E-ISSN: 2620-5904
SOUMATERA LAW REVIEW
(http://ejournal.kopertis10.or.id/index.php/soumlaw)
Volume 3, Nomor 2, 2020

Perlindungan Data Elektronik Dalam Formulasi Kebijakan Kriminal Di Era Globalisasi

Yasmirah Mandasari Saragih* **Dudung Abdul Azis***
Submitted: 07-06-2020, Reviewed: 31-10-2020 Accepted: 31-10-2020
DOI: http://doi.org/10.22216/soumlaw.v3i1.4125

Abstract: *The development of information and communication technology has changed the behavior of society globally (cultural transformation) and caused the world to be without limits and social changes that are so rapidly progressing. The rate of development of information technology and a communication is one of the criteria that must be met for the progress of the nation. Cybercrime is one of the new forms or dimensions of today's crimes gaining widespread attention internationally. Utilization of computer technology continues to evolve has led to the process of convergence between information technology, media and communications to ultimately produce a new tool known as the Internet, as well as the beginning of the birth of civilization in cyberspace. Data is a form of jama from datum, derived from Latin meaning "given something". At present, information is a very decisive medium for the economic development of a country both developing and developed countries. Information about individuals is always administered by government and private, but the advent of the computer age creates a greater threat to the privacy of the individual, as well as the likelihood of individuals suffering losses as a result of inattention or leakage of information will be much greater. It should be noted, however, that in the cybercrime world, the majority of illegal access to computer systems or networks is used as a first step towards actions that lead to other forms of cybercrime. In this paper the author discusses about how electronic data protection as a cybercrime in the era of globalization today and how the criminal policy formulation review in an effort to protect electronic data. Although cybercrime or cybercrime generally refers to criminal activity with computers or computer networks as its primary element, it is also used for traditional criminal activities where computers or computer networks are used to facilitate or enable such crimes to occur.*
Keywords: *Electronic Data, Formulation, Criminal Policy.*

Abstrak: Perkembangan teknologi informasi dan komunikasi telah mengubah perilaku masyarakat secara global (transformasi kultural) dan menyebabkan dunia menjadi tanpa batas serta perubahan sosial yang secara signifikan berlangsung demikian cepat. Laju perkembangan teknologi informasi dan suatu komunikasi merupakan salah satu kriteria yang harus dipenuhi untuk kemajuan bangsa. *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Pemanfaatan teknologi komputer yang terus berevolusi telah menyebabkan proses konvergensi antara teknologi informasi, media dan komunikasi hingga pada akhirnya menghasilkan sarana baru yang dikenal sebagai internet, sekaligus menjadi awal lahirnya peradaban di dunia maya. Data adalah bentuk jama dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan". Pada dewasa ini, informasi merupakan suatu media yang sangat menentukan bagi perkembangan ekonomi suatu negara baik negara berkembang

* Universitas Pembangunan Panca Budi Medan, yasmirahmandasari@gmail.com, S.H.,M.H (Universitas Pembangunan Panca Budi Medan).,DR (Universitas Islam Sultan Agung)
* Universitas Bung Karno, dudungazis@yahoo.com, S.H., (Sekolah Tinggi Hukum Indonesia Jakarta) M.H (Universitas Pancasila).,DR (Universitas Dipenegoro)

maupun negara maju. Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidak telitian atau pembocoran informasi akan jauh lebih besar. Perlu diketahui pula, bahwa di dunia *cybercrime*, mayoritas dilakukan suatu akses tidak sah (*illegal access*) terhadap sistem atau jaringan komputer sebagai langkah awal dari perbuatan yang mengarah pada bentuk-bentuk *cybercrime* lainnya. Dalam tulisan ini penulis membahas tentang bagaimanakah perlindungan data elektronik sebagai suatu *cybercrime* di era globalisasi dewasa ini dan bagaimanakah tinjauan formulasi kebijakan kriminal dalam upaya perlindungan data elektronik tersebut. Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.
Kata kunci: Data Elektronik, Formulasi, Kebijakan Kriminal.

