Cyber Law: Rights and Obligations

Transkrip
Minggu 7: Cybercrime, Evidence, Cybersecurity

Video 1: Cybercrime

Pemirsa IndonesiaX, kita telah merampungkan pembahasan tentang e-commerce, e-goverment, konstitusi dan telematika, dan juga kita bicara perlindungan data pribadi, yaitu tentang kebendaan dan aspek beberapa digital content.

Kali ini kita akan merampungkan pembicaraan kita tentang cybercrime, cybersecurity dan cyber resilience. Jangan lupa, waktu kuliah pertama, saya menyampaikan suatu gambar diagram yang terdiri dari berbagai lingkaran. Yang satu kotak itu, di mana di situ ada semesta dari hukum informasi dan komunikasi, artinya hukum yang terkait dengan berbagai ragam informasi dan berbagai moda komunikasi. Lalu kita mempersempit menjadi cyberspace law karena cyberspace identik dengan apa yang terjadi lewat internet.

Jadi media komunikasi kan bukan hanya internet, ada existing electronic dalam konteks transmisi penyiaran, terus ada juga yang media cetak, juga ada yang media computer to computer tapi bukan TCP/IP. Jadi gambar itu menjelaskan bahwa hukum informasi dan komunikasi lebih luas, kemudian cyberspace law. Di dalam cyberspace law, ada cybersecurity, di dalamnya ada e-goverment, ada e-commerce, dan kita bicara crime.

Kali ini mari kita perdalam sedikit tentang crime. Apakah itu crime? Sebagaimana kita ketahui, crime itu adalah tindak pidana atau kejahatan. Apa yang dmaksud dengan kejahatan? Ada suatu perbuatan yang memenuhi rumusan pidana. Rumusan pidana itu harus jelas, sehingga kalau tidak memenuhi rumusan pidana, berarti bukanlah tindak pidana.

Poin pentingnya adalah yang disebut dengan ‘Nullum Delictum (Nulla Poena) Sine Praevia Lege Poenali’. Artinya bukanlah suatu tindak pidana jika tidak memenuhi unsur-unsur dalam perbuatan pidana yang dirumuskan dalam perumusan hukum pidana.

Nah, dalam konteks cyber, apakah benar terjadi suatu kejahatan dalam lingkup cyber? Kita sudah membahas apa itu cyberspace, yang intinya adalah computer network secara global dimana yang menjadi kejahatan itu mungkin akan melibatkan tiga perspektif. Pertama, kejahatan terhadap sistemnya. Jadi sistem yang jadi sasaran;

yang tadinya beroperasi menjadi tidak beroperasi. Jadi kejahatannya terhadap sistemnya.

Atau sistemnya enggak jadi objek kejahatan, tapi dia menjadi sarana untuk melakukan kejahatan. Artinya, ini seperti suatu hal yang dulu sudah dilakukan, sekarang modanya saja yang berbeda.

Dulu tukang fitnah, begitu masuk internet, ya fitnah di internet. Tukang tipu, masuk internet, ya jadi tukang tipu via internet. Artinya kejahatannya lama, kemasannya yang baru. Istilah yang berkembang itu 'old wine in the new bottle'.

Komputer sebagai sasaran, komputer sebagai target, atau komputer sebagai sarana untuk memfasilitasi kejahatan, atau yang ketiga, keberadaan komputer ini ternyata terkait dengan suatu tindak pidana. Menerangkan sesuatu tindak kejahatan yang dilakukan secara konvensional.

Misalnya, ditemukan mayat mengambang dalam, di atas sebuah danau. Tindak pidananya ya pembunuhan. Mungkin sebelum pembunuhan, ada perkosaaan. Tetapi ternyata untuk bisa menemukan itu, informasi elektronik menjadi penentu adanya tindak pidana tersebut. Yaitu, ternyata ada pembicaraan antara si korban dengan si pelaku sebelumnya via website, atau ikut dalam chat, atau hal-hal yang terkait melibatkan keberadaan network tentang informasi dan jaringannya yang menerangkan akan terjadinya suatu tindak pidana. Beberapa hal pernah terjadi toh di Indonesia.

Jadi kalau kita lihat dalam dua lingkaran, kita bicara computer crime dan cybercrime ini, mau tidak mau akan bicara dua lingkaran. Yang lingkaran pertama adalah kejahatan lama. Yang lingkaran kedua adalah kejahatan baru. Nah, dalam konteks ini, berbicara cybercrime, itu intinya adalah pembicaraan tentang suatu tindak kejahatan yang dapat dilakukan via cyber, via cyberspace atau tindakan-tindakan kejahatan yang dilakukan di dalam cyberspace, baik itu yang menjadi sasaran, atau itu menjadi sarana, atau terkait dengan suatu tindak pidana dimana dia menjadi medium penyimpan atau medium, ya, sebagaimana selayaknya suatu kesaksian. Dalam konteks ini, information storage-nya menjadi, menjadi bukti adanya suatu tindak pidana.

Video 2: Karakteristik Kejahatan Cyber

Dalam melihat ini, maka mau tidak mau, kita harus lihat dulu, karateristik bagaimana pemidanaan itu berada dalam sistem perundang-undangan. Jangan lupa, hampir semua negara, untuk yang namanya pidana, akan ada general criminal code-nya, atau kalau di kita, Kitab Undang-undang Hukum Pidana-nya. Kemudian ada juga perkembangan pidana yang dirumuskan secara terpisah, yang intinya karena kekhususannya, karena kekhususannya dia jadi melengkapi dari general code-nya itu. General code itu bisa bentuk criminal code atau procedural code-nya.

Nah, di sini menarik. Dalam sistem hukum nasional kita, kitab Undang-undang Hukum Pidana bicara soal tindak pidana yang secara umum. Yang di luar itu, yang sifatnya extraordinary, atau karena kekhususan. Demikian pula yang Kitab Undang-undang Hukum Acara Pidana yang dimana penyelesaian hukum acara dalam konteks extraordinary berbeda dengan general procedural criminal code-nya.

Ini menjadi bekal pertama kita dalam melihat bagaimana karakteristik sistem hukum pidana kita, atau karateristik sistem hukum pidana pada umumnya, dalam pendekatannya dengan tindak pidana cyber. Maka, mau tidak mau kita harus

menjelaskan, apakah benar dia menjadi suatu tindak pidana khusus? Apa yang menjadi karateristik khusus dari cybercrime ini?

Pertama, di dalam cybercrime, terjadi dunia ubiquitous. Ubiquitous itu artinya begini, saya ada, Anda pun di sana ada. Saya ngetik-ngetik di sini, Anda pun menerima informasi itu. Artinya kita punya kesatuan waktu, walaupun berbeda tempat. Artinya kalau berbicara paradigma konvensi pidana pada umumnya, biasanya kan akan bicara 'lex locus delicti, lex tempus delicti'. Kalau sekarang, saatnya bersamaan, di saya ada informasinya, di tempat Anda pun ada informasinya.

Ubiquitous berarti pada saat yang bersamaan secara longitudinal. Lalu kita melakukannya dengan kesadaran yang relatif lebih tinggi, kenapa? Pada saat Anda mengoperasikan komputer, berarti Anda sudah mengetahui sistem operasi komputer. Setidak-tidaknya Anda bisa juga berbahasa Inggris, bukan?

Di sini, secara elektronik, tingkat kejahatannya dilakukan oleh orang yang relatif lebih berintelektual. Lalu bagaimana efeknya? Efeknya tidak bisa terprediksi multiplier effect-nya. Kenapa? Anda kirimkan di sini, sampai kapanpun, akan selalu dapat dibaca orang. Dan pada saat Anda melakukan pengumuman, kalau Anda pakai media cetak, dia terbatas oplah. Tapi kalau kita bicara lewat internet, semua tiap hari bertambah usernya. Dengan sendirinya, multiplier effect-nya tidak dapat kita prediksikan. Artinya siapapun yang mau menciderai orang lain, atau mau menjahati orang lain via medium ini, berarti sudah tahu multiplier effect-nya tak terhingga.

Lalu demikian juga dengan sifat permanent data-nya. Kalau hari ini saya fitnah orang di media cetak, maka besok jangan-jangan media cetak tersebut telah berubah menjadi bungkus atau tidak dibaca orang lain. Tapi kalau Anda jelek-jelekkan orang di internet, sampai kapanpun masih akan dapat terbaca. Lalu bagaimana dengan kegiatan cross-border-nya? Kegiatan cross-border-nya juga kita bisa katakan tidak terhingga.

