Analisis Kebutuhan Regulasi Terkait dengan Internet of Things

The Analysis of The Required Regulation of Internet of Things

Diah Kusumawati[1], **Bagus Winarko**[2], **Riva'atul Adaniah Wahab**[3], **Wirianto Pradono**[4]
[1,2,3,4]*Puslitbang SDPPPI, Kementerian Komunikasi dan Informatika*
[1,2,3,4]*Medan Merdeka Barat No. 9, Jakarta, Indonesia*
email: [1]diah012@kominfo.go.id, [2]bagu001@kominfo.go.id, [3]riva002@kominfo.go.id, [4]wiri001@kominfo.go.id

INFORMASI ARTIKEL

Naskah diterima 4 Desember 2017
Direvisi 10 Desember 2017
Disetujui 10 Desember 2017

Keywords:
IoT
Regulation
RIA
BOCR

ABSTRACT

IoT Indonesia Forum predicted that IoT Indonesia market potential in 2020 reach about 35 billion dollars. This paper analyzes the IoT's regulatory requirements in Indonesia, which are safety standards, device standards, business implementation models, and IoT ecosystems, adapted to Indonesia's current conditions. The study uses qualitative approach. Primary data are obtained through in-depth interview and FGD and analyzed using three early stages of Regulatory Impact Analysis and Benefit, Opportunity, Cost, and Risk theory on each alternative. As the results, the parameters that needed to be regulated for each IoT issue include 1) Security standards: personal data protection, interoperability, data network security, and applications security; 2) Device standards: TKDN devices, system authentication, and device security, 3) Business model: spectrum utilization, and 4) Ecosystems: spectrum allocation. Recommendations that can be conveyed include the need for stakeholder cooperation to develop the IoT Indonesia Roadmap, increasing the amount of bandwidth in the existing frequency spectrum, reviewing existing equipment regulations according to the most widely used IoT technology in the world, what sector mapping is highly potential in Indonesia, privacy regulation and device security, reviewing TKDN policy requirements, and specific business models between domestic IoT producers for IoT use in the government sector.

Kata kunci :
IoT
Regulasi
RIA
BOCR

ABSTRAK

Forum IoT Indonesia memprediksi potensi pasar IoT Indonesia tahun 2020 mencapai sekitar 35 miliar dolar. Tulisan ini menganalisis kebutuhan regulasi IoT di Indonesia yaitu standar keamanan, standar perangkat, model penyelenggaraan bisnis, serta ekosistem IoT yang disesuaikan dengan kondisi Indonesia saat ini. Penelitian menggunakan pendekatan kualitatif. Data primer diperoleh melalui wawancara mendalam dan FGD serta dianalisis menggunakan 3 tahap awal metode Regulatory Impact Analysis dan teori *Benefit, Opportunity, Cost and Risk* terhadap masing-masing alternatif. Hasil penelitian menunjukkan bahwa parameter yang perlu diregulasi untuk masing-masing isu IoT antara lain 1) Standar keamanan: perlindungan data pribadi, interoperabilitas, keamanan jaringan, dan keamanan aplikasi, 2) Standar perangkat: TKDN perangkat, sistem otentifikasi, dan keamanan perangkat, 3) Model bisnis: pemanfaatan spektrum, dan 4) Ekosistem: alokasi spektrum. Rekomendasi yang dapat disampaikan yaitu perlu kerjasama antar*stakeholder* untuk menyusun *Roadmap* IoT Indonesia, penambahan jumlah *bandwidth* pada spektrum frekuensi eksisting, mengkaji regulasi eksisting perangkat sesuai teknologi IoT yang paling banyak digunakan di dunia, pemetaan sektor apa yang sangat berpotensi di Indonesia, regulasi privasi dan keamanan perangkat, mengkaji kebijakan persyaratan TKDN, dan model bisnis khusus antara produsen IoT dalam negeri untuk penggunaan IoT di sektor pemerintah.

1. Pendahuluan

Teknologi *Internet of Things* (IoT) termasuk dalam 14 (empat belas) teknologi yang diprediksi oleh *World Economic Forum* akan digunakan oleh dunia pada tahun 2020 (Montresor, 2014). *Gartner's Hype Cycle for Emerging Technology* (pada Gambar 1), menunjukkan bahwa teknologi yang berhubungan dengan IoT seperti *connected home*, *smart dust*, *smart robots* hingga IoT *platform* masih berada dalam fase

pertama yaitu *innovation trigger* yang memerlukan waktu kira – kira 5 – 10 tahun untuk mencapai puncak teknologi. Hal tersebut dapat diartikan bahwa teknologi ini belum matang dan akan terus dikembangkan oleh dunia. Di satu sisi, badan standardisasi telekomunikasi dunia atau *International Telecommunication Union* (ITU) masih melakukan riset mengenai standar protokol komunikasi untuk IoT sehingga sampai saat ini belum ada standar IoT yang baku. Kondisi ini menjadi salah satu hambatan dalam pengembangan IoT. Di sisi lain, pengembangan teknologi IoT merupakan potensi bagi suatu negara untuk mengambil peluang ekonomi dari pemanfaatan teknologi tersebut.

Gambar 1. *Gartner's Hype Cycle for Emerging Technology (Gartner.com/SmarterWithGartner, 2017)*

Terkait dengan potensi yang dapat didorong dari pemanfaatan teknologi IoT, beberapa lembaga survei mencoba memprediksi nilai ekonomi dari teknologi tersebut. Munich RE bersama dengan ERGO dalam laporan IT *Trend* 2016 memprediksi nilai valuasi dari IoT adalah 28,1 miliar dolar pada tahun 2020 (Munich RE, 2016). Riset Mc Kinsey mengestimasi nilai potensi ekonomi IoT pada tahun 2025 untuk beberapa aplikasi. Dalam satuan triliun dollar (USD)/tahun, potensi ekonomi aplikasi tersebut antara lain pada sektor kesehatan (*healthcare*) sebesar 1,1 – 2,5; industri (*manufacturing*) sebesar 0,9 – 2,3; kelistrikan (*electricity*) sebesar 0,2 – 0,5; infrastruktur perkotaan (*urban-infrastructure*) sebesar 0,1 – 0,3; keamanan (*security*) sebesar 0,1 – 0,2; sumber daya (*resource extraction*) sebesar 0,1 – 0,2; pertanian (*agriculture*) sebesar 0,1; transportasi (*vehicle*) sebesar 0,02 – 0,1; dan aplikasi potensial lainnya sebesar 0,05 (Manyika et al., 2013).

Forum IoT Indonesia telah memprediksi potensi pasar IoT Indonesia di tahun 2020 mencapai kurang lebih 35 miliar dolar. Segmentasi pasar IoT di Indonesia diprediksi sebesar 10% dari sektor retail dan *service*; 14% dari sektor manufaktur; 19% dari sektor perbankan, keamanan dan finansial; serta 57% dari sektor media, transportasi, dan komunikasi. Riset oleh Li Da Xu menganalisis teknologi serta aplikasi kunci untuk industri IoT yaitu teknologi pendukung IoT antara lain teknologi identifikasi dan *tracking*, teknologi telekomunikasi, kompleksitas jaringan, serta manajemen layanan di IoT. Sektor industri yang

berpotensi berkembang dengan adanya IoT antara lain industri kesehatan, pertambangan, transportasi dan logistik, serta penanganan bencana (Perera & Liu, 2015).

Selain sektor aplikasi, kebutuhan spektrum untuk IoT juga menjadi perhatian bagi beberapa negara dan institusi. India melalui riset yang dilakukan oleh *The Indus Entrepeneurs* (TIE) merekomendasikan untuk mengalokasikan spektrum sebesar 10 MHz untuk layanan IoT dengan skenario untuk mendorong pertumbuhan *smart city*. Wilayah perkotaan India dengan tingkat kepadatan yang tinggi akan membutuhkan lebih dari 40.000 perangkat IoT/km^2 dengan pendekatan 5-10 perangkat IoT per rumah tangga. Selain India, Monaco, dan Barcelona juga memiliki proyek *smart city* yang menempatkan sekitar 20.000 perangkat setiap 2 km^2 hanya untuk penggunaan *metering*, *lighting*, dan *parking* (Tiwary, 2015). Terkait dengan inovasi dan pengembangan *industry*, IoT OFCOM Inggris juga telah mengalokasikan spektrum khusus untuk layanan IoT di pita frekuensi 55 - 68 MHz, 70,5 – 71,5 MHz dan 80 – 81,5 MHz. OFCOM telah menyediakan perangkat berlisensi untuk akses IoT ke spektrum *Very High Frequency* (VHF) dan mencari jalan tengah agar layanan IoT dapat berjalan berdampingan dengan ekosistem lainnya (OFCOM, 2016).

Selain isu potensi ekonomi serta kebutuhan spektrum untuk layanan IoT yang mendorong inovasi dan industri serta pengembangan *smart city*, isu lain yang perlu mendapatkan perhatian adalah model penyelenggaraan bisnis IoT. ITU merekomendasikan 5 (lima) model bisnis yang diperkirakan akan muncul sehubungan dengan bisnis IoT yaitu *device provider*, *network provider*, *application provider*, *platform provider*, dan *application customer*. Berdasarkan rekomendasi model bisnis tersebut, permasalahan yang perlu didiskusikan lebih lanjut salah satunya terkait dengan bentuk perizinan penyelenggaraan model bisnis. Dalam praktiknya, model bisnis IoT sangat bervariasi bergantung pada jenis sektor serta teknologi yang digunakan.

Selain itu, isu yang tidak kalah pentingnya adalah keamanan data. Adanya beberapa kasus penyalahgunaan data pengguna sejalan dengan riset oleh Ernita yang menekankan pentingnya standar keamanan privasi data dalam IoT. Pengguna harus memiliki akses penuh terhadap sistem sehingga memiliki hak untuk dapat memilih antara membagikan data atau tidak. Secara umum, salah satu metode untuk menjamin privasi yaitu manajemen identitas, otentikasi, dan otorisasi. Untuk menjaga integritas data pada *Radio Frequency Identification* (RFID), sensor, maupun basis data dari serangan *tampering* (mengubah atau memodifikasi data), maka data harus disimpan dalam bentuk enkripsi (Meutia, 2015). Tahun 2015 juga terjadi serangan terhadap perangkat *smart* meter dan *smart home.* Serangan juga dapat dilakukan pada lapisan fisik misalnya *side-channel attacks* (SCA) yang dapat digunakan untuk mengekstrak kunci dari perangkat elektronik yang menggunakan daya, gelombang elektromagnetik, atau getaran suara. Pendekatan yang disarankan untuk standar keamanan pada perangkat IoT adalah menggunakan identifikasi dan otentikasi yang spesifik dengan konsep *Physical Unclonable Function* (PUF). PUF ditanam pada saat proses manufaktur perangkat terutama pada saat desain *chip.* Teknologi ini juga memiliki manfaat lain yaitu tahan terhadap serangan *tampering* (Neill, 2016).

Berdasarkan poin–poin permasalahan yang telah dijelaskan maka penelitian ini akan menganalisis kebutuhan regulasi terhadap isu–isu IoT diantaranya standar keamanan, standar perangkat, model penyelenggaraan bisnis, serta ekosistem IoT di Indonesia untuk disesuaikan dengan kondisi eksisting di Indonesia. Penelitian ini diharapkan dapat bermanfaat langsung bagi direktorat teknis dalam penyusunan atau revisi regulasi terkait dengan teknologi IoT.

2. Tinjauan Pustaka

Beberapa penelitian terkait isu penerapan IoT telah dilakukan. Adapun yang dijadikan sebagai referensi antara lain:

1) *The Regulation of Technology and The Technology of Regulation* (Wiener, 2004). Paper ini menganalisis hubungan antara regulasi dengan teknologi. Regulasi mungkin dapat menghambat atau mendorong perubahan teknologi. Keterkaitan antara keduanya bergantung pada regulasi yang mengatur teknologi tersebut, misal desain dan alternatif instrumen kebijakan. Penelitian ini menguji sejarah regulasi

ekonomi dan sosial selama tiga dekade, kekuatan dari teori politik regulasi, pilihan instrumen regulasi, penilaian dampak terhadap regulasi, dan pengaruh dari setiap faktor tersebut terhadap inovasi dan difusi teknologi. Kesimpulan dari penelitian ini adalah a) harus ada penguatan terhadap kebijakan untuk pengusaha, sesuai dengan teori inovasi *Schumpeter* bahwa pengusaha swasta memegang peranan penting sehingga perlu kebijakan untuk inovator, b) merekonstruksi pasar sebagai salah satu alternatif untuk mencegah kegagalan, c) harus jelas intervensi pemerintah dalam sistem, d) harus mendorong jaringan untuk difusi regulasi inovasi, e) pengalaman dalam tiga dekade terakhir (bertentangan dengan teori–teori regulasi politik terkemuka saat ini), harus memahami kondisi regulasi politik saat ini, f) perbatasan antara regulasi dan teknologi adalah *global commons*, dan g) harus lebih empiris (mengevaluasi pengalaman regualsi sebelumnya) terhadap desain regulasi. Secara umum dari semua rekomendasi tersebut adalah perlu pengembangan struktur institusi yang mendukung kebijakan pemberian penghargaan terhadap inovasi.

2) *Towards Quality of Service for Long-range IoT in Unlicensed Radio Spectrum* (Pham, n.d.). Untuk menjamin kualitas layanan yang lebih baik pada transmisi jarak jauh maka dalam riset ini direkomendasikan mekanisme *activity time sharing*. Perangkat yang beroperasi di waktu terbatas dapat meminjam waktu dari perangkat yang lain (*sharing time*). Mekanisme tersebut telah dicoba untuk diimplementasikan pada proyek-proyek eksisting. Latar belakang diusulkannya mekanisme tersebut adalah teknologi radio *long – range* merupakan teknologi yang menjanjikan untuk mendorong pertumbuhan IoT. Hingga saat ini teknologi yang telah digunakan untuk IoT belum menyediakan mekanisme jaminan kualitas layanan untuk memastikan sebuah perangkat yang membutuhkan pengiriman *critical* data dapat berjalan dengan baik tanpa terbatas oleh waktu atau mekanisme lain.

3) *Research on IoT Security Risks* (Xi, 2016). Penelitian ini mempelajari penyebab risiko keamanan privasi dan mengusulkan beberapa pencegahan risiko IoT. Beberapa penyebab risiko keamanan privasi disebabkan oleh *risk of safety certification*, *risk of RFID technology security*, dan *risk of information leakage*. Upaya pencegahan terhadap risiko tersebut adalah mempercepat kebijakan dan regulasi terkait untuk peningkatan sistem keamanan, meningkatkan level proteksi privasi terhadap IoT teknologi dan memperkuat kesadaran terhadap keamanan privasi IoT.

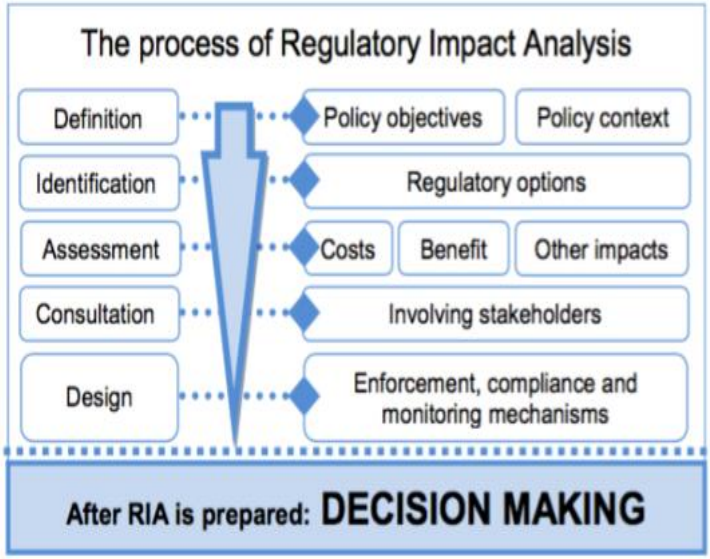
4) *IoT Business Models and Extended Technical Requirements* (Jia, Xueqin; Jing, Wang; He, n.d.). Hingga saat ini belum ada model bisnis IoT yang umum yang dapat digunakan sebagai *framework* global. Riset ini mencoba untuk mengusulkan bisnis model IoT menjadi 3 (tiga) tipe yaitu bisnis telekomunikasi, bisnis internet, dan bisnis industri. Bisnis model telekomunikasi dioperasikan oleh operator telekomunikasi dan menawarkan fitur layanan kepada publik. Bisnis model internet juga memberikan layanan kepada publik yang dioperasikan secara bersama oleh s*ervice provider* dan operator telekomunikasi. Sedangkan bisnis model IoT industri menyediakan layanan yang spesifik sesuai permintaan industri dan dioperasikan oleh masing–masing industri.

Selain penelitian terdahulu, analisis penerapan IoT di Indonesia juga perlu untuk mengamati model bisnis IoT dari Rec. ITU-T Y.2069 (07/2012) agar dapat disesuaikan dengan kondisi di Indonesia dan kompatibel dalam skala global.Ekosistem *Internet of Things* terdiri dari berbagai macam pelaku usaha. Setiap pelaku usaha setidaknya melakukan satu peran bisnis, walaupun tidak menutup kemungkinan untuk memiliki lebih dari satu peran. Secara garis besar, pelaku usaha di dalam ekosistem IoT terdiri dari *Network Provider* (penyedia jaringan), *platform provider* (penyedia *platform*), *application provider* (penyedia aplikasi), dan *application customer* (pelanggan aplikasi).