A. Pendahuluan

Eksistensi era globalisasi telah menjadi suatu motivator lahirnya era perkembangan teknologi informasi dan komunikasi. Fenomena tersebut telah mewabah di seluruh belahan dunia, bukan hanya di negara yang berkategorikan negara maju tapi telah merebak pula kenegara-negara yang sedang berkembang. Perkembangan teknologi informasi dan komunikasi yang berlangsung hampir di semua bidang kehidupan merupakan ciri dari suatu peradaban dunia pada masa kini. Perkembangan teknologi informasi dan komunikasi telah mengubah perilaku masyarakat secara global (transformasi kultural) dan menyebabkan dunia menjadi tanpa batas serta perubahan sosial yang secara signifikan berlangsung demikian cepat. Laju perkembangan teknologi informasi dan suatu komunikasi merupakan salah satu kriteria yang harus dipenuhi untuk kemajuan bangsa.

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional (Arief, 2006b). Perkembangan teknologi informasi ditunjukkan dengan adanya suatu invensi terhadap perangkat elektronik yang dinamakan komputer. Komputer adalah alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmetika, dan penyimpanan. Pengertian komputer bukan hanya mengarah pada bentuk *personal computer*, *notebook* dan laptop sebagaimana lazim digunakan di perkantoran saat ini, tetapi mencakup segala peralatan yang memenuhi pengertian dan fungsi tersebut, termasuk pesawat *handphone* (Widodo, 2006). Pemanfaatan teknologi komputer yang terus berevolusi telah menyebabkan proses konvergensi antara teknologi informasi, media dan komunikasi hingga pada akhirnya menghasilkan sarana baru yang dikenal sebagai internet, sekaligus menjadi awal lahirnya peradaban di dunia maya.

Jaringan internet adalah media yang paling cepat terinovasi ke segala lini dan paling adaptif dengan kebutuhan masyarakat (Bungin, 2005).

Kebutuhan akan teknologi informasi yang dapat diaplikasikan dengan jaringan internet dalam segala bidang telah menjadi sesuatu yang lumrah. Internet telah menciptakan sebuah dunia komunikasi berbasis komputer yang menawarkan realitas baru berbentuk virtual (tidak langsung dan tidak nyata) membuat segala bidang kehidupan masyarakat tidak dapat terlepas dari keberadaan internet. Melalui dunia internet atau yang sering disebut dengan istilah *cyberspace*, segala bentuk kegiatan kreativitas masyarakat dapat dilakukan secara *borderless* yang dapat menembus berbagai batas negara di dunia. Perkembangan teknologi informasi tidak saja mampu menciptakan dunia global, namun juga telah mengembangkan ruang gerak kehidupan baru bagi masyarakat yaitu kehidupan masyarakat maya *(cyber community)*. Seiring dengan perkembangan internet yang semakin hari semakin meningkat dan menunjukkan kelajuan yang sangat pesat, tidak dipungkiri bahwa internet dapat membawa kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia. Hal tersebut ditunjukkan dengan adanya pemanfaatan internet yang digunakan untuk mempermudah manusia dalam melakukan aktivitas sehari-hari seperti: e-banking (aktivitas perbankan melalui media internet), e-learning (aktivitas pembelajaran atau pendidikan melalui media internet), *ecommerce* (aktivitas transaksi perdagangan melalui media internet), *e-government* (aktivitas pelayanan pemerintahan melalui media internet), dan sebagainya.

Pada dewasa ini, informasi merupakan suatu media yang sangat menentukan bagi perkembangan ekonomi suatu negara baik negara berkembang maupun negara maju (Dewi, 2009). Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai akibat dari ketidaktelitian atau pembocoran informasi akan jauh lebih besar (Marrett, 2002). Era digital telah memicu ledakan pertumbuhan data pribadi yang dibuat, disimpan dan ditransmisikan pada komputer dan perangkat mobile, broadband dan situs internet dan media (Shilling, 2011). Kemajuan teknologi juga menimbulkan ancaman serius bagi privasi pribadi dan keamanan informasi. Dalam konsep hukum telematika, data merupakan representasi formal suatu konsep, fakta, atau instruksi. Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Data adalah bentuk jama dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan" (Purwanto, 2007). Data adalah setiap informasi yang

diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan.

