IoT - Internet das Coisas – o Decreto 9.854 e o Plano Nacional de IoT

André Guskow Cardoso
Mestre em Direito do Estado pela UFPR
Sócio – Justen, Pereira, Oliveira & Talamini

1. Introdução

O Decreto nº 9.854/2019 instituiu o Plano Nacional de Internet das Coisas (IoT), estabelecendo premissas relevantes para setor essencial do desenvolvimento tecnológico e da transformação digital.

2. A internet das coisas (IoT)

A internet das coisas consiste na conexão dos mais diversos objetos e equipamentos à internet, com o efeito de promover a sua interconexão em rede. A conectividade ampliada aos diversos equipamentos produz novas funcionalidades e amplia o volume de dados gerado pela sua utilização.

Trata-se de tecnologia que constitui base para o desenvolvimento de vários aplicativos e funcionalidades, seja no campo industrial (cadeias de fornecimento inteligentes) ou no âmbito residencial (equipamentos para casas inteligentes – *smart home appliances*).

3. Aspectos essenciais do Plano Nacional de IoT

3.1 – Finalidade

O Decreto nº 9.854/2019 indica que o Plano Nacional de Internet das Coisas (IoT) tem a finalidade de "implementar e desenvolver a Internet das Coisas no País".

3.2 – O respeito às diretrizes de segurança da informação e proteção de dados

O Plano Nacional de Internet das Coisas (IoT) terá por base a livre concorrência e a livre circulação de dados. Em qualquer caso, o decreto ressalva que o plano deverá observar as diretrizes de segurança da informação e da proteção de dados pessoais.

Trata-se de dois aspectos essenciais.

Por um lado, a implementação de uma base de dispositivos de IoT depende da imprescindível observância de cuidados e medidas destinados a garantir a segurança da informação. Basta verificar que um grande percentual de ataques de *cyberterrorismo* ou mesmo de *cyberwarfare* envolve o aproveitamento de falhas de segurança em dispositivos de IoT.

Pode-se citar a violação e roubo de dados de placas e motoristas coletados por câmeras de segurança utilizadas pela US Customs and Border Patrol americana, que foi recentemente divulgado (https://www.theregister.co.uk/2019/06/10/us_custom_border_patrol_contractor_hacked/).

A questão é tão relevante que o governo do Japão editou lei que o autoriza a invadir sistemas particulares de IoT para testar as vulnerabilidades da rede e como forma de preparação para os Jogos Olímpicos (https://www.technologyreview.com/the-download/612835/japan-plans-to-hack-into-millions-of-its-citizens-connected-devices/). Segundo estudo realizado pelo National Institute of Information and Communications Technology (NICT) japonês, os dispositivos de IoT foram alvo de 57% dos ciberataques detectados pelo Instituto em 2017.

Por outro lado, a questão da proteção de dados pessoais é igualmente essencial. A utilização ampla das tecnologias de IoT potencializa os riscos à violação de dados pessoais e de dados pessoais sensíveis. Ampliam-se os meios de coleta, processamento e distribuição de dados (inclusive de cunho pessoal). Tais dados devem ser necessariamente protegidos, na forma da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

E esse será um aspecto muito relevante da implementação concreta do plano nacional de IoT. As medidas necessárias à proteção de dados exigirão um esforço relevante dos desenvolvedores desses sistemas e igual esforço daqueles que serão responsáveis pela fiscalização dessas atividades. A Lei nº 13.709/2018 exige que todas as empresas e entidades cujas atividades envolvam tratamento de dados pessoais adotem medidas efetivas para a obtenção de consentimento e para a garantia e segurança de tais dados.

Note-se que o tratamento é um conceito amplo, envolvendo, nos termos da Lei nº 13.709/2018 “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (art. 5º, inc. X).

E, por sua vez, dado pessoal é qualificado pela Lei como sendo toda e qualquer “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, inc. I).

Por isso, a proteção de dados pessoais é e será um aspecto essencial do desenvolvimento da IoT.

3.3 – Objetivos do Plano Nacional de IoT

O Decreto nº 9.854 estabelece que o Plano Nacional de Internet das Coisas (IoT) terá como objetivos (art. 3º):

> (a) melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT;
>
> (b) promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital;
>
> (c) incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor;
>
> (d) buscar parcerias com os setores público e privado para a implementação da IoT; e
>
> (e) aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País.