Lalu apa yang dilakukan juga oleh si pelaku? Dia bisa menggunakan nama lain. Dia merasa lebih leluasa karena dia menggunakan nama anonim. Jadi intinya siapapun yang melakukan kejahatan lewat internet ini, sebenarnya bukan berada pada faktor yang biasa-biasa saja. Orang ini mempunyai kecerdasan lebih, intelektual yang lebih.

Sayangnya dengan intelektual yang lebih, justru dia malah bersifat lebih jahat. Dengan sendirinya, sanksi terhadap ancaman pidananya tentunya akan lebih berat ketimbang yang konvensional. Jadi fitnah biasa dengan fitnah lewat internet, ya otomatis fitnah internet lebih berat.

Nah, hal-hal yang dapat dimungkinkan terhadap kualifikasi dari kegiatan yang sebelumnya telah ada, begitu masuk elektronik, perlu diberati, itu masih kita katakan memfasilitasi kejahatan yang lama. Tetapi ada sesuatu tindakan yang dulu enggak pernah dikriminalisasi, sekarang dikriminalisasi. Contoh, dulu Anda tukar-tukaran PIN orang, mungkin enggak masalah. Tapi sekarang, PIN itu adalah Personal Identification Number seseorang, yang sifatnya rahasia. Kalau Anda memperjualbelikan itu berarti Anda kena pidana.

Atau dulu Anda memasuki akses ke dalam sistem secara tidak licensed, Anda merasa itu biasa-biasa saja. Tapi kenyataannya, illegal access sekarang sudah dikatakan kriminalisasi, Artinya suatu tindakan yang dulu mungkin Anda merasa itu leluasa, padahal itu salah, pada saat dirumuskan pidana, disampaikan perumusan pidananya, maka tindakan itu namanya mengkriminalisasi, dikriminalisasi.

Nah, dalam konteks itu, maka kriminalisasi dalam cyber itu harus mengikuti kaidah global. Nah, di sini menariknya, bahwa di perkembangannya, sejak tahun 2001, sudah ada yang namanya Budapest Convention, yaitu Cybercrime Convention, walaupun itu dibuat di negara Eropa, tapi dia di-strongly recommended by United Nation. Artinya semua negara, termasuk Amerika, mengaksesnya. Cuma memang belum tentu bisa diakses oleh negara ASEAN karena standar perlindungannya mungkin dalam prosedural hukumnya berbeda. Nanti akan kita bahas bagaimana scope perlindungan dari Convention on Cybercrime.

Video 3: Lingkup Pengaturan Hukum Cyber – Part 1

Pemirsa IndonesiaX, kita teliti lebih lanjut tentang Convention on Cybercrime ini, yang merupakan konvensi regional Eropa, tapi dia dirujuk oleh seluruh dunia tentang beberapa ketentuannya. Bahkan United Nation mendorong para negara lain untuk bisa mengakses ini. Hanya untuk mengakses perjanjian ini, standar prosedurnya mungkin tidak mudah. Bahkan menjadi pertanyaan, apa sih isi Convention on Cybercrime ini?

Setidak-tidaknya kita harus memperhatikan tiga hal besar. Yang pertama adalah criminalising conduct, yaitu tindakan-tindakan yang perlu dikriminalisasi, yang harus dikriminalisasi. Kemudian ada aspek penegakan hukum terhadap substantif tadi, ingat, kalau tadi kan subtantif law itu intinya adalah hukum pidana materiil, tindakan-tindakan yang dikriminalisasi. Ada perumusan pidananya.

Yang berikutnya adalah procedural-nya, penegakannya, atau hukum acara pidana. Bagaimana menerapkan pemidanaan terhadap konteks ini? Lalu, yang berikutnya adalah perlu kerjasama internasional. International cooperation untuk dapat memidanakan ini, untuk dapat menerapkan penerapannya, melakukan pelaksanaan penerapannya, dimana hukum acara perlu mendapatkan bantuan kerjasama internasional dalam penegakannya.

Satu, tentang criminalising conduct. Dua, procedural laws. Yang ketiga adalah international cooperation. Baik, kita mulai satu-satu.

Dalam aspek substantive law, dalam aspek criminalising conduct, maka kita harus memperhatikan bahwa ada beberapa subtantif law itu secara umum adalah sebagai berikut. Satu, bicara illegal access, segala akses yang dilakukan tanpa dasar hak, itu salah dan kategorinya bisa beberapa hal. Yang berikutnya adalah illegal interception. Illegal interception itu adalah tindakan pencegatan informasi atau penyadapan informasi secara ilegal. Yang berikutnya, data interference, tindakan mengubah-mengubah, mengintervensi data. Yang keempat, tindakan mengintervensi sistem atau system interference.

Illegal access, illegal interception, data interference, system interference, dan yang kelima, misuse of devices. Selain itu, ada lagi IPR-offences dan child pornography. Itu tujuh standar yang seringkali dikemukakan, bahwa ada yang substantive law terhadap konten, yaitu terkait IPR dan child pornography. Ada komputer as a target, illegal access, illegal interception, data interference, system interference, dan misuse of devices. Lalu, dalam konteks procedural law-nya, mari kita cermati tabel tentang Convention on Cybercrime. Di sana, ada tiga kriteria.

Pemirsa, saya ulang sedikit ya. Tentang criminalising conduct tersebut, illegal access, illegal interception, data interference, system interference, misuse of devices, kemudian ada IPR-offences, child pornography dan jangan lupakan, fraud and forgery. Jadi komputernya enggak diserang, tapi komputernya digunakan untuk melakukan fraud

and forgery. Itu criminalising conduct atau kita sebut substantive law. Hukum substansial yang mempidanakan.

Lalu ada procedural-nya. Untuk melakukan procedural-nya, maka mau tidak mau dibutuhkan kejelasan tentang ketiga hal. Pertama, bicara expedited preservation, pemercepatan untuk pengamanan bukti elektronik tadi. Lalu ada search and seizure: pemeriksaan, pengeledahan dan penyitaan terhadap bukti-bukti elektronik baik di perangkat setiap orang maupun sampai kepada jaringan. Lalu, intersepsi, perlu ada suatu ketentuan secara prosedural yang memungkinkan dilakukannya intersepsi.

Lalu dalam rangka kerjasama antarnegara untuk memastikan bahwa prosedural ini berjalan, di international cooperation mau tidak mau dibuat suatu ketentuan tentang 24/7 networks. Artinya 24 jam dalam 7 hari, sistem yang siap siaga untuk para penegak hukum dapat bekerjasama menegakkan hukum tentang cybercrime ini.

Lalu ada spontaneous information, lalu ada kejelasan tentang ekstradisi, ada juga kejelasan tentang mutual legal assistance, untuk akses computer data, dan juga tentang intersepsi. Jadi mutual legal assistance untuk interception, ada, dan perservasi data. Access computer data, interception, dan point of contact untuk 24/7 network. Lebih lanjut, kita akan perlu perhatikan tabel yang akan saya sampaikan.

Pemirsa, dalam perkembangannya, Convention on Cybercrime yang dirumuskan tahun 2001, kemudian mendapatkan kritisi sehingga International Telecommunication Union membuat research untuk melihat apakah perumusan yang 2001 tadi, perlu dikembangkan lebih lanjut atau tidak. Mereka membuat panduan buat negara berkembang, tool kit untuk memberantas cybercrime tersebut.

Namun, International Telecommunication membingkainya dalam pembicaraan tentang cybersecurity. Sehinggacyber security paling tidak salah satu agendanya membicarakan cybercrime law.

Jadi ada lima agenda dalam cybersecurity menurut ITU yang nanti akan saya paparkan khusus dalam sesi tentang cybersecurity. Cuma menarik untuk kita lihat, mungkin nanti pemirsa mencermati, tolong mencermati tabel yang saya buat, bagaimana Indonesia juga mengakomodir tentang substantive law dari CoC dan ITU tadi.

Baik, mari kita telaah satu-satu. Convention on Cybercrime setidak-tidaknya untuk substantive ada lima title. Title pertama adalah offences against the confidentiality, integrity and availability of computer data and computer sytems. Apa saja yang di di dalamnya? Illegal access, illegal interception, data interference, system interference, dan misuse of devices.

Dalam title yang kedua, ada computer-related offences yaitu computer-related forgery - forgery itu pemalsuan, computer-related fraud, itu penipuan dan pencurian. Lalu ada title tiga, content-related offences yaitu tindak pidana-tindak pidana yang terkait dengan konten: child pornography dan pelanggaran terhadap copyright dan neighbouring rights atau hak-hak yang berkaitan dengan hak cipta.

Lalu title yang keempat bicara tentang offences related to infringements of copyright and related rights, ya. Maaf tadi agak sedikit kecampur ya. Offences terhadap copyright and related infringement rights. Dan title kelima tentang pemidanaan terhadap ancillary atau tindakan-tindakan keikutsertaan: ancillary liability and sanctions-nya. Jadi substantive law akan bicara seperti itu.

Video 4: Lingkup Pengaturan Hukum Cyber - Part 2

Lalu kita perlu cermati bagaimana ITU memberikan suatu model untuk perumusan substantive law-nya. Terdapat di title dua dari dokumen tersebut, yaitu acts against computers, computer systems, networks, computer data, content data, and traffic data. Di dalam section 2, terdapat unauthorized access to computers, computer systems, and networks. Dalam section 3, unauthorized access to or acquisiton of computer data, content data and traffic data. Kemudian tindakan interference and disruption, tindakan interception, misuse and malware, digital forgery, digital fraud, procure economic benefit, extortion, aiding, abetting and attempting, atau dia membedakan antara tindakan turut serta, perbantuan dan percobaan, dan tanggung jawab dari corporate.

Nah menarik di Indonesia. Kalau kita cermati Indonesia, secara substantif hal itu telah diakomodir. Ada illegal access, ada illegal interception, ada tentang data interference, tindakan pengubahan data, pengganggguan terhadap sistem, interference system, dan penyalahgunaan perangkat. Secara umum, semua ketentuan substantive law tadi sudah masuk dalam UU ITE, khususnya ketentuan-ketentuan tentang perbuatan dilarang dan ancaman pemidanaannya.

Bahkan kalau kita setidak-setidaknya mempunyai tiga pasal terkait dengan konten ilegal itu. Ada konten yang terkait pendistribusian dari konten ilegal, pengumuman dan perbanyakannya. Itu termasuk informasi tentang pemfitnahan, hoax, kekerasan, dan sebagainya. Anda bisa lihat sendiri di dalam konteks UU 11/2008 tentang perumusan pasal 27, 28, 29.

Apa saja itu? Penyebaran informasi ilegal, pelanggaran hak cipta, pemalsuan. Ya, komputer sebagai sasaran akan mencakup kepada akses tanpa hak, intersepsi melawan hukum, gangguan data, gangguan atau perusakan sistem dan penyalahgunaan perangkat.

Kita akan masuk dalam perbandingan berikutnya, yaitu perbandingan tentang procedural law. Jika kita cermati tabel berikut ini tentang procedural law, kita lihat convention on cybercrime, title satunya bicara tentang common provisions atau ketentuan umum terkait dengan lingkup procedural provision-nya. Conditions and safeguards, dan prinsip, yaitu penerapan prinsip proporsionalitas dalam penegakan hukum. Artinya due process of law dalam konteks berelektronik, itu menjadi perhatian penting.

Lalu title yang kedua, tentang expedited preservation of stored computer data. Di situ mencakup tentang preservation of stored computer data dan juga preservation and partial disclosure of traffic data. Computer stored data artinya komputer yang ada di dalam sini. Komputer yang terkait dengan traffic data adalah komputer mempunyai data yang bisa diakses dalam konteks komunikasi.

Lalu yang berikutnya, title tiga tentang production order. Yang berikutnya lagi tentang search and seizure of stored computer data, bagaimana mengeledah dan kemudian menyita computer data yang tersimpan. Tolong diperhatikan, ada computer stored data, artinya data yang tersimpan dalam komputer. Pada saat ini berkomunikasi, maka itu sudah communication data, bukan lagi yang ada di sini.

Jadi untuk menerangkan bahwa saya diancam oleh email seseorang, maka bukan hanya informasi yang ada di computer stored data, tetapi komputer yang ada di komunikasi. Misalnya saya pakai Yahoo. Yahoo juga menceritakan tentang informasi itu.

Lalu ada real-time collection of computer data. Harus ada upaya sedapat mungkin kalau bisa real-time itu diambil, diamankan. Pihak penegak hukum diminta tolong, data ini tolong diamankan. Hal itu juga serupa, diatur dalam ITU, ada expedited preservation and partial disclosure of traffic data, ada production order, ada search and seizure of stored data, ada interception baik real time maupun terhadap traffic data itu. Dan ada intersepsinya serta penentuan yurisdiksinya.

Hal yang menarik bahwa bicara tentang yurisdiksi itu tidak mudah. Kenapa? Karena pada, pada intinya, memberlakukan hukum pidana suatu negara pada suatu tindak pidana yang menyangkut negara itu atau dilakukan di negara itu, ini tidak mudah untuk diselesaikan, karena CoC atau Convention on Cybercrime belum putus bicara soal itu. Karena mereka menganut asas national active. Artinya negara melindungi bangsanya. Jadi kalau ada bangsa, ada warga negara melakukan sesuatu maka, hukum negara mengatakan harusnya hukum negara yang bersangkutan mengadili warga negaranya. Tapi konteks cross border ternyata tidak semudah itu.

Kalau di Indonesia, upaya penggeledahan rumah dan badan, penyitaan dan pemeriksaan surat sudah diatur dalam KUHAP. Cuma, memang masih ada silang sengketa, apakah surat yang dimaksud sudah menjangkau tentang keberadaan informasi elektronik? Sebagian menyatakan iya, sebagian lagi tidak. Dan kemudian dalam perkembangannya, ada Undang-undang tentang Pidana yang baru, tindak pidana yang khusus dengan dalih extraordinary dan kemudian memilah, bagaimana status alat buktinya. Nanti kita bahas dalam bentuk pembahasan dari evidence.

Tetapi dalam Undang-udang 11/2008, prinsip proporsionalitas sebagai bentuk jaminan terhadap condition and safeguards, dimana suatu pengamanan informasi elektronik jangan semena-mena, itu juga sudah diatur. Lalu dalam konteks telekomunikasi, sebelumnya di Undang-undang 36/1999, dalam kerahasiaan berita, yaitu informasi yang dikomunikasikan juga telah terjaga.

Intinya, kalau kita gambarkan dalam tabel, parsial kita juga sudah memenuhi procedural law ini. Namun untuk ekstradisi, kita tidak mudah. Ataupun dengan remote interception. Karena intinya, di Indonesia, prinsip penerapan ekstradisi adalah perjanjian bilateral. Tapi kalau konvensi regional Eropa, telah memungkinkan masing-masing member untuk bisa saling bekerjasama dengan lebih baik.

Tapi, dalam praktek pelaksanaannya, tetap saja, kedaulatan negara untuk melindungi data yang berada pada wilayahnya, itu menyelesaikannya bukan persoalan yang mudah. Sehingga beberapa waktu yang belakangan ini, mereka bahas itu dalam forum National Cybersecurity dan Global Cybersecurity bahwa perlu ada jaminan nih, akses terhadap suatu data-data yang berada pada satu negara jika ternyata isu kedaulatannya tidak mudah untuk diselesaikan.

Kita bahas lagi lebih lanjut, setelah tabel procedural law, tentang perbandingan international cooperation. Intinya, sebagaimana saya telah kemukakan, untuk Convention on Cybercrime, karena dia merupakan regional convention, masing-masing mereka tidak perlu ada perjanjian bilateral untuk menyelesaikan ekstradisi. Tapi di negara kita, itu tidak bisa dilakukan.

Lalu antarnegara mereka, memungkinkan adanya remote interception, atau remote access untuk computer stored data. Kalau kita enggak bisa karena ada kedaulatan kita untuk tetap menjaga bangsa dan datanya. Jadi untuk menyelesaikan ini, diperlukan suatu forum atau suatu sarana yang disebut mutual legal assistance. Ada negara yang

meminta dan ada negara yang dengan kerjasama internasionalnya me-reply permintaan tersebut.

Lalu, secara tidak langsung, kita telah menyelesaikan ya, substantive law-nya, perbandingannya, procedural law-nya dan international cooperation. Indonesia telah berupaya untuk mengakses Convention on Cybercrime tersebut. Tapi karena mengingat procedural law kita tidak sama dengan standar Eropa, maka dengan sendirinya kita sulit mengakses.

Hal ini juga bukan hanya dihadapi Indonesia, ini juga dihadapi oleh negara-negara ASEAN yang lain. Yang sukses mengakses hanya sebagian negara, contohnya adalah Amerika, yang mungkin hampir sama pola pikirnya dengan mereka dan standar procedural law-nya. Selanjutnya kita akan bahas lagi dalam pembahasan tentang materi penerapan yurisdiksi.