Ancaman penyalahgunaan data pribadi di Indonesia menjadi kian mengemuka, terutama sejak pemerintah menggulirkan program KTP elektronik (e-KTP), serta rencana kepolisian untuk membangun Indonesia *Automatic Fingerprints Identification System* (INAFIS). Walau pada akhirnya polisi kemudian membatalkan rencana tersebut, karena dianggap tumpang tindih dengan program e-KTP. Selain program perekaman data pribadi oleh pemerintah, perekaman juga dilakukan oleh swasta, seperti bank dan penyedia layanan telekomunisi. Terkait hal ini, beberapa waktu lalu publik sempat dihebohkan dengan adanya informasi mengenai dugaan bocornya 25 juta data pelanggan telepon seluler ”Ancaman penyalahgunaan data pribadi” dalam Mengenai program e-KTP untuk pertama kalinya pemerintah meluncurkannya pada awal tahun 2011. Program e-KTP merupakan implementasi dari program Nomor Induk Kependudukan (NIK). Program ini menghendaki identitas tunggal setiap penduduk, yang berlaku seumur hidup, satu kartu untuk setiap penduduk, yang di dalamnya terdapat NIK.

Selanjutnya perekaman data penduduk dilakukan pemerintah dalam rangka pelaksanaan program ini. Seluruh informasi pribadi warga negara direkam, termasuk identitas dan ciri-ciri fisiknya. Khusus perekaman ciri-ciri fisik, dilakukan dengan pemindaian terhadap sidik jari dan retina mata, yang akan digunakan untuk validasi biometrik pemegang KTP. Menurut informasi Kemendagri, hasil dari perekaman data tersebut kemudian akan ditanam di dalam KTP, dengan terlebih dahulu dienkripsi menggunakan algoritma kriptografi tertentu. Beberapa pertanyaan layak dilontarkan terhadap praktik perekaman data e-KTP. Kenyataannya terdapat Perbedaan penafsiran dalam peraturan dengan praktek di lapangan. Misalnya terkait dengan sistem pengaman e-KTP. Menurut Perpres No. 67 Tahun 2011, sistem pengaman (validasi biometrik) hanya akan menggunakan pemindaian sidik jari, akan tetapi dalam praktik perekaman data, ternyata dilakukan pula perekaman terhadap retina mata. Bocoran informasi dari kawat Wikileaks yang berisikan presentasi sebuah perusahaan Inggris ThorpeGlen (2008), mengenai metode pengamatan (*surveilence*) yang bisa dilakukan dengan menggunakan e-KTP, kian menambah kekhawatiran. Menurut informasi tersebut,

dengan menggunakan perangkat e-KTP, warga negara dapat dilacak keberadaan dan aktivitasnya. Memanfaatkan metode ini, negara bisa dengan mudah mengamati kehidupan pribadi setiap warganyayang menyebabkan kebebasan sipil dilanggar dengan semena-mena.

Perlu diketahui pula, bahwa di dunia *cybercrime*, mayoritas dilakukan suatu akses tidaksah (*illegal access*) terhadap sistem atau jaringan komputer sebagai langkah awal dari perbuatanyang mengarah pada bentuk-bentuk *cybercrime* lainnya. Jika setelah melakukan akses tidak sah, kemudian pelaku melakukan gangguan atau perubahan atau perusakan atau penghalangan akses data pada komputer pihak lain secara tidak sah, maka perbuatan itu disebut data i*nterference*. Jika data yang diubah secara melawan hukum tersebut adalah *frontpage* suatu website milik pihak lain maka perbuatan tersebut dikategorikan *defacing* (Widodo, 2013). Seiring dengan meningkatnya aktivitas cracking serta defacing di Indonesia, pemerintah seharusnya sudah memiliki suatu konsep kebijakan penanggulangan kejahatan (*criminal policy*) yang lebih efektif, baik melalui sarana penal (hukum pidana) maupun sarana non-penal (di luar hukum pidana). Berkaitan dengan upaya penanggulangan kejahatan melalui sarana penal, sebenarnya Indonesia memiliki beberapa ketentuan undang-undang yang sekiranya dapat diterapkan terhadap kejahatan terhadap data elektronik yang telah digunakan aparat penegak hukum sebagai dasar penjerat pelakunya, seperti : Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP), Undang-Undang No. 16 Tahun 2016 tentang Perubahan atas Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (selanjutnya disebut UU Telekomunikasi), dan undang-undang lain yang berkaitan dengan perbarengan tindak pidana lain yang dilakukan pelaku kejahatan terhadap data elektronik.