3. Metode Penelitian

Penelitian menggunakan pendekatan kualitatif. Lokasi penelitian yaitu Kota Jakarta, Depok, Bandung, Bogor, Yogyakarta, Bali, dan Surabaya. Data primer diperoleh melalui wawancara mendalam (*in-depth interview*) dan *Focus Group Discussion* (FGD) dengan *stakeholder* operator telekomunikasi, vendor telekomunikasi, industri IoT, akademisi dan praktisi bidang telekomunikasi, serta kementerian, lembaga, pemerintah daerah yang berpotensi memanfaatkan IoT.

Data dianalisis secara deskriptif menggunakan *framework RIA* untuk mengetahui pandangan industri terhadap isu IoT. Tujuan analisis menggunakan RIA adalah untuk mengetahui bentuk regulasi yang sesuai dengan ekosistem IoT di Indonesia berdasarkan pandangan *stakeholder* terkait. Metode RIA yang digunakan menggunakan referensi dari OECD. Tahap – tahap dalam metode RIA yang telah dilakukan dalam penelitian ini adalah 1) *Definition*, yaitu mendefinisikan konteks kebijakan dan tujuan, khususnya identifikasi permasalahan yang menjadi dasar tindakan pemerintah, 2) *Identification*, yaitu menganalisis opsi – opsi regulasi terkait dengan permasalahan yang telah didefinisikan pada tahap sebelumnya, dan 3) *Assesment*, yaitu menganalisis keuntungan dan kerugian serta dampak lainnya dari opsi yang telah diidentifikasi pada tahap kedua. Idealnya, metode RIA terdiri dari dua tahapan selanjutnya yaitu *consultation* (publik konsultasi dari hasil yang telah diperoleh dari tahap 3) dan *design* (mekanisme penyusunan, penetapan, dan evaluasi terhadap regulasi). Dalam penelitian ini, tahap metode RIA hanya dilakukan sampai tahap 3 karena tahap keempat dan kelima disarankan untuk dilakukan oleh Direktorat Teknis terkait sesuai dengan tugas pokok dan fungsi yang telah ditetapkan di lingkungan organisasi Kementerian Komunikasi dan Informatika. Gambar 2 menunjukkan tahapan dari *framework* analisis menggunakan metode RIA.



Gambar 2. Tahapan Analisis RIA (OECD, 2008)

Setelah mendapatkan usulan bentuk regulasi dari tahapan RIA, dilakukan analisis menggunakan teori *Benefit, Cost, Opportunity, and Risk* (BOCR) terhadap masing-masing alternatif berdasarkan data *Focus Group Discussion* (FGD). Adapun alur penelitian yang dilakukan adalah 1) *In-depth interview* untuk memperoleh gambaran permasalahan terkait dengan IoT, usulan regulasi, dan parameter–parameter yang diusulkan perlu untuk diregulasi, 2) Hasil *in-depth interview* diolah dan dianalisis dengan data tambahan dari *benchmark* untuk menentukan alternatif bentuk regulasi, 3) Parameter yang diusulkan perlu untuk diregulasi, 4) Hasil data FGD 1 diolah kemudian dianalisis berdasarkan data hasil *in-depth interview*, kemudian menyusun bahan untuk FGD 2, 5) Melakukan FGD 2 dengan *stakeholder* spesifik pelaku bisnis industri IoT lokal sebagai mekanisme iterasi untuk menentukan alternatif bentuk regulasi dan parameter–parameter yang diusulkan perlu untuk diregulasi. Selain itu, dalam FGD ini juga dielaborasi hambatan–hambatan yang dihadapi oleh industri IoT lokal, dan 6) Hasil olahan data FGD 2 digunakan sebagai bahan untuk penyusunan kuesioner dengan responden industri IoT lokal. Kuesioner ini bertujuan untuk iterasi FGD 2 mengenai alternatif bentuk regulasi, penyusunan prioritas parameter yang perlu diregulasi dan penyusunan prioritas hambatan yang dihadapi oleh industri IoT dalam negeri.

4. Hasil Penelitian dan Pembahasan

Hasil Pengumpulan Data
Hasil Wawancara

Permasalahan terkait IoT yang diperoleh dari hasil wawancara dengan akademisi bidang keahlian telekomunikasi, informatika, dan keamanan informasi yaitu:

1) Isu Standar Perangkat IoT. Standar teknis dan protokol diusulkan untuk mengikuti standar yang berlaku secara internasional. Dalam mengadopsi suatu standar, diperlukan analisis mendalam terkait dengan tren IoT di masa mendatang dikaitkan dengan kepentingan bangsa Indonesia terhadap IoT (*national interest*). Jika ingin melakukan proteksi terhadap produk dalam negeri, disarankan untuk membuat standar khusus yang berlaku seperti *gateway* atau protokol keamanan tertentu untuk semua perangkat IoT yang masuk ke Indonesia. Standar khusus tersebut disebutkan dalam regulasi sertifikasi perangkat sebagai salah satu bentuk proteksi terhadap ekosistem industri dalam negeri. Sektor IoT yang paling memungkinkan diterapkan di Indonesia dan diperkirakan akan banyak penggunanya adalah IoT bidang kesehatan (*smart health/telemedicine*) dan keamanan rumah (*smart home*);
2) Isu Model Bisnis IoT. Secara umum, model bisnis dari IoT akan sama dengan model bisnis yang telah diidentifikasi oleh ITU. Poin penting yang perlu digali adalah menemukan model bisnis yang dapat mendatangkan keuntungan untuk Indonesia. Indonesia diharapkan dapat mengambil potensi IoT di bidang aplikasi dengan melakukan pemetaan terhadap aplikasi apa saja yang sangat potensial dan spesifik khas Indonesia. Selain itu, jika ingin mengembangkan ekosistem industri IoT dalam negeri, disarankan agar ada model bisnis spesifik terkait dengan penyediaan IoT untuk kebutuhan pemerintah;
3) Isu Standar Keamanan IoT. Terdapat banyak isu terkait dengan standar keamanan IoT. Secara garis besar, isu keamanan terbagi menjadi dua yaitu keamanan secara teknis (meliputi perangkat keras sampai perangkat lunak) dan keamanan secara non teknis (terutama menyangkut keamanan terhadap data pribadi). Secara teknis, aspek keamanan yang harus diperhatikan adalah keamanan pada perangkat dan keamanan pada saat proses pengiriman data *end-to-end* (secara garis besar adalah keamanan pada *network* dan *device*. Regulasi untuk layer aplikasi dinilai cukup sulit karena terlalu luas cakupannya. Dari aspek non teknis, hal yang sangat perlu mendapat perhatian adalah perlindungan terhadap data pribadi konsumen serta manajemen akses data;
4) Isu Alokasi Spektrum untuk IoT. IoT sementara ini sepertinya hanya beroperasi sebagai layanan yang tidak spesifik membutuhkan spektrum khusus;
5) Usulan Regulasi terkait IoT. Regulasi yang paling mendesak bagi Indonesia di era IoT adalah regulasi terkait dengan perlindungan data. Setelah itu, regulasi terkait dengan standar perangkat yang mengikuti standar internasional, penyesuaian regulasi terkait dengan perangkat misalnya maksimum *power* atau konektivitas yang digunakan, dimana pengaturannya disesuaikan dengan tren yang paling banyak digunakan oleh dunia.

Permasalahan terkait IoT yang diperoleh dari hasil wawancara dengan operator telekomunikasi, *vendor* perangkat IoT dan industri IoT dalam negeri.

1) Isu Standar Perangkat IoT. Penentuan standar perangkat IoT disarankan untuk mengikuti standar yang berlaku secara internasional sehingga biaya investasi awal maupun produksi menjadi terjangkau dari sudut pandang bisnis. Jika harus ada standar perangkat IoT Indonesia, disarankan untuk membuat ketentuan berdasarkan kelasnya, misalnya berdasarkan jarak jangkauan atau berdasarkan aplikasi kegunaannya;
2) Isu Model Bisnis IoT. Jika mengacu pada model bisnis yang telah diusulkan oleh ITU, dari sudut pandang industri, model bisnis IoT tidak bisa diseragamkan karena tergantung dengan orientasi dan kondisi internal masing-masing industri. Bahkan satu perusahaan dapat memiliki beberapa model bisnis yang berbeda-beda sesuai kebutuhan dengan pihak konsumen;

3) Isu Standar Keamanan IoT. Standar keamanan IoT penting untuk diregulasi, akan tetapi lebih disarankan untuk mengacu pada standar *International Organization for Standardization* (ISO). Jika akan meregulasi standar keamanan disarankan per layer layanan;
4) Isu Alokasi Spektrum untuk IoT. Industri akan melihat potensi penggunaan teknologi konektivitas IoT berdasarkan tren dan efisiensi biaya. Jika dilihat saat ini, tidak menutup kemungkinan industri juga memanfaatkan konektivitas yang tidak berbayar dengan menggunakan teknologi di spektrum yang tidak berlisensi. Terkait dengan isu ini, diusulkan untuk mengidentifikasi kemungkinan penggunaan teknologi dan harmonisasinya dengan penggunaan spektrum saat ini;
5) Usulan Regulasi terkait IoT. Pengaturan mengenai IPv6 untuk mengantisipasi jumlah perangkat IoT yang jumlahnya diprediksi semakin meningkat. Pengaturan mengenai *roaming* dari esim adalah hal yang krusial karena menyentuh aspek keamanan. Di beberapa negara, misal Brazil, *permanent roaming* sudah dilarang. Solusi untuk *permanent roaming* misalnya esim masih kosong (tidak ada nomor yang dimasukkan), penerapan *Mobile Portability Number*, atau dengan esim *platform* yang bisa men-*swap* nomor asal dengan nomor lokal. Selain itu, pengaturan mengenai standardisasi perangkat dan Tingkat Komponen Dalam Negeri (TKDN) juga perlu mendapat perhatian untuk perlindungan industri dalam negeri.

Permasalahan terkait IoT yang diperoleh dari hasil wawancara dengan Kementerian/Lembaga, Pusat Riset, serta Pemerintah Daerah, poin pentingnya adalah diperlukan kerjasama antara Kementerian/Lembaga dalam pemanfaatan IoT secara nasional. Jika perlu, dapat merujuk pada pola koordinasi dalam membuat kebijakan mengenai *Indonesia Broadband Plan*. Pada dasarnya, Kementerian/Lembaga lain secara langsung/tidak langsung pasti akan membutuhkan IoT. Dengan demikian, diharapkan terdapat arahan terpadu yang dapat didukung secara bersama dalam pengembangan IoT di Indonesia. Pemerintah diharapkan memiliki satu tujuan yang dituangkan dalam *Roadmap* IoT Nasional. Dengan adanya panduan tersebut, secara tidak langsung pusat riset pemerintah melalui perguruan tinggi akan mengembangkan *prototype* yang mendukung kebutuhan *Roadmap* IoT Nasional.Hasil wawancara dengan Pemerintah Daerah menunjukkan secara umum Pemerintah Daerah sudah menggunakan IoT, minimal pada penggunaan *Closed-Circuit Television* (CCTV) untuk monitoring kota. Masalah mayoritas yang dihadapi saat ini terkait dengan penggunaan IoT adalah belum adanya *blueprint*/rencana pengembangan kota dengan memanfaatkan IoT. Rencana penggunaan IoT kedepannya adalah untuk mendukung implementasi *smart city.*

Hasil FGD

Informan yang hadir dalam FGD 1 adalah vendor telekomunikasi, operator telekomunikasi, dan perusahaan IoT dalam negeri. Usulan alternatif bentuk regulasi IoT yang dihasilkan pada kegiatan FGD 1 disajikan melalui Tabel 1.

Tabel 1. Hasil FGD 1 Terkait Alternatif Bentuk Regulasi IoT

Stakeholder	**Pilihan Alternatif**	**Catatan**
Perusahaan IoT A	Alternatif 3	
Perusahaan IoT A	Alternatif 3	
Vendor Telekomunikasi	Alternatif 2	Regulasi bersifat fasilitasi Less Regulation Khusus untuk data privasi Dukungan spektrum untuk kebutuhan IoT
Perusahaan IoT A	Alternatif 2	
Operator Telekomunikasi A	Alternatif 2	
Operator Telekomunikasi B	Alternatif 3	Dengan arahan yang jelas bagaimana kepastian pasar IoT untuk Indonesia
Operator Telekomunikasi C	Alternatif 2	Endorsment untuk pengembangan ekosistem IoT

Adapun usulan parameter yang perlu diatur dalam regulasi yang disarikan dari hasil FGD 1 dapat dilihat melalui Tabel 2.

Tabel 2. Usulan Parameter yang Perlu Diatur Dalam Regulasi

Aspek IoT	Usulan Parameter yang Perlu Diatur Dalam Regulasi
Standar Keamanan	a) Enkripsi data b) Keamanan data pribadi c) Keamanan *network* dan aplikasi
Standar Perangkat	a) Protokol IoT b) Standardisasi perangkat berdasarkan kategori c) TKDN perangkat IoT d) Keamanan perangkat IoT
Alokasi Spektrum	a) Akomodir teknologi LPWA e.g. LoRA b) Penambahan lebar *bandwidth* pada spektrum eksisting
Model Bisnis	a) Model bisnis IoT spesifik untuk pemerintah

Informan yang hadir dalam FGD 2 adalah empat CEO perusahaan IoT dalam negeri. FGD 2 menghasilkan daftar hambatan yang dihadapi oleh industri dalam negeri. Dalam sesi ini juga didiskusikan mengenai bentuk model bisnis yang spesifik khas dan hanya dilakukan oleh pelaku industri dalam negeri. Sebagian besar industri IoT lokal melakukan tipe bisnis IoT horizontal dikarenakan keterbatasan finansial.

Tabel 3. Data Olahan Prioritas Hambatan dan Parameter yang Diusulkan untuk Diregulasi

Prioritas	Hambatan	Usulan Parameter	
		Standar Perangkat	Standar Keamanan
1	Kesulitan untuk memenuhi syarat perijinan untuk memperoleh sertifikasi dalam negeri misal sertifikat TKDN atau SNI	TKDN Perangkat IoT	Keamanan Perangkat
2	Biaya produksi lebih murah jika beberapa step dilakukan di luar negeri (misalnya : produksi PCB di China jauh lebih murah dibanding dengan produksi di dalam negeri)	Protokol IoT	Keamanan *Network*
3	Harga komponen dalam negeri lebih mahal	*Platform* aplikasi IoT	Keamanan Transmisi
4	Belum tersedia SDM yang menguasai bidang IoT	Interoperabilitas antarperangkat	Enkripsi Data
5	Rendahnya tingkat kepercayaan pengguna terhadap produk dalam negeri		Manajemen Akses Data
6	Kesulitan untuk edukasi bidang IoT		Peletakan *server* dalam negeri
7	Adanya ketidakpastian pasar Indonesia		

Pembahasan

Tahap Definisi

Untuk mendefinisikan permasalahan terkait dengan kebutuhan regulasi IoT, dalam penelitian ini telah dilakukan pengumpulan data melalui proses *in-depth interview* dengan pihak-pihak terkait yaitu akademisi dan industri. Dari hasil pengumpulan data, diperoleh matriks permasalahan sesuai dengan batasan isu IoT dalam penelitian ini yang terdapat dalam Tabel 4.

Tabel 4. Matriks Definisi Permasalahan dari Akademisi dan Industri IoT

Isu Terkait dengan IoT	Akademisi	Industri IoT
Spektrum Frekuensi	a) Perlu dikaji lebih lanjut mengenai ketersediaan *bandwidth* saat ini apakah memadai untuk menumbuhkan ekosistem IoT di Indonesia b) Pemanfaatan pita frekuensi untuk IoT lebih baik mengacu pada standar global dengan tambahan kebijakan spesifik untuk penumbuhan ekosistem IoT	a) Kecukupan dari lebar *bandwidth* eksisting versus prediksi jumlah perangkat IoT di masa mendatang b) Pengaturan pemanfaatan pita–pita frekuensi yang boleh digunakan untuk teknologi konektivitas IoT yang tidak berlisensi (LPWAN)

Isu Terkait dengan IoT	Akademisi	Industri IoT
Standar Perangkat	a) Lebih baik mengacu pada standar teknis global untuk perangkat b) Identifikasi penggunaan IoT yang spesifik di Indonesia untuk membuat regulasi spesifik terkait dengan perangkat	a) Penggunaan standar *open* protokol untuk perangkat IoT
Standar Keamanan	a) Kebutuhan dasar yang paling penting dalam penerapan IoT adalah privasi (perlindungan data pribadi) b) Parameter lain yang berpotensi menimbulkan masalah adalah keamanan pada perangkat, keamanan pada saat transmisi data, dan keamanan di sisi penerima c) Belum ada standar untuk keamanan IoT d) Celah keamanan dari perangkat IoT dapat digunakan untuk menyebarkan *malware*. Hal ini menjadi ancaman bagi pengguna perangkat IoT. e) Aspek keamanan yang harus diperhatikan dalam penerapan IoT tergantung dari aplikasinya, seperti kesehatan yang penting adalah enkripsi data.	a) Terdapat perbedaan kebutuhan standar keamanan di setiap layer dalam ekosistem IoT. Harus jelas siapa yang menyediakan dan apa yang harus distandarkan terkait dengan keamanan di setiap layer
Model Bisnis	a) Perlu pemetaan di layer mana Indonesia mampu untuk berkompetisi. Jika melihat tren saat ini yang sedang berkembang pesat di Indonesia adalah sektor aplikasi, sehingga model bisnis *application provider* sepertinya akan paling cepat beradaptasi di era IoT	a) Ketidakpastian pasar di Indonesia menjadi permasalahan b) Secara umum, terdapat 2 pilihan model bisnis yaitu menjadi penyedia IoT vertikal (*end-to-end solution*) atau IoT horizontal c) Pengalaman dari salah satu industri menyatakan bahwa sangat berat untuk bermain model bisnis IoT vertikal di Indonesia karena belum ada dukungan ekosistem yang kuat, baik dari sisi produsen maupun konsumen
Ekosistem IoT (potensi IoT di Indonesia)	a) Sektor yang paling berpotensi untuk dikembangkan di Indonesia adalah Kesehatan dan Transportasi	a) Saat ini teknologi IoT masih belum *mature.* Hal tersebut bisa menjadi potensi bagus atau justru berdampak negatif bagi industri b) Kedepannya, diperkirakan aplikasi yang berbasis individu, *home automation*, retail *services* dan *smart city* yang akan banyak permintaan di Indonesia