Video 5: Extraterritorial Jurisdiction

Pemirsa IndonesiaX, sebagaimana yang telah saya sampaikan sebelumnya, maka isu cross-border itu tidaklah mudah karena ujung-ujungnya kita akan bicarakan yurisdiksi negara mana yang harus berlaku untuk menyelesaikan tindak pidana itu. Mari kita ambil contoh. Saya tampilkan slide yang mungkin Anda bisa tertarik untuk mencermatinya.

Misalkan ada seorang warga negara AS, tinggal di Swiss. Mereka menyebarkan virus yang hosting-nya di Paris. Lalu merusak situs komersial di Thailand. Namun di sisi lain, merusak public utility di Indonesia, walhasil banyak kecelakaan yang terjadi di Indonesia. Karena pelayanan publik sudah online, maka sistem transportasi tersusupi virus dan kemudian terjadi kecelakaan, demikian pula transportasi darat dan transportasi laut. Misalkan seperti itu. Akibatnya di Indonesia, berakibat banyak hilangnya nyawa di negara kita.

Lalu, pertanyaannya, bagaimana menyelesaikan hal ini? Warga negaranya asing, kemudian dimana warga negara itu akan diambil, di wilayah negara yang lain, usia juga akan menentukan, kemudian negara yang bersangkutan apakah juga melakukan pemidanaan terhadap hal itu?

Kalau di kita dipidana, misalnya pornografi, tetapi di negara lain tidak dipidana, kita tidak akan mendapatkan mutual legal assistance untuk menangkap si pelaku dan mengamankan bukti. Karena kata kunci pidana kan adalah amankan bukti-bukti karena bukti itu akan menjadi bahan di persidangan dan kemudian mengamankan pelaku. Bisa menangkap, bisa menangkap si pelaku. Kalau tidak? Ya percuma. Si pelaku enggak bisa, bagaimana mau dipidana?

Nah, menarik ini. Apakah terjadi dual criminality dalam kasus tadi? Artinya negara yang bersangkutan dimana rampung perbuatan itu dilakukan, juga mengancam pidananya, juga mengancam tindakan tersebut sebagai pidana. Lalu, apakah tindakan itu dirumuskan secara formil deliknya atau secara materil? Kalau secara formil, maksudnya begini, begitu ada intention untuk merusak dan tindakan merusak itu rampung dilakukan, maka pada saat itu pula, berlaku hukum pidananya. Nah, kalau dalam negara yang merumuskan seperti itu, maka tidak harus terjadi di mana akibatnya.

Tapi kalau ada rumusan pidana yang menyatakan justru bukan formilnya, dia ingin mempidanakan kalau terjadi akibatnya, merusak dan kemudian terjadi akibat merusak,

maka mau tidak mau di mana perbuatan itu berakibat. Jadi perspektif yang satu menyatakan rampung perbuatan formilnya, yang satu terpenuhi dulu akibatnya.

Contoh yang paling mudah kalau kita melihat kepada delik pembunuhan adalah barang siapa mengakibatkan hilangnya nyawa orang lain, yang penting hasilnya harus tercapai dulu, baru berlaku itu pasal. Itu bagaimana teknik merumuskannya berbeda-beda antarnegara, meskipun sama-sama punya cybercrime regulation di negaranya.

Lalu, apakah ancaman pemidanaannya dianggap serius? Misalnya tadi, kalau di negara tersebut, dianggap anak kecil dan anak kecil tidak dipidana, maka menjadi masalah pada suatu negara, yang akibatnya, berakibat hilangnya nyawa. Di sana dianggap iseng-iseng, kemudian dihukum di bawah satu tahun, di kita ancaman serius. Sama dengan pembunuhan, di atas pembunuhan.

Maka dengan sendirinya, itu tidak mudah untuk menyatakan bahwa kita melepaskan si pelaku di negara tersebut, untuk lolos begitu saja. Sementara di negara kita, tentunya punya tendensi yang lebih kuat untuk menyelesaikan, bahwa harus berlaku hukum pidana kita.

Selain melihat hal ancaman yang serius tadi, apakah diancam serius pada suatu negara atau tidak, juga perlu dipertimbangkan, di mana bukti dapat diperoleh? Di mana saksi dapat, dapat diminta kerjasamanya, dihadirkan? Dan di mana tersangka bisa ditangkap?

Lalu selain itu, juga harus dibicarakan, diperhatikan, di negara mana yang dia mendapatkan kepastian dia akan mendapatkan peradilan yang fair? Impartiale, artinya kalau di situ negaranya ternyata tidak menguntungkan buat si tersangka karena belum apa-apa sudah tidak bisa dipercaya impartial-nya, maka tentunya negara yang memiliki warga negara berada di wilayah lain dan berakibat jelek kepada negara lain, tidak mau melepaskan kewenangannya untuk mengadilinya.

Nah, ini menarik. Karena si A, negara A beranggapan dia bisa menegakkan hukumnya, punya kepentingan untuk melindungi warga negaranya, misalnya warga negara Amerika Serikat yang tinggal di Swiss tadi. Lalu Swiss, kalau dia punya ketentuan cybercrime juga akan melakukan, berhak untuk mempidanakan, karena rampungnya terjadi di situ. Perbuatannya, tinggalnya di situ sehingga start-nya di situ.

Bisa juga negara di mana hosting berada, karena merasa bendanya ada di situ. Dan akibatnya juga terjadi di negaranya. Bisa terjadi Indonesia yang korbannya paling banyak. Maka untuk menentukan negara mana yang paling berwenang untuk menetapkan hukum pidananya dan melakukan peradilan pidana bagi si tersangka tersebut tidaklah mudah.

Nah, isu tentang hal ini belum sepakat di konvensi international. Tetapi pada sisi yang lain, hal ini harus dikemukakan, harus diambil titik tengahnya. Tapi setidak-tidaknya, konon kabarnya tengah ada pembicaraan secara internasional, apakah mungkin peradilan pidana dapat diselesaikan pada suatu negara dengan menerapkan hukum pidana dari negara lain. Mungkin bentuknya secara tidak langsung, seperti mandatory proceedings yang ditransfer, transfer of proceedings.

Tapi hal itu belum ada perkembangan terakhirnya, jadi istilah untuk penentuan cybercrime jurisdiction, itu kembali kepada negara tersebut punya pengaruh besar enggak untuk bisa mendapatkan bukti, mendapatkan saksi, menangkap si tersangka sehingga dia bisa menerapkan hukum pidana di negaranya.

Lalu, dari sisi yang lain, kalau kita melihat hal ini, dalam perkembangan, semuanya enggak ada yang berpikir bahwa enggak aktif keluar. Artinya, maksud saya begini. Tidak ada negara dalam konteks cross-border tadi berpikir, “Oh, yang berlaku negara lain untuk negara saya.” Enggak begitu. Yang ada adalah setiap negara memperluas jangkauan yuridiksinya atau lebih dikenal dengan extraterritorial jurisdiction.

Dengan paradigma KUHP sebenarnya sudah ada, extraterritorial jurisdiction, yaitu hukum negara Indonesia berlaku kepada pesawat Indonesia yang terbang ke negara lain, begitu, jika terjadi suatu tindak pidana di dalam pesawat. Atau di dalam kapal berbendera Indonesia. Atau, walaupun dia terjadi di negeri lain, warga negara lain yang melakukan, tapi akibatnya terhadap kita. Misalnya seperti layaknya pembakaran bendera Indonesia di luar negeri misalnya. Kita wajar memprotes dan sebagainya.

Posisinya, extraterritorial jurisdiction bukanlah hal barang baru. Nah, kalau untuk Indonesia dalam menerapkan hal ini, maka demi kepentingan nasional Indonesia, tidak hanya melindungi kepentingan warga negara Indonesia, tetapi kepentingan ekonomi nasionalnya, Indonesia bisa saja memberlakukan yurisdiksinya keluar.

Artinya, berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-undang ITE, dalam Undang-undang ITE 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. Anda bisa lihat dari pasal 2 Undang-undang 11/2008 tentang Informasi dan Transaksi Elektronik.

Video 6: Penyidikan dan Penyadapan dalam Hukum Indonesia

Selanjutnya, kita akan membicarakan pemikiran tentang penyidikan. Penyidikan mau tidak mau akan melihat kepada kewenangan si penyidik berdasarkan kitab Undang-undang Hukum Acara Pidana. Dan dalam kitab Undang-undang Hukum Acara Pidana, jelas dimungkinkan juga adanya penyidik pegawai negeri sipil, PPNS. Dalam konteks siapa pelaku penyidik, baik PPNS maupun kepolisian, harus memperhatikan beberapa prinsip-prinsip dalam hak perlindungan hak asasi manusia terkait benda dan privacy orang.

