PENGATURAN CYBERSCURITY SEBAGAI BAGIAN DARI PEMENUHAN HAK ASASI MANUSIA

[1]Lutfiadi, [2]Win Yuli Wardani, [3]Febrina Heryanti, [4]Mahfud
[1,2,3)] Dosen Fakultas Hukum Universitas Madura
[4)] Mahasiswa Fakultas Hukum Universitas Madura

lutfiadi@unira.ac.id

Abstrak

Konfrontasi di dunia cyber tidak hanya berdampak pada individu, ekonomi, namun juga terhadap kedaulatan suatu negara dan stabilitas global. cyberwarfare merupakan ancaman serius. Ini juga menjadi medan perang intelijen dan meliter. Cyberspace menyediakan ruang dan sarana untuk baik mengancam ataupun melindungi warga negara dan negara itu sendiri. Untuk menghadapi tantangan itu, negara di seluruh dunia gencar mencari tahu untuk bisa memahmi secara pasti berbagai dampak dari kemajuan teknologi ini yang kemudian bermuara pada kebijakan-kebijakan regulasinya. Indonesia salah satu negara yang dikategorikan negara yang rentan akan cybercrime. Indonesia juga masih belum mempunyai payung hukum khusus mengenai cyber scurity. negara harus ikut andil dalam menangkal serangan siber bergandeng tangan dengan swasta yang salah satu yang harus dilakukannya adalah membuat kebijakan khusus terkait cyber attack. Namun terkadang kebijakan itu tidak berbanding lurus dengan harapan yang ada untuk menjamin keamanan dan kebebasan masyarakat. tidak mudah untuk menyatukan antara rasa keamanan digital dengan hak asasi manusia. Oleh karena itu, negara sebelum membuat kebijkan terkait keamanan digital harus juga memperhatikan batasan-batasan dan aturan-aturan HAM yang ada. Sehingga bisa mengharmonikan dua aspek tersebut. Oleh karena itu, dalam menyusu kebijakan harus proporsional dengan perlindungan HAM, khususnya dalam freedom of expresion and privacy. Konsekuensi dari itu, kebijakan harus merujuk pada norma-norma tentang HAM baik Internasional ataupun nasional. Penelitian ini merupakan penelitian normatif yang menfokuskan kajian pada norma baik di level hukum positif, teori atau azaz-azaz hukum. Pendekatan yang digunakan adalah pendekatan peraturan perundang-undangan dan konseptual.

Kata Kunci: cyberscurity, Hak Asasi Manusia, Kebijakan.

Abstract

Confrontation in the cyber world not only has an impact on individuals and the economy, but also on a country's sovereignty and global stability. Cyberwarfare is a serious threat. It is also an intelligence and military battlefield. Cyberspace provides the space and means to either threaten or protect citizens and the state itself. To face this challenge, countries throughout the world are aggressively seeking to be able to understand with certainty the various impacts of technological advances which then lead to regulatory policies. Indonesia is one of the countries categorized as a country that is vulnerable to cybercrime. Indonesia also still does not have a specific legal umbrella regarding cyber security. The state must take part in preventing cyber attacks by joining hands with the private sector, one of the things it must do is create a special policy regarding cyber attacks. However, sometimes these policies are not directly proportional to existing hopes to guarantee people's security and freedom. It is not easy to reconcile a sense of digital security with human rights. Therefore, before making policies related to digital security, countries must also pay attention to existing human rights restrictions and regulations. So that we can harmonize these two aspects. Therefore, in formulating policies it must be proportional to the protection of human rights, especially freedom of expression and privacy. The consequence

of this is that policies must refer to norms regarding human rights, both international and national. This research is normative research which focuses on studying norms at the level of positive law, theory or legal principles. The approach used is a statutory and conceptual approach.

***Keyword**: Cyberscurity, Human Rights, Policy.*

PENDAHULUAN

Konfrontasi di dunia cyber tidak hanya berdampak pada individu, ekonomi, namun juga terhadap kedaulatan suatu negara dan stabilitas global. Nigel Inkster mengatakan, cyberwarfare merupakan ancaman serius. Ini juga menjadi medan perang intelijen dan meliter. Cyberspace menyediakan ruang dan sarana untuk baik mengancam ataupun melindungi warga negara dan negara itu sendiri. Menurut Deibert dan Rohozinski, cyberspace sudah menjadi komponen yang fundamental dalam kekuatan politik, sosial, ekonomi dan meliter di seluruh dunia.

IT Governance merilis, pada caturwulan pertama 2019, setidaknya terjadi 1.769.185.063 kebocoran data.pribadi akibat serangan cyber di seluruh dunia. Menurut situs Hackmageddon, sepanjang 2018 ada 1337 kasus. Perincian dari angka tersebut sebagai berikut: 34,4% Malware/Pos Malware, targetnya 22,5% individu, 15,6% industri dan yang ketiga administrasi publik/keamanan nasioanl 14,8%. Adapun kerugian yang ada sebagai berikut: akibat serangan Ransomeware 2017 US$ 5 Miliyar, 2019 US$ 11 Miliyar. Kerugian yang diakibatkan pencurian data pribadi menurut laporan IMB rata-rata sedikitnya US$ 3,86 juta untuk setiap data yang hilang. Data tersebut berisi informasi data-data yang sensitif dan rahasia. Sedangkan versi laporan Harjavec Group, pada tahun 2021 diperkirakan kerugian yang diakibatkan oleh cybercrime mencapai US$ 6 Triliyun.

Untuk menghadapi tantangan itu, negara di seluruh dunia gencar mencari tahu untuk bisa memahmi secara pasti berbagai dampak dari kemajuan teknologi ini yang kemudian bermuara pada kebijakan-kebijakan regulasinya. Indonesia salah satu negara yang dikategorikan negara yang rentan akan cybercrime. BSSN di tahun 2018 dari Januari-Juni melaporkan bahwa sudah terjadi 143.4 juta cyber attacks. Indonesia juga masih belum mempunyai payung hukum khusus mengenai cyber scurity. Global Cyberscurity Index menempatkan Indonesia di posisi 9 sebagai negara yang berkometmen memnghadapi cyber attack di antara negara-negara asia lainnya. Hal itu

diukur dengan lima parameter: Hukum. Teknis. Organisasional. Pengembangan Infrastruktur. Kerja Sama.

Sekarang cyber attack menjadi ancaman yang serius terhadap keamanan nasional suatu negara. Oleh karena itu negara harus ikut andil dalam menangkal serangan siber bergandeng tangan dengan swasta yang salah satu yang harus dilakukannya adalah membuat kebijakan khusus terkait cyber attack. Namun terkadang kebijakan itu tidak berbanding lurus dengan muatan regulasi yang ada untuk menjamin keamanan dan kebebasan wmasyarakat.

Contoh dari hal tersebut adalah Thailand dan Vietnam. Vietnam membuat undang-undang yang memerintahkan perusahaan teknologi harus menyimpan data usernya di server pemerintah dengan dasar negara ingin melindungi. Namun pihak perusahan berpikiran bahwa ini sebagai upaya pemerintah untuk dengan mudah mengakses data warga sipil. Sehingga dengan begitu pemerintah bisa mengontrol warga masyarakat. Di Thailand pun sama dengan Vietnam. Para perusahaan yang menghimpun data user khawatir pemerintah abuse of power. Ini merupakan contoh gagalnya mengintegrasikan antara kebijakan untuk melindungi dengan hak asasi manusia.

Memang tidak mudah untuk menyatukan antara rasa keamanan digital dengan hak asasi manusia. Oleh karena itu, negara sebelum membuat kebijkan terkait keamanan digital harus juga memperhatikan batasan-batasan dan aturan-aturan HAM yang ada. Sehingga bisa mengharmonikan dua aspek tersebut. Oleh karena itu, dalam menyusu kebijakan harus proporsional dengan perlindungan HAM, khususnya dalam freedom of expresion and privacy. Konsekuensi dari itu, kebijakan harus merujuk pada norma-norma tentang HAM baik Internasional ataupun nasional. PBB pun menegaskan dengan Resolusinya No 73/27 dan 73/266.14. menurut Wolfgang Kleinwachter, cyber scurity penting untuk menjamin keterbukaan dan kebebasan internet.

Dari uraian di atas penulis akan membahas isu hukum terkait bagaimana untuk membuat kebijakan cyberscurity yang tidak melanggar batas-batas hak asasi manusia.

HASIL DAN PEMBAHASAN

a. Konsep Keamanan Siber

Sebagaimna uraian di atas, untuk merespon berbagai ancaman di ruang siber, membutuhkan formula untuk menjamin cyberscurity. Fakta yang ada sekarang istilah cyberscurity masih ambigu. Berbagai kelompok mendefinisikan istilah itu, meliter, polisi, pejabat, pengusaha dan para internet user itu sendiri. Bagi internet user, cyberscurity sama halnya dengan keamanan data pribadinya yang terkait dengan berbagai aktivitas di internet dengan istilah lainnya, bahwa cyberscurity merupakan kebebasan melalui jaringan internet tanpa rasa takut akan ancaman terhadap properti, privasi dan hak pribadi lainnya. Sementara bagi pejabat, meliter, polisi keamanan siber sama halnya dengan keamanan nasional, yang juga terkait dengan public services. Sedangkan bagi pengusaha. Cyberscurity merupakan hal yang fundamnetal untuk menjaga sumber daya secara efektif, baik berupa aset keuangan maupun data-data digital lainnya.