B. Metodologi Penelitian

Penelitian ini merupakan penelitian yang bersifat normatif. Jenis penelitian yang digunakan adalah yuridis normatif. Pendekatan penelitian yang digunakan meliputi pendekatan undang-undang, dan pendekatan kasus (Laurensius Arliman S, 2018). Jenis data yang digunakan adalah data sekunder. Sumber data sekunder yang digunakan mencakup bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Bahan-bahan hukum primer terdiri dari perundang-undangan, risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim . Undang-undang yang diteliti adalah UU ITE. Teknik pengumpulan

data yang digunakan berupa bahan pustaka melalui buku-buku literatur, peraturan perundang-undangan, serta pengumpulan data, melalui media elektronik yang berhubungan dengan masalah yang diteliti. Analisis yang digunakan adalah kualitatif yaitu menganalisis data penelitian untuk selanjutnya dikaji secara mendalam dan diinterpretasikan oleh peneliti untuk mendapatkan kesimpulan yang diharapkan (Yasmirah Mandasari Saragih, Teguh Prasetyo, 2018). Bahan hukum yang sudah disistematisasi kemudian dianalisis secara kualitatif.

C. Hasil dan Pembahasan

1. Perlindungan Data Elektronik Sebagai Suatu Cyber Creame di Era Globalisasi

Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual. Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *cybercrime, Internet Fraud*, dan lain-lain (Laurensius Arliman S, 2020). Sedangkan Volodymyr Golubev menyebutnya sebagai *"the new form of antisocial behavior"* (Arief, 2007). *Cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. (Hamzah, 2014) mengartikan *cybercrime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.Kejahatan dunia maya atau *cybercrime* adalah istilah yang mengacu kepada aktivitas kajahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Terdapat tiga pendekatan untuk mempertahankan keamana di *cyberspace*. Pertama adalah pendekatan teknologi. Kedua, pendekatan sosial, budaya dan etika. Ketiga, pendekatan hukum. Untuk mengatasi gangguan keamanan, prndekatan teknologisifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak. *Cybercrime* dapat dilihat dari dua sudut pandang:

1) Kejahatan yang menggunakan teknologi informasi sebagai fasilitas, seperti: pembajakan, pornografi, pemalsuan/pencurian kartu kredit, penipuan lewat email (fraud), email spam, perjudian online, pencurian account internet, terorisme, isu sara, situs yang menyesatkan, dan sebagainya;
2) kejahatan yang menjadikan sistem teknologi informasi sebagai sasaran, seperti: pencurian abstracts pribadi, pembuatan/ penyebaran virus komputer, pembobolan/ pembajakan situs, *cyberwar, Denial of Service* (DoS), kejahatan berhubungan dengan nama domain, dan sebagainya. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain: a) *Unauthorized Access*, merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya, seperti *probing* dan *port*, b) *Illegal Contents*, Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, seperti: penyebaran pornografi, dan c) Penyebaran virus secara sengaja, penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Menurut F-Secure, pada tahun 2007 terdapat sekitar 500.000 kode jahat lahir;
3) Data *Forgery*, Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *web database*;
4) *Cyber Espionage, Sabotage and Extortion, Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet;
5) *Cyberstalking*, kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan

dilakukan berulang-ulang. Kejahatan ini menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya;

6) *Carding, carding* merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet;
7) *Hacking dan Cracker*, istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. *Cracker* adalah *hacker* yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*), merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan;
8) *Cybersquatting and Typosquatting*, *Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. *Typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain, yang merupakan nama domain saingan perusahaan;
9) *Hijacking*, *Hijacking* merupakan kejahatan melakukan pembajakan hasil karya orang lain yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak), dan
10) *Cyber Terorism*, suatu tindakan *cybercrime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.