Tahap Identifikasi Opsi Regulasi

Setelah diperoleh matriks permasalahan pada tahap definisi, tahap selanjutnya adalah menyusun opsi regulasi sebagai alternatif penyelesaian masalah. Dalam penelitian ini, didefinisikan tiga alternatif kondisi terkait dengan bentuk regulasi IoT. Pendefinisian opsi alternatif ini dianalisis secara kualitatif dengan menggunakan metode *benchmark* regulasi yang telah dilakukan oleh negara – negara lain.

a) India

1) India melalui MCIT of India telah merilis *Draft Policy on Internet of Things* tahun 2015 dengan tujuan meningkatkan industri IoT, mengembangkan sumber daya manusia IoT, mengembangkan *Research and Development*, dan produk khusus IoT. Program terkait pengembangan ekosistem IoT antara lain digital India dan *startup* India. Selain itu, *Department of Telecom* (DoT) menerbitkan *National Telecom* M2M *roadmap*, bertujuan mendorong pertumbuhan ekosistem M2M dan menumbuhkan keuntungan ekonomi dan sosial untuk pengguna, sektor bisnis, masyarakat, dan pemerintah.

Rekomendasi dari *Telecom Regulatory Authority* of India adalah :

1) Seluruh operator pemegang lisensi spektrum diperbolehkan menyediakan konektivitas M2M di dalam wilayah eksisting masing-masing.

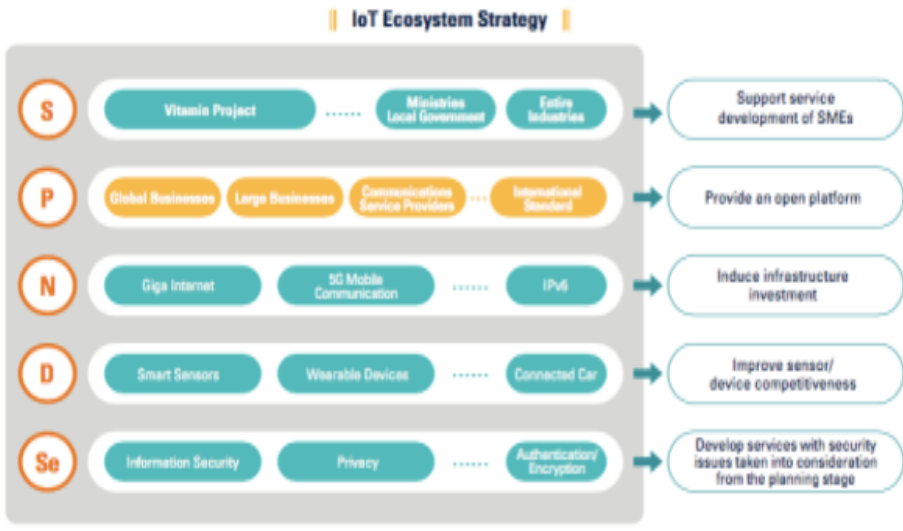
2) Seluruh pemegang lisensi layanan dasar dan lisensi *Internet Service Provider* (ISP) diperbolehkan menyediakan konektivitas M2M di dalam wilayah eksisting masing-masing.
3) *Connectivity provider* yang menggunakan teknologi *Wireless Personal Area Network* (WPAN)/ *Wireless Local Area Network* (WLAN) untuk konektivitas M2M komersil yang beroperasi di pita *unlicensed* harus mendaftar melalui DoT.
4) *Connectivity provider* yang menggunakan teknologi WPAN/WLAN yang beroperasi di pita *unlicensed*, lisensinya berada di bawah autorisasi baru di bawah *Unified Licensed* (UL) M2M.
5) Autorisasi UL tersebut dibagi 3: kategori A-wilayah nasional, kategori B-wilayah kota (metro), kategori C- wilayah distrik/kabupaten.
6) Layanan kritikal M2T hanya disediakan oleh penyedia konektivitas menggunakan *spectrum licensed*.
7) Koordinator M2M adalah DoT.
8) Pabrikan *device* IoT harus mengimplementasikan "*security by design*" sehingga menjamin enkripsi *end-to-end.*
9) Alokasi *spectrum* IoT harus merupakan layanan dan teknologi yang bersifat netral.
10) Tidak ada spektum yang dialokasikan secara ekslusif untuk layanan M2M.
11) Untuk memfasilitasi transisi layanan M2M menggunakan spektrum *license exempt*, 1 MHz dari pita 867-868 MHz dan 6 Mhz dari 915-935 MHz direkomendasikan untuk *delicense*.

Secara keseluruhan, langkah – langkah yang dilakukan Pemerintah India sebagai respon terhadap perkembangan teknologi IoT adalah 1) mendefinisikan national *interest*/kepentingan bangsa yang akan dicapai secara nasional (dapat dilihat pada dokumen *policy* of IoT), kemudian 2) menyesuaikan regulasi eksisting terhadap kebutuhan pengembangan IoT yang mendukung *national interest*.

b) Korea Selatan

Dalam dokumen *Master Plan for Building the Internet of Th*ings (IoT) (*Ministry of Science ICT and Future Planning - Ministries of the Republic of Korea*, 2014), Korea Selatan telah mendefinisikan visi, tujuan dan strategi nasional. Tujuan nasional Korea Selatan ditargetkan dalam nilai mata uang sehingga dapat diketahui berapa valuasi yang diinginkan dari teknologi ini. Strategi nasional disusun dalam beberapa tahapan yaitu

1) Tahap 1. Peningkatan kolaborasi di antara pelaku industri dalam ekosistem (*Service*, *Platform*, *Network*, *Device* dan *Security*). Dalam tahap ini, pemerintah akan berkolaborasi dengan pemain industri serta antarsektor pemerintah dalam pengembangan produk dan layanan IoT. Adapun strategi ekosistem IoT terdapat dalam Gambar 3.



Gambar 3. Strategi Ekosistem IoT

2) Tahap 2. Membuka inovasi sebesar-besarnya melalui mekanisme pergeseran dari ekosistem tertutup menjadi ekosistem terbuka. Maksud dari ekosistem terbuka adalah setiap orang dapat mengembangkan dan menyediakan layanan menggunakan *open platform* yang telah dikembangkan secara bersama-sama oleh pemerintah, *industry*, dan akademisi/lembaga riset. Dalam konteks inovasi terbuka, pemikiran/ide akan dikembangkan menjadi layanan/produk, membuat kondisi dimana potensi masing–masing individu dapat dimaksimalkan.
3) Tahap 3. Mengembangkan dan memperluas target pengguna layanan menuju pasar bebas melalui sistem kerjasama antara pemerintah dengan pihak swasta (pemain global) dalam memproduksi produk dan layanan IoT.
4) Tahap 4. Mengembangkan strategi untuk masing – masing skala bisnis, yaitu bisnis skala besar, *Small Medium-Sized Enterprises* (SME), dan *startup*. Pasar IoT dapat diklasifikasikan menjadi 1) pasar untuk *home electronics, automobiles*, dan *wearable devices* yang saat ini dipimpin oleh pemain global dalam skala besar, 2) pasar untuk *small-scale apps* yang dipimpin oleh SME dan 3) pasar yang dimotori oleh *startup*.

Sama halnya dengan langkah–langkah yang dilakukan oleh Pemerintah India, secara keseluruhan Pemerintah Korea Selatan mendefinisikan visi besar negara dan valuasi target yang akan dicapai kemudian strategi–strategi yang lebih spesifik untuk setiap target. Saat ini, belum diperoleh informasi selanjutnya mengenai regulasi–regulasi apakah yang mengalami perubahan untuk mengantisipasi perubahan teknologi.

c) Malaysia

Malaysia juga memiliki *roadmap* strategi nasional IoT yang disusun oleh Kementerian Sains, Teknologi, dan Inovasi. Dalam *roadmap* tersebut dijelaskan visi, misi, serta tujuan yang akan dicapai oleh negara Malaysia. Visi negara Malaysia dalam teknologi IoT ini adalah menjadi penghubung utama IoT di regional dengan misinya adalah menciptakan ekosistem IoT nasional untuk mendorong pertumbuhan IoT secara masif sebagai salah sumber pertumbuhan ekonomi baru. Strategi pencapaian visi dan misi disusun dalam tiga periode yaitu strategi jangka pendek, jangka menengah dan jangka panjang.