Cyberscurity merupakan ilmu baru, sehingga masih belum ada definisi tunggal yang disepakati. Menurut definisi dari beberapa ahli bahwa cyberscurity adalah sinergi yang disengaja dari teknologi, proses, dan praktik untuk melindungi informasi dan jaringan sistem dan peralatan komputer dan program yang digunakan untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi, dari serangan, kerusakan, dan akses tidak sah. Jadi cyberscurity merupakan rangkaian holistik yang bertujuan melindungi informasi penting suatu institusi/organisasi/individu. Mulai dari teknologi dan proses penggunaannya. Keamanan siber harus mampu menjaga kerahasiaan, integritas dan ketersediaan informai, perlindungan dari serangan pihak yang tak bertanggung jawab.

Para ahli cyberscurity mengklasifikasikan cyberscurity ke dalam tiga kategori tujuan: integrity, confidentiality, availability (CIA Triad). Kerahasiaan mengacu pada upaya pencegahan pengungkapan informasi yang tidak sah. Integritas mengacu pada jaminan bahwa pesan yang dikirim akan sampai sama dengan yang dikirim. Availability mengacu pada jaminan bahwa informasi akan tersedia bagi konsumen secara tepat waktu dan tanpa gangguan. Fischer mengatakan, istilah cyberscurity mengacu pada keamanan informasi/data. Keamanan informasi mengacu kepada

semua aspek untuk melindungi informasi yang diklasifikasikan ke tiga kategori: kerahasiaan, intergritas dan ketersediaan informasi.

Guiora mendefinisikan keamanan siber sebagai upaya untuk melindungi informasi, komunikasi, dan teknologi dari bahaya yang disebabkan baik disengaja atau tidak. Penting juga menekankan bahwa cyber attack sangatlah berbeda dengan serangan fisik. Menurutnya keamanan siber sebagai upaya untuk memastikan kerahasiaan, intergritas dan ketersediaan data, sumber daya dan proses melalui kontrol administratif, fisik dan teknis. Menurutnya serangan siber adalah tindakan agresif yang disengaja dan langsung dengan tujuan merusak infrastruktur yang strategis.

Menurut ITU keamanan siber adalah sebagai kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan dan organisasi siber dan aset pengguna. Aset organisasi dan pengguna termasuk komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim/disimpan dalam dunia siber. Keamanan siber berusaha untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap resiko keamanan yang relevan di lingkungan siber.

Unsur mencegah, mendeteksi, merespon adalah tujuan umum dari keamanan fisik dan siber, yang ingin memastikan musuh tidak bisa melakukan suatu serangan. Oleh karena itu butuh perencanaan dan persiapan juga mencakup metode untuk mendeteksi ketika serangan berlangsung, dan berbagai upaya untuk melakukan minimalisasi kerusakan dari serangan itu. Sementara unsur proses, orang dan teknologi terkait dengan metode umum yang terkait dengan manajemen teknologi dan cyberscurity sebagai sebuah bidang yang spesifik. Sedangkan unsur kerahasiaan, intergritas, dan ketersediaan merupakan tujuan khusus yang mengacu pada kemampuan sistem untuk membatasi penyebaran informasi untuk keperluan resmi. Integritas mengacu kemampuan untuk mempertahankan keaslian, akurasi dan orisinalitas informasi. Ketersediaan mengacu pada pengiriman tepat waktu.

Keamanan siber sangat terkait dengan konsep keamanan informasi, jaminan informasi, keamanan komputer, keamanan jaringan, dan perlindungan infrastruktu informasi strategis. Infrastruktu informasi strategis digambarkan sebagai bagian dari

infrastruktur informasi global dan nasional yang penting untuk suatu layanan infrastruktu strategis, atau di Indonesia dikenal Objek Vital Nasional. Dalam hal itu ada unsur fisik dan material. Unsuru fisiknya: jaringan yang berkecapatan tinggi, interaktif, pita sempit, jaringan broadband, sistem komunikasi satelit, trestrial, nirkabel, komputer, televesi, telepon, radio dan lainnya yang digunakan masyarakat untuk mengakses informasi. Sedangkan unsur inmaterinya: informasi dan konten yang dialirkan.