Trata-se de objetivos de extrema relevância, mas que o Decreto nº 9.854 não chega a especificar como serão atendidos. A questão apresenta relevância, na medida em que vários desses objetivos foram estabelecidos de modo genérico e abstrato, como a "promoção da capacitação profissional", a "geração de empregos na economia digital" e o "incremento na produtividade e fomento da competitividade das empresas brasileiras desenvolvedoras de IoT".

Por isso, o atingimento efetivo de tais objetivos dependerá tanto da definição de atos normativos específicos, em cada uma dessas áreas, como da adoção de medidas concretas pelo Estado brasileiro para a sua concretização – o que se confirma pelo teor do art. 5º do Decreto nº 9.854, que define os temas que integrarão plano de ação destinado a identificar soluções para viabilizar o Plano Nacional de IoT.

3.4 – Ambientes prioritários

O plano estabelece que ato do Ministro de Ciência, Tecnologia, Inovações e Comunicações irá indicar os ambientes em que haverá prioridade para as aplicações de IoT. Desde logo, o Decreto nº 9.854 menciona que, dentre estes, deverão estar os ambientes de saúde, de cidades, de indústria e rural (art. 4º).

O decreto estabelece que essa priorização será relevante e servirá de referência para (i) acesso a mecanismos de fomento à pesquisa científica, desenvolvimento tecnológico e inovação e (ii) apoio ao empreendedorismo de base tecnológica (art. 4º, §2º).

3.5 – Compatibilidade e alinhamento com a Estratégia Brasileira para a Transformação Digital

O Decreto nº 9.854 estabelece no parágrafo único do art. 5º que as ações do plano de ação destinado a viabilizar o Plano Nacional "deverão estar alinhadas com as ações estratégicas definidas na Estratégia Brasileira para a Transformação Digital".

As referidas ações estratégicas constam da Estratégia Brasileira para a Transformação Digital (Decreto nº 9.319), aprovada pela Portaria nº 1.556/2018 do Ministério da Ciência, Tecnologia, Inovações e Comunicações https://www.mctic.gov.br/mctic/export/sites/institucional/arquivos/estrategiadigital.pdf).

Esse alinhamento é essencial, considerando a necessidade de coordenação da atuação governamental para assegurar a transformação digital do País (e as tecnologias e questões a ela associadas, como *Big data*, inteligência artificial, tecnologias baseadas nas plataformas blockchain, Iot e segurança cibernética - *cybersecurity*).

Como já mencionado em outro trabalho a respeito do tema "O papel do Estado é fundamental para o desenvolvimento das infraestruturas necessárias para a transformação digital" (CARDOSO, André Guskow. Infraestrutura e transformação digital. In. *Direito da Infraestrutura: Estudos de Temas Relevantes*. Coord. Marçal Justen Filho e Marco Aurélio de Barcelos Silva. Ed. Fórum, 2019).

Tal como lá mencionado, a atuação do Estado pode se dar em várias frentes (outorga de serviços e bens de sua titularidade a terceiros, para exploração via autorização, permissão ou concessão, atuação de fomento e incentivo e regulação). Muitas vezes, a atuação reguladora do Estado terá por objetivo apenas assegurar a liberdade necessária à atuação privada para o desenvolvimento de tecnologias.

3. Conclusão

Verifica-se que, embora o Decreto nº 9.854/2019, ao instituir o Plano Nacional de Internet das Coisas (IoT), tenha estabelecido premissas relevantes para o tema, deixou várias questões em aberto. O desenvolvimento efetivo da tecnologia de IoT dependerá de ações subsequentes do Estado brasileiro e dos particulares. Em qualquer caso, o Decreto nº 9.854/2019 tem o mérito de estabelecer determinados parâmetros normativos para a IoT, que constitui relevante aspecto da transformação digital.

Informação bibliográfica do texto:

CARDOSO, André Guskow. IoT - Internet das Coisas – o Decreto 9.854 e o Plano Nacional de IoT. *Informativo Justen, Pereira, Oliveira e Talamini*, Curitiba, n.º 148, junho de 2019, disponível em http://www.justen.com.br/informativo, acesso em [data].