Perbuatan hukum yang dilakukan di dunia maya merupakan perbuatan hukum yang dilakukan oleh manusia yang berlokasi di dunia nyata, hanya perbuatan hukum tersebut menggunakan sarana internet. Interaksi dari perbuatan hukum melalui dunia maya tersebut sesungguhnya merupakan interaksi antar manusia di dunia nyata tetapi hanya menggunakan sarana yang disebut sebagai internet, sehingga apabila terjadi pelanggaran hak atas perbuatan hukum yang dilakukan oleh manusia dari dunia nyata dan hak yang dilanggar adalah hak dari

manusia dari dunia nyata, maka hukum yang berlaku dan harus diterapkan adalah hukum dari dunia nyata (Suparni, 2009). Secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia cyber (*cybercrime*) adalah upaya memasukidan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut (Merry Magdalena, 2007).

Pengertian tersebut, dapat disimpulkan bahwa adanya upaya untuk memasuki jaringan komputer orang lain tanpa sepengetahuan orang tersebut yang memiliki tujuan untuk mengetahui hal-hal yang bersifat privacy yang dapat menimbulkan perubahan pada komputer tersebut. Aktifitas kejahatan komputer dapat digolongkan menjadi dua golongan diantaranya penipuan terhadap data dan penipuan tehadap program. Bentuk penipuan terhadap data yaitu data yang tidak sah dimasukan ke dalam sistem atau jaringan komputer, atau data yang sah dan seharusnya di-entry kemudian diubah sehingga menjadi tidak valid atau sah lagi. Bentuk ini tertuju kepada pemalsuan dan atau perusakan data input dengan maksud mengubah output. Bentuk penipuan terhadap program yaitu seseorang mengubah program komputer baik dilakukan langsung di tempat komputer tersebut berada maupun dilakukan secara remote melalui jaringan komunikasi data (Merry Magdalena, 2007).

Data pribadi yang berkaitan langsung dengan data elektronik UU ITE dijadikan referensi utama untuk menjawab pertanyaan seputar perlindungan informasi atau data pribadi di internet. UU ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Tetapi, secara implisit UU ini mengatur pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Sedangkan, hal yang berkaitan dengan penjabaran tentang data elektronik pribadi, UU ITE mengamanatkannya lagi dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Perlindungan data pribadi dalam sebuah sistem elektronik dalam UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal. Terkait perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 UU ITE mensyaratkan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.

Bunyi Pasal 26 UU ITE adalah sebagai berikut: 1) Penggunaan Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan; 2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini; 3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan; 4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan; dan 5) Ketentuan mengenai tata cara penghapusan Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah."

Pasal 26 UU ITE dalam penjelasannya, menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. Sedangkan, definisi data pribadi dapat dilihat dalam Pasal 1 PP PSTE yaitu data perorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaan. Saat ini belum adanya perhatian terhadap korban kejahatan didalam masyarakat yang merupakan tanda belum adanya keadilan dan kesejahteraan dari keadaan masyarakat tersebut. Dalam hal ini korban kejahatan diartikan sebagai seseorang yang telah menderita kerugian sebagai akibat suatu kejahatan dan atau rasa keadilannya secara langsung telah terganggu sebagai akibat pengalamannya sebagai target (sasaran) kejahatan (Yulia, 2010). Sebagai korban kejahatan, korban berhak mendapatkan perlindungan hukum, dalam memberikan perlindungan hukum ini harus secara maksimal khususnya korban-korban yang bergolongan lemah ekonomi. Perlindungan hukum yang dimaksud dapat berupa kompensasi, restitusi dan bantuan hukum yang diatur dalam Peraturan Pemerintah No.44 Tahun 2008 Tentang Pemberian Kompensasi, Restitusi, Dan, Bantuan Kepada Saksi Dan Korban.

Korban lebih tepat mendapatkan Restitusi, dalam hal kejahatan dunia *cyber*. Menurut Pasal 1 angka 5 "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga, dapat berupa pengembalian harta milik, pembayaran ganti kerugian untuk kehilangan atau penderitaan, atau penggantian biaya untuk tindakan tertentu". Pencurian informasi pribadi merupakan salah satu ancaman kejahatan

paling lazim saat ini, yang dilakukan dengan cara mencuri data penting orang lain. Data penting dalam hal ini tentu saja mulai dari data pribadi (nama, alamat, email, nomor handphone, dll), lalu data terkait dengan keuangan antara lain data bank(nomor rekening), data ATM, serta data kartu kredit. Pelaku pencurian informasi pribadi dapat dikenakan sanksi pasal 30 ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik".

Melihat pasal tersebut pelaku pencurian informasi telah memenuhi unsur-unsur pasal 30 ayat (2) UU ITE, cara apa pun yang dimaksud disini adalah dengan menyusup sistem keamanan komputer baik dengan menggunakan *software* tertentu ataupun tidak yang bertujuan untuk mencuri data atau informasi seseorang. Sesuai dengan ketentuan Pasal 46 ayat (2) pelaku dapat dikenakan sanksi pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

2. Formulasi Kebijakan Kriminal Dalam Upaya Perlindungan Data Elektronik

Istilah "kebijakan" diambil dari istilah "*policy*" dalam Bahasa Inggris atau politick" dalam bahasa Belanda. Dengan demikian, maka istilah "kebijakan hukum pidana" dapat pula disebut dengan istilah "politik hukum pidana". Dalam kepustakaan asing, istilah "politik hukum pidana" ini juga dikenal dengan berbagai istilah yang lain, diantaranya adalah "*penal policy*", "*criminal law policy"atau "strafrechtspolitiek"* (Arief, 2006a). Tahap kebijakan formulasi merupakan tahap awal dan sumber landasan dalam proses kongkritisasi bagi penegakan hukum pidana selanjutnya, yaitu tahap aplikasi dan eksekusi. Adanya tahap formulasi menunjukkan bahwa upaya pencegahan dan penanggulangan kejahatan juga menjadi tugas dan kewajiban dari para pembuat hukum, bukan hanya tugas aparat penegak/penerap hukum. Apalagi tahap formulasi ini merupakan tahap yang paling strategis, karena adanya kesalahan pada tahap ini akan sangat menghambat upaya pencegahan dan penanggulangan pada tahap aplikasi dan eksekusi.

Sebagaimana ditulis oleh (Arief, 2007), kebijakan formulasi merupakan tahapan yang paling strategis dari ”*penal policy*” karena pada tahapan tersebut legislatif berwenang dalam hal menetapkan atau merumuskan perbuatan apa yang dapat dipidana yang berorientasi pada permasalahan pokok hukum pidana meliputi perbuatan yang bersifat melawan hukum,

kesalahan, pertanggungjawaban pidana dan saksi apa yang dapat dikenakan. Oleh karena itu upaya penanggulangan kejahatan bukan hanya tugas aparat penegak hukum tetapi juga tugas aparat pembuat undang-undang (aparat legislatif). Selanjutnya menurut (Arief, 2003), kebijakan kriminalisasi bukan sekedar kebijakan menetapkan atau merumuskan atau memformulasikan perbjatan apa yang dapat dipidana (termasuk sanksi pidananya) melainkan juga mencakup masalah bagaimana kebijakan formulasi/legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.

Kebijakan penanggulangan *cybercrime* secara teknologi, diungkapkan juga dalam IIIC (*Internatonal Information Industry Congress*) yang rnenyatakan (ITAC, 2000): *The IIIC recognizes that goverment action and international traties to harmonize laws and coordinate legal procedures are key in the fight against cybercrime, but warns that these should not be relied upon as the only instuments. Cybercrime is enabled by technology and requires a healty reliance on technology for its solution.* Bertolak dari pengertian di atas maka upaya atau kebijakan untuk melakukan penanggulangan tindak pidana di bidang teknologi informasi yang dilakukan dengan menggunakan sarana "penal" (hukum pidana) maka dibutuhkan kajian terhadap materi/substansi (*legal subtance reform)* tindak pidana teknologi informasi saat ini. Dalam penanggulangan melalui hukum pidana (penal policy) perlu diperhatikan bagaimana memformulasikan (kebijakan legislatif) suatu peraturan perundangundangan yang tepat untuk menanggulangi tindak pidana di bidang teknologi informasi pada masa yang akan datang, serta bagaimana mengaplikasikan kebijakan legislatif (kebijakan yudikatif/yudisial atau penegakan hukum pidana in conereto) tersebut oleh aparat penegak hukum atau pengadilan.

Meningkatnya aktivitas elektronik, maka alat pembuktian yang dapat digunakan secara hukum harus juga meliputi informasi atau dokumen elektronik untuk memudahkan pelaksanaan hukumnya. Selain itu hasil cetak dari dokumen atau Informasi tersebut juga harus dapat dijadikan bukti yang sah secara hukum. Untuk memudahkan pelaksanaan penggunaan bukti elektronik (baik dalam bentuk elektronik atau hasil cetak), maka bukti elektronik dapat disebut sebagai perluasan alat bukti yang sah, sesuai dengan hukum acara yang berlaku di Indonesia, sebagaimana tertulis dalam Pasal 5 UU ITE: 1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah; 2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah

sesuai dengan Hukum Acara yang berlaku di Indonesia; dan 3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. Namun bukti elektronik tidak dapat digunakan dalam hal-hal spesifik sebagaimana yang tertulis dalam Pasal 5 ayat (4) UU ITE menyatakan Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a) Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b) Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Surat yang menurut undang-undang harus dibuat tertulis(Laurensius Arliman S, 2019) seperti dalam pembuatan dan pelaksanaan surat-surat terjadinya perkawinan dan putusnya perkawinan, surat-surat yang menurut undang-undang harus dibuat dalam bentuk tertulis, perjanjian yang berkaitan dengan transaksi barang tidak bergerak, dokumen yang berkaitan dengan hak kepemilikan dan juga dokumen lainnya yang menurut peraturan perundang-undangan mengharuskan adanya pengesahan notaris atau pejabat yang berwenang. Bukti elektronik baru dapat dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan peraturan yang berlaku di Indonesia. Suatu bukti elektronik dapat memiliki kekuatan hukum apabila informasinya dapat dijamin keutuhannya, dapat dipertanggungjawabkan, dapat diakses dan dapat ditampilkan, sehingga menerangkan suatu keadaan orang yang mengajukan suatu bukti elektronik harus dapat menunjukkan bahwa informasi yang dimilikinya berasal dari sistem elektronik yang terpercaya. Berdasarkan Pasal 5 ayat (1) UU ITE, informasi elektronik memiliki kekuatan hukum sebagai alat bukti yang sah, bila informasi elektronik ini dibuat dengan menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi. Bahkan secara tegas, Pasal 6 UU ITE menentukan bahwa "Terhadap semua ketentuan hukumyang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli selain yang diatur dalam Pasal 5 ayat (4), persyaratan tersebut telah terpenuhi berdasarkan undang-undang ini jika informasi elektronik tersebut terjamin keutuhannya dan dapat dipertanggungjawabkan, dapat diakses, dapat ditampilkan sehingga menerangkan suatu keadaan".

D. Penutup

Dari uraian terdahulu dapat ditarik kesimpulan sebagai berikut: Bentuk perlindungan hukum tindak pidana ini sudah ada pengaturan di Indonesia bila ditinjau dari Undang-Undang No. 16 Tahun 2016 tentang Perubahan atas Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pencurian informasi pribadi merupakan salah satu ancaman kejahatan paling lazim saat ini, yang dilakukan dengan cara mencuri data penting orang lain. Data penting dalam hal ini tentu saja mulai dari data pribadi (nama, alamat, email, nomor handphone, dll), lalu data terkait dengan keuangan antara lain data bank (nomor rekening), data ATM serta data kartu kredit. Secara sederhana dapatlah dibedakan, bahwa upaya penanggulangan kejahatan lewat jalur "penal" lebih menitik beratkan pada sifat "repressive" (penindasan / pemberantasan / penumpasan) sesudah kejahatan terjadi, sedangkan jalur "non penal" lebih menitikberatkan pada sifat "preventif" (pencegahan / penangkalan / pengendalian) sebelum kejahatan terjadi. Pengertian *penal policy* (kebijakan hukum pidana) adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada penyelenggara atau pelaksana putusan pengadilan.Penggunaan kebijakan penal dalam suatu tindakan kejahatan memang bukan suatu kebijakan yang strategis. Namun sebaliknya bukan pula suatu langkah kebijakan yang bisa di sederhanakan dengan mengambil sikap ekstrim untuk menghapuskan saja hukum pidana itu sama sekali. Persoalan tidak terletak pada masalah eksistensinya, namun lebih kepada masalah kebijakan penggunaannya. Sebagai suatu masalah kebijakan sudah barang tentu penggunannya pun tidak dapat dilakukan secara absolute, karena memang pada hakikatnya tidak ada hal yang absolute didalam suatu bidang kebijakan. Pencegahan dan pendekatan kejahatan dengan sarana penal merupakan "*penal policy*" atau "*penal law enforcement policy*" yang fungsionalisasi dan atau operasionalisasinya melalui beberapa tahap yaitu : Formulasi (kebijakan legislative / legislasi), Aplikasi (kebijakan yudikatif /yudicial) dan Eksekusi (kebijakan eksekutif / administrasi).

Daftar Pustaka

Arief, B. N. (2003). *Kapita Selekta Hukum Pidana*. Bandung: PT Citra Aditya Bakti.

Arief, B. N. (2006a). *Bunga Rampai Kebijakan Hukum Pidana*. Bandung: Citra Aditya Bhakti.

Arief, B. N. (2006b). *Tindak Pidana Mayatara, Perkembangan Cyber crime Di Indonesia*. Jakarta: PT. RajaGrafindo.

Arief, B. N. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penaggulangan Kejahatan*. Jakarta: Kencana.

Bungin, B. (2005). *Pornomedia: Sosiologi Media, Konstruksi Sosial Teknologi Telematika, & Perayaan Seks di Media Massa*. Jakarta: Prenada Media.

Dewi, S. (2009). *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran.

Hamzah, A. A. (2014). *Ancaman Pidana Dalam Hubungan Dengan Keluarga Berencana*. Universitas Indonesia. https://doi.org/10.1007/s13398-014-0173-7.2

ITAC. (2000). IIIC Common Views Paper On: Cybercrime. In *IIIC 2000 Millenium Congress*. IIIC 2000 Millenium Congress.

Laurensius Arliman S. (2018). Peranan Metodologi Penelitian Hukum di Dalam Perkembangan Ilmu Hukum di Indonesia. *Soumatera Law Review*, *1*(1).

Laurensius Arliman S. (2019). Surat Dakwaan dalam Hukum Acara Pidana Sebagai Bentuk Mendukung Penegakan Hukum di Indonesia. *Jurnal Kosmik Hukum*, *19*(1).

Laurensius Arliman S. (2020). Penanganan Perkara Tindak Pidana Pungutan Liar Oleh Penyidik Direktorat Kriminal Khusus. *Kanun Jurnal Ilmu Hukum*, *22*(1), 49–72.

Marrett, P. (2002). *Information Law in Practice : 2nd Edition*. Cornwall: MPG Books Ltd.

Merry Magdalena, M. R. S. (2007). *Cyberlaw, Tidak Perlu Takut*. Yogyakarta: Andi Offset.

Purwanto. (2007). *Penelitian Tentang Perlindungan Hukum Data Digital*. Jakarta: Badan Pembinaan Hukum Nasional.

Shilling, C. G. (2011). Privacy and Data Security : New Challenges of The Digital Age. *New Hampshire Bar Journal*, *13*(1).

Suparni, N. (2009). *Cyberspace Problematika & Antisipasi Pengaturannya*. Jakarta: Sinar Grafika.

Widodo. (2006). *Kebijakan Kriminal Terhadap Kejahatan yang Berhubungan dengan Komputer di Indonesia*. Pascasarjana Universitas Brawijaya.

Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo.

Yasmirah Mandasari Saragih, Teguh Prasetyo, J. H. (2018). Analisis Yuridis Kewenangan Komisi Pemberantasan Korupsi Sebagai Penuntut Pelaku Tindak Pidana Korupsi. *Unifikasi : Jurnal Ilmu Hukum*, *5*(1).

Yulia, R. (2010). *Viktimologi Perlindungan Hukum Terhadap Korban Kejahatan*. Yogyakarta: Graha Ilmu.