Pasal 42 mengatakan bahwa penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-undang ini. Perlu kita catat bahwa sepanjang tidak diatur lebih khusus dalam Undang-undang ITE, maka tentunya kembali kepada KUHAP.

Dengan kata lain, jika karena suatu kepentingan perlu dan mendesak, maka suatu benda elektronik, dalam konteks di sini adalah informasi elektroniknya, bukan sistem elekroniknya lho ya. Kalau sistem elektroniknya kalau mau disita, minta penetapan pengadilan.

Tapi kalau contohnya USB, data-data informasi elektroniknya perlu mendapatkan tindakan secepatnya, itu tidak perlu harus digantungkan pada izin peradilan dulu untuk menyita data elektronik tadi. Karena itu adalah kondisinya benda bergerak. Tapi kalau benda tidak bergerak, barulah membutuhkan penetapan pengadilan.

Selanjutnya perhatikan pasal 43 Undang-undang ITE, dimana penyidik harus memperhatikan aspek privacy, kelancaran pelayanan publik, dan keutuhan data yang diperoleh sebagai bukti. Dengan kata lain, integritas data dan kerahasiaannya. Kalau

seseorang penyidik menyadap, tidak dengan sendirinya hasil sadapan dilakukan penyidik itu boleh-boleh saja diungkapkan begitu saja kepada publik.

Karena apapun yang diperoleh oleh penyidik adalah rahasia penyidikan. Demikian pula halnya dengan kita melakukan intersepsi, tidak boleh dengan sewenang-wenang. Intersepsi itu ada tata caranya. Setidak-tidaknya tata cara intersepsi, tidak boleh bertentangan dengan HAM. Isu untuk penyadapan tadi sebenarnya itu bisa dipelajari di KUHAP, Undang-undang HAM, Undang-undang Telekomunikasi, dan juga Undang-undang ITE.

Tetapi yang menarik, yang harus kita waspadai adalah setiap upaya meng-intercept, itu dua kepentingan. Kalau kepentingan intelijen, dia tidak perlu, tidak harus selalu memperoleh informasi karena suatu kala, dia membutuhkan suatu tindakan pencegatan informasi agar komunikasi itu tidak terjadi.

Contoh, misalnya ada suatu ruangan, orang meletakkan ransel berisi bom. Dan detonatornya dipicu oleh hubungan komunikasi berdasarkan handphone. Jadi seluler kepada seluler lain, di-call, kemudian dia bisa meledak. Jika dia mengetahui seperti itu, maka yang terjadi, harus dilakukan apa? Di-intercept, dicegat, di-jammed, akibatnya komunikasi tidak terjadi. Di situ, poinnya tidak diperoleh informasi untuk jadi bukti, tetapi upaya pencegahan jangan sampai terjadi suatu ledakan.

Demikian pula upaya-upaya intelijen. Intinya, upaya-upaya yang seperti itu tidak menginginkan informasi jadi bukti, tetapi untuk mengetahui informasi itu saja. Demi kepentingan masyarakat yang lebih besar, yaitu kepentingan keamanan negara atau kepentingan hal-hal yang seperti teror tadi.

Menarik untuk dicermati, intersepsi sekarang ini seringkali dilakukan oleh orang dengan yang enggak ada urusannya dengan penegakan hukum. Coba perhatikan baik-baik beberapa fenomena yang sebelumnya. Bahkan dalam praktik di internet, kita melihat ada beredarnya alat-alat sadap. Padahal penyadapan terlarang, kecuali dilakukan oleh aparat penegak hukum.

Aparat penegak hukum melakukan dengan prosedur yang ketat. Jadi hati-hati. Prosedur yang ketat itu saja masih dapat mempidanakan penegakan hukum jika dia melakukannya secara sewenang-wenang. Jadi intersepsi tidak dapat dilakukan oleh setiap orang dan dia harus memenuhi tata cara yang ketat agar informasi elektronik yang diperolehnya dapat menjadi alat bukti di persidangan.

Penting untuk dicermati, scope of power, dari si penyidik tadi. Convention on Cybercrime, menginginkan bahwa aspek procedural law yang digulirkan oleh Convention on Cybercrime, tidak hanya digunakan untuk menegakkan pidana cyber, tapi tindak pidana yang terkait dengan cyber, itu selayaknya dapat digunakan. Sehingga sepanjang informasi elektronik yang menjadi bukti, gunakanlah procedural law yang enggak ada dalam Convention on Cybercrime.

Hal serupa juga ada dalam pemikiran Indonesia. Kenapa? Kalau Undang-undang ITE menyatakan informasi elektronik sebagai alat bukti yang sah baru ada di Undang-undang ITE, maka keberadaan alat-alat bukti dalam 184 Kitab Undang-Undang Hukum Acara Pidana, dilengkapi dengan keberadaan Undang-undang ITE. Dengan sendirinya, Undang-undang ITE sebagaimana layaknya menghadirkan alat bukti yang lain, yaitu di luar lima kategori dari 184 Kitab Undang-undang Hukum Acara Pidana tersebut.

Apa saja upaya yang dilakukan untuk menggeledah dan menyita, ya? Search and seizure. Dalam konteks ini adalah melakukan akses kepada sistem dan melakukan

copying terhadap data. Saya ulangi. Geledah dan sita tadi sama kedudukannya dengan secara elektronik melakukan akses dan mengkopinya. Ya dia memeriksa, masuk ke dalam, melakukan akses, dan menyita dalam bentuk membuat salinan kopi terhadap file itu.

Selanjutnya, juga harus diperhatikan, bahwa penelusuran terhadap data-data tadi, itu harus yang kaidahnya adalah relevan. Jadi bahasa umumnya dalam acara pidana ini, intinya begini, hadirkanlah segala sesuatu sepanjang itu diperoleh secara halal oleh aparat penegak hukum yang bersangkutan, relevan dengan kasus, dan valid.

Jika tidak diproses secara halal, maka dengan sendirinya tidak dapat dihadirkan di muka persidangan. Karena itu dipahami sebagai, sebagaimana layaknya buah dari pohon beracun, istilahnya seperti itu. Tapi poin pentingnya adalah kalau aparat penegak hukum mendapatkan bukti, dia tidak boleh sewenang-wenang, jangan sampai bertentangan dengan due process of law.

Apalagi dalam menyadap. Karena menyadap, intinya adalah seseorang diberangus dengan ungkapannya sendiri dalam komunikasi yang dilakukannya kepada pihak lain. Itu artinya, seseorang dengan tidak sadar menyatakan sesuatu, kemudian dengan hal itu, dianggap pengakuan apa yang dilakukannya. Padahal belum tentu seperti itu.

Ambillah contoh begini. Saya dengan Anda, bergunjing tentang seseorang, ada orang kaya pakai mobil Alphard misalnya. Kemudian kita berdua berbicara, “Ayo, kita ambil yuk nanti, kalau orangnya pergi.” Apakah kata-kata penuhi suatu tindak pidana di sana? Belum, baru omongan gila-gilaan. Tapi ternyata 10 menit kemudian mobil itu memang hilang. Lalu apakah ada orang yang mendengarkan percakapan kita, langsung mengatakan, pelakunya kita berdua. Kan tidak seperti itu mestinya.

Artinya enggak bisa kita menyatakan bahwa informasi elektronik yang hasil intersepsi atau proses intersepsi itu dilakukan dalam rangka mencari bukti permulaan yang cukup. Apalagi jika dalam hukum acara yang bersangkutan, menyatakan bahwa dia hanya perluasan alat bukti petunjuk.

Tolong diwaspadai sedikit ya, pasal 5 di Undang-undang ITE dan pasal 6-nya, dimana dikatakan alat bukti yang sah menurut hukum acara yang berlaku, berarti dua pemikirannya. Hukum acara, ada yang menyatakan dia sebagai kategori alat bukti lain, melengkapi lima kategori alat bukti sebelumnya. Atau dia mengikuti hukum acara yang menyatakan bahwa informasi elektronik ini sebagai perluasan dari salah satu alat bukti berdasarkan KUHAP, yaitu alat bukti petunjuk. Ini karateristik dari, sedikit kelucuan ya, dalam hukum acara pidana yang sifatnya extraordinary.

Dia menyatakan sebagai perluasan alat bukti petunjuk, berarti dia harus ada kesesuaian satu dengan yang lain, baru boleh. Atau dia berdiri sendiri. Nah, ini sebenarnya yang harus diselesaikan oleh Undang-undang ITE, sepanjang dia diperoleh secara halal, relevan, dan valid. Selain itu, memenuhi apa? Pasal 6. Perhatikan, pasal 6 bahwa functional equivalent approach terpenuhi.

Artinya sepanjang writing unsurnya terpenuhi, original terpenuhi, signed terpenuhi, maka informasi elektronik tadi, tidak boleh ditampik. Kalau dia diperoleh secara halal oleh penyidik, maka dia harus menjamin, privacy-nya tidak terganggu, kelancaran pelayanan publik tidak terganggu, dan keutuhan data terjaga dengan baik. Bentuk-bentuk electronic digital tersebut, kita akan bahas lagi lebih lanjut dalam materi berikutnya.

Video 7: Digital Evidence – Part 1

Pemirsa IndonesiaX, kita perlu perdalam tentang aspek pembuktian ini. Inti pembuktian adalah menghadirkan segala sesuatu yang terkait dengan tindak pidana, diperoleh secara halal, relevan, dan valid ya.

Baik, sekarang kita lihat digital evidence ini. Ada di mana saja? Digital evidence kalau dalam suatu computer networking, maka dapat diperoleh di sini, di komputer si pelaku, di network yang dilaluinya, maupun di komputer si korbannya.

Dalam konteks seperti ini, kita tadi, saya telah, dalam pertemuan sebelumnya, saya telah sampaikan, ada computer stored data, di sini, akses terhadap computer stored data. Dan akses terhadap communication data. Communication data ini ada tiga hal.

Yang pertama, subscriber information. Katakanlah ingin mengetahui siapa sih pemilik, yang bertanggung jawab membuat IP ini, atau nomor handphone ini. Maka akan ditanyakan kepada si operatornya, “Itu nomor telepon, pelanggannya siapa?” Personal data pribadinya keluar, nomor kosong sekian-sekian, pelaku, namanya, subscriber-nya adalah si A, bla, bla, bla, bla, bla.

Lalu aktivitas dari si A ini menghubungi siapa saja. Seperti Anda kenal call data record, biasanya kalau kita pakai yang pasca bayar, kita langsung diberi tahu nomor telepon yang dihubungi siapa saja, berapa menit, kan begitu. Itu traffic data.

Lalu, pada saat kita bicara, nomor telepon ini ke nomor telepon ini, isi percakapannya itu content data. Selama ini, selama tidak ada kepentingan, si operator tidak perlu menyimpan content data tadi. Tapi content data seringkali diperlukan oleh aparat penegak hukum.

Dalam prakteknya, dahulu, operator yang merekam content tersebut berdasarkan permintaan dari penegak hukum. Seiring dengan perkembangannya teknologi, aparat penegak hukum mempunyai perangkat sendiri, yang dia perlukan cuma berkoneksi ke switch center-nya. Sehingga ini kita sebut sebagai remote interception.

Aparat penegak hukum mempunyai monitoring center, kemudian dia dikoneksikan dengan si swith center-nya si operator, dan operator cukup melayani permintaan tadi. Artinya begitu sudah terhubung online, maka penegak hukum akan mengindentifikasi siapa pelaku, kemudian menyasar, mencapai sasarannya, dan merekam konten data itu.

Ada standar dari European Telecommunications Standards Institute untuk hal tersebut. Ada H1, H2 dan H3. Hal itu terlalu teknis untuk saya jelaskan dalam forum Cyber Law. Tapi setidak-tidaknya yang perlu dikenali oleh peserta sekalian adalah digital evidence itu ada di sini, komputer si pelaku, misalnya, komputer si korban, dan ada juga yang direkam oleh network.

Perolehan data-data tadi perlu dipertimbangkan oleh penegak hukum untuk langsung mendapatkan dari pihak yang punya otorisasi ketimbang melakukan upaya paksa untuk memasuki digital evidence tersebut. Jadi, terkait communication data, perlu saya jelaskan, ada subscriber information, ada traffic data, ada content data. Dahulu permintaan content data diminta oleh para penegak hukum kepada si operator, operator yang dengan ruang sarananya merekamkan tersebut.

Dalam perkembangan teknologi, aparat penegak hukum terhubung dengan sistem tersebut dan melakukan perekaman sendiri. Untuk mengakses ini, tentunya dia memerlukan izin pengadilan jika ingin menjadikan bukti. Ini adalah kinerja aparat penegak hukum. Tapi kalau intelijen, dia cuma mendengarkan tapi tidak menjadi alat bukti di persidangan. Itu kondisi default-nya.

Apa yang terjadi di Indonesia belakangan ini, beberapa tahun yang lalu, sebagaimana kita ketahui, itu hanya adalah suatu kejadian yang extraordinary, yang secara kaidah hukumnya kurang tepat. Tapi mungkin karena keadaan saat itu adalah extraordinary, kita kurang tahu. Akibatnya pengungkapan hasil intersepsi dilakukan di depan mahkamah konstitusi yang sebenarnya itu tidak relevan dengan kasus.

Karena kasus yang harus dilakukan adalah kalau ada kasus pidana, kemudian ingin membuat terang siapa pelaku tindak pidana, baru alat bukti yang namanya hasil sadapan diungkapkan. Itu pun dengan catatan, bahwa tata cara perolehannya dilakukan dengan ketat dan itu upaya terakhir, dengan kata lain duly exhausted. Kalau enggak ada upaya lain, baru.

Dalam konteks ini, perlu diperhatikan, memperoleh semua data-data tadi tersebut dan mengolahnya sampai nanti ke muka persidangan, hal itu juga tetap memerlukan pendekatan-pendekatan yang konvensional. Jadi Anda bisa perhatikan slide saya tentang pendokumentasian TKP. Bahwa pada saat pelaku melakukan, jangan-jangan dia melakukan perhitungan dengan suatu rumus-rumus tertentu, ada bukti-bukti di sini, pada saat online dia seperti apa, offline seperti apa.

Kalau aparat penyidik ternyata mendapati dalam keadaan tertangkap tangan misalnya, pintu didobrak, kemudian dia melihat komputer dalam keadaan hidup, jangan dimatikan. Komputer dalam keadaan mati, jangan dihidupkan.

Karena itu, aparat penegak hukum memerlukan petunjuk pelaksanaan untuk hal ini, selain data tools kit, ya, perangkat-perangkat yang dipakai oleh para penegak hukum untuk mengamankan data tersebut. Selain bicara tentang pengamanan seperti itu, ada juga upaya pengamanan secara network forensic. Ilmu-ilmu seperti ini adalah ilmu forensik.

Video 8: Digital Evidence - Part 2

Dalam rangka digital evidence diamankan dengan baik, maka Anda memerlukan pengetahuan tentang forensik. Forensik itu intinya adalah segala sesuatu yang ingin disampaikan ke muka persidangan, untuk menjadi konsumsi persidangan, terutama pada saat pembuktian. Dimana hasil-hasil bukti itu akan dapat diterima hakim sehingga dapat menerangkan suatu informasi tentang siapa pelaku pidananya.

Ingat, sebagaimana Anda ketahui di dalam Kitab Undang-undang Hukum Acara Pidana, ada proses penyelidikan yaitu proses bagaimana memastikan apakah peristiwa itu adalah peristiwa pidana. Kemudian prosesnya berikutnya adalah penyidikan, dimana si penyidik berupaya mencari tahu, atau mencari bukti-bukti siapa pelaku tindak pidana. Sehingga pada saat ditemukan si pelaku, jadi tersangka, tersangka kemudian dituntut jadi, kemudian jadi terdakwa. Setelah itu, kemudian dia baru menjadi terpidana.

Baik, dalam konteks pengamanan bukti tadi, saya kemukakan ilmunya adalah tentang digital forensic. Selain teknik-teknik bagaimana mengamankan data, memperolehnya, dan menganalisisnya, teknik konvensional terkait dengan bagaimana konteks pada

saat pelaku melakukan, itu tetap memerlukan juga pendokumentasian terhadap TKP-nya.

Jadi selain komputernya posisinya di mana; mati, apakah mati atau hidup; bagaimana letak printer; dan semua surroundings tadi. Sehingga menjadi clue apakah benar si pelaku melakukan dalam kontekstual seperti itu. Jadi printernya juga mesti dilihat, CPU-nya seperti apa, dan sebagainya, ya.

Itu yang penting untuk diperhatikan selain kita bicara digital forensic, pengolahan data elektronik itu sendiri sebagai bukti digitalnya, ada software yang digunakannya, ada CPU lokasinya di mana, saluran telekomunikasinya, apakah dia pakai secondary storage, dan sebagainya. Dalam konteks ini, biasanya aparat penegak hukum, kalau dia masuk, kemudian dia lihat, maka alat-alat, tools yang dia pakai pun, itu juga spesial.