Istilah umum "keamanan siber" sering ditempatkan sebagai "payung" yang sering mengacaukan masalah keamanan yang mungkin serupa dalam sifat teknisnya, namun sangat berbeda dalam aspek hukum dan kebijakan sehingga memerlukan treatment yang berbeda. Beberapa istilah keamana siber (cyberscurity) kejahatan siber (cybercrime) perang siber (cyberwar) serangan siber (cyberattack) terorisme siber (cyberterrorism). Karena masih belum ada kesepakatan penamaan maka sering istilah ini digunakan secara bergantian, dan hal ini menlahirkan kebingungan dan melahirkan kesalah pahamana terhadap masalah utamanya. Sehingga hal ini berdampak pada respon hukum dan kebijakan yang diambil oleh negara.

b. Pembentukan kebijakan Keamanan Cyber Dengan Pendekatan HAM

Jaringan internet menjadi alat terbaik untuk mengkomunikasikan antara orang yang berlainan tempat. Internet sangat berkontribus dalam hal pengetahuan, sosial dan ekonomi. Namun di sisi lain, internet juga menjadi instrumen untuk melakukan hal-hal negatif (kejahatan). Internet juga dinilai sebagai alat untuk surveillance digital. Oleh karena internet mempunyai dua sisi nilai, baik yang positif maupun yang negatif.

Kita harus sadar, bahwa segala yang kita lakukan di dunia digital selalu meninggalkan jejak. Jejak tersebut bisa diolah oleh pihak-pihak tertentu yang mengambil manfaat dari pengulahan jejak tersebut sehingga kumpulan data jejak tersebut menjadi serangkaian informasi-informasi yang bernilai, baik nilai itu negatif ataupun positif. Dalam kenyataannya, ada platform dari internet yang tidak dengan mudah bagi penggunanya mengontrol data pribadi mereka, padahal seharusnya penguna itu bertanggung jawa atas segala informasi yang mereka publikasikan tentang mereka, bukan dengan mudahnya mereka memberikan informasi pribadi mereka, preferensi dan aktivitas mereka, serta mengungkapkan lokasi keberadaanya.

Kecepatan jangkauan internet mengakibatkan data tersebar jauh di luar kendali penggunanya. Hal ini semakin besar dikarenakan semakin maraknya perniagaan internet, yang diantaranya didasarkan oleh model bisnis yang berbasis iklan, dimana pengguna membayar dengan data pribadi mereka. Meningkatnya konvergensi perangkat yang terhubung ke internet juga menyebabkan kesulitan untuk mengontrol data pribadi, sehingga banyak pengguna dengan mudahnya mengklik "accept" yang artinya setuju menyediakan data pribadi mereka tanpa membaca terlebih dahulu tentang dampak yang akan diakibatkan dari mengklik itu.

Data pribadi dianggap sebagai aset komersial, khususnya di negara yang masih belum mempunyai payung hukum khusus tentang perlindungan data pribadi atau meskipun ada tetapi masih lemah. Data mining bukan sekedar kelompok bisnis, namun juga organisasi kriminal dan bisa juga individu yang memang ahli dibidang ini dan menggunakan keahliannya untuk meraup keuntungan dari data pribadi tersebut. Masalahnya sekarang adalah, para pengguna itu melihat kebutuhan perlindungan data pribadi ini lebih nelihat sebagai hambatan yang berdampak pada bisnisnya dari pada melihat sebagai kebutuhan dari pemenuhan hak asasinya. Mereka tidak sadar bahwa keamanan atas data pribadi mereka merupakan prasyarat menentukan nasib sendiri yang pada nanti berkonotasi dengan kebebasab berbicara, ekspresi serta menjamin jalannya demokrasi.

Sebab itu, pengguna harus memastikan keseimbangan antara kebutuhan dan kewajiban atas perlindungan, antara perlindungan individu dan umum, antara menghormati kedaulatan nasional dan kebutuhan untuk kerja sama internasional, untuk menjamin tegaknya hak asasi manusi. Titik keseimbangan inilah yang seharusnya menjadi pangkal utama pengembangan kebijakan keamanan siber nasional. Langkah-langkah dalam keamanan siber, baik teknologi, prosedur, organisasi dan payung hukumnya harus saling sesuai dan saling melengkapi dan juga koheren dengan kebutuhan masyarakat atas informasi, serta melindungi hak asasi manusia. Terkait hal ini. pada 21 Desember 2009, PBB telah mengeluarkan Resolusi 64/211 tentang Penciptaan Budaya Global keamanan siber dan inventarisasi upaya nasional untuk melindungi infrastruktu informasi yang penting. Resolusi ini memberikan dua penenkanan terhadap negara-negara:

Ajakan untuk menggunakan instrumen penilaian yang tepat bagi kebutuhan nasional mereka untuk memastikan perlindungan infrastruktur informasi penting, dalam hal ini guna memberikan keamanan siber merka, yang akan berkontribusi bagi peningkatan budaya global keamanan siber.

Mendorong negara-negara dan organisasi-organisasi regional dan internasional yang relevan untuk mengembangkan berbagai strategi guna memastikan kemanan siber dan perlindungan infrastruktur informasi yang penting.

Dalam Resolusi 73/266 yang diadopsi oleh Majelis Umum pada 22 Desember 2018 PBB juga menggaris bawahi pentingnya penghormatan hak asasi manusi dan kebebasan dasar dalam pemanfaatan teknologi informasi dan komunikasi. Hal ini sebagai upaya memajukan perilaku negara-negara yang bertanggung jawab di ruang siber dalam konteks keamana internasional. Sebelumnya dalam Resolusi 73/27 yang diadopsi oleh Majelis Umum pada 5 Desember 2018 PBB menegaskan negara-negara dalam memastikan keamanan pengguna teknologi informasi dan komunikasi untuk menghormati Resolusi Dewan HAM 20/8 5 Juli 2012 dan 26/13 26 Juni 2014 tentang promosi perlindungan dan penikmatan hak asasi manusia di internet, dan Resolusi Majelis Umum 68/167 18 Desember 2013 dan 69/166 18 Desember 2014 tentang hak privasi di era digital, untuk menjamin penghormatan penuh terhadap hak asasi manusia termasuk hak atas kebebasan berekspresi.

Sebelumnya dalam laporan Majelis Umum PBB (A/68/98) juga ditetapkan bahwa hukum humaniter internasional berlaku secara offline dan online, sehingga ditegaskan dalam upaya untuk mengatasi keamanan teknologi informasi dan komunikasi harus berjalan seiring dengan penghormatan terhadap hak asasi manusia dan kebebasan dasar yang ditetapkan dalam Deklarasai Universal Hak Asasi Manusia dan instrument Internasional lainnya. Resolusi yang sama juga menyerukan kepada negara-negara untuk mendorong sektor swasta dan masyarakat sipil untuk berperan dengan tepat untuk meningkatkan keamanan dan dalam peningkatan teknologi informasi dan komunikasi.

Beberapa instrument di atas sebagai pijakan untuk mengembangkan kerangka kerja pendekatan berbasis hak asasi manusia dalam membuat kebijakan keamanan siber. Klaus Schwab mengatakan bahwa pendekatan ini diperlukan karena adanya kebutuhan untuk artikulasi yang lebih jelas dari kerangka kerja etis, standar normatif

dan model tata kelola berbasis nilai untuk membantu membimbing organisasi dalam pengembangan dan penggunaan alat-alat yang kuat di masyarakat, dan untuk memungkinkan pendekatan yang menekankan pada manusia-sentris, untuk pembangunan yang melampau batas geografis dan politik. Menurutnya hak asasi manusia sebagai ujung tombak nilai-nilai dan kerangka kerja hak asasi manusia internasional memberikan dasar subtantif untuk mengatasi masalah-masalah pemanfaatan teknologi informasi dan komunikasi.

Freedom Online Coalition mengembangkan pendekatan yang sama untuk merespon peningkatan rentannya siber, dengan tingginya frekuensi dan kompleksitas ancaman sehingga membutuhkan kerja sama seluruh pemangku kepentingan untuk menjaga hak asasi manusia, khususnya privasi dan kebebasan berekspresi. Koalisi membentuk kelompok kerja "An Internet Free and Secure", kelompok ini melaporkan bahwa keamanan individu adalah tujuan utama dari keamanan siber dan internet yang merupakan pusat perlindungan hak asasi manusi dalam dimensi digital. Kelompok ini juga mendefinisikan keamanan siber bahwa privasi dan kerahasiaan informasi adalah penting untuk keamanan individu, juga terhadao data, khususnya dalam hal digital, dimana keamanan fisik dan informasi digital saling berhubungan.

Hak asasi manusia dan keamanan siber saling bertautan, menguatkan, dan saling bergantung satu sama lain seperti halnya prinsip-prinsip hak asasi manusia. Keduanya harus diupayakan bersama untuk secara efektif mempromosikan kebebasan dan kemananan. Mengatakan keamanan individu sebagai inti keamanan siber berarti perlindungan terhadap hak asasi manusia harus menjadi pusat pengembangan keamanan siber. Menurut koalisi, pendekatan yang didasarkan pada hak asasi manusia sangat penting dalam mengingatkan para pembuat kebijakan bahwa keamanan siber harus juga mempertimbangkan keamanan individu dan hak asasi manusia dan konsekuensi dari itu adalah kebijakan keamanan siber harus ditujukan untuk menghormati hak asasi manusia.

Pendekatan berbasis hak asasi manusia adalah kerangka kerja konseptual untuk suatu proses pembentukan kebijakan yang secara normatif didasarkan pada standar hak asasi manusia. Pendekatan ini mencoba untuk menggabungkan prinsip dan standard hak asasi manusia sebagai sarana dan tujuan dari suatu proses, dan mengintegrasikan pencapaian dan pemenuhan hak asasi manusia ke dalam desain,

implementasi, pemantauan dan evaluasi semua kebijakan dan tindakan. Pendekatan ini tidak hanya menitik beratkan pada pengarusutamaan hak asasi manusia, tetapi juga menambahkan beberapa elemen tambahan melalui peningkatan kesadaran tentang hak asasi manusia, dampak dari kebijakan, dan mengklarifikasi tujuan dari setiap tindakan, sehingga tidak hanya memenuhi kebutuhan tradisional. Artinya adalah semua kebijakan, program, dan kegiatan terkait yang diterapkan dengan pendekatan berbasis hak asasi manusia akan ditujukan secara konkret dan langsung berkontribusi pada realisasi hak asasi manusia dan mengintegrasikan hak asasi manusia pada setiap langkah dan tindakan.

Menurut Marry Robinson, pendekatan berbasis hak asasi manusia menambah nilai, karena memberikan kerangka kerja normatif untuk menempatkan pemerintah sebagai pihak yang bertanggung jawab terhadap hak asasi manusia. Secara konseptual, pendekatan berbasis hak asasi manusia ini telah dipromosikan oleh PBB dengan mengeluarkan seperangkat prinsip dasar hak asasi manusia untuk inisiatif pembangunan. Jumlah dan urutan prinsip itu memang berbeda-beda, namun tetap mengacu pada pertimbangan etis yang sama untuk memastikan keadilan dan martabat bagi individu. Prinsip-prinsip dalam pendekatan berbasis hak asasi manusia setidaknya meliputi: (1) Ketidak terpisahan. Kesaling tergantungan. Keutuhan HAM. (2) pemberdayaan dan partisipasi. (3) akuntabilitas. (4) kesetaraan dan non-diskriminasi. (5) prinsip-prinsip HAM dalam pendekatan berbasis HAM

Kaitannya dengan keamanan siber, dalam rekomendasi Kelompok Kerja "An Internet Free and Secure" dalam bagian pembukaan disebutkan bahwa hukum hak asasi manusia internasional dan hukum humaniter internasional berlaku secara offline maupun online. Keamanan siber harus melindungi inovasi teknologi dan pelaksanaan hak asasi manusia. Kelompok ini mengacu pada standar ISO 2 7000 dengan mengatakan bahwa keamanan siber adalah pelestarian melalui hukum, kebijakan, teknologi dan pendidikan dari ketersediaan, kerahasiaan dan integritas informasi dan infrastruktur yang mendasarinya, sehingga meningkatkan keamanan orang baik online maupun offline. Kelompok ini merekomendasikan 13 poin:

Kebijakan keamanan siber dan proses pengambilan keputusan harus melindungi dan menghormati hak asasi manusia.

Pengembangan undang-undang, kebijakan, dan praktik terkait keamanan siber harus dimulai sejak awal dengan desain yang menghormati hak asasi manusia.

Undang-undang, kebijakan, dan praktik harus meningkatkan keamanan orang secara online dan offline, dengan mempertimbangkan ancaman yang tidak proporsional yang dihadapi individu dan kelompok yang beresiko.

Pengembangan dan penerapan undang-undang, kebijakan dan praktik harus konsisten dengan hukum internasional, termasuk hukum hak asasi manusia dan hukum humaniter internasional.

Undang-undang, kebijakan dan praktik tidak boleh digunakan sebagai dalih untuk melanggar hak asasi manusia terutama kebebasan bereskpresi, berserikat, berkumpul dan privasi.

Respon terhadap insiden siber tidak boleh melanggar hak asasi manusia.

Undang-undang, kebijakan, dan praktik harus menjunjung tinggi dan melindungi stabilitas dan keamanan internet, dan tidak boleh merusak integritas infrastruktur, perangkat keras, perangkat lunak, dan layanan.

Undang-undang, kebijakan, dan praktik harus mencerminkan peran utama enkripsi dan anomitas dalam berbagai area hak asasi manusia, terutama kebebasan berekspresi, berserikat dan privasi.

Undang-undang, kebijakan dan praktik tidak boleh menghalangi perkembangan teknologi yang berkontribusi pada perlindungan hak asai manusia.

Undang-undang, kebijakan dan praktik di tingkat nasional, regional dan internasional harus dikembangkan melalui pendekatan terbuka, inklusif dan transparan yang melibatkan semua pemangku kepentingan.

Para pemangku kepentingan harus mempromosikan pendidikan, literasi digital dan pelatihan teknis dan hukum sebagai cara untuk meningkatkan keamanan siber dan realisasi hak asasi manusia.

Hak asasi manusia yang menghormati praktik terbaik keamanan siber harus dibagikan dan dipromosikan di antara semua pemangku kepentingan.

Peningkatan kapasitas keamanan siber memiliki peran penting dalam meningkatkan kemanan orang-orang baik online dan offline. Upaya semacam itu harus mempromosikan pendekatan yang menghormati hak asasi manusia terhadap keamanan siber.

Penegasan itu berarti perlindungan hak asasi manusia, termasuk kaidah pembatasnya juga melekat saat negara ingin membuat kebijakan tentang pemanfaatan teknologi internet, termasuk yang berkaitan dengan alasan keamanan siber. Semisal ketika negara akan melakukan pembatasan akess internet dalam bentuk pemblokiran, maka seluruh kaidah pembatasan harus menjadi dasarnya. Pembatasan diatur dalam undang-undang untuk tujuan yang sah, kebutuhan mendesak, proporsional, dalam masyarakat demokratis dan didasari alasan seprti ketertiban umum, keamanan nasional, moral, kesehatanm publik atau dalam rangka melindungi hak dan reputasi orang lain.

KESIMPULAN

Konfrontasi di dunia cyber tidak hanya berdampak pada individu, ekonomi, namun juga terhadap kedaulatan suatu negara dan stabilitas global. Untuk menghadapi tantangan itu, negara harus memahmi secara pasti berbagai dampak dari kemajuan teknologi ini yang kemudian bermuara pada kebijakan-kebijakan regulasinya. Memang tidak mudah untuk menyatukan antara rasa keamanan digital dengan hak asasi manusia. Oleh karena itu, negara sebelum membuat kebijkan terkait keamanan digital harus juga memperhatikan aturan-aturan HAM yang ada. Sehingga bisa mengharmonikan dua aspek tersebut.

Guiora mendefinisikan keamanan siber sebagai upaya untuk melindungi informasi, komunikasi, dan teknologi dari bahaya yang disebabkan baik disengaja atau tidak. Penting juga menekankan bahwa cyber attack sangatlah berbeda dengan serangan fisik. Menurutnya keamanan siber sebagai upaya untuk memastikan kerahasiaan, intergritas dan ketersediaan data, sumber daya dan proses melalui kontrol administratif, fisik dan teknis. Menurutnya serangan siber adalah tindakan agresif yang disengaja dan langsung dengan tujuan merusak infrastruktur yang strategis.

Hak asasi manusia dan keamanan siber saling bertautan, menguatkan, dan saling bergantung satu sama lain. Keduanya harus diupayakan bersama untuk secara efektif mempromosikan kebebasan dan kemananan. Mengatakan keamanan individu sebagai inti keamanan siber berarti perlindungan terhadap hak asasi manusia harus menjadi pusat pengembangan keamanan siber. Pendekatan berbasis hak asasi manusia adalah kerangka kerja konseptual untuk suatu proses pembentukan kebijakan yang secara

normatif didasarkan pada standar hak asasi manusia. Pendekatan ini mencoba untuk menggabungkan prinsip dan standard hak asasi manusia sebagai sarana dan tujuan dari suatu proses, dan mengintegrasikan pencapaian dan pemenuhan hak asasi manusia ke dalam desain, implementasi, pemantauan dan evaluasi semua kebijakan dan tindakan.

DAFTAR PUSTAKA

BUKU

Amos N. Guiora, Cyberscurity: Geopolitics, Law, and Policy, (New York: Routledge, 2017.

Aanchal Kapur & Nata Duvvury, A Rights-Based Approach to Realizing the Economic and Social Rights of Poor and Marginalized Women: A Synthesis of Lessons Learned, (Washington, DC: International Center for Research on Women, 2006).

Deborah L. Wheeler, Understanding Cyber Threats, dalam Kim Andreasson (ed), Cyberscurity Public sector Threats and Responses, (New York: CRC Press Taylor & Francis Group, 2012).

Grogory J. Touhill & C. Joseph Touhill, Cyberscurity for Executives: A Practical Guide, (New Jersey: John Wiley & Sons, Inc, 2014).

Jakob Kirkeman Boesen & Tomas Martin, Applying A Rights-Based approach: anInspirational Guide for Civil Society, (Copenhagen: Danish institue for HumanRights, 2007).

Juanna Kulesza & Roy Balleste (eds), Cyberscurity and Human Rights in the Age of Cyberveillance, (London: Rowman & Littlefield, 2016).

Jennefer L Bayuk, dkk, Cyberscurity Policy Guidebook, (New Jersey: John Wiley & Sons, Inc).

Klaus Schwab, Shaping the Future of the fourth Industrial Revolustion: A Guide to Building a Better World, (London: Penguin Random House, 2018).

Myriam Dun Cavelty, Cyberscurity in Switzerland, (Dordrecht: Springer, 2015).

Nir Kshetri, The Quest to Cyber Superiority Cyberscurity Regulations, Frameworks, and strategies of Major economies, (London: Springer, 2016).

Tatiana Tropina & Cormac Callanan, Self-and-Co-Regulations in Cybercrime, cyberscurity and National Scurity, (Heidelberg, Springer, 2015).

Tim Maurer, Cyber Norm Emergance at The United Nations- An Analysis of the UN`s Activities Regarding Cyber-security, (Cambridge: Belfer Center for Science and International Affairs, 2011).

Thomas A. Johnson (ed), Cyberscurity: Protecting Critical Infrastructure from Cyber Attack and Cyber Warfare, (New York: CRC Pres Taylor & Francis Group, 2015), hal. 201 205.

Urban Jonsson, et.al., Frequently Asked Questions on A Human Rights-Based Approach to Development Cooperation, (Geneva: Office of The United Nations High Commissioner for Human Right, 2006).

Wahyudi Djafar dan Justitia Avila Veda, Internet Untuk Semua: Mengintegrasikan Prinsip Hak Asasi Manusia dalam Pengaturan Internet di Indonesia, (Jakarta: ELSAM,
2015).
Wolfgang Kleinwachter, Internet Governance and Cyberscurity, dalam Collaboratory Discussion Paper series, No, 1. (Berlin: Multistaholder Internet Dialog, October 2013).

JURNAL

Ashish Agarwal & Aparna Agarwal, The Scurity Risk Associated With Cloud Computing, 1 Int`I J. Computer Aplications Engineering Sci. (Special Issue On Cns)
European Commision, Oprational Human rights Guidance for EU external cooperation actions addresing Terrorism, Organised crime and Cybersecurity Integrating the Rights-Based Approach (2012).
Eric A. Fischer, Creating a National Framework for Cyberscurity: An Analysis of Issues and Options, 22 February 2005, CRS Report for Congress, Order Code RI. 32777.
IISS Global Perspectives, Power in Cyberspace. Q&A with Nigel Inkster , Director, Transnational Threats and Political Risk, IISS, 18 Januari 2011
R. J. Deibert and R. Rohozinski, "Risking Scurity: Polices and Paradoxes of Cyberspace Scurity." International Political Sociology. 4:1(March 2010).

WEB

https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FOC-WG1-Recommendations Discussion-draft-IGF-20151.pdf.
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january 2019-1769185063-records-leaked.
https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/.
https://cyberscurityventures.com/ransomeware-damage-report-2017-5-bilion/.
https://www.ibm.com/scurity/data-breach.
https://www.herjavecgroup.comwp-content/uploads/2018/12/CV-HG-2019-Official-AnnualCybercrime-Report.pdf.
https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136.
https://www.itu.int/en/ITU-D/Cyberscurity/Documents/draft-18-00706_Global-Cyberscurity Index-EV5_print_2.pdf.
https://www.reuters.com/article/us-thailand-cyber-idUSKCN1QH10B.
https://www.un.org/ga/search/viewe_doc.asp?symbol=A/RES/68/167.
https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Narrative-Final 28-April-2016.pdf