Berdasarkan *benchmark* regulasi terkait dengan IoT yang telah dilakukan oleh negara lain, maka alternatif yang diusulkan dalam penelitian ini adalah:

Alternatif 1. Status quo

Keadaan tetap yang berarti mempertahankan kondisi regulasi eksisting tanpa menambah dan atau mengurangi parameter – parameter regulasi saat ini.Keuntungan alternatif ini adalah tidak membutuhkan waktu untuk penyesuaian regulasi karena menggunakan mekanisme eksisting regulasi. Sedangkan kekurangannya antara lain kedepannya belum tentu dapat mengakomodir jumlah konektivitas perangkat dalam jumlah yang besar dan tidak ada kepastian regulasi, Indonesia mengikuti pasar teknologi yang mana

Alternatif 2. Perubahan pada regulasi eksisting

Kondisi ini didefinisikan dengan adanya perubahan pada regulasi yang berlaku saat ini sebagai contoh usulan perubahan pengunaan pita frekuensi ISM pada Peraturan Menteri Kominfo No. 35 Tahun 2015 tentang Persyaratan Teknis alat dan Perangkat Telekomunikasi Jarak Dekat. Perubahan tersebut diusulkan untuk mengakomodir teknologi *Low Power Wide Area* (LPWA).

(+) fleksibel terhadap isu terkait dengan teknologi IoT.

(-) membutuhkan waktu untuk penyesuaian regulasi.

(-) diperkirakan akan terjadi perubahan – perubahan regulasi tergantung dari tren teknologi IoT yang sedang berkembang.

Alternatif 3. Membuat regulasi khusus untuk *Internet of Things* (IoT)

Alternatif ketiga adalah membuat aturan khusus yang membuat regulasi seluruh aspek dari IoT (seperti yang diakukan oleh Korea Selatan yang mendefinisikan IoT sebagai layanan khusus seperti *mobile broadband* dan bukan aplikasi yang dapat beroperasi diatas layanan eksisting).

(+) *national interest* tergambar jelas dalam regulasi khusus IoT.
(+) arah dan target Indonesia dalam ekosistem IoT jelas.
(-) membutuhkan waktu yang lama untuk menyusun regulasi baru.
(-) ketinggalan dengan negara lain yang telah mengadopsi teknologi lebih dulu.

Pemilihan opsi alternatif tersebut sedikit berbeda dengan *benchmark* dari negara–negara yang sudah memiliki kebijakan nasional untuk IoT. Setelah mengidentifikasi opsi regulasi, ketiga opsi tersebut didiskusikan dalam FGD untuk dapat mengetahui opsi yang sesuai dengan ekosistem IoT di Indonesia. Dalam penelitian ini dilakukan dua kali proses FGD untuk mengetahui opsi regulasi serta parameter–parameter yang perlu diatur.

Berdasarkan FGD 1 dan 2 yang diselenggarakan dengan *stakeholder* industri baik itu industri IoT lokal maupun global, diperoleh hasil bahwa 50% mengusulkan bentuk regulasi sesuai dengan alternatif 2 dan sisanya adalah alternatif 3. *Stakeholder* industri IoT yang mengikuti proses FGD terdiri dari *device provider*, *network provider*, *platform provider*, *application provider*, serta *application customer*. Dari angka 50% tersebut, 40% nya adalah industri IoT lokal/dalam negeri. Hal tersebut menunjukkan bahwa industri IoT dalam negeri mengusulkan agar Indonesia memiliki regulasi khusus IoT. Opsi tersebut memiliki nilai positif antara lain arah Indonesia dalam IoT menjadi jelas dan merupakan salah satu alternatif untuk menumbuhkan ekosistem industri IoT dalam negeri.

Tahap Asesmen Opsi Regulasi

Setelah memperoleh opsi usulan bentuk regulasi melalui proses FGD, dalam tahap asesmen akan dianalisis BOCR secara kualitatif dari setiap opsi tersebut. Tabel 5 adalah matriks BOCR dari opsi regulasi 2 dan 3.

Tabel 5. Analisis BOCR Alternatif Opsi 2 dan 3

	Benefit	***Cost***	***Opportunity***	***Risk***
Alternatif Opsi 2 Perubahan pada regulasi eksisting	a) responsif terhadap perubahan teknologi utama maupun pendukung IoT b) membutuhkan waktu relatif lebih cepat untuk penyesuaian regulasi c) tidak ketinggalan dengan negara yang sudah mengadopsi	a) penyusunan regulasi	a) fleksibel terhadap perubahan teknologi b) memiliki momen yang tepat untuk terjun ke pasar (karena kurva teknologi IoT yang belum *mature*)	a) diperkirakan akan terjadi perubahan – perubahan regulasi tergantung dari tren teknologi IoT yang sedang berkembang b) ketidakpastian pasar c) margin keuntungan dibagi dengan banyak pemain d) industri IoT dalam negeri kurang dipersiapkan/dikondisikan untuk menghadapi kompetisi e) berpeluang besar untuk menjadi negara konsumen
Alternatif Opsi 3 Membuat regulasi khusus untuk *Internet of Things* (IoT)	a) arah/ *national interest* negara Indonesia dalam IoT jelas b) produsen IoT dalam negeri lebih siap untuk terjun dalam kompetisi pasar	a) penyusunan regulasi	a) dapat mendapatkan potensi ekonomi dari pasar IoT b) dapat menumbuhkan ekosistem industri IoT dalam negeri c) dapat melakukan mekanisme proteksi terhadap produksi dalam negeri	a) kurang cepat tanggap terhadap perubahan teknologi utama maupun pendukung IoT b) membutuhkan waktu lebih lama dalam penyusunan regulasi c) ketinggalan dengan negara-negara lain yang lebih dulu mengadopsi teknologi d) kompetisi menjadi berat

Parameter – Parameter yang Diusulkan untuk Masuk Dalam Regulasi

Berdasarkan matriks permasalahan yang telah diidentifikasi pada Tabel 5, selanjutnya dilakukan proses analisis terhadap poin–poin yang perlu untuk diregulasi. Beberapa parameter yang diusulkan industri untuk diregulasi terdapat dalam Tabel 6.

Tabel 6. Parameter yang Diusulkan untuk Masuk Dalam Regulasi

Isu terkait IoT	Usulan Parameter
Standar Keamanan	a) Keamanan perangkat b) Keamanan *network* c) Keamanan transmisi d) Enkrispsi data e) Peletakan *server* dalam negeri f) Keamanan data pribadi g) Manajemen akses data h) *Device management* (*device identity*, OTA *update*)
Standar Perangkat	a) TKDN perangkat IoT b) Protokol IoT c) *Platform* aplikasi IoT d) Interoperbilitas antarperangkat e) *Technologies for network layers*
Model Bisnis Penyelenggaraan	a) Perizinan penggunaan spektrum frekuensi untuk bisnis IoT
Lainnya (ekosistem IoT, kebutuhan spektrum, dll)	a) Alokasi spektrum khusus untuk aplikasi IoT b) Penambahan *bandwidth* eksisting untuk aplikasi IoT c) *National gateway* d) Penyelenggaraan edukasi (formal dan non formal) terkait IoT e) *Power*/daya perangkat IoT f) Dukungan berupa *makerspace* untuk menumbuhkan ekosistem IoT

Usulan Parameter–Parameter yang Diusulkan untuk Masuk Dalam Regulasi Versus Regulasi Eksisting

Setelah melakukan FGD mengenai usulan parameter–parameter yang diperlukan untuk masuk dalam regulasi, langkah berikutnya adalah mengidentifikasi produk regulasi Kementerian Komunikasi dan Informatika yang terkait dengan parameter tersebut. Tujuan dari tahapan ini adalah untuk memberikan masukan kepada direktorat teknis terkait mengenai perkiraan regulasi apa saja yang berpotensi dapat memenuhi tantangan teknologi IoT berdasarkan pandangan akademisi, praktisi, industri, dan regulator terkait (Kementerian, Lembaga dan Pemerintah Daerah yang diperkirakan memanfaatkan IoT kedepannya).

Tabel 7. Parameter yang Diusulkan Versus Regulasi Eksisting

Usulan Parameter yang Diregulasi	Regulasi Eksisting Kementerian Kominfo Terkait dengan Usulan Parameter
Standar Keamanan	
Perlindungan Data Pribadi Keamanan Data Manajemen Akses Data Tata Kelola Data	a) Permen Komifo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik b) Permen Kominfo No. 5 Tahun 2015 tentang Registrasi Nama Domain Instansi Penyelenggara Negara c) Permen Kominfo No. 26 Tahun 2015 tentang Pelaksanaan Penutupan Konten dan/atau Hak Akses Pengguna Pelanggaran Hak Cipta dan/atau Hak Terkait dalam Sistem Elektronik d) PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik e) Permen Kominfo No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi f) Permen Kominfo No. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif
Interoperabilitas Keamanan Transmisi Data Enkripsi Data	a) Permen Kominfo No. 7 Tahun 2013 tentang Pedoman Penerapan Interoperabilitas Dokumen Perkantoran Bagi Penyelenggara Sistem Elektronik Untuk Pelayanan Publik

Keamanan Jaringan Keamanan Konektivitas	a) Permen Kominfo No. 32 Tahun 2015 tentang Pengelolaan Nomor Protokol Internet b) Permen Kominfo No. 24 Tahun 2011 tentang Perubahan Ketiga atas Permen Kominfo No 26 Tahun 2007 tentang Pemanfatan Jaringan Telekomunikasi Berbasis Protokol Internet
Keamanan pada Aplikasi IoT	a) SE Menkominfo No. 3 Tahun 2016 tentang 2016 tentang Penyediaan Layanan Aplikasi dan / atau Konten melalui Internet (*Over The Top*)
Standar Perangkat	
TKDN Perangkat IoT	a) Permen Kominfo No. 27 Tahun 2015 tentang Persyaratan Teknis Alat dan Perangkat Telekomunikasi Berbasis Standar Teknologi *Long Term Evolution* b) Permen Kominfo No. 28 Tahun 2015 tentang Persyaratan Teknis Alat dan Perangkat Telekomunikasi yang Beroperasi pada Pita Frekuensi Radio 2,4 GHz dan/atau Pita Frekuensi Radio 5,8 GHz
Protokol Komunikasi yang Digunakan untuk Menghubungkan Perangkat ke *Platform* IoT	a) n/a
Sistem Otentifikasi Pada Perangkat IoT	a) n/a
Keamanan Pada Perangkat IoT	a) Permen Kominfo No. 11 Tahun 2017 tentang Tata Cara Pelaksanaan Uji Petik Alat dan/atau Perangkat Telekomunikasi
Standar Power / Daya yang Digunakan untuk Perangkat IoT	a) Permen Kominfo No. 23 Tahun 2016 tentang Sertifikasi Telekomunikasi Pesawat Telepon Seluler, Komputer Genggam dan Komputer Tablet b) Permen Kominfo No. 1 Tahun 2015 Perubahan atas Peraturan Menteri Komunikasi dan Informatika No. 18 Tahun 2014 tentang Sertifikasi Alat dan Perangkat Telekomunikasi c) Permen Kominfo No. 1 Tahun 2014 tentang Sertifikasi Alat dan Perangkat Telekomunikasi d) Permen Kominfo No. 35 Tahun 2015 tentang Persyaratan Teknis Alat dan Perangkat Telekomunikasi Jarak Dekat (*Short Range Devices*) e) Permen Kominfo No. 5 Tahun 2013 tentang Kelompok Alat dan Perangka Telekomunikasi
Model Bisnis	
Model Penyelenggaraan Bisnis IoT	a) Permen Kominfo No. 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik b) Permen Kominfo No. 7 Tahun 2015 tentang Perubahan Kedua atas Permen Kominfo No. 1 Tahun 2010 tentang Penyelenggaraan Jaringan Telekomunikasi c) SE Menkominfo No. 3 Tahun 2016 tentang 2016 tentang Penyediaan Layanan Aplikasi dan / atau Konten melalui Internet (*Over The Top*) d) SE Menkominfo No. 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia *Platform* dan Pedagang (*Merchant*) Perdagangan melalui Sistem Elektronik (*ElectronicCommerce*) yang Berbentuk *User Generated Content*
QoS Jaringan	a) Permen Kominfo No. 15 Tahun 2013 tentang Standar Kualitas Pelayanan Jasa Teleponi Dasar pada Jaringan Tetap Lokal b) Permen Kominfo No. 16 Tahun 2013 tentang Standar Kualitas Pelayanan Jasa Teleponi Dasar Pada Jaringan Bergerak Seluler
c) **Alokasi Spektrum Frekuensi**	
Alokasi Spektrum Khusus untuk Aplikasi IoT Penambahan *Bandwidth* Eksisting untuk Aplikasi IoT	a) PP No. 53 Tahun 2000 tentang Penggunaan Spektrum Frekuensi Radio dan Orbit Satelit

Perkembangan Regulasi IoT di Organisasi Internasional

Resolusi 938 (*World Radiocommunication Conferences*/WRC-15) menyatakan bahwa ITU-R masih melakukan studi terkait dengan aspek teknis dan operasional sistem radio dan jaringan serta spektrum yang dibutuhkan termasuk kemungkinan harmonisasi penggunaan spektrum baik untuk *narrowband* atau *broadband machine type communication* (MTC)/IoT. Perkembangan studi tersebut saat ini adalah mengeluarkan draft teks *Communications Processor Module* (CPM) yang mengidentifikasi spektrum untuk *mobile communications* (suara dan data) untuk *broadband* dan *narrowband* MTC/IoT berbasis *International Mobile Telecommunication* (IMT) yang sudah menjamin *Quality of Service* (QoS). Aplikasi dan perangkat MTC/IoT dapat menggunakan keuntungan secara efektif dari pita *mobile broadband* eksisting dan spektrum frekuensi IMT baru yang sedang dipelajari. Pendekatan tersebut menjauhi kemungkinan untuk identifikasi spektrum baru khusus (*dedicated spectrum*) untuk aplikasi MTC/IoT sehingga tidak diperlukan perubahan pada Radio *Regulation.*

Sementara itu, pada pertemuan *Asia-Pasific Telecommunity Conference Preparatory Group for WRC-19* (APG) 19-2 yang diselenggarakan di Bali pada tanggal 17–21 Juli 2017, menghasilkan keputusan bahwa negara–negara anggota APG mendukung studi yang telah terpublikasi dalam draft teks CPM yang menyatakan bahwa tidak akan ada perubahan pada *Radio Regulation*. Adapun pandangan dari beberapa organisasi lain terkait dengan MTC/IoT terdapat dalam Tabel 8.

Tabel 8. Pandangan Organisai Lain Terkait dengan MTC/IoT

Nama Organisasi	Pandangan Organisasi terkait dengan MTC/IoT
Arab *Spectrum Management Group* (ASMG)	Mendukung penggunaan harmonisasi pita frekuensi baik secara regional maupun global pada pita frekuensi IMT yang telah diidentifikasi untuk sistem dan aplikasi IoT.
The Inter-American Telecommunication Commission (CITEL)Brazil dan Canada	Mendukung studi draft teks CPM, yaitu menggunakan pita frekuensi eksisting tanpa pengubahan pada Radio *Regulation*.
Regional Commonwealth in The Field of Communication (RCC)	Mendukung studi draft teks CPM, yaitu menggunakan pita frekuensi eksisting tanpa pengubahan pada Radio *Regulation*, dengan penambahan harus ada justifikasi yang mempertimbangkan fitur dan prospek penggunaan teknologi IMT atau non-IMT.
European Conference of Postal and Telecommunications (CEPT)	Mendukung studi draft teks CPM, yaitu menggunakan pita frekuensi eksisting tanpa pengubahan pada Radio *Regulation*, dengan mempertimbangkan teknologi MTC/IoT berbasis non-IMT (di WP 1B dan 5A).
The International Amateur Radio Union (IARU)	Mendukung penggunaan spektrum untuk teknologi MTC/IoT karena perangkatnya biasanya akan digunakan secara bersama-sama dengan stasiun di layanan amatir sehingga diperkirakan akan ada masalah terkait penggunaan kedua layanan tersebut.

Model Bisnis dan Hambatan Industri IoT Dalam Negeri

Beberapa industri IoT dalam negeri memilih untuk menjadi industri IoT horizontal (yang tidak *end-to-end solution*) dikarenakan isu permodalan yang belum stabil. Berdasarkan hasil FGD 1 dan 2, rata–rata industri IoT dalam negeri bergerak sekaligus sebagai *device provider, platform provider, application provider* untuk industri yang basisnya memproduksi sebagian besar perangkat dan hanya sebagai *application provider* dan *application customer* untuk basis industri yang memproduksi *software*. Potensi industri IoT seharusnya dapat menjadi besar karena permasalahan yang terjadi di Indonesia lebih spesifik dan kompleks, misalnya solusi untuk pertanian di daerah Pulau Sumatera bisa jadi berbeda dengan Pulau Bali. Begitu juga dengan permasalahan perikanan yang berbeda–beda di setiap wilayah di Indonesia. Akan tetapi, hingga saat ini belum ada industri IoT lokal yang berani memberikan solusi vertikal (*end-to-end solution*) dari setiap permasalahan.

Pemanfaatan IoT Saat Ini dan Kedepannya dari Sudut Pandang Pemerintah Daerah

Selain menganalisis dari sudut pandang akademisi, praktisi, dan industri dalam penelitian ini juga dianalisis pemanfaaatan IoT dari sudut pandang pemerintah daerah. Alasan menganalisis dari sektor ini adalah berdasarkan program *smart city* yang saat ini sedang dicanangkan untuk diimplementasikan di seluruh wilayah kota/kabupaten di Indonesia. Tabel 9 menunjukkan matriks penggunaan IoT saat ini dan rencana kedepannya dari analisis terhadap data hasil *in-depth interview* dengan beberapa sampel pemerintah daerah di Indonesia.

Tabel 9. Matriks Penggunaan IoT Eksisting, Permasalahan yang Dihadapi, dan Rencana Pemanfaatan Selanjutnya

Isu	Catatan
Penggunaan IoT eksisting	a) Monitoring perkotaan seperti implementasi CCTV di beberapa lokasi dan beberapa sensor–sensor seperti sensor pengukur ketinggian level air, sensor kelembapan, sensor polusi udara. b) *Tracking* sistem untuk memberikan input data dalam sistem manajemen transportasi cerdas di perkotaan dan *tracking* untuk kendaraan dinas pemerintah daerah seperti alat berat, truk sampah, mobil satpol PP, ambulans, bus sekolah maupun bus umum (transjakarta/*busway*/damri). c) Aplikasi *panicbutton* yang sudah diimplementasikan di beberapa rumah yang dihuni lansia.
Permasalahan yang dihadapi saat ini terkait dengan IoT	a) Kesulitan koordinasi antar Satuan Kerja Perangkat Daerah (SKPD) terutama untuk pertukaran data dan standar keamanan data karena belum ada regulasi. b) Kurangnya sumber daya manusia yang menguasai bidang IoT. c) Antusiasme masyarakat terhadap penggunaan beberapa aplikasi di *smart city* masih rendah (belum pro aktif). d) Ketidakpastian pelaksananan program/*roadmap* IoT (dikhawatirkan ganti pemerintahan ganti fokus program, sehingga diharapkan jika ada acuan/pedoman secara nasional untuk pengembangan *smart city*).
Rencana Pemanfaatan IoT untuk *Smart City*	a) Pengembangan aplikasi berbasis IoT didasarkan pada prioritas permasalahan di setiap kota. Rata–rata fokus di kota besar adalah peningkatan sistem manajemen transportasi karena sistem pelayanan administrasi sudah berjalan dengan baik.

5. Simpulan dan Saran

Berdasarkan hasil analisis yang telah diuraikan pada bagian hasil penelitian dan pembahasan maka dapat disimpulkan beberapa hal tentang kebutuhan regulasi untuk implementasi IoT antara lain:

a) Regulasi mengenai teknologi IoT diperlukan dengan pendasaran bahwa teknologi merupakan *enabler* bagi pertumbuhan ekonomi lainnya;
b) Bentuk regulasi dapat berupa perubahan pada regulasi eksisting (alternatif 2) atau penyusunan regulasi spesifik mengenai IoT (alternatif 3); dan
c) Parameter yang dibutuhkan dalam regulasi terkait dengan IoT adalah:
    1) Dari spektrum frekuensi, dibutuhkan regulasi mengenai alokasi penggunaan spektrum yang diperbolehkan untuk IoT. Selain itu, dibutuhkan penambahan *bandwidth* (baik dalam spektrum berlisensi atau tidak) untuk mendukung pengembangan ekosistem di Indonesia;
    2) Model bisnis penyelenggaraan IoT tidak perlu diregulasi secara bentuknya. Poin yang perlu diregulasi adalah pemanfaatan penggunaan spektrum frekuensi untuk IoT;
    3) Parameter yang perlu diregulasi terkait dengan standar perangkat adalah TKDN perangkat IoT, protokol komunikasi yang digunakan untuk menghubungkan perangkat ke *platform* IoT, sistem otentifikasi pada perangkat IoT, dan keamanan pada perangkat IoT, dan standar power/daya yang digunakan untuk perangkat IoT;
    4) Terkait dengan standar keamanan, poin–poin yang perlu diregulasi adalah perlindungan data pribadi, keamanan data, manajemen akses data, tata kelola data, interoperabilitas, keamanan transmisi data, enkripsi data, keamanan jaringan, keamanan konektivitas, dan keamanan pada aplikasi IoT.

Adapun rekomendasi yang dapat disampaikan berdasarkan hasil penelitian antara lain:

a) Diperlukan kerjasama antar *stakeholder* untuk menyusun *Roadmap* IoT Indonesia sehingga dapat menentukan kepentingan nasional negara Indonesia dalam IoT. Perlu pendefinisan target apa yang akan dicapai (disertai dengan berapa nilai potensi ekonominya) dengan strategi yang spesifik untuk mencapai target tersebut;
b) Terkait dengan isu alokasi spektrum frekuensi untuk IoT, dalam *Working Party* 5D ITU masih dilakukan studi teknis terkait dengan teknologi–teknologi konektivitas IoT sehingga untuk saat ini tidak diperlukan adanya alokasi spektrum khusus (*dedicated spectrum*) untuk IoT dengan kondisi bahwa IoT merupakan aplikasi yang dapat beroperasi dalam layanan eksisting dan bukan merupakan layanan yang spesifik seperti satelit atau *mobile broadband.* Direkomendasikan untuk menentukan penambahan jumlah *bandwidth* (dengan besaran yang perlu dikaji lebih detail) pada spektrum frekuensi eksisting yang mendukung aplikasi IoT, baik itu spektrum berlisesnsi atau tidak berlisensi;
c) Dari sisi standar perangkat, direkomendasikan untuk mengkaji regulasi eksisting agar sesuai dengan teknologi IoT yang paling banyak digunakan di dunia. Selain itu, identifikasi/pemetaan sektor apa yang sangat berpotensi di Indonesia sehingga dapat menentukan standar yang spesifik khusus untuk perangkat yang beroperasi di Indonesia. Hal tersebut sebagai salah satu upaya untuk perlindungan produk IoT dalam negeri;
d) Dari sisi standar keamanan, dua hal yang sangat perlu untuk segera diregulasi di era IoT adalah privasi dan keamanan perangkat. Hingga saat ini belum ada standar keamanan yang spesifik terkait dengan perangkat IoT. Sementara dapat mengelaborasi standar ISO yang sudah ada;
e) Direkomendasikan untuk mengkaji kebijakan yang melindungi produksi industri IoT dalam negeri. Dari persyaratan TKDN misalnya belum ada konten "telematika" dalam penilaian untuk memperoleh sertifikat TKDN sehingga *firmware* (yang justru merupakan letak nilai originalitas dari sebuah inovasi teknologi) tidak mendapatkan poin penilaian yang lebih besar dibandingkan dengan persentase komponen elektronika;
f) Rata–rata industri IoT dalam negeri bergerak sebagai *device provider + platform provider + application provider* untuk industri yang basisnya memproduksi sebagian besar perangkat dan hanya *application provider + application customer* untuk basis industri yang memproduksi *software*.

6. Ucapan Terima Kasih

Terima kasih disampaikan kepada seluruh pihak yang membantu terselesaikannya tulisan ini di antaranya narasumber/informan atas masukannya untuk memperkaya materi, Tim Peneliti IoT Puslitbang SDPPPI, rekan-rekan yang membantu proses penelitian, serta Puslitbang SDPPPI sebagai fasilitator terlaksananya penelitian ini.

Daftar Pustaka

Accenture. (2017). Technology for People : The Era of the Intelligent Enterprise.

Jia, Xueqin; Jing, Wang; He, J. (n.d.). IoT Business Models and Extended Technical Requirements, *1*, 5–8.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy.

Meutia, E. D. (2015). Internet of Things – Keamanan dan Privasi.

Ministry of Science ICT and Future Planning - Ministries of the Republic of Korea. (2014). Master Plan for Building the Internet of Things (IoT).

Montresor, F. (2014). 14 Tech Predictions for our World in 2020.

Munich RE, E. (2016). *IT Trend Report 2016*.

Neill, M. O. (2016). Insecurity by Design : Today ' s IoT Device Security Problem. *Engineering*, *2*(1), 48–49. http://doi.org/10.1016/J.ENG.2016.01.014

OECD. (2008). Building an Institutional Framework for regulatory impact analysis (RIA), 77.

OFCOM. (2016). *VHF radio spectrum for the Internet of Things*.

Perera, C., & Liu, C. H. I. H. (2015). A Survey on Internet of Things From Industrial Market Perspective, *2*.

Pham, C. (n.d.). Towards Quality of Service for Long-range IoT in Unlicensed Radio Spectrum, 1–3.

Tiwary, A. (2015). *Digital India : IoT Spectrum Needs Report by IESA TiE IoT Forum*.

Wiener, J. B. (2004). The regulation of technology, and the technology of regulation. *Technology in Society*, *26*(2–3), 483–500. http://doi.org/10.1016/j.techsoc.2004.01.033

Xi, W. (2016). Research on IoT Privacy Security Risks. http://doi.org/10.1109/ICIICII.2016.80