacoes.decea.gov.br/?i=publicacao&id=4510

exemplo, temos as atividades de aerolevantamento[507] e de aplicação de defensivos agrícolas.[508]

Por fim, é importante indicar que além desses regulamentos específicos, a operação de *drones* está sujeita também à aplicação da legislação no que tange às **responsabilizações nas esferas civil, administrativa e penal**.[509]

a) *Discussões no ambiente rural*

Durante as entrevistas e *workshops* realizados, muitos participantes indicaram que a regulamentação atual para a utilização de *drones* dificultaria o desenvolvimento de aplicações de IoT, em especial em decorrência dos custos para se cumpri-la. Segundo esses participantes, **a regulamentação estaria focada na utilização urbana de *drones*, o que limita as oportunidades e possibilidades de escala em seu uso no ambiente rural**, ambiente esse que possuiria condições muito diferentes, exigindo menos requisitos técnicos. Entre os exemplos indicados, estariam a **impossibilidade de operações autônomas, a redundância de sistemas e a necessidade de observadores na utilização de drones em alguns cenários**.

No que tange a nova regulamentação estabelecida pela ANAC em seu RBAC-E nº 94, o regulamento trouxe segurança jurídica para o setor que opera *drones*, definindo requisitos claros para a utilização desses dispositivos em diferentes categorias. Além disso, o diálogo e maior integração entre os sistemas dos três entes reguladores têm diminuído a complexidade para o cumprimento das obrigações relacionadas a operação de drones.

Uma das preocupações apontadas, relacionada à operação autônoma, foi, inclusive, objeto de clarificação pela ANAC, visto que a proibição das operações autônomas não implica em uma vedação de voos totalmente automatizados, que podem ser feitos desde que haja a possibilidade de intervenção, a qualquer momento, do piloto remoto.[510] Exige-se, portanto, apenas um monitoramento da atividade do equipamento.

É certo, entretanto, que por se tratarem de regulamentos sujeitos a mudança no estado da arte da tecnologia – caso haja melhorias na tecnologia de modo a se ter garantias

[507] Caso sejam usados para atividades definidas como de aerolevantamento, é necessário também observar as normas do Ministério da Defesa: http://www.defesa.gov.br/index.php/cartografia-e-aerolevantamento-claten/legislacao-relacionada

[508] Lei 7.802, em 11 de julho de 1989, regulamentada pelo Decreto 4.074, de 04 de janeiro de 2002.

[509] Como exemplo podemos mencionar: Código Penal – art. 132 e 261; Código Brasileiro de Aeronáutica – art. 289 e 291; Código Civil – art. 186; Lei das Contravenções Penais – art. 33 e 35.

[510] Resposta a contribuição nº 19 à audiência pública sobre o regulamento: "O voo autônomo é definido como aquele em que o piloto remoto não tem a capacidade de intervir na operação da aeronave durante o voo. Um voo realizado de forma totalmente automatizado com uma rota pré-programada não está proibido desde que exista a capacidade de intervenção do piloto remoto (que deve supervisionar todo o voo) em caso de necessidade.". Disponível em: http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC_13_2015.pdf. Acesso em: 22.09.2017.

técnicas de que as precauções postas pela regulamentação não mais se justifiquem no ambiente rural –, parece ser viável a defesa de um regime regulatório mais flexível para a operação em ambientes rurais.

Desse modo, com vistas a buscar o desenvolvimento do quadro regulatório relacionado a *drones* no ambiente rural, **seria importante se articular com o setor privado e a Comissão Brasileira de Agricultura de Precisão ("CBAP"), dentro de suas competências, um aprofundamento técnico do estado da arte da tecnologia de drones no ambiente rural, com vistas a identificar possibilidades seguras de flexibilização do atual quadro regulatório aplicável.**

Esse material poderia servir de subsídio para se dialogar com os entes reguladores em busca de propostas de mudanças nos regulamentos em vigor. Nessa linha, vale mencionar que o próprio enquadramento dado pela ANAC no seu regulamento sobre *drones* (regulamento especial) indica a intenção da Agência de amadurecer o quadro regulatório referente a matéria, conforme a experiência e a tecnologia forem se desenvolvendo.[511]

3.3.2 Proteção e propriedade de dados e bases de dados

Outro ponto destacado na análise do consórcio e nas informações obtidas do mercado é a **preocupação acerca da proteção e propriedade dos dados e bases de dados gerados através do uso de tecnologias IoT no ambiente rural, bem como de possíveis dados pessoais** que estariam envolvidos em soluções de IoT. Esse debate traz contornos complexos, e há divergências profundas entre os dois grandes grupos envolvidos – agricultores, de um lado, e empresas de insumos/tecnologias agrícolas, de outro.

De início é importante apresentar as divergências quanto ao tema.

Buscando garantir uma maior proteção para os agricultores e pecuaristas na nova economia de dados, a Confederação da Agricultura e Pecuária - CNA Brasil tem apresentado preocupações com a privacidade e segurança de dados rurais (sem restringir a dados pessoais). O foco da referida entidade está nos dados estratégicos no campo, incluindo "dados básicos", como os dados de sensores de uma "colhedora" (isto é, a possibilidade de ter em tempo real dados sobre a colheita e safra).

