LEMBAGA
PENELITIAN &
PENGABDIAN MASYARAKAT

PROSIDING

SEMILOKA PENELITIAN DOSEN STIHPADA TAHUN 2019

ISBN : 978-623-90705-0-2

DAFTAR ISI

ISBN : 978-623-90705-0-2

TELAAH NORMATIF UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP PENYADAPAN (INTERSEPSI) DATA PRIBADI PADA PENGGUNA INTERNET

Oleh :
H. Bambang Sugianto, S.H., M.Hum.[1]
Putrisari Nilamcayo, S.H., M.H.[2]

Abstrak

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tindak pidana penyadapan data pribadi pada pengguna internet berdasarkan yaitu tertuang dalam Pasal 31 ayat (1) dan (2). Pasal tersebut merupakan landasan hukum bagi para pengguna internet dari tindakan penyadapan yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain.

Kendala dalam penegakkan hukum terhadap penyadapan data pribadi pada pengguna internet yaitu dalam upaya pembuktian, keterangan para ahli, dan masalah yuridiksi peradilan, dimana hukum suatu negara tidak dapat menjangkau pelaku kejahatan diluar negaranya.

Kata Kunci : Penegakan Hukum, Penyadapan, Perlindungan Hukum

Abstract

Law Number 11 of 2008 concerning Information and Electronic Transactions regulates criminal acts of tapping personal data on internet users based on those stated in Article 31 paragraph (1) and (2). The article is a legal basis for internet users from acts of wiretapping carried out by someone who intentionally and without the right to access entrance to other people's electronic information or personal electronic documents.

Constraints in law enforcement against tapping personal data on internet users are in the effort of proof, information of experts, and the issue of judicial jurisdiction, where the law of a country cannot reach offenders outside the country.

Keywords: Law Enforcement, Tapping, Legal Protection

A. Latar Belakang

Teknologi informasi *(information technology)* memegang peran yang penting, baik di masa kini maupun di masa yang akan datang[3]. Ditengah era globalisasi yang semakin terpadu, teknologi informasi menjadi suatu kebutuhan yang tidak dapat dilepaskan dari kepentingan hidup manusia. Salah satu yang sangat berpengaruh dari perkembangan teknologi tersebut adalah dalam bidang telekomunikasi. Dengan sarana telekomunikasi

---

[1] Penulis adalah Dosen Tetap Pada STIHPADA, Dengan NIDN. 0201016901
[2] Penulis adalah Dosen Tetap Pada STIHPADA, Dengan NIDN. 0227106703
[3] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, hlm. 1

ISBN : 978-623-90705-0-2

seseorang dapat berkomunikasi atau berhubungan dengan yang lain tanpa harus bertatap muka secara langsung. Salah satu media telekomunikasi yang sangat popular pada saat ini adalah dengan menggunakan sarana internet. Dengan internet, informasi-informasi dapat dengan cepat dan mudah untuk didapatkan bahkan dari belahan dunia yang lain sekalipun. Dengan semakin popularnya internet seakan telah membuat dunia semakin sempit dan semakin memudarkan batas-batas negara berikut kedaulatan dan tatanan masyarakatnya. Ironisnya dinamika masyarakat Indonesia yang masih baru tumbuh dan berkembang sebagai masyarakat industri dan masyarakat informasi seolah belum siap untuk mengikuti perkembangan teknologi tersebut.

Komputer sebagai suatu hasil dari teknologi yang digunakan sebagai alat bantu manusia dengan didukung oleh perkembangan teknologi informasi yang sangat maju telah menjadi suatu sarana yang dapat membantu manusia untuk mengakses masuk kedalam jaringan-jaringan publik serta melakukan pemindahan data dan informasi. Dengan kemampuan komputer dan jaringan elektronik yang semakin berkembang maka kegiatan berkomunikasi pun dilakukan dalam jaringan tersebut. Internet adalah nama yang diberikan pada koleksi jaringan komputer terbesar di dunia, dalam jaringan internet itu terdiri dari jaringan-jaringan yang lebih kecil yaitu jaringan komputer. Ketika seseorang meminta data dari internet, permintaan itu berpindah dari suatu komputer ke komputer di seluruh jaringan hingga mencapai lokasi tempat data itu disimpan[4].

Internet atau disebut juga dengan *cyberspace* yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual[5], pada saat ini dapat dikatakan sebagai suatu sarana yang dibutuhkan oleh banyak orang, baik digunakan untuk berkomunikasi, sekedar mencari informasi, hingga digunakan untuk melakukan transaksi bisnis. Dengan menggunakan internet, pengguna dimanjakan untuk berkelana menelusuri dunia *cyberspace* dengan menembus batas kedaulatan suatu negara, batas budaya, batas agama, politik, ras, hierarki, birokrasi, dan sebagainya[6]. Karena tingginya kebutuhan manusia akan internet maka semakin banyak juga orang yang menyalahgunakan sarana tersebut. Hingga saat ini kasus-kasus kejahatan internet atau disebut juga dengan

---

[4] Israel Fanny, 2011, *Analisis Hukum Mengenai Tanggung Jawab Operator Seluler Terhadap Pelanggan Seluler Terkait Spam*, Unikom, Jakarta, hlm. 2

[5] http://www.irepuspa.staff.jak-stik.ac.id, *Pengertian Cyberspace*, diakses pada tanggal 12 April 2018

[6] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, hlm. 91

ISBN : 978-623-90705-0-2

cybercrime semakin banyak bermunculan, dengan jenis-jenis kejahatan baru yang sulit untuk diidentifikasi[7].

Penggunaan *password* pada zaman dahulu adalah sebagai suatu sandi untuk dapat melewati penjagaan sebuah kota (tentunya ini terjadi pada saat perang). Namun pada zaman modern sekarang ini, orang menggunakannya untuk melindungi ATM, Kartu Debit, *Online Banking*, sistem operasi seperti *Windows*, bahkan komputer itu sendiri. *Password* adalah sebuah kode rahasia yang biasanya digunakan untuk menjalankan proses "autentikasi", yakni sebuah proses untuk melakukan konfirmasi apakah seseorang memiliki izin untuk mengakses informasi atau data yang dirahasiakan. *Password* sendiri selalu dijadikan sebuah rahasia yang hanya diketahui oleh individu/kelompok yang memiliki hak untuk mengakses data/informasi yang dilindungi tersebut. Orang yang tidak mendapatkan akses, namun membutuhkan informasi tersebut, kerapkali mencoba untuk mendapatkannya[8].

Bagaimana cara melakukan pencurian *password?* Pertanyaan ini yang sering keluar di setiap milis keamanan, tipikal dan sudah ada semenjak ditemukannya komputer dan internet[9]. Penyadapan yang dilakukan oleh seseorang yang tidak bertanggung jawab untuk mencuri data dari pengguna internet merupakan salah satu bentuk *cybercrime*, karena seseorang yang tidak bertanggung jawab tersebut telah melewati batas-batas haknya dengan memasuki wilayah pribadi orang lain. Penyadapan biasanya dilakukan dengan menggunakan program-program atau *software* yang diaplikasikan pada komputer. Banyak *software* yang di buat secara khusus untuk melakukan penyadapan dalam jaringan komputer. Salah satu program yang sering digunakan untuk melakukan penyadapan itu dinamakan dengan istilah *"sniffing tools"* atau jika diterjemahkan dalam bahasa Indonesia berarti "alat pemantau jaringan", dimana *software* yang telah diaplikasikan pada sebuah komputer yang terhubung dengan suatu jaