Jurnal Bina Mulia Hukum
Volume 3, Nomor 1, September 2018 P-ISSN: 2528-7273 E-ISSN: 2540-9034
Artikel diterima 12 Agustus 2018, artikel direvisi 18 September 2018, artikel diterbitkan 28 September 2018
DOI: 10.23920/jbmh.v3n1.4 Halaman Publikasi: http://jurnal.fh.unpad.ac.id/index.php/jbmh/issue/archive

PEMBENTUKAN PRINSIP *JURISDICTION TO PREVENT* (*PRE-EMPTIVE JURISDICTION)* DAN PRINSIP PERLINDUNGAN AKTIF DALAM HUKUM SIBER

Purna Cita Nugraha*

ABSTRAK

Ruang siber telah mengubah cara masyarakat dalam berkomunikasi dan berinteraksi tanpa dibatasi oleh batas-batas negara. Dengan karakteristiknya yang transnasional, hingga saat ini masih sulit menemukan kesepahaman internasional dalam konsep pengaturan yang sesuai. Belum terdapatnya rezim internasional yang mengatur hal ini mengakibatkan munculnya ketidakpastian hukum dalam tataran pengaturan internasional dan nasional. Dalam rangka untuk mencari konsep yang sesuai dan tepat waktu untuk mengatur dunia maya yang menghadapi berbagai tantangan dan hambatan terkait dengan yurisdiksi antar negara, *Lex Informatica* telah memberikan para pembuat kebijakan suatu opsi dengan pengaturan teknis melalui teknologi yang dapat melampaui batas-batas masing-masing negara (*ekstrateritorial*). Kombinasi rezim hukum dan *Lex Informatica* akan menghasilkan prinsip-prinsip baru dalam mengatur dunia maya, seperti Prinsip Yurisdiksi untuk Mencegah dan Prinsip Perlindungan Aktif. Prinsip *jurisdiction to prevent (pre-emptive jurisdiction)* dan prinsip perlindungan aktif merupakan prinsip hukum utama yang dapat digunakan untuk mendukung konsepsi kedaulatan negara guna membentuk rezim *extraterritorial juridiction* dalam *cyberlaw* di Indonesia. Penelitian ini merupakan penelitian hukum yuridis normatif yang menitikberatkan penelitian pada ketentuan hukum yang berlaku. Penulis juga menggunakan metode pendekatan yuridis *futuristik* (hukum yang akan datang).

Kata kunci: *lex informatica*; prinsip; ruang siber.

ABSTRACT

Cyberspace has changed the way society interacts and communicates to each other withour border. Because of its transnational characteristics, up until today, it is still difficult to find international agremeent on the right and proper instrument to regulate cyberspace. The legal gap caused by the absence of international legal regime will in fact produce a legal uncertainty in the context of international and national regulation. In order to find the appropriate and timely concept to regulate cyberspace which are facing now multifacet challanges and obstacles regarding jurisdiction among States, the Lex Informatica has provided policy makers with technical arrangements through technology that can reach beyond each States' borders (extraterritorial). The combination of legal regime and the Lex Informatica will produce new principles in regulating cyberspace, such as the Principle of Jurisdiction to Prevent and the Principle of Active Protection. The Principle of Jurisdiction to Prevent and the Principle of Active Protection will become the

* Diplomat Indonesia, saat ini bertugas sebagai Sekretaris Kedua (Second Secretary) di Perutusan Tetap Republik Indonesia untuk PBB di New York, email: purna.cita@kemlu.go.id

main principles in supporting the concept of the state sovereignty in developing extraterritorial jurisdiction regime for cyberlaw in Indonesia. This researh is considered as a legal research focussing on examining existing rules and regulations and also considers legal futuristic research in nature in trying to find which legal instrument should be developed in the future".

***Keywords**: cyberspace; lex informatica; principle.*

PENDAHULUAN

Ruang siber meskipun sudah banyak yang mencoba untuk menemukan konsep pengaturan yang sesuai dan *timely,* namun kenyataannya masih susah untuk ditaklukkan. Perubahan terus-menerus, konvergensi teknologi informasi, dan konflik yurisdiksi menjadi beberapa kendala yang melatarbelakangi hal tersebut. Sebagai suatu realita, internet mengubah cara berkomunikasi yang konvensional menjadi suatu fenomena sosial dalam konteks ruang komunikasi publik, dunia baru bernama *cyberspace* dimana satu pihak dapat berkomunikasi tanpa dibatasi oleh batas-batas negara (*borderless*) atau *transnational*.

Beberapa peristiwa kongkrit yang terjadi misalnya fenomena *Arab Spring* di Timur Tengah yang dimulai dengan pergerakan di internet dengan menggunakan media sosial. Contoh peristiwa kongkrit lainnya adalah ketika *Newsweek* tiba-tiba menghentikan penerbitan versi cetaknya setelah selama 80 tahun lebih terbit secara cetak. Munculnya fenomena konvergensi media ini, memaksa media konvensional melebarkan sayap dan masuk ke dalam jaringan internet guna mempertahankan bisnisnya dan memperluas bisnisnya. Dengan pertimbangan tersebut, Newsweek kini hanya menerbitkan versi online dalam format *e-paper* atau *e-magazine* yang dapat diperoleh secara berlangganan.

Hal ini sesuai dengan pendapat yang dikemukakan Ahmad M. Ramli sebagai berikut:

> "*It can not be denied that the increased development and usage of information technology, media and communication have given some contributions which influence all aspects of life in the field of politics, economy, social and culture. Such contributions have also caused some impacts. The positive impact is to improve human welfare, while the negative impact is to make information technology, media and communication as an effective targets and instruments for cybercrimes*."[1]

Dari paparan di atas dijelaskan bahwa meningkatnya perkembangan dan penggunaan teknologi informasi merupakan sesuatu yang tidak dapat dihindari, komunikasi dan media telah memberikan sejumlah kontribusi yang mempengaruhi seluruh aspek kehidupan di bidang politik, ekonomi, sosial dan budaya. Kontribusi tersebut memiliki sejumlah dampak. Dampak positifnya adalah peningkatan kesejahteraan masyarakat, sementara dampak negatifnya adalah penggunaan teknologi informasi, komunikasi dan media sebagai suatu target empuk dan alat tindak pidana siber.

Lebih lanjut ditambahkan oleh Svetlana Anggita Prasasti sebagai berikut:

> "*Influence on society is not only social, cultural, institutional, economic or*

[1] Ahmad M. Ramli, "The Urgency of Ratification of Convention on Cybercrime", *Indonesia Law Journa*l Vol. 2 No. 2, National Law Development Agency, Mininstry of Law and Human Rights, Jakarta: 2007, hlm. 1.

> *political, but also technological. The internet's role in the societal system, having the ability to deviate from dominant structures, practices and actors within that system, also connects to a wider world. The internet today has developed to be public sphere ranging from individuals, organizations, companies, and member of the government services, including diplomats and other foreign service officials as such.*"[2]

Pengaruh pada masyarakat tidak hanya secara sosial, budaya, institusional, ekonomi, politik, tetapi juga secara teknologi. Peran internet dalam sistem kemasyarakatan, memiliki kemampuan untuk menyimpang dari aktor, praktik, dan struktur yang dominan pada sistem tersebut, juga menghubungkan pada sebuah dunia yang lebih luas. Internet sekarang ini telah berkembang menjadi ranah publik mulai dari individu, organisasi, perusahaan, dan pemerintah, termasuk diplomat dan pejabat dinas luar negeri lainnya.

Dunia siber pada kenyataannya masih sulit untuk dijinakkan. *Cyberspace* merupakan dunia virtual yang lokasinya tidak akan pernah kita temukan dalam Atlas, tetapi dapat dikunjungi oleh berjuta pengguna yang tersebar di seluruh dunia setiap saat. Karakteristik *ubiquitous* dan *borderless* ini mempengaruhi tindak pidana yang terjadi di dalamnya bahwa pada kenyataannya tindak pidana siber sering bersifat lintas negara sehingga menimbulkan pertanyaan mengenai yurisdiksi yang berlaku atas perbuatan atau akibat tindak pidana serta atas pelakunya. Banyak negara termasuk Indonesia, telah menyadari keterbatasan perundang-undangan konvensionalnya untuk menjawab permasalahan ini sehingga memandang perlu untuk menyesuaikan hukumnya untuk tetap menjaga kedaulatan negara serta kepentingan negara dan warganya.[3]

Salah satu terobosan dalam pengaturan hukum siber adalah pendekatan prinsip yurisdiksi ekstrateritorial (*extraterritorial jurisdiction*). Hal dimaksud dikarenakan tidak serta merta dapat diterapkannya yurisdiksi teritorial dalam kegiatan di cyberspace yang sering kali terjadi dalam teritorial beberapa negara sekaligus. Perdekatan prinsip yurisdiksi ekstrateritorial merupakan upaya untuk dimungkinkannya penerapan Hukum Teknologi Informasi (*Cyberlaw*).[4]

Prinsip yurisdiksi ekstrateritorial dalam hukum nasional dimuat dalam Pasal 2 Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal tersebut menjelaskan bahwa UU ITE memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas teritorial atau universal.[5]

---

[2] Svetlana Anggita Prasasti, "Developing Indonesia's Digital Diplomacy Strategy" *Jurnal Diplomas*i Vol.5 No.1, Jakarta, 2013, hlm. 95.

[3] Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, PT. Tata Nusa, Jakarta: 2012, hlm. 136.

[4] Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran, dan Teknologi Informasi (Regulasi dan Konvergensi)*, Refika Aditama, Bandung: 2010, hlm. 136.

[5] *Ibid.*

Sehubungan dengan hal tersebut di atas, perlu kiranya melihat dan memahami prinsip-prinsip hukum apa yang dapat digunakan untuk mendukung konsepsi kedaulatan negara untuk membentuk rezim *extraterritorial juridiction* dalam *cyberlaw* di Indonesia. Hal ini berkaitan dengan perlunya pemahaman yang sama di antara negara-negara sehingga nantinya dimungkinkan suatu proses harmonisasi dan sinkronisasi peraturan. Harmonisasi dan sinkronisasi peraturan dibutuhkan guna mengatasi hambatan kedaulatan negara ke luar khususnya yang menyangkut dengan penerapan prinsip *extrateritorial jurisdiction* kepada negara lain. Dalam konteks ini misalnya, prinsip yurisdiksi ekstrateritorial dalam Pasal 2 UU ITE tidak dapat dilaksanakan sepenuhnya karena suatu negara pada kenyataannya tidak dapat melaksanakan kekuasaannya di wilayah negara lain walaupun mempunyai yurisdiksi atas suatu perbuatan hukum tersebut.

Dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang 2005-2025 telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus memanfaatkan ilmu pengetahuan dan teknologi. Salah satunya dengan pemanfaatan *e-commerce* dan peraturan-peraturan yang mengaturnya termasuk melalui peraturan yang terkait dengan privasi.[6] Dengan demikian Pemerintah Indonesia dituntut untuk mewujudkannya dengan *legal policy* (politik hukum) yang tepat dan sesuai guna mewujudkan tujuan yang terdapat dalam Rencana Pembangunan Jangka Panjang tersebut.

Disamping itu sebagai salah satu anggota masyarakat internasional, Indonesia harus menyesuaikan peraturan perundang-undangannya dengan perkembangan internasional yang dewasa ini telah banyak diatur sehingga diperlukan adanya harmonisasi pengaturan antara Indonesia dengan negara lain yang selanjutnya akan menciptakan suatu kepastian hukum bagi pengguna yang akan mendorong pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik khususnya perkembangan dan kemajuan industri *e-commerce* di Indonesia.[7]

Berdasarkan uraian dalam latar belakang, masalah yang hendak dikaji adalah prinsip-prinsip hukum apa yang dapat digunakan untuk mendukung konsepsi kedaulatan negara untuk membentuk rezim *extraterritorial juridiction* dalam *cyberlaw* di Indonesia

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yuridis normatif yang menitikberatkan penelitian pada ketentuan hukum yang berlaku yang mencakup penelitian terhadap asas-asas dan prinsip-prinsip hukum, sistematika hukum, sinkronisasi hukum dalam merumuskan politik hukum untuk membentuk rezim *extraterritorial jurisdiction* dalam *cyberlaw* dan kaitannya terhadap konsepsi kedaulatan Negara.

Spesifikasi atau sifat dari penelitian ini adalah eksploratif analitis, yaitu menjelaskan atau menggambarkan sesuatu yang belum ada dalam hal ini berusaha menganalisis hukum apa yang seyogianya diciptakan untuk masa datang berdasarkan ketentuan hukum dan

---

[6] Shinta Dewi, *Cyberlaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasiona*l, Widya Padjadjaran, Bandung: 2009, hlm. 6.

[7] *Ibid.*

perundang-undangan dihubungkan dengan teori-teori hukum dan hukum positif yang berlaku yang terkait dengan politik hukum pembentukan rezim *extraterritorial jurisdiction* dalam *cyberlaw* dan kaitannya dengan konsepsi Negara yang berdaulat.

Penelitian ini dilakukan terhadap kepustakaan (*library research*), Penulis juga menggunakan metode pendekatan yuridis komparatif, yaitu studi perbandingan hukum yang dilakukan dengan membandingkan antara sistem hukum Indonesia dengan sistem hukum Negara lain dalam kaitannya dengan politik hukum dalam pembentukan rezim extraterritorial jurisdiction dalam cyberlaw dan kaitannya dengan konsepsi kedaulatan Negara. Selain itu, dilakukan juga studi banding terhadap peraturan perundang-undangan nasional dan peraturan teknis terkait antara Indonesia dan Negara-Negara lain yang berkaitan langsung dengan politik hukum pembentukan rezim *extraterritorial jurisdiction* dalam *cyberlaw* dan kaitannya dengan konsepsi kedaulatan Negara.

Penelitian ini berusaha untuk mencari cara bagaimana suatu peraturan atau pranata hukum dapat menyelesaikan suatu masalah sosial atau ekonomi, atau bagaimana suatu pranata hukum atau pengaturan suatu pranata sosial atau ekonomi dapat menghasilkan prilaku yang diinginkan. Metode penelitian perbandingan hukum fungsional digunakan untuk mencari jawaban mengenai bagaimana hukum mengatur suatu hubungan atau masalah sosial. Namun demikian, metode ini juga dipakai untuk meneliti *the existing national law in its day to day practice, and the law in action* dari setiap sistem atau pranata atau kaidah hukum yang akan dibandingkan.[8] Akhirnya dari penelitian ini bertujuan untuk meneliti mengenai hukum apa yang seyogianya diciptakan untuk masa datang yaitu untuk menyusun suatu peraturan perundang-undangan atau untuk menyusun kebijakan baru di bidang hukum khususnya di bidang *cyberlaw,* dan menyusun suatu rencana pembangunan hukum. Oleh karena itu, Penulis juga menggunakan metode pendekatan yuridis futuristik (hukum yang akan datang).[9]

PEMBAHASAN

Masyarakat Informasi memiliki permasalahan-permasalahan yurisdiksi yang penting, hal ini dikarenakan aktivitas-aktivitas di internet dapat dilakukan pada media yang bersifat transnasional. Untuk rezim hukum, banyak otoritas nasional dan pembuat kebijakan mempunyai klaim yang sah untuk mengatur pengguna dan arus informasi. Akan tetapi, sifat dasar dari karakter jaringan membuat klaim tersebut tunduk pada keputusan-keputusan pemilihan hukum yang kompleks. Negara-Negara pada umumnya enggan untuk memberlakukan hukumnya pada aktivitas-aktivitas yang dilakukan di yurisdiksi asing. Oleh karena itu, yurisdiksi menjadi suatu hambatan yang kritis bagi pembuatan kebijakan informasi yang tepat. Hal tersebut dapat dilihat dari paparan sebagai berikut:

> "T*he Information Society poses important jurisdictional issues. Network activities may take place on a transnational basis. For the legal regime, various national authorities and policymakers may make legitimate claims to regulate users and information flows. However, the very*

[8] Sunaryati Hartono, *Penelitian Hukum di Indonesia pada Akhir Abad ke-20*, PT. Alumni, Bandung: 2006, hlm. 171.
[9] *Ibid*, hlm. 146.

nature of network behavior makes these claims subject to complex choice of law decisions. States are generally reluctant to impose their laws on activities taking place in foreign jurisdictions. Consequently, jurisdiction becomes a critical threshold obstacle to sensible information policymaking."[10]

Dalam hal ini yurisdiksi *Lex Informatica* adalah jaringan itu sendiri. Aturan-aturan teknologi dilaksanakan berlaku di seluruh jaringan yang relevan. Dengan demikian, *Lex Informatica* dapat lintas batas dan tidak menghadapi yurisdiksi yang sama, masalah pilihan hukum yang rezim hukum hadapi ketika jaringan melewati garis yurisdiksi teritorial atau negara. *Lex Informatica* menghadapi konflik aturan di gerbang antar jaringan. Jika standar teknologi di kedua sisi *gateway interoperable*, arus informasi dapat melewati *gateway* tanpa kesulitan. Ketika standar tidak kompatibel, arus akan terhambat oleh perbedaan dalam spesifikasi teknis. Sebagai contoh, modul perangkat lunak yang didesain untuk sistem operasi satu komputer biasanya tidak dapat berfungsi pada sistem operasi lain. Namun, suatu masalah hukum yang timbul dari suatu rezim hukum memaksa untuk memilih satu hukum yang diberlakukan, sementara kedua perangkat aturan teknis yang tidak kompatibel dapat diterapkan melalui penggunaan terjemahan dan konversi. Pada contoh sistem operasi, program *software* didesain untuk menerjemahkan standar antara sistem operasi komputer. Fitur dualitas ini memungkinkan fleksibilitas dalam mengakomodasi banyak pilihan aturan kebijakan informasi secara simultan.

Formulasi aturan teknis untuk akses informasi juga dapat menghindari risiko kewajiban yang dikenakan oleh aturan-aturan hukum yang saling bertentangan dan dapat menawarkan solusi bagi masalah *self-censorship* yang didorong oleh regulasi konten yang bertentangan. Kebijakan teknologi menawarkan aturan substantif dalam *Lex Informatica* yang menggeser persoalan dari penyensoran, atau pemblokiran distribusi, menjadi filterisasi penerimaan informasi. Pergeseran ini memungkinkan aturan yang berbeda untuk berlaku untuk penerima yang berbeda. Keputusan kebijakan tentang penerimaan informasi dapat dilakukan pada berbagai tingkatan. Penerima sendiri dapat memiliki kewenangan/otoritas untuk membuat keputusan tentang konten informasi. Suatu komputer tertentu dapat dikonfigurasi dengan aturan *filtering* tersendiri. Sebuah jaringan area lokal mungkin memiliki aturan kebijakan jaringan yang luas, sedangkan penyedia jasa/ layanan informasi dapat mengadopsi berbagai sistem aturan tertentu. Semua Penyedia Jasa Internet di negara tertentu bahkan mungkin memiliki kebijakan filter yang sama. Fleksibilitas ini dan penekanan pada penerimaan berarti bahwa aturan yang unik tidak diperlukan untuk distribusi global informasi karena distributor dalam satu yurisdiksi tidak perlu bertentangan dengan norma-norma yurisdiksi lain.

Respon teknis dan solusi untuk konflik kebijakan menunjukkan cara-cara baru untuk menetapkan aturan arus informasi. Pembuat kebijakan biasanya, meskipun selalu mengaitkannya dengan elaborasi dan pembuatan hukum melalui proses politik di dalam dan di antara negara-negara. Aturan yang

[10] Joel R. Reidenberg, Lex Informatica: "The Formulation of Information Policy Rules Through Technology" , *Tax Law Review,* Volume 76, Number 3, 1998, hlm. 572-573.

ditetapkan dengan motode ini membentuk rezim peraturan hukum konvensional (tradisional). Dalam konteks arus informasi pada jaringan, solusi teknis mulai menggambarkan bahwa teknologi jaringan itu sendiri memaksakan aturan untuk akses dan penggunaan informasi. Arsitektur teknologi dapat melarang tindakan tertentu pada jaringan, seperti akses tanpa izin, atau mungkin mewajibkan arus tertentu, dan data routing alamat wajib untuk pesan elektronik (*mandatory address routing data for electronic messages*). Teknologi mungkin juga menawarkan pilihan kebijakan aturan arus informasi melalui keputusan konfigurasi. Akibatnya, seperangkat aturan teknis yang mewajibkan informasi mengalir melalui sistem teknologi dan konfigurasi baku menawarkan dua jenis aturan substantif: 1) kebijakan baku yang terdapat dalam standar teknologi yang tidak dapat diubah; dan 2) kebijakan yang fleksibel terdapat dalam arsitektur teknis yang memungkinkan variasi pada pengaturan baku.

Lex Informatica memiliki sejumlah fitur bersifat analog yang membedakannya dengan peraturan hukum dan mendukung perannya sebagai sistem aturan yang penting bagi Masyarakat Informasi. Pada dasarnya, pilihan kebijakan yang tersedia baik melalui teknologi itu sendiri, melalui hukum/undang-undang yang menyebabkan teknologi untuk mengecualikan kemungkinan opsi, atau melalui undang-undang yang menyebabkan pengguna untuk membatasi tindakan-tindakan tertentu. Kebijakan teknologi informasi khusus yang menetapkan aturan arus informasi menunjukkan pentingnya *Lex Informatica* sebagai sistem aturan yang bersifat paralel.

Lex Informatica merupakan aturan teknis yang berasal atau didesain sedemikian rupa dari jaringan teknologi sebagai suatu sumber yang berbeda dari pembuatan aturan di bidang arus informasi (*distinct source of information flow rule-making*) harus mulai dilihat oleh para pembuat kebijakan dalam membuat kebijakan-kebijakan di masa depan khususnya kebijakan yang terkait dengan pembentukan rezim *extraterritorial jurisdiction* yang terkendala dengan yurisdiksi asing atau negara lain. *Lex Informatica* merupakan suatu alternatif bagaimana Negara-Negara dapat mengatasi masalah yurisdiksi tersebut menggunakan solusi-solusi dan respon-respon teknis dengan menggunakan teknologi.

Keuntungan dan dampak dari *Lex Informatica* merefleksikan hubungan yang bersinggungan antara *Lex Informatica* dan hukum. *Lex Informatica* dapat berkerja untuk memaksa kemampuan hukum untuk mengatasi suatu masalah. *Lex Informatica* juga dapat menggantikan hukum ketika aturan-aturan teknis/teknologi lebih baik untuk menyelesaikan masalah-masalah kebijakan. Sebagai contoh, *Lex Informatica* dapat menawarkan solusi filterisasi konten (*content filtering*) daripada pilihan kebijakan sensor (*distribution censorship*).

Tentu saja dengan segala kelebihannya, *Lex Informatica* juga membutuhkan peran hukum konvensional pada pelaksanaannya. Hukum dalam hal ini dapat menjatuhkan sanksi bagi penghindaran/pelanggaran *Lex Informatica*. Sebagai ilustrasi, apabila aturan baku dari kebijakan informasi diterobos, maka hukum dapat masuk untuk memulihkan pelanggaran ini dengan memaksakan sanksi. Sebagai contoh, hukum tentang tindak pidana siber dapat mengatasi masalah dengan pihak ketiga yang membuat mekanisme untuk merusak mekanisme filterisasi yang dilekatkan ke dalam *web browsers*.

Lebih jauh lagi, hukum dapat saja digunakan untuk mendorong pengembangan *Lex Informatica* dengan mewajibkan berbagai pemangku kepentingan, dan mungkin saja kedepannya kebijakan hukum dapat memberikan imunitas bagi pelaksanaan aturan-aturan teknis. Sebagai contoh, dalam kasus data personal dan aturan-aturan privasi secara internasional, sebuah situs yang selalu dilaporkan atas aktivitasnya harus tunduk pada klaim-klaim penipuan baik secara pidana maupun perdata, tapi bagi situs yang dilabeli dan disertifikasi oleh pihak ketiga yang terakreditasi dapat menikmati praduga bahwa mereka telah sesuai dan melaksanakan standar internasional.

Di sisi lain, hukum juga dapat membuat pendekatan pengaturan aktivitas dan tingkah laku. Hal ini feasible dilakukan dengan pendekatan pengaturan tingkah laku (*the regulated-behavior approach*). Pendekatan ini akan memberikan stimulus atau rangsangan yang signifikan secara tidak langsung bagi pembentukan norma dari *Lex Informatica*. Dalam hal ini, Pemerintah dapat menuntut dan melarang kegiatan-kegiatan tertentu seperti pendistribusian pornografi atau transaksi uang secara eletronik yang tidak sah. Aturan tingkah laku ini dapat mengarahkan *Lex Informatica* untuk memastikan cara-cara yang sesuai dengan praktik yang berlaku. Aturan-aturan teknis tersebut dapat menjadi pijakan terhadap jaminan tersebut. Terkait dengan *regulated-behavior approach*, Lawrence Lessig menyatakan bahwa:

> "*regulability is the capacity of a government to regulate behavior within its proper reach. In the context of the Internet, that means the ability of the government to regulate the behavior of (at least) its citizens while on the Net*."[11]

Hal tersebut di atas berarti bahwa regulability adalah kemampuan suatu Pemerintah untuk mengatur perilaku/tingkah laku sesuai dengan jangkauannya. Dalam konteks internet, hal itu berarti kemampuan pemerintah untuk mengatur/meregulasi tata prilaku (paling tidak) warga negaranya ketika beraktifitas di internet.

Para pembuat kebijakan juga dapat mengatur mengenai standar-standar teknis tertentu. Sebagai contoh, Pemerintah Indonesia dapat membuat pengaturan bebas sadap (*wiretap safe*) terhadap alat-alat dan sistem komunikasi Kepala Negara untuk urusan pemerintahan/resmi dan menghindari penyadapan dari Negara lain. Sedangkan untuk kepentingan penegakan hukum, Pemerintah dapat mewajibkan bahwa industri harus memastikan bahwa alat-alat komunikasi yang didistribusikan kepada masyarakat umum harus dapat disadap (*wiretap ready*) dan tentunya penyadapan harus dilakukan berdasarkan hukum atau undang-undang.

Dari segi penegakan hukum, *Lex Informatica* mempunyai alat penegakan yang berbeda. Peraturan hukum konvensional bergantung hanya kepada para penegak hukum. Para pelanggar hukum akan diproses ke pengadilan setelah perbuatannya dilakukan (*on an ex post basis*). Sedangkan *Lex Informatica* menawarkan penegakan hukum secara otomatis (*automated*) dan eksekusi mandiri (*self-executing*) sebelum perbuatan dilakukan (*ex ante measures*). Aturan-aturan teknis dapat saja didesain sedemikian rupa untuk mencegah

[11] Lawrence Lessig, *Code Version 2.0*., Basic Books, New Yor:, 2006, hlm. 23.

pelanggaran ataupun kejahatan terjadi tanpa izin terlebih dahulu secara resmi. Hal tersebut di atas dapat dilihat dari paparan sebagai berikut:

> "*Lex Informatica has distinct enforcement properties. Legal regulation depends primarily on judicial authorities for rule enforcement. Rule violations are pursued on an ex post basis before the courts. Lex Informatica, however, allows for automated and self-executing rule enforcement. Technological standards may be designed to prevent actions from taking place without the proper permissions or authority*."[12]

Sebagai contoh dari penegakan hukum secara otomatis (*automated*) dan eksekusi mandiri (*self-executing*) sebelum perbuatan dilakukan (*ex ante measures*) dapat implementasikan dengan pemblokiran transaksi jika ternyata *credentials* dari pelaku transaksi tidak terverifikasi dengan benar. Sistem manajemen transaksi dapat mengecek keaslian dari kunci kriptografik (*cryptographic key*) sebelum membolehkan permrosesan transaksi, melakukan verifikasi bahwa pemegang password tersebut memenuhi kriteria dalam melakukan transaksi tersebut. Sistem manajemen transaksi dapat mengecek validitas dari *password* bagi perintah pembayaran secara elektronik dan memverifikasi bahwa *password* tersebut dimiliki oleh petugas korporasi yang berwenang untuk mengeluarkan perintah pembayaran tersebut. Apabila *password* tersebut salah atau pemegang *password* tersebut tidak memiliki kewenangan yang membolehkan perintah pembayaran, sistem manajemen transaksi dapat memblokir transaksi tersebut. Proses pencegahan ini (*ex ante measures*) dimungkinkan pelaksanaannya menggunakan kemampuan dalam memproses informasi.

Paparan-paparan tersebut di atas melahirkan pemikiran bahwa kedepannya baik rezim hukum dan *Lex Informatica* dapat saling melengkapi dalam melakukan proses pencegahan (*ex ante process*) terutama terhadap pelanggaran atau tindak pidana siber. Pemikiran tersebut dapat melahirkan suatu konsep yurisdiksi baru selain dari *jurisdiction to prescribe, jurisdiction to enforce*, dan *jurisdiction to adjudicate* yang disebut dengan Prinsip *Jurisdiction to Prevent (Pre-Emptive Jurisdiction)* yaitu yurisdiksi untuk melakukan tindakan pencegahan secara hukum dengan menggunakan arsitektur teknis/teknologi.

Pada tataran konsepsi, rezim hukum dapat memberikan kewenangan bagi para ahli teknologi untuk mengembangkan standar-standar teknis yang ditujukan untuk mencegah terjadinya pelanggaran atau tindak pidana siber, kemudian hukum juga dapat memberikan kewenangan bagi Penyedia Jasa Internet *(Internet Service Providers/ISP)* dan pihak ketiga yang terkait yang memfasilitasi penggunaan internet untuk melakukan "pencegahan hukum" secara otomatis (*automated*) dan eksekusi mandiri (*self-executing*) sebelum perbuatan dilakukan (*ex ante measures*).

Sebagai contoh, untuk menanggulangi atau mengantisipasi kejahatan terhadap kartu kredit, Pemerintah membentuk suatu peraturan nasional yang mewajibkan para pelaku perbankan untuk memperkuat sistem elektronik kartu kreditnya (pengaturan teknis di serahkan kepada masing-masing bank). Hal ini tentunya dapat memberikan stimulus atau rangsangan secara signifikan bahkan

[12] Joel R. Reidenberg, *Op. Cit*., hlm. 568.

memaksa dunia perbankan dan ahli teknologi sistem perbankan untuk pembentukan dan pengembangan norma dari *Lex Informatica* atau aturan-aturan teknis tertentu guna memperkuat sistem elektronik *credit card*-nya.

Dalam kasus pelarangan konten pornografi misalnya, pemerintah mengingatkan peraturan yang mewajibkan ISP untuk melakukan filterisasi terhadap konten-konten pornografi yang diakses oleh pelanggannya. Pada praktiknya, hal ini sudah lama diterapkan oleh Pemerintah Indonesia. Pemerintah RI c.q. Kementerian Komunikasi dan Informatika RI (Kominfo) dalam kasus filterisasi konten pornografi di tahun 2010 mengingatkan ISP terhadap kewajibannya untuk patuh (*comply*) dengan peraturan perundangan yang ada dalam memberikan layanan mereka. Kominfo melalui Surat Edaran No. 1598/SE/DJPT.1/KOMINFO/7/2010 tanggal 21 Juli 2010 yang ditujukan terhadap Penyelenggara Jasa Akses Internet (*Internet Service Provider*) dan Penyelenggara Jasa Interkoneksi Internet (*Network Access Point*) yang ada di Indonesia, mengingatkan agar semua ISP dan NAP di Indonesia agar mematuhi peraturan perundang-undangan yang terkait dengan pornografi seperti Pasal 21 UU No. 36 Tahun 1999 tentang Telekomunikasi, Pasal 27 Ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dan Pasal 4 Ayat (1) dan Pasal 7 UU No. 44 Tahun 2008 tentang Pornografi.[13]

Surat Edaran tersebut juga menyebutkan mengenai kewajiban ISP dan Penyelenggara Jasa Interkoneksi Internet (*Network Access Point*) terkait pengamanan jaringan yang tertuang dalam izin penyelenggaraan telekomunikasi, sebagai berikut:

> "...wajib mengikuti ketentuan-ketentuan peraturan yang terkait dengan usaha-usaha untuk menjaga keamanan internet, termasuk penyamaan setting waktu (clock synchronizer), menjaga gangguan hacking, spamming, pornografi."[14]

Surat Edaran tersebut akhirnya melahirkan suatu kebijakan filterisasi yang disebut Trust Positive yang diterapkan hingga kini oleh semua ISP dan NAP di Indonesia. Pada langkah awal, Kementerian Komunikasi dan Informatika menyediakan daftar informasi sehat yang dapat diunduh di http://www.trustpositif.kominfo.go.id. Informasi ini berfungsi sebagai filter terhadap konten-konten yang tidak sesuai dengan nilai-nilai etika, moral, dan kaedah-kaedah Bangsa Indonesia.[15]

Sebagai langkah selanjutnya, Kominfo bekerja sama dengan ahli teknologi kemudian mengembangkan suatu aplikasi yang disebut dengan TRUS+™ Positif. Pada implementasinya, aplikasi ini memanfaatkan penggabungan antara 2 (dua) aplikasi, yaitu Proxy/Caching System dipadu dengan Content Filtering System yang terdiri dari Squid-Cache sebagai *Proxy/Caching System* dan *SquidGuard* sebagai *Content Filtering System*[16]. Cara kerja dari TRUS+™ Positif dapat dilihat dari bagan di bawah ini:[17]

---

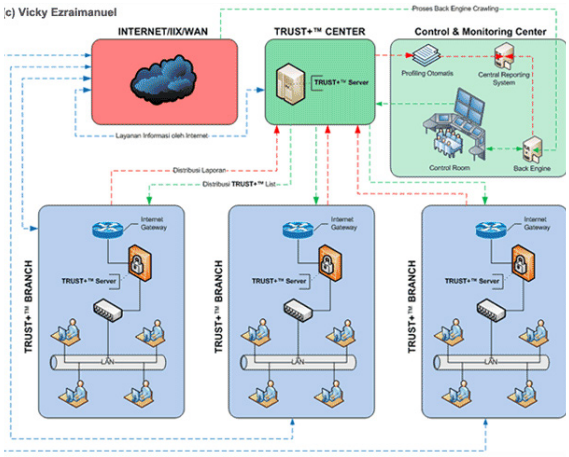
[13] Surat Edaran No. 1598/SE/DJPT.1/KOMINFO/7/2010 tanggal 21 Juli 2010 tentang Kepatuhan Terhadap Peraturan Perundang-Undangan yang terkait dengan Pornografi.

[14] Lihat juga Surat Edaran No. 1598/SE/DJPT.1/KOMINFO/7/2010 tanggal 21 Juli 2010 tentang Kepatuhan Terhadap Peraturan Perundang-Undangan yang terkait dengan Pornografi, hlm. 2.

[15] Surat Edaran Menteri Komunikasi dan Informatika Nomor: 03/SE/M.KOMINFO/10/2010 mengenai Penggunaan Internet Sehat dan Aman di Instansi Pemerintah.

[16] Paket Aplikasi dan Panduan Teknis TRUS+™ Positif, http://trustpositif.kominfo.go.id/, diakses tanggal 13 Desember 2013.

[17] *Ibid.*



Aplikasi TRUS+™ Positif bertujuan untuk: 1) menciptakan internet yang aman dan sehat dengan perlindungan terhadap akses internet berdasarkan daftar informasi sehat dan terpercaya (TRUST+™ List); 2) perlindungan pada masyarakat terhadap nilai-nilai etika, moral, dan kaedah-kaedah yang tidak sesuai dengan citra bangsa Indonesia; 3) penghematan terhadap pemborosan penggunaan akses internet (internet utilization) di Indonesia.[18]

Aplikasi TRUS+™ Positif ini juga digunakan semua ISP dan NAP di Indonesia untuk: 1) memberikan perlindungan terhadap *Top-Level Domain*; 2) memberikan perlindungan terhadap URL; 3) memberikan perlindungan terhadap konten. Sistem TRUS+™ Positif menerapkan mekanisme kerja adanya *server* pusat yang akan menjadi acuan dan rujukan kepada seluruh layanan akses informasi publik (fasilitas bersama), serta menerima informasi-informasi dari fasilitas akses informasi publik untuk menjadi alat analisa dan *profiling* penggunaan internet di Indonesia.[19] Khusus untuk masalah konten pronografi, TRUS+™ Positif berfungsi sebagai *filter* bagi ISP dan NAP bagi segala aktivitas yang dilakukan oleh pelanggan jasa internetnya untuk mengakses konten-konten yang berbau pornografi.

Pendekatan yang hampir sama dilakukan Amerika Serikat dengan menetapkan hukum federal *U.S. Children's Online Privacy Protection Act of 1998* (COPPA) yang berlaku efektif tanggal 21 April 2000.[20] Undang-undang ini berlaku untuk pengumpulan informasi online secara pribadi oleh orang atau badan di bawah yurisdiksi AS dari anak di bawah usia 13 (tiga belas) tahun. Undang-undang ini mengatur bahwa operator *website* harus menyertakan kebijakan privasi, kapan dan bagaimana untuk meminta verifikasi persetujuan dari orang tua atau wali, dan mengatur apa tanggung jawab operator dalam melindungi privasi dan keamanan *online* anak-anak termasuk pembatasan pada pemasaran untuk mereka yang di bawah (13 tiga belas) tahun. Undang-undang ini juga mengatur mengenai anak-anak di bawah 13 (tiga belas) tahun yang secara legal dapat memberikan informasi pribadi dengan izin orang tua mereka, hal ini mengakibatkan banyak situs yang sama sekali melarang anak di bawah umur menggunakan layanan mereka karena akan menambah pekerjaan mereka.

Secara umum, prinsip *jurisdiction to prevent* (yurisdiksi pencegahan) akan menyelesaikan permasalahan yurisdiksi yang selama ini menghambat penerapan asas yurisdiksi ekstraterritorial ketika berhadap-hadapan dengan yurisdiksi asing atau Negara lain. Hal ini karena *Lex Informatica* mempunyai

---

[18] *Ibid.*

[19] *Ibid*.

[20] Jonathan L. Zittrain, *The Future of the Internet and How to Stop It, Yale University Press Haven and London*, United Stated of America: 2008, hlm. 232.

paralel jurisdiction yaitu jaringan (*networks*) yang lintas batas dan sifat eksekusi mandiri (*self-executing*) dan otomatisasi (*automated*) dari *Lex Informatica* yang bersifat ekstraterritorial. Sebagai ilustrasi dari sifat ekstrateritorial *Lex Informatica*, terhadap implikasi dari bentuk filterisasi konten pornografi di atas, pelanggan dari ISP di Indonesia tidak akan dapat membuka atau mengakses konten pornografi perusahaan *adult industries* yang *servernya* terdapat di Los Angeles, Amerika Serikat.

Menurut penulis, *prinsip jurisdiction to prevent* (yurisdiksi pencegahan) ini dapat diterapkan dengan mengaplikasikan tautannya dengan prinsip yurisdiksi teritorial (*subjective territorial jurisdiction* dan *objective territorial jurisdiction*) yang juga diatur dalam *The Tallinn Manual*. Prinsip *jurisdiction to prevent* (yurisdiksi pencegahan) ini dapat juga diterapkan dengan memperhatikan: a) prinsip nasionalitas/kewarganegaraan pelaku tindak pidana (pihak yang aktif); b) prinsip nasionalitas/ kewarganegaraan dari korban (pihak penderita); c) ancaman terhadap keamanan nasional dari Negara (prinsip perlindungan/proteksi); dan d) pelanggaran terhadap norma internasional, seperti kejahatan perang (yurisdiksi universal).

Prinsip hukum lain yang dapat digunakan untuk mendukung konsepsi kedaulatan negara untuk membentuk rezim *extraterritorial jurisdiction* dalam *cyberlaw* di Indonesia adalah prinsip/asas perlindungan. Prinsip Perlindungan adalah prinsip yang digunakan untuk menerapkan yurisdiksi suatu negara berdasarkan perlindungan kepentingan negara yang bersifat vital seperti keamanan dan integritas atau kepentingan ekonomi negara. Berdasarkan prinsip ini negara memiliki yurisdiksi terhadap orang asing yang melakukan tindak pidana di luar wilayah negara tersebut dan mengancam keamanan dan keutuhan negara yang bersangkutan.[21] Prinsip ini merupakan prinsip yurisdiksi yang sudah mapan dan diterima masyarakat internasional, walaupun dalam praktik tidak ada kepastian sejauh mana prinsip perlindungan digunakan khususnya mengenai perbuatan-perbuatan apa saja yang termasuk di dalam yurisdiksi yang dituntut.[22]

Menurut Starke, terdapat 2 (dua) alasan untuk menerapkan yurisdiksi berdasarkan prinsip perlindungan adalah: 1) akibat yang ditimbulkan oleh tindak pidana tersebut sangat besar bagi negara; 2) apabila yurisdiksi negara tersebut tidak dilaksanakan terhadap tindak pidana maka pelaku tindak pidana dapat lolos dari peradilan pidana karena di negara tempat perbuatan pidana dilakukan (locus delicti) perbuatan tersebut bukan merupakan tindak pidana atau ekstradisi akan ditolak dengan alasan tindak pidana politik.[23]

Berdasarkan prinsip perlindungan setiap negara mempunyai kewenangan untuk melaksanakan yurisdiksi terhadap tindak pidana yang menyangkut keamanan dan integritas atau kepentingan ekonomi yang vital[24]. Pasal 4 sub1, sub 2, dan sub 3 KUHP memberlakukan yurisdiksi ekstrateritorial dengan berdasarkan prinsip

---

[21] Sigid Suseno, *Implikasi Yurisdiksi Terhadap Tindak Pidana Siber Berdasarkan Peraturan Perundang-Undangan Indonesia Dihubungkan dengan Konvensi Dewan Eropa 2001*, Disertasi, Program Doktor Ilmu Hukum pada Pascasarjana Universitas Padjadjaran, Bandung, 2011, hlm. 107.

[22] *Ibid.*

[23] J.G. Starke, *Pengantar Hukum Internasional,* Sinar Grafika, Jakarta: 2004, hlm. 304.

[24] *Ibid*, hlm. 303-304.

perlindungan yaitu hukum pidana berlaku terhadap pelaku tindak pidana yang berada di luar wilayah Indonesia yang melakukan tindak pidana-tindak pidana tertentu yang merugikan kepentingan-kepentingan Indonesia. Tindak pidana tersebut meliputi: tindak pidana terhadap keamanan negara (Pasal 104, Pasal 106, Pasal 107, Pasal 108, Pasal 110, Pasal 111 bis ke-1, Pasal 127), tindak pidana terhadap Presiden dan Wakil Presiden (pasal 131), tindak pidana mata uang, materai, merek yang dikeluarkan/digunakan Pemerintah Indonesia, pemalsuan surat hutang atau sertifikat hutang atau tanggungan Indonesia/daerah Indonesia.[25]

Prinsip perlindungan juga terkandung pada Pasal 2 UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, sebagai berikut:

> "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia."[26]

Pada penjelasan Pasal 2 UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik disebutkan bahwa Undang-Undang ini memberikan pengertian "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.[27]

Prinsip Perlindungan dalam Pasal 2 UU ITE terkandung dalam rumusan "di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia". Prinsip perlindungan dalam ketentuan ini lebih luas dari yurisdiksi perlindungan dalam KUHP dan prinsip perlindungan pada umumnya yaitu melindungi kepentingan vital suatu negara.[28]

Konvensi Dewan Eropa 2001 tentang Tindak Pidana Siber tidak menggunakan prinsip perlindungan (*protective principle*) untuk melaksanakan yurisdiksi ekstra-territorial terhadap tindak pidana siber. Prinsip perlindungan sesungguhnya relevan digunakan untuk perlindungan satelit. Negara-Negara yang menempatkan satelit di orbit untuk komunikasi global memerlukan perlindungan baik terhadap propertinya maupun teknologinya dari setiap tindak pidana[29], namun berdasarkan ketentuan dari Pasal 22 Ayat (4) Konvensi Dewan Eropa 2001 tentang Tindak Pidana Siber, Negara Pihak dimungkinkan untuk menentukan yurisdiksi kriminal yang sesuai dengan legislasi hukum nasionalnya. Pada intinya, ketentuan yurisdiksi yang terdapat dalam Konvensi Dewan Eropa 2001 tentang Tindak Pidana Siber tidak meniadakan yurisdiksi kriminal yang telah diterapkan Negara Pihak dalam hukum nasionalnya. Pasal 22 Ayat (3) Konvensi Dewan Eropa tersebut menyatakan sebagai berikut:

> "*This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*"

---

[25] Sigid Suseno, *Op. Cit,* hlm. 18-19.

[26] Lihat Pasal 2 Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[27] Lihat Penjelasan Pasal 2 Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[28] Sigid Suseno, *Yurisdiksi terhadap Tindak Pidana Siber dalam Perundang-Undangan Indonesia Dihubungkan dengan Konvensi Dewan Eropa*, dalam Yudha Bhakti, *et. al, Penemuan Hukum Nasional dan Internasional*, Fikahati Aneska, Jakarta: 2012, hlm. 542.

[29] Sigid Suseno, *Op. Cit*, hlm. 414.

Untuk itu terkait dengan masalah prinsip perlindungan ini, Sigid Suseno menyarankan agar prinsip perlindungan diperluas termasuk "kepentingan kepentingan vital negara lainnya" dan tidak terbatas hanya pada kepentingan kepala negara dan keuangan atau ekonomi negara serta tindak pidana yang dilakukan di dalam yurisdiksi negara lain tetapi juga untuk "tindak pidana yang dilakukan di luar yurisdiksi teritorial negara manapun".[30]

Mengingat sifat dari dunia siber yang transnasional dan *borderless,* tentu saja akan terjadi *overlapping claim* atas yurisdiksi khususnya yurisdiksi dengan menggunakan prinsip perlindungan. Hal ini terjadi karena lebih dari satu Negara Pihak mengklaim punya kepentingan yang harus dilindungi dan memiliki yurisdiksi hukum terhadap tindak pidana siber. Untuk itu, perlu kiranya mempertimbangkan yurisdiksi *Lex Informatica* untuk menyelesaikan masalah ini.

Penerapan yurisdiksi *Lex Informatica* ini didasarkan pada perbedaannya dengan yurisdiksi hukum konvensional. Yurisdiksi hukum utamanya didasarkan pada wilayah. Hukum konvensional/tradisional dapat diberlakukan hanya pada tempat yang nyata-nyata dapat ditentukan dimana kedaulatan dapat melaksanakan kekuasaannya. Sebaliknya, yurisdiksi dari *Lex Informatica* adalah jaringan (*networks*) sehingga dapat menembus batas-batas secara fisik (*transnasional*). Oleh karena itu, prinsip perlindungan melalui *Lex Informatica* dapat diterapkan secara aktif berdasarkan *jurisdiction to prevent*.

Prinsip perlindungan pada Pasal 2 UU ITE dalam rumusan "di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia" mengandung "prinsip perlindungan pasif". Hal ini dikarenakan penerapan prinsip tersebut didasarkan pada perbuatan/tindak pidana yang sudah terjadi (*on an ex post basis*) sehingga sifatnya pasif. Sedangkan *Lex Informatica* menawarkan penerapan "prinsip perlindungan aktif" secara otomatis (*automated*) dan eksekusi mandiri (*self-executing*) sebelum perbuatan dilakukan (*ex ante measures*). Sebagai ilustrasi dari prinsip perlindungan aktif, Pemerintah Indonesia dapat membuat suatu standar khusus baik secara aturan maupun standar teknis untuk melindungi komunikasi resmi kepala negara atau dalam hal ini Presiden RI.

Langkah pembentukan prinsip perlindungan aktif tersebut dapat dimulai dengan dibentuknya peraturan tertentu yang akan merangsang dikembangkannya teknologi tertentu yang bersifat bebas sadap (*wiretap-safe*) dari pelaku industri dan ahli teknologi. Hal ini terlihat dari paparan sebagai berikut:

> "*First, the government can use its bully pulpit to cajole and threaten the ICT industry to develop technical rules and new technology. In the context of wiretapping, government must encourage the industry to provide encryption technologies for official state use. Second, the government should work with standarization bodies to develop a standart operating procedure for communications. The govenrment can work with stakeholders from the industry and technology developers to define the standart. Third, the government can encourage the development of particular technological capabilities, such as a wiretap-safe technology, using public*

[30] *Ibid*, hlm. 545.

funds and realized under public sector procurement".[31]

Dari paparan di atas diketahui bahwa dalam pembentukan prinsip perlindungan aktif terhadap komunikasi Presiden RI dari tindak pidana, dapat diterapkan 3 (tiga) hal, yaitu: 1) Pemerintah dapat menggunakan pengaruh dan kekuasaannya untuk memaksa industri TIK untuk mengembangkan aturan-aturan teknis dan teknologi baru. Dalam konteks penyadapan, Pemerintah harus mendorong industri untuk menyediakan teknologi terenkripsi untuk penggunaan negara secara resmi; 2) Pemerintah harus bekerja sama dengan badan standarisasi, industri, dan pengembang teknologi untuk mengembangkan suatu SOP dalam berkomunikasi bagi Kepala Negara; 3) Pemerintah dapat mendorong pengembangan kapasitas teknologi tertentu seperti teknologi bebas-sadap dengan menggunakan mekanisme pengadaan Pemerintah.

Prinsip perlindungan aktif ini juga tersirat dalam Surat Edaran No. 1598/SE/DJPT.1/KOMINFO/7/2010 tanggal 21 Juli 2010 tentang Kepatuhan Terhadap Peraturan Perundang-Undangan yang terkait dengan Pornografi, sebagai berikut:

> "*dalam rangka memberikan kepastian hukum dan* ***perlindungan bagi warga negara dari pornografi****, para penyelenggara Jasa Akses Internet (Internet Service Provider) dan Penyelenggara Jasa Interkoneksi (Network Access Point/NAP) agar memenuhi kewajiban dan tidak melakukan pelanggaran terhadap ketentuan-ketentuan sebagaimana tersebut di atas, serta* ***secara aktif menerapkan program Internet Sehat***."

Prinsip perlindungan aktif ini juga terkandung secara tegas dalam Reservasi Indonesia pada *Final Acts ITU of the Plenipotentiary Conference* (Guadalajara, 2010) yang diratifikasi oleh Indonesia melalui Peraturan Presiden Nomor 5 Tahun 2012, sebagai berikut:

> "*The Government of the Republic of Indonesia does hereby reserve as follows: a)* ***the right to take any action and preservation measures*** *it deems necessary to safe guard its national interests should any provision of the Constitution, the Convention and the Resolutions, as well as any decision of the Plenipotentiary Conference of the ITU (Guadalajara, 2010), directly or indirectly affect its sovereignty or be in contrantion to the Constitution, Laws and Regulations of the Republic of Indonesia as well as the existing rights acquired by the Republic of Indonesia as a party to other treaties and conventions and any principles of international law; and b)* ***the right to take any action and preservation measures*** *it deems necessary to safeguard its national interests should any Member in any way fail to comply with the provisions of the Constitution and the Convention of the International Telecommunication Union (Guadalajara, 2010) or should the consequences of reservations by any Member jeopardize its telecommunication services or result in an unacceptable increase of its contibutory share towards defraying expenses of the Union*."[32]

---

[31] Purna Cita Nugraha, *London's Wiretapping: How Should We Respond?*, Artikel yang ditulis di Jakarta Post, tanggal 2 Agustus 2013.

[32] Lihat Lampiran Peraturan Presiden Republik Indonesia Nomor 5 Tahun 2012 tentang Pengesahan Final Acts of the Plenipotentiary

Dari paparan di atas dapat diketahui bahwa Pemerintah Indonesia mensyaratkan bahwa: a) memiliki hak untuk mengambil tindakan apapun dan langkah-langkah pencegahan/penjagaan yang dinilai perlu untuk mengamankan kepentingan nasionalnya apabila ada ketentuan dari Konstitusi, Konvensi dan Resolusi, maupun keputusan apapun dari Konferensi Yang Berkuasa Penuh Itu secara langsung atau tidak langsung mempengaruhi kedaulatannya atan bertentangan dengan Konstitusi, Hukum dan Aturan Republik Indonesia maupun hak-hak yang ada yang diperoleh oleh Republik Indonesia sebagai kelompok dari traktat-traktat dan konvensi-konvensi-konvensi serta prinsip-prinsip hukum internasional apapun lainnya; dan b) memiliki hak untuk mengambil tindakan apapun dan langkah-langkah pencegahan/penjagaan yang dinilai perlu untuk mengamankan kepentingan nasionalnya apabila ada Anggota dengan cara apapun gagal memenuhi ketentuan-ketentuan dalam Konstitusi dan Konvensi Perhimpunan Telekomunikasi Internasional (Guadalajara, 2010) atau apabila konsekuensi pensyaratan-pensyaratan pada Anggotan manapun membahayakan layanan-layanan telekomunikasinya atau mengakibatkan kenaikan saham kontribusi untuk pembayaran biaya-biaya Perhimpunan yang tidak dapat diterima.

Dalam reservasi tersebut di atas, Pemerintah Indonesia menegaskan bahwa Indonesia memiliki hak untuk mengambil tindakan apapun dan langkah-langkah pencegahan/penjagaan yang dinilai perlu untuk mengamankan kepentingan nasionalnya. Sehubungan dengan ini, tindakan dan langkah-langkah pencegahan/penjagaan tersebut dapat berarti perlindungan secara aktif *(on ex ante basis)* ataupun perlindungan secara pasif *(on ex post basis).* Bentuk reservasi Indonesia pada *Final Acts ITU of the Plenipotentiary Conference* (Guadalajara, 2010) tersebut merupakan *legal policy* yang hingga saat ini masih diberlakukan. Politik hukum untuk mereservasi *Final Acts* tersebut sudah dilakukan sejak Indonesia menandatangani dan meratifikasi *Final Acts ITU of the Plenipotentiary Conference* (1994), Minneapolis (1998), Marrakesh (2002), dan Antalya (2006).[33]

Dalam tataran konsepsi, prinsip perlindungan aktif merupakan prinsip kombinasi antara rezim hukum dan Lex Informatica yang diterapkan secara otomatis (*automated*) dan eksekusi mandiri (*self-executing*) sebelum perbuatan dilakukan (*ex ante measures*) berdasarkan pertimbangan perlindungan kepentingan negara yang meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Berdasarkan prinsip ini negara memiliki yurisdiksi ekstrateritorial untuk mencegah orang/pihak asing yang melakukan tindak pidana di luar wilayah negara tersebut dan mengancam keamanan dan keutuhan negara yang bersangkutan dengan menerapkan aturan-aturan teknis/teknologi.

Conference, Guadalajara, 2010 (Akta-Akta Akhir Konferensi yang Berkuasa Penuh, Guadalajara, 2010), R*eservation to the Amendment of the Constitution and Convention as A Result of the Plenipotentiary Conference*, Guadalajara, 2010.

[33] Lihat Piagam Pengesahan No. 02/HI/01/2012/IR tanggal 26 Januari 2012.

Syarat untuk menerapkan prinsip perlindungan aktif ini dapat dilaksanakan dengan mengaktualisasikan konsep Starke dalam konteks kekinian, yaitu dengan melihat 2 (dua) alasan untuk menerapkan yurisdiksi berdasarkan prinsip perlindungan aktif adalah: 1) akibat yang ditimbulkan oleh tindak pidana tersebut sangat besar bagi negara; 2) apabila yurisdiksi dalam jaringan pada pihak asing/ Negara lain tersebut tidak dilaksanakan.

PENUTUP

Prinsip *jurisdiction to prevent (pre-emptive jurisdiction)* dan prinsip perlindungan aktif merupakan prinsip hukum utama yang dapat digunakan untuk mendukung konsepsi kedaulatan negara guna membentuk rezim *extraterritorial juridiction* dalam *cyberlaw* di Indonesia. Prinsip-prinsip ini dapat dibentuk dengan mengkombinasikan rezim hukum dengan *Lex Informatica* sehingga tercipta hubungan yang saling mengisi (substitusi) dan melengkapi (komplementer). Rezim yurisdiksi ektrateritorial yang akan dibentuk di masa depan juga akan bersifat lebih aktif, responsif, dan *pre-emptive.*

DAFTAR PUSTAKA

Buku

Ahmad M. Ramli, *Cyberlaw dan HAKI dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung: 2006.

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran, dan Teknologi Informasi (Regulasi dan Konvergensi),* Refika Aditama, Bandung: 2010.

Darrel C. Menthe, J*urisdiction in Cyberspace: A Theory of International Spaces*, 4 Mich, Telecomm. Tech. L. Rev. 69 (1998).

Jonathan L. Zittrain, The Future of the Internet and How to Stop It, Yale University Press Haven and London, United Stated of America: 2008.

Josua Sitompul, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, PT. Tata Nusa, Jakarta: 2012.

J.G. Starke, *Pengantar Hukum Internasional,* Sinar Grafika, Jakarta: 2004.

Lawrence Lessig, *Code Version 2.0.*, Basic Books, New York: 2006.

Shinta Dewi, *Cyberlaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional,* Widya Padjadjaran, Bandung: 2009.

Sunaryati Hartono, *Penelitian Hukum di Indonesia pada Akhir Abad ke-20*, PT. Alumni, Bandung: 2006.

Yudha Bhakti, *et. al, Penemuan Hukum Nasional dan Internasional*, Fikahati Aneska, Jakarta: 2012.

Jurnal

Amit M. Sachdeva, "International Jurisdiction in Cyberspace: A Comparative Perspective", C.T.L.R., Issue8, 2007.

Ahmad M. Ramli, "The Urgency of Ratification of Convention on Cybercrime", *Indonesia Law Journal* Vol. 2 No. 2, National Law Development Agency, Mininstry of Law and Human Rights, Jakarta, 2007.

Joel R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Tax Law Review*, Volume 76, Number 3, 1998.

Samuel F. Miller, "Prescriptive Jurisdiction over Internet Activity: The Need to Define and Establish the Boundaries of Cyberliberty", Indiana University School of Law, Digital Repository @Maurer Law, I*ndiana Journal of Global Legal Studies*, Volume 2, Issue 2, 2003.

Svetlana Anggita Prasasti, "Developing Indonesia's Digital Diplomacy Strategy", *Jurnal Diplomasi* Vol.5 No.1, Jakarta, 2013.

Peraturan Perundang-undangan

Peraturan Presiden Republik Indonesia Nomor 5 Tahun 2012 tentang Pengesahan *Final Acts of the Plenipotentiary Conference*, Guadalajara, 2010 (Akta-Akta Akhir Konferensi yang Berkuasa Penuh, Guadalajara, 2010).

Convention on Cybercrime 2001.

Tallinn Manual on the International Law Applicable to Cyber Warfare 2012.

Sumber Lain

Paket Aplikasi dan Panduan Teknis TRUS+™ Positif, http://trustpositif.kominfo.go.id/, diakses tanggal 13 Desember 2013.

Piagam Pengesahan No. 02/HI/01/2012/IR tanggal 26 Januari 2012.

Purna Cita Nugraha, *London's Wiretapping: How Should We Respond?*, Artikel yang ditulis di Jakarta Post, tanggal 2 Agustus 2013.

Surat Edaran No. 1598/SE/DJPT.1/ KOMINFO/7/2010 tanggal 21 Juli 2010 tentang Kepatuhan Terhadap Peraturan Perundang-Undangan yang terkait dengan Pornografi.

Surat Edaran Menteri Komunikasi dan Informatika Nomor: 03/SE/M. KOMINFO/10/2010 mengenai Penggunaan Internet Sehat dan Aman di Instansi Pemerintah.

Purna Cita Nugraha, *Penyelesaian Sengketa Electronic Commerce melalui Online Dispute Resolution dan Penerapannya di Indonesia*, Tesis pada Program Pascasarjana Ilmu Hukum, Magister Hukum BKU Hukum Bisnis, Universitas Padjadjaran, Bandung, 2010.

Sigid Suseno, *Implikasi Yurisdiksi Terhadap Tindak Pidana Siber Berdasarkan Peraturan Perundang-Undangan Indonesia Dihubungkan dengan Konvensi Dewan Eropa 2001*, Disertasi, Program Doktor Ilmu Hukum pada Pascasarjana Universitas Padjadjaran, Bandung, 2011.