[511] Nessa linha, veja a própria resposta dada pela ANAC acerca da contribuição nº 229 recebida na audiência pública sobre o novo regulamento: "(...) O Regulamento ora proposto foi pensado para ser um regulamento dinâmico, que seja constantemente emendado conforme surgirem as inovações tecnológicas, com o fim de se manter sempre atual, o que não impede um usuário específico de solicitar à ANAC algo que a regra ainda não permita, sob a modalidade de isenção de cumprimento de regra segundo o RBAC nº 11." Disponível em: http://www.anac.gov.br/participacao-social/audiencias-e-consultas-publicas/audiencias/2015/aud13/RAC_13_2015.pdf. Acesso em: 22.09.2017.

Dentre as preocupações apresentadas pela CNA, está a possibilidade de os dados rurais serem potencialmente utilizados para influenciar mercados de *commodities*,[512] e de que haja um compartilhamento inadvertido desses dados, especialmente diante da realidade do mercado hoje.[513]

Com vistas a lidar com esse cenário, a CNA tem defendido uma maior proteção aos dados rurais, apresentando como exemplo o **documento de autorregulação negociado pela *American Farm Bureau Federation* (*AFBF*)**, denominado "*Privacy and Security Principles for Farm Data*",[514] que foi assinado por 39 empresas do setor de prestação de serviços tecnológicos para a agricultura de precisão nos Estados Unidos.

De modo geral, os princípios propostos nessa autorregulação americana estabelecem um regime de proteção de dados rurais com algumas disposições semelhanças às regras do modelo europeu de proteção de dados pessoais. Abaixo apresentamos os principais pontos definidos nesse modelo de autorregulação:

a) A propriedade dos dados gerados em operações no campo é do agricultor. Entretanto, é responsabilidade do agricultor concordar com a utilização e compartilhamento desses dados com outros *stakeholders* que possuam um interesse econômico, como arrendatários, proprietário da terra, cooperativa, dono do *hardware* do sistema de agricultura de precisão e/ou provedor de tecnologia agrícola;

b) A coleta, acesso e uso de dados rurais devem apenas ser feitas após a obtenção de consentimento afirmativo e explícito do agricultor;

c) O provedor de tecnologia agrícola deve explicar os efeitos e habilidades do agricultor de realizar o *opt-in*, *opt-out* ou de desativar a disponibilidade dos serviços e funcionalidades oferecidos;

d) Os agricultores devem ser notificados de que os seus dados estão sendo coletados e como os dados rurais serão disponibilizados e usados. Essa notificação deve ser provida em um local de fácil acesso e em formato acessível;

e) Os provedores de tecnologia agrícola devem informar aos agricultores acerca das finalidades para as quais eles estão coletando e usando os dados rurais. Dentre as

[512] Audiência Pública realizada na Comissão Especial sobre proteção de dados pessoais na Câmara dos Deputados no dia 11 de julho de 2017. Os slides da apresentação do CNA estão disponíveis no seguinte link: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-publicas/sut.apres.audinciapblicaAP.11jul2017.pdf

[513] Idem.

[514] Privacy and Security Principles for Farm Data. Disponível em: https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data. Acesso em: 04.09.2017.

informações necessárias, deve haver a indicação de um ponto de contato para tirar dúvidas e receber reclamações, deve-se indicar os tipos de terceiros para os quais serão disponibilizados dados e as alternativas que o provedor fornece ao agricultor para limitar os seus usos e disponibilização. O provedor de tecnologia agrícola não irá mudar os termos do contrato com o cliente sem o seu consentimento;

f) Dentro do contexto do contrato e da política de retenção de dados do provedor, os agricultores devem ter a capacidade de realizar a portabilidade dos seus dados rurais para armazená-los ou usá-los em outros sistemas. Essa regra não se aplica para os dados que já tenham sido anonimizados ou agregados;

g) O provedor de tecnologia agrícola não pode vender e/ou disponibilizar dados rurais não-agregados para um terceiro sem antes estabelecer com ele um acordo vinculante no qual ele garanta que seguirá os mesmos termos e condições que o provedor tem com o agricultor. Os agricultores devem ainda ser notificados de que referida venda acontecerá de modo a poder realizarem o *opt-out* ou ter seus dados excluídos antes da venda. O provedor de tecnologia agrícola não compartilhará ou disponibilizará os dados rurais originais com um terceiro de uma maneira que seja inconsistente com o contrato com o agricultor;

h) Os provedores de tecnologia agrícola devem promover a remoção, destruição segura e a devolução dos dados rurais originais da conta do agricultor, a pedido do agricultor ou após um período de tempo predefinido;

i) Os agricultores devem ter a possibilidade de descontinuar o serviço ou interromper a coleta de dados a qualquer momento, sujeito as obrigações em curso;

j) O provedor de tecnologia agrícola não deve usar os dados rurais para atividades ilícitas ou anticompetitivas. Como exemplo, é proibido ao provedor de tecnologia agrícola utilizar os dados rurais com a finalidade de especular no mercado de commodities;

k) Os dados rurais devem ser protegidos com padrões de segurança razoáveis, para evitar riscos de perda, modificação, destruição ou acesso não autorizado dos dados. Deve haver ainda uma política clara para notificação e resposta em casos de vazamento de dados.

Na mesma linha princípios da AFBF, a europeia **COPA-COGECA[515] publicou documento no qual recomenda princípios para o tratamento de dados rurais**, possuindo grande interface e similitude com os princípios estabelecidos pela AFBF.[516]

Por sua vez, a Associação Brasileira de Sementes e Mudas ("ABRASEM") tem defendido, no âmbito dos debates sobre proteção de dados pessoais no Congresso, uma posição mais voltada à liberdade de uso dos dados rurais.

Durante a audiência pública do dia 12 de julho de 2017 na Comissão Especial sobre Proteção de Dados Pessoais na Câmara dos Deputados, a **ABRASEM indicou que os PLs em tramitação possuem disposições que colocam em risco à inovação do setor de agricultura de precisão**, acarretando em uma perda da competitividade nacional. Dentre os riscos, foram indicados: a) a falta de clareza sobre alguns conceitos quando observada a realidade da agricultura; b) as restrições existentes nos PLs à transferência internacional de dados; c) dificuldades de se inovar no ambiente da agricultura de precisão; d) e tratamento igualitário para setores que possuem distinções, como o da agricultura de precisão.

Na contribuição submetida pela ABRASEM ao texto do Projeto de Lei nº 5.276/2016,[517] é possível identificar, por exemplo, a preocupação do setor com a aplicação do conceito de dado pessoal do PL ao tratamento de dados georreferenciados, visto que o georreferenciamento é um dos princípios fundamentais da agricultura de precisão.[518]

Além desses dois grandes grupos, é relevante, ainda, indicar o debate acadêmico desenvolvido pelo Grupo de Pesquisa em Ensino e Inovação ("GEPI") da Escola de Direito da Fundação Getúlio Vargas de São Paulo. Em pesquisa recentemente publicada sobre agricultura de precisão/digital,[519] o GEPI identificou que uma parcela dos dados tratados no ambiente rural estaria relacionada com dados pessoais. Nessa esteira, torna-

[515] Committee of Professional Agricultural Organisations (COPA) e General Committee for Agricultural Cooperation in the European Union (COGECA)

[516] COPA; COGECA. **Main Principles Underpinning the Collection, Use and Exchange of Agricultural Data**, no QJ (16)2689:6 – DA/FG/mvs. Brussels: Farmers European Agri - Cooperatives, [S.d.]. Disponível em: https://ec.europa.eu/futurium/en/system/files/ged/main_principles_underpinning_the_collection_use_and_exchange_of_agricultural_data_.pdf.

[517] Contribuição enviada pela ABRASEM à Comissão Especial sobre Tratamento e Proteção de Dados Pessoais (PL 4060/12). Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/ABRASEM.pdf.

[518] É relevante identificar que atualmente a definição de dados pessoais trazida pelo Decreto Regulamentador do Marco Civil da Internet já inclui dados que identifiquem ou que possam identificar uma pessoa natural (art. 14, I do Decreto nº 8.771/16).

[519] SILVA, A. P. *et al.* **Um Novo Mundo de Dados - Relatório Final**. Grupo de Ensino em Pesquisa e Inovação (GEPI-FGV). 2017. Disponível em: http://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd_relatorio_fgv.pdf. Acesso em: 06.09.2017.

se possível a identificação ou possibilidade de se identificar a pessoa natural do produtor através do tratamento desses dados.

Desse modo, "achar que não existem dados pessoais na área de agricultura" seria, na visão do Grupo, um contrassenso. Entretanto, conforme a análise, embora os dados pessoais estejam presentes no ambiente rural, eles não seriam "tão significativos" ou importantes dentro de sua lógica, em especial quando comparado com a dinâmica e a lógica de outros ambientes, tais como Saúde e Cidades.

Parece-nos que há, nesse tema, dois debates distintos, e que vão exigir abordagens complementares: I) aplicação do quadro legal de proteção de dados pessoais, e II) propriedade e proteção de dados não-pessoais, ou seja, aqueles que digam respeito à atividade econômica rural.

No que tange a **aplicação do quadro legal de proteção de dados pessoais** (atual ou futuro) a dados envolvidos em aplicações de IoT, afigura-nos que essa aplicação se daria apenas para situações específicas e que não representariam barreiras ao desenvolvimento de IoT no ambiente rural, visto que nesses casos bastar-se-ia cumprir com os requisitos legais para tratamento de dados pessoais. Para a maior parte das aplicações rurais de IoT, entretanto, não se estará diante de dados pessoais (relacionados à pessoa natural identificada ou identificável), mas sim diante de **dados não-pessoais da atividade econômica do agronegócio**, e que possuem pontos próprios para serem endereçados, **como a questão da propriedade e da sua proteção.**

Esse último ponto é o foco do segundo debate, **o qual ainda é conflituoso no Brasil e precisará de um denso aprofundamento com os principais atores interessados, de modo a identificar as abordagens possíveis no contexto brasileiro, para, assim, endereçar as preocupações de todos as partes interessadas**. Nessa linha, uma das alternativas para avançar esse debate pode ser centralizá-lo também na CBAP, que conta com ampla participação dos setores-chave no debate de IoT no ambiente rural.