Data tools kit, misalnya, oh ternyata, handphone-nya itu dalam keadaan hidup, maka bagaimana caranya kondisinya tidak berubah, dia biasanya punya tool kit sendiri. Kemudian untuk mengamankan, apakah harus komputernya, kalau komputernya pada jaringan, misalnya server, maka yang harus dia lakukan cuma melakukan copying-nya saja.

Ada istilah itu, cloning atau imaging. Kalau cloning itu, metadata berubah. Kalau cloning, tidak berubah. Maaf terbalik. Cloning berubah. Imaging tidak berubah. Nah pada saat pengamanan data dilakukan, kemudian masuk, dapat first original copy, maka data di sini tidak berubah, maka penyidik membawa ini.

Ini di-hash, kemudian di-custody dengan baik, sehingga pada saat menjadi bukti, diberikan kepada analis forensiknya, analis forensik melakukan otopsi terhadap data tersebut, kemudian dia menganalisis, ini ilmu-ilmunya kalau misalnya Anda belajar ilmu komputer itu pada tahapan pengenalan dimana bagaimana menyimpan data pada suatu medium storage. Bagaimana suatu data ditemukan dalam network. Itu semua teknik-teknik dasar dari ilmu komputer.

Pada saat nanti diberikan, dianalisis, disampaikan, oh ada hubungan dengan ini, oh kegiatan penghilangan data dan sebagainya, itu dirangkai oleh si ahli tadi. Sama seperti pada saat seorang dokter memeriksa mayat, kurang lebih begitulah ahli-ahli IT akan bekerja dalam memeriksa semua digital-digital tadi, dirangkaikan, dan dia memberikan opini terhadap hal itu.

Jadi, kalau kita sarikan, computer forensic itu tersebut akan bicara soal segala apapun upaya dari si penyidik dan dibantu dengan para ahlinya untuk mendapatkan bukti tadi, mengamankannya, mengolahnya, dan mempresentasikannya di depan muka persidangan. Lalu pertanyaannya, apakah tindakan-tindakan tadi, cuma melakukan upaya untuk mengamankan bukti guna kepentingan penyidikan dan penuntutan? Ataukah ada hal lagi yang lain yang harus diperhatikan?

Kalau orientasinya cuma hukum, maka yang kepikiran adalah mengamankan bukti, dan akibatnya jangan-jangan sistemnya tidak bekerja. Padahal demi kelancaran publik, itu harus pulih kembali. Jadi kerja aparat penegak hukum dalam mengamankan bukti itu akan berbanding lurus dengan kebutuhan sistem elektronik untuk dipulihkan kembali. Recovery.

Nah, dalam konteks ini, maka bicaranya sudah incident response. Jadi kalau ada sesuatu kejadian, tindakan-tindakan pelanggaran terhadap suatu bekerjanya sistem, maka yang kemungkinan terjadi adalah incident response tetap harus dijaga, pengamanan bukti juga harus dijaga.

Nah, konteks-konteks seperti ini, kita akan bicara dalam tataran yang lebih luas, yaitu dalam lingkup pengertian tentang cyber security. Kita akan bahas berikut ini dalam percakapan berikutnya.

Video 9: Cybersecurity

Berbicara tentang cybersecurity, tidaklah suatu hal yang cukup mudah untuk ditelusuri lebih lanjut. Karena ada dua pendekatan. International Telecommunication, International Telecommunication Union, itu mendekati dalam perspektif civilian. Sementara untuk pertahanan, itu pendekatan ala NATO, yaitu Pertahanan Atlantik Utara itu.

Investigasi dan incident response, itu satu pasang. Dalam investigasi, upaya-upaya penyidik untuk mengamankan bukti-bukti, mengamankan bukti diperlukan untuk bisa membuat terang siapa si pelaku pidananya. Sementara di sisi lain, pihak-pihak yang terkait dengan penyelenggara sistem elektronik ini membutuhkan recovery secepatnya. Sehingga pembicaraan tentang cybersecurity ini, bukan isu yang mudah untuk diselesaikan.

Dalam konteks tertentu, memang tindak pidana. Tapi di sisi lain, jika ada upaya sistematis terhadap pelayanan publik, maka patut diduga ini sasarannya adalah untuk meluluh-lantakkan sistem elektronik negara tersebut. Bayangkan, kalau sistem transportasi udara kita diserang, system interference, dilakukan upaya ngutak-ngatik, kemudian sistemnya shut down, berapa ancaman jiwa yang akan terganggu di angkasa raya itu? Demikian pula, kalau transportasi umum. Demikian pula kalau ternyata itu listrik.

Maka semua tindakan, kalau dalam kacamata kriminal, mungkin itu hanya dilakukan oleh orang. Tapi jika itu diolah terus lebih jauh, jangan-jangan ada upaya sistematis, di belakang ini ada state actor, bukan lagi orang biasa. Maka terhadap pengolahan ini, untuk mampu mendeteksinya, menganalisisnya, bertahan, menyelesaikan, dan melakukan serangan balik, itu ilmunya cybersecurity plus resilience.

Jadi cybercrime, bicara soal penegakan hukum terhadap pelanggaran tadi. Kemudian ditegakkan hukum pidana, maka pelaku dapat dipidana. Ditemukan, kemudian dipidana. Tetapi ternyata di pembicaraan tentang hal ini tidak bicara-bicara dalam lingkup kecilnya saja. Perlu diperhatikan dalam lingkup luasnya.

Ini kejadiannya adalah misalnya Denial of Service Attack, cuma nge-ping nge-ping. Tapi kok dilakukan secara sistematis? Lewat botnet yang ada di luar negeri, itu berarti ada upaya eksplorasi. Atau ternyata mengirim virus, kecil, kecil, kecil, tapi ada upaya yang serangkai yang secara sistematis. Maka kita memerlukan suatu kejelasan.

Ada suatu sistem yang bisa mengenali, mendeteksi, mem-protect, membangkitkan kembali, dan harus ada ukuran seberapa jauh bangsa kita mampu bangkit kembali setelah serangan. Jadi ilmunya, pertama, crime. Ilmu berikutnya adalah tentang sejauh mana response ditangani dengan baik dan pulih kembali, ini ilmunya ketahanan nasional, cybersecurity and resilience.

Untuk melihat hal ini, ada tiga pendekatan. Pertama, pendekatan cuma computer security, Anda bisa lihat pada tabel yang nanti akan saya tayangkan. Pemahaman umum tentang cybersecurity itu adalah computer security dan information security-nya.

Dalam pemahaman yang civilian, yang dari ITU, itu ada lima hal yang harus diperhatikan. Yang direkomendasikan kepada semua negara. Kepada setiap negara yang terhubung dengan internet, harap perhatikan bahwa semua aset yang terhubung tadi, itu berbanding lurus dengan perlindungan private, individu, dan negaranya. Intinya, segala aset yang terhubung dengan internet, harus dilindungi.

Ada lima Global Cybersecurity Agenda yang digaungkan oleh ITU. Pertama, bicara tentang pembuatan cybercrime pada setiap negara. Kemudian, ada teknis dan prosedur-prosedur yang diperlukan untuk bagaimana menangani response, berkoordinasi dengan yang lain, terjadi information sharing, terjadi mutual legal assistance, sehingga semua tindakan-tindakan pelanggaran tadi dapat diselesaikan penyelesaiannya secara patut dan tidak mengganggu kelancaran layanan publik. Artinya, jangan demi pengamanan bukti, ternyata pelayanan publik terganggu oleh kinerja aparat. Aparat harus bekerja sementara kelancaran pelayanan publik tetap harus dipulihkan.

Lalu struktur organisasi. Struktur organisasi mana dari semua yang punya kewenangan, kita ketahui, BIN dengan investigasi intelijennya, polisi dengan investigasi penyelidikan hukumnya, pertahanan dengan kemampuan resilience dan defence, kemudian dari sisi yang lain untuk CERT, Computer Emergency Response Team. Goverment dilakukan oleh Kominfo. Swasta melakukan sendiri namanya private untuk CERT, yaitu Computer Emergency Response Team, ID-CERT, itu swasta. Semua harus berada dalam satu rangkaian sistem yang memungkinkan semua ancaman, semua kerentanan keamanan dapat teridentifikasi dengan baik dan terselesaikan dengan baik dengan kinerja semua aparat ini.