Os modelos apresentados, tanto em relação aos princípios da AFBF quanto aos da COPA-COGECA, buscam tratar exatamente do aspecto de como regular as questões envolvendo a propriedade e a proteção dos dados não-pessoais no ambiente rural. Em nossa visão, esses modelos podem servir como exemplos no debate a ser desenvolvido, de forma a se buscar um regime que promova tanto a inovação no campo quanto garanta a proteção de cada produtor individual em relação aos dados não-pessoais gerados em suas atividades.

4 Sumário de conclusões do Capítulo Regulatório

Essa seção, busca apresentar um sumário com as principais conclusões e recomendações contidas nesse capítulo regulatório, divididas em cada um dos tópicos abordados até aqui.

4.1 Horizontais Regulatórias

4.1.1 Horizontal de Telecomunicações

Como identificado no *Roadmap* Tecnológico, um dos requisitos essenciais de aplicações Internet das Coisas é a existência de conectividade. Como se sabe, o conceito de conectividade está diretamente relacionado à infraestrutura de suporte à prestação de serviço de telecomunicações, o que traz para o debate de Internet das Coisas a necessidade de uma análise aprofundada da regulamentação setorial para identificar potenciais obstáculos ao desenvolvimento de Internet das Coisas no Brasil.

Nessa linha, a partir dos temas de regulação de telecomunicações mapeados no Relatório da Fase I – Horizontal Regulatório, foi possível propor medidas para o endereçamento das principais questões relevantes para o desenvolvimento de Internet das Coisas no Brasil: (i) conceitos inerentes ao desenvolvimento da Internet das Coisas; (ii) infraestrutura necessária; (iii) debates correlatos à outorga; (iv) uso racional do espectro de radiofrequência; (v) obrigações de qualidade; (vi) certificação e homologação de dispositivos; e (vii) taxas do FISTEL.

Conceitos inerentes ao desenvolvimento da IoT:

- Avaliar a conveniência de alterar a redação do Decreto nº 8.234/2014 para introduzir conceito que comporte o racional de "predominância" de automatização e que possa conduzir a Anatel à promoção de uma regulação mais detalhada que impeça distorções.

Infraestrutura de telecomunicações:

- Aprimorar o quadro regulatório de telecomunicações para viabilizar o investimento na ampliação de rede no país.

Aspectos relacionados à outorga para prestação de serviços de telecomunicações:

- Avaliar a possibilidade de editar ato normativo para tratar expressamente do tema de conectividade embarcada, de modo a trazer segurança jurídica aos agentes de mercado interessados no provimento de aplicações de IoT;
- Importância do SLP como regime para prestação de serviços de telecomunicação de escopo mais específico para suporte de aplicações de IoT, o qual não possui barreiras para sua utilização atual;

- Avaliar a necessidade de se submeter o atual regulamento de MVNO à revisão, para adequá-lo ao novo contexto tecnológico e regulatório trazido pelas aplicações de IoT;
- Realizar avaliação detida do real impacto do roaming internacional permanente à disseminação de aplicações IoT no Brasil, com a implementação de uma definição regulatória clara acerca do seu uso ou proibição.

Uso racional do espectro:

- Realizar mapeamento do uso do espectro licenciado no Brasil, fazendo uso da previsão contida no art. 5º, I, da Resolução Anatel nº 671, de 3 de novembro de 2016 (comprovação periódica de uso efetivo de radiofrequências). A medida objetiva avaliar se o uso do espectro no Brasil é racional e se o modelo de comercialização é adequado para o desenvolvimento de IoT.

Certificação e homologação de equipamentos:

- Aprimorar o processo de certificação e homologação de equipamentos com vistas a otimizar o processo e atender o aumento na demanda gerado por IoT;
- Aperfeiçoar os requisitos técnicos previsto na regulamentação para a avaliação da conformidade de equipamentos de radiocomunicação restrita, de modo a evitar a criação ou manutenção de barreiras de entrada a tecnologias específicas.

Obrigações de qualidade:

- Avaliar a possibilidade de flexibilização nos RGQs de SCM e SMP, de modo a possibilitar uma maior liberdade para as operadoras desenvolverem modelos de negócios destinados às aplicações IoT.

Debate sobre a isenção do FISTEL:

- Rever as atuais taxas do FISTEL, diante da importância dessa questão para difundir e democratizar o uso de dispositivos de comunicação M2M.

4.1.2 Horizontal de Privacidade e Proteção de Dados Pessoais

Até o momento, o regime de proteção à privacidade no Brasil apresenta significativas lacunas, relacionadas à ausência de legislação e inexistência de uma instituição que centralize o tratamento da temática. Neste cenário, consideramos imprescindível a promulgação de uma lei geral de proteção de dados pessoais e a criação de instância reguladora sobre a proteção de dados pessoais.

A co-regulação representa modelo regulatório mais apropriado para regulamentar e fiscalizar a privacidade. Todavia, enquanto não aprovada legislação específica para a proteção de dados pessoais e instituída autoridade competente em modelo de co-regulação, práticas transitórias de auto-regulação podem ser estimuladas, visando à proposição de códigos de conduta e regras setoriais pelo setor privado.

Recomenda-se que a autoridade a ser criada seja única e centralizada, possibilitando a participação de atores relevantes, sendo composta por corpo técnico especializado (nos campos tecnológico, jurídico, econômico, mercadológico, entre outros) e dotada de independência financeira e decisória.

Dentre suas atribuições, propomos que a autoridade possa (i) editar normas complementares à legislação federal; (ii) realizar auditoria no tratamento de dados pessoais; (iii) promover ações educacionais; (iv) adotar providências em incidentes de segurança; (v) gerir a transferência de dados pessoais para o exterior; (vi) verificar o cumprimento de normas ou códigos de conduta elaborados em regime de auto-regulação (i.e., *binding corporate rules* na União Europeia); (vii) atuar como *ombudsman*, recebendo e investigando reclamações individuais contra a má-administração de dados pessoais por entidades públicas e privadas; e (viii) impor sanções diversas (como advertência, imposição de multas e suspensão de atividades).

Especificamente em relação às formas de financiamento, apresenta-se três modelos: (i) dotação orçamentária específica, modelo adotado atualmente na União Europeia e nos Estados Unidos; (ii) financiamento por meio de multas aplicadas (modelo da *Agencia Española de Protección de Datos*); ou (iii) registro obrigatório de bancos de dados, em uma adaptação de práticas uruguaias.

4.1.3 Horizontal de Segurança da Informação

Diante do desenvolvimento da Internet das Coisas no Brasil, da expansão de vulnerabilidades em redes e da natureza "sem fronteiras" de incidentes em segurança da informação, a discussão sobre medidas relacionadas à cibersegurança nos âmbitos do Poder Público e da iniciativa privada ganha destaque.

Discutem-se modelos de governança tanto para a cooperação internacional, quanto em relação ao arranjo institucional interno brasileiro. No âmbito local, faz-se necessário, ainda, encontrar alternativas para incentivar a adoção de medidas protetivas à segurança da informação pela iniciativa privada, seja pela adoção de mecanismos voluntários de

certificação de dispositivos ou pelo respeito a critérios mínimos de segurança em infraestruturas críticas.

Um dos pontos em que se prevê a adoção de medidas concretas é a certificação voluntária sobre a segurança de dispositivos ligados à Internet das Coisas. A estruturação de sistema de certificação baseado na auto-avaliação voluntária, sem a imposição de obrigações legais aos aderentes, tem o potencial de criar cultura de transparência na prestação de informações ao usuário e incentivar a adoção de alto padrão de segurança pela iniciativa privada. Para viabilizá-lo, sugerimos a criação de "aliança" por representantes da iniciativa privada, que deverá ser responsável organização estrutural e elaboração de diretrizes públicas. Abaixo, apresentamos os encaminhamentos identificados:

Cooperação internacional

- Aprimorar os mecanismos de cooperação internacional para a prevenção e tratamento de incidentes de segurança da informação, como pela adesão em Acordos de Troca e Proteção Mútua de Informações Classificadas;
- Incentivar a adoção de standards internacionais na temática de segurança da informação pela iniciativa privada.

Arranjo institucional brasileiro

- Estruturar governança baseada em modelo multissetorial, com a criação ou designação de estrutura específica para a coordenação de atividades baseadas em segurança da informação, na forma de conselho permanente, órgão/entidade pública ou agência reguladora independente. A entidade criada ou designada deverá atuar na elaboração de políticas nacionais, criação de mecanismos de resposta a incidentes, dentre outras atribuições;
- Estimular a cooperação e interação entre o Poder Público, sociedade civil, iniciativa privada e academia, com o fim de promover medidas de conscientização e fomento da segurança da informação.

Incentivo à adoção de certificação voluntária de dispositivos

- Incentivar a criação de sistema de certificação de segurança da informação em dispositivos em Internet das Coisas, baseada em modelo de autorregulação pela iniciativa privada. O modelo deve ser baseado em auto-avaliação voluntária, com a adoção de selo/sinalização de conformidade ao consumidor, evitando a imposição de obrigação legal e repercussões negativas a aderentes, como, por exemplo, alto custo de entrada;
- Mediante a consolidação do modelo de certificação voluntária, estruturar modelo de corregulação ou regulação híbrida para a certificação de dispositivos Internet das Coisas, com a participação de conselho multissetorial ou agência pública focada em segurança da informação.

Segurança da informação em infraestruturas críticas

- Fortalecer a estrutura institucional dedicada à segurança de infraestruturas críticas no âmbito da Administração Pública Federal, com a coordenação de esforços, fomento do compartilhamento de informações sobre vulnerabilidades entre órgãos e entidades da Administração e a prestação de assistência em caso de incidentes de segurança;
- Criar quadros de referência a setores de infraestruturas críticas no âmbito de órgãos/entidades competentes, com o fim de prevenir incidentes de segurança, prevenir e gerir crises;
- Exigir, por parte de agências regulatórias, o respeito a aspectos mínimos de segurança da informação, em particular nos setores de infraestrutura crítica.

4.2 Ambientes Priorizados

4.2.1 Cidades Inteligentes

4.2.1.1 - Privacidade em Cidades Inteligentes

A crescente utilização de dispositivos tecnológicos dispersos pelo espaço urbano, capazes de coletar dados sobre os cidadãos, monitorar suas atividades e até mesmo identificá-los, traz à tona diversas questões referentes à proteção da privacidade e dos dados pessoais dos indivíduos. Nesse cenário, para que o planejamento público de cidades inteligentes seja uma realidade bem-sucedida, consideramos imprescindível que a privacidade dos cidadãos seja tratada como prioridade.

Para tal, faz-se necessário adotar uma lei geral para a proteção de dados. A legislação deve ser capaz de abranger todos os âmbitos da federação e implementar uma série de garantias, que incluem o princípio do legítimo interesse, da finalidade, da transparência, o direito de retificação, o princípio da necessidade e proporcionalidade, dentre outros.

Além da edição de norma específica, entendemos ser necessário que o Poder Público respeite uma série de boas práticas relacionadas à coleta, processamento, armazenamento e compartilhamento de dados pessoais, como a implementação de medidas técnicas de privacidade "por desenho", e organizacionais, a exemplo da oferta de programas de capacitação de servidores públicos e autoridades policiais. Abaixo, apresentamos os principais encaminhamentos identificados:

Definir estratégias locais para proteção de dados

- Municípios e estados devem definir e tornar públicas as suas práticas na temática da proteção de dados, com o fim de regular de forma específica as possibilidades de coleta e processamento de dados pessoais no âmbito da Administração Pública, de forma a proteger o cidadão e conferir segurança jurídica para a implementação de serviços de IoT.

Adoção de boas-práticas pelo Poder Público, incluindo:

- Adotar medidas para a prestação de informações ao cidadão, inclusive por meio de Políticas de Privacidade, disponibilizadas publicamente e capazes de informar com clareza aos cidadãos sobre as práticas de coleta, processamento, armazenamento e compartilhamento de dados pessoais;
- Implementar medidas técnicas de privacidade e segurança "por desenho" em soluções IoT para a proteção de dados pessoais, incluindo o uso de criptografia e técnicas de privacidade diferencial;

4.2.1.2 - Rede de Energia Elétrica Inteligente

O modelo de prestação do serviço público de energia elétrica vem passando por significativas transformações decorrentes da adoção de novas tecnologias na rede e que culminaram na composição das redes elétricas inteligentes (*smart grids*), que incorporam, dentre outros dispositivos, medidores elétricos inteligentes.

Desde 2010, a ANEEL vem enfrentando, por meio do estabelecimento de regras setoriais, os desafios regulatórios relacionados à implementação de Redes Elétricas Inteligentes, entre as quais apontamos: (i) implementação de medidores adequados às novas demandas do mercado; (ii) facilitação do desenvolvimento de geração distribuída por mini ou micro geração; e (iii) previsão de novas modalidades tarifárias, tais como a tarifa branca e a tarifa pré-paga.

Dessa forma, a Agência mostra-se diligente em viabilizar a modernização do setor elétrico. Não obstante, para que o planejamento de redes elétricas inteligentes seja uma prática bem-sucedida, reiteramos:

- Estimular a adoção de medidores eletrônicos que possuam mecanismos avançados e confiáveis de comunicação, com vistas à modernização do setor de energia;
- Estimular que entes públicos e privados adotem padrões de conduta adequados ao quadro legislativo vigente sobre privacidade e proteção de dados pessoais.

4.2.1.3 - Iluminação Pública Inteligente

As redes e infraestrutura de iluminação pública, cuja competência para exploração e regulação cabe aos municípios, vêm sendo transformadas pela incorporação de novas tecnologias, em especial pela substituição das lâmpadas a vapor metálico por placas de LED.

Nesse cenário, a instalação de dispositivos IoT em postes ou braços de iluminação pública deverá observar normas municipais. Além disso, por vezes os braços de iluminação pública são instalados em postes de energia elétrica, de modo que deverá ser observada também a legislação federal e as regras setoriais sobre o compartilhamento de infraestrutura (como a Lei nº 9.472/1997 e a Resolução Conjunta Anatel, Aneel e Anp nº 01/1999).

A expansão da instalação de dispositivos de IoT poderá enfrentar óbices em relação ao montante dispendido sua instalação em postes e às limitações na quantidade de pontos que poderão ser acoplados a essa infraestrutura (sem prejudicar sua integridade e segurança).

Outro impasse diz respeito à possibilidade de se endereçar verbas da COSIP para o financiamento de Parcerias Público-Privadas que objetivem modernizar serviços de iluminação pública. Recomenda-se que os editais de PPP prevejam multiplicidade de fontes de receita para além de verbas oriundas da COSIP, de modo que eventual interpretação restritiva a respeito da utilização da COSIP pelos Tribunais de Contas competentes não inviabilize financeiramente a implementação de iluminação pública inteligente.

Por fim, para que a modernização das redes de iluminação nas cidades seja uma prática bem-sucedida, reiteramos:

- Possibilidade de estimular o compartilhamento de um mesmo ponto de fixação por mais de um serviço ou por diversas empresas prestadoras de um mesmo serviço (a exemplo do compartilhamento praticado em torres de telecomunicações);
- Incentivar também o compartilhamento de dispositivos de IoT entre serviços, públicos ou privados, e investir em alternativas como a instalação de antenas em topos de edifícios, a implementação de Estações Rádio Base subterrâneas e a implantação de infraestrutura passiva subterrânea;
- Possibilidade de aprovação de PEC para inserir ao texto Constitucional autorização para a destinação da COSIP à implementação de rede de iluminação pública inteligente;
- Implementar PPPs para a modernização dos serviços de iluminação, observando os requisitos da legislação específica e o posicionamento dos Tribunais de Contas e Poder Judiciário.

4.2.1.4 - Mobilidade Urbana

A regulação acerca das soluções IoT em mobilidade inteligente, em especial aquelas relativas ao controle e adaptação do trânsito e monitoramento da circulação de transporte público, possui alta complexidade, visto que se deve observar tanto leis federais, como a legislação estadual e municipal específica sobre trânsito e transporte.

Em relação ao **trânsito**, em razão da competência legislativa exclusiva da União, a incorporação de novas tecnologias ao sistema de gestão do tráfego deverá levar em consideração o disposto no Código de Trânsito Brasileiro e a regulamentação do Conselho Nacional de Trânsito (CONTRAN). Com efeito, o órgão vem emitindo

normativas para regulamentar a utilização de determinados dispositivos, tais como os sistemas de videomonitoramento, os medidores de velocidade e os instrumentos de identificação de veículos.

Não obstante a regulação federal, órgãos e entidades de trânsito municipais são responsáveis pela implantação, manutenção e operação de equipamentos de controle viário. Essa atividade deverá ser prevista em normativo específico, como o plano direito e a política de mobilidade municipal.

No caso do **transporte público**, a regulamentação e fiscalização de seus serviços são exercidas conjuntamente por todas as esferas federativas, a depender da área territorial na qual o transporte será realizado.

Todavia, função relevante na regulação e execução dos serviços de transporte é atribuída aos Municípios, que geralmente não possuem a devida capacidade institucional ou financeira para investir na melhoria do referido serviço. Nesse cenário, se considera positiva a intensificação de cooperação entre os diferentes âmbitos da federação na gestão conjunta do adimplemento dos contratos de serviço de transporte público.

Sugerimos também que as soluções de IoT sejam, na medida do possível, baseadas em padrões abertos, em *software* livre ou *open source*, e com API para dados abertos. Ainda, à medida em que aplicações de IoT passam a ter suas operações integradas a sistemas *inteligentes* de tomada de decisão (baseados em algoritmos ou inteligência artificial), é fundamental que os códigos e *hardwares* sejam conhecidos, transparentes e auditáveis, em atendimento aos princípios de impessoalidade, publicidade e eficiência que regem a Administração Pública. Por fim, deve-se estimular a abertura e transparência nas aplicações de IoT baseadas em sistemas *inteligentes* de tomada de decisão.

4.2.1.5 - Segurança Pública Inteligente

Ao Estado é permitido implementar mecanismos de vigilância por intermédio de aplicações IoT, uma vez que ações públicas de monitoramento encontram respaldo na Constituição Federal, que confere ao Estado o dever de garantir aos cidadãos brasileiros segurança através da execução de políticas de segurança pública eficientes.

Nesse cenário, justifica-se o tratamento de dados pessoais sem a obtenção de consentimento prévio e expresso, desde que o tratamento seja estritamente necessário e

proporcional à finalidade a que se destina (garantia da segurança pública), bem como seja realizado apenas por autoridades do sistema de segurança pública.

Entretanto, o aprimoramento tecnológico das capacidades dos sistemas de monitoramento desafia os limites da mencionada prerrogativa constitucional do Estado, dado que a progressiva integração de novas tecnologias aos mecanismos já existentes de vigilância tem o potencial de atingir significativamente direitos fundamentais (tais como direito à privacidade e à liberdade de expressão).

Com o objetivo de coibir abusos no uso de dados, o Poder Público deve impor limites às atividades de segurança pública por meio de balizas de proibição do excesso e com relação à finalidade à qual os dados são coletados e processados. Deve também avaliar os níveis de efetividade do uso dessas novas soluções de monitoramento, já que falhas de efetividade em tais aplicações podem gerar questionamentos sobre a necessidade da implementação do sistema.

Recomendamos, ainda, que o Poder Público aprimore seu arcabouço de boas práticas. Dentre as iniciativas possíveis estão a adoção de documento de avaliação do impacto na proteção de dados (*data protection impact assessment*), a fim de identificar problemas de privacidade e decidir quais procedimentos seguir para gerir riscos; e a concepção de código de conduta que estabeleça diretrizes para os órgãos de segurança pública na implementação e operação de atuais e futuros sistemas de monitoramento.

4.2.2 Saúde

A utilização de aplicações de Internet das Coisas no ambiente de saúde pode trazer benefícios para toda a sociedade brasileira, tanto no que tange ao aumento da qualidade de vida como para aumentar a eficiência do sistema público de saúde.

Com vistas a possibilitar esse desenvolvimento, o objeto dessa parte da análise foi identificar os aspectos regulatórios relacionados à IoT no ambiente da saúde e mapear eventuais barreiras regulatórias que impactem o desenvolvimento dessa tecnologia no setor, notadamente em relação às seguintes aplicações priorizadas: *(i)* monitoramento remoto das condições dos pacientes com diabetes; *(ii)* localização de ativos dentro de unidades de saúde; *(iii)* apoio ao diagnóstico de Sepse; *(iv)* diagnóstico descentralizado; e *(v)* identificação e controle de epidemias.

Para se atingir o objetivo proposto, a metodologia utilizada para a elaboração do diagnóstico regulatório de IoT no ambiente de saúde envolveu (i) o mapeamento das normas que impactam o setor, especialmente as normas e diretrizes estabelecidas pelo Ministério da Saúde (MS), pela Agência Nacional de Vigilância Sanitária (ANVISA) e pelo Conselho Federal de Medicina (CFM); (ii) entrevistas com técnicos da ANVISA; e (iii) contribuições dos agentes do setor de saúde que participaram dos workshops conduzidos pelo BNDES e pelo MCTIC.

Regulação da Agência Nacional de Vigilância Sanitária – ANVISA

- Importância de cumprir com a legislação vigente do setor de saúde, em especial atentando para as obrigações e procedimentos definidos nos regulamentos da ANVISA, no desenvolvimento de aplicações de IoT no ambiente de saúde.

Produtos para a Saúde

- Aplicações de IoT enquadradas como produtos para a saúde devem passar pelo procedimento de cadastro ou registro na ANVISA, a depender da classe de risco da aplicação;
- Importância de se clarificar a regulação aplicável a *software* como dispositivo médico, de modo a trazer segurança jurídica e garantir convergência regulatória com as mais avançadas práticas e normas internacionais do setor.

Regulação dos Conselhos de Medicina

- Importância de assegurar que as normas dos Conselhos continuem atualizadas com os avanços tecnológicos proporcionados pela Internet das Coisas.

Debates sobre Privacidade

- O consentimento expresso do usuário é imprescindível para a coleta de dados pessoais para finalidades diversas da realização do serviço de saúde contratado;
- O uso de dados de IoT pelo Poder Público no ambiente de saúde deve respeitar os princípios da legalidade e do interesse público. O que significa dizer que as finalidades para as quais o Estado utiliza dados de seus cidadãos devem possuir previsão legal e constituir finalidade que atenda ao interesse público;
- Para garantir uma maior segurança ao armazenamento de dados de IoT no ambiente da saúde é recomendável a utilização de ferramentas como agregação e anonimização das informações coletadas por dispositivos IoT;
- O compartilhamento de dados coletados é tema de extrema relevância que encontra alguns desafios, como a necessidade de proteção à privacidade, a

garantia de interoperabilidade e o adequado intercâmbio de informações entre sistemas de informação de instituições de saúde.

4.2.3 Rural

A Internet das Coisas tem trazido também novas perspectivas para o desenvolvimento da agropecuária nacional, com um foco baseado na análise de dados para garantir precisão as decisões no campo. Nesse sentido, o uso de drones, máquinas autônomas, sensores e atuadores na produção agrícola e na pecuária vêm abrindo novas perspectivas de produtividade.

Do ponto de vista de desafios jurídicos, o ambiente rural possui um conjunto de características e questões que tornam sua análise particular em relação aos outros ambientes priorizados. Em especial, ao longo da Fase III, além da temática de telecomunicações extensamente abordada na horizontal específica, outros dois temas regulatórios se destacaram diante dos seus impactos diretos no desenvolvimento de IoT no ambiente rural: a regulamentação para a utilização de drones em aplicações IoT rurais e as disputas acerca da propriedade e proteção de dados no ambiente rural.

Uso drones em aplicações de IoT

- Importância de cumprir com a legislação vigente para a utilização segura e dentro da lei de drones ambiente rural, observando-se todas as obrigações estabelecidas pela ANATEL, ANAC e DECEA;
- Articular com o setor privado e a Comissão Brasileira de Agricultura de Precisão, dentro de suas competências, um aprofundamento técnico do estado da arte da tecnologia de drones no ambiente rural, com vistas a identificar possibilidades seguras de flexibilização do atual quadro regulatório aplicável.

Proteção e propriedade de dados e bases de dados rurais

- Aprofundar os debates e buscar um alinhamento com os principais atores interessados acerca de qual seria o melhor regime jurídico para a propriedade e proteção dos dados rurais (dados não-pessoais).