Kalau kita bawa pendekatan defence, maka tentunya semua seakan-akan dalam keadaan tercekam dan perlu ada tindakan serangan balik. Tapi kalau kita lihat dalam kacamata penegakan hukum, jangan-jangan semua dianggap kecelakaan kecil saja. Atau dianggap sebagai suatu tindak pidana ringan saja, tidak dilihat bahwa ternyata di belakangnya, jangan-jangan ada organized state actor, selain hanya kecenderungan pelakunya.

Bisa jadi loh, orang yang menyebarkan virus justru dapat dari yang lain. Bisa jadi loh intelijen negara lain menanamkan semua pelaku hacker seakan-akan di Indonesia. Bisa jadi juga ada gerakan-gerakan yang menaruh botnet di dalam infrastruktur pelayanan publik kita. Ujung-ujungnya semua itu menjadi ukuran sejauh mana ketahanan nasional kita diterapkan dalam lingkup cyber tersebut.

Kita lihat cybersecurity itu lebih jauh. Kalau ITU berpikir dengan Global Cybersecurity Agenda tadi, yang sebagaimana tadi saya sampaikan, lima hal yaitu legal measures-nya, yaitu cyber law-nya adakah? Kemudian technical and procedural measures, organizational structures, kemudian upaya meningkatkan capacity building dan user's education awareness, dan keberadaan international cooperation untuk penanganannya. Terutama untuk mutual legal assistance.

Tapi ada pendekatan lain juga yang disampaikan NATO, yaitu, lihat military cybercrime, military cyber harus ada, counter cybercrime, intelligence and counter-intelligence, critical infrastructure protection and national crisis management, cyber diplomacy and internet governance. Yang intinya, pemerintah juga melihat dan memberdayakan sistem pertahanan semesta dari bangsanya.

Ada lima dilema mau tidak mau. Yaitu bagaimana mem-balance antara cost dan benefit dari national cybersecurity tersebut. Menstimulasi ekonomi, secara sisi yang lain, menjaga national security-nya. Memodernisasikan infrastrukturnya versus menjaga

critical infrastructure-nya. Menumbuhkembangkan private sector sementara harus menjaga public sector. Menjaga data proteksi sambil berbanding lurus national security plus information sharing. Jangan sampai dengan privacy, kemudian seseorang bisa saja menyembunyikan aktivitas dia selaku pelaku kejahatan. Kemudian, freedom of expression dengan stabilitas negaranya.

Video 10: Ketahanan dan Keamanan Cyber

Menarik untuk dicermati bahwa cybersecurity akan bicara sejauh mana negara tersebut mampu mensinkronisasi, berkoordinasi, melakukan pengendalian terhadap semua kejadian tersebut. Dalam perkembangannya, cybersecurity itu akan setidak-tidaknya melihat bukan hanya aset yang terhubung, tapi menjamin digital access dari setiap warga negaranya kepada internet. Karena itu salah satu perlindungan hak asasi manusia.

Yang kedua, semua yang terhubung dengan internet, semua institusi-institusi strategis tadi tetap stabil. Dan yang ketiga, economic development. Semua yang berhubungan dengan ekonomi via internet, tetap terjaga dan menumbuhkembangkan perekonomian bangsa dan negara itu sendiri. Jadi dengan sendirinya cyber resilience akan bicara sejauh mana, secepat mana negara itu bangkit kembali setelah adanya serangan.

Gampangnya begini. Dia mampu mengenali ancaman tersebut, berkoordinasi, bersama menghadapi ancaman dan serangan tersebut, kemudian memulihkan sekiranya terjadi setelah serangan tersebut, menemukan siapa pelakunya, menangkap, dan mempidanakannya. Di sisi lain, cepat recovery. Kemudian mengambil pembelajaran dari situ, tumbuh kembali apa yang tadinya sudah tertata, jadi direspon cepat, kemudian bangkit kembali, dan akibatnya masyakatnya tetap ter-service dengan baik via internet.

Secara security, saya kembali mengingatkan sebagaimana pada materi sebelumnya, ada individual security dulu. Kemudian working group-nya dia, enterprise-nya dia, regionalnya dia, dan internasional. Secara keseluruhan, kepentingan cybersecurity global adalah cyberspace tetap berjalan terus dengan baik, penanganan penyalahgunaannya, dikoordinasikan antara satu negara, saling bekerjasama untuk mengamankan data, dan menemukan pelaku. Kemudian mencari jalan-jalan damai sekiranya terjadi perseteruan-perseteruan yang tidak perlu antarhubungan cyber tadi.

Lebih lanjut lagi kita pelajari, bahwa di Indonesia diperlukan suatu koordinasi yang sifatnya lintas sektoral, yang mungkin belum dapat dijalankan oleh existing government agency. Dalam konteks ini, Kominfo mungkin bisa mengkoordinasikan untuk government security, tetapi belum tentu kepada military-nya.

Intinya, kalau kita kembali mengulang, kondisi ketahanan nasional itu posisinya apa sih? Asta Gatra? Ipoleksosbudhankam? Indonesia harus memperhatikan kondisi strategisnya, kondisi bangsanya. Strategi hubungan keluar ke dalamnya, sehingga kita perlu perapihan kembali peraturan perundangan-undangan terkait ketahanan dan keamanan.

Maka sangat menarik bahwa di Indonesia pada saat setelah masa reformasi bergulir, pertahanan dan keamanan dulu satu pasang, kini terpisah. Definisi keamanan sendiri bahkan kita tidak temukan sebagai satu kondisi yang clear. Ketertiban, keamanan masyakat berada dalam wilayah penegakan hukum. Pertahanan bicara soal ketahanan dan perlindungan terhadap kedaulatan negara.

Yang menarik, semua perkembangan terakhir ini, telah teridentifikasi oleh kajian-kajian dari Dewan Ketahanan Nasional. Demikian pula dari Lembaga Ketahanan Nasional. Kemudian kajian juga dari Kominfo tentang perlunya suatu lembaga koordinasi dalam menyingkapi semua aspek keamanan tadi.

Baik yang memberdayakan swasta, individu, akademisi, lembaga intelijen, lembaga pengolah kriptografi, lembaga sandi negara, kemudian lembaga kepolisian, lembaga yang terkait dengan sistem pertahanan. Semua harus kompak untuk bisa menjaga negeri ini dalam suatu rangkaian koordinasi.

Satu koordinasi, ia menjalankan koordinasi. Yang sektor riil, sebagai yang implementing, ia berjalan dengan implementing-nya. Ini ke depan membutuhkan bahwa ada suatu lembaga khusus untuk melakukan koordinasi keamanan dan pertahanan tadi, agar jangan sampai segala sesuatu disikapi dengan begitu simpel, padahal di belakangnya ada ancaman yang luas. Juga begitu, pada sisi yang lain jangan sampai semua khawatir dengan ancaman yang luas, padahal itu kejadiannya cuma kenakalan biasa.

Idealnya, begitu masuk ke dalam level yang lebih tinggi lagi, kalau sekiranya itu serangan, seorang presiden mendapatkan supply informasi yang baik dari semuanya. Sebelum dia tanya masing-masing agencies tadi, lembaga koordinasi tadi telah mampu mengolah kepada si top management negara.

Ia akan bertanya, “Ada apa di belakang ini?” “Oh, yang belakang ini, kemungkinan terjadi, alternatif satu, dua, tiga, empat.” Oh, serangan. Kalau serangan, apakah kita akan mampu membalasnya? Apakah kita mampu membalas dan menghadapi serangan baliknya?

Apakah lebih bagus kita menjalankan cyber diplomacy saja? Itu semua terjawab kalau kita punya satu lembaga sentral koordinasi untuk menangani semua ancaman tadi dan serangan, bahkan mengindentifikasi dan memproteksi negara kita secara berkelanjutan. Sehingga pemanfaatan cyberspace dapat mengatakan menjamin freedom of speech, menjaga security negara, membuka akses pelayanan publik menjadi lebih baik, security bertambah dengan sendirinya, economic growth akan tercapai.

Peserta IndonesiaX, materi cybersecurity adalah materi penutup kajian kita. Dimana negara dan bangsa membutuhkan sistem pertahanan dan keamanan yang baik untuk dapat membuat bangsa dan negara ini eksis dalam pergaulan dunia, tidak hanya secara konvensional, bahkan juga secara elektronik. Jangan sampai connectivity yang tidak baik, tidak diiringi dengan kesadaran security, justru malah akan membuat luluh lantak negara. Itu menjadi perhatian kita bersama. Mari kita mulai dengan user security awareness, kesadaran setiap kita bahwa keamanan itu adalah hak kita dan juga kewajiban kita dalam menjaga ketahanan nasional negara ini, dalam komunikasi cyberspace-nya. Terimakasih atas perhatian Anda, sampai berjumpa lagi dalam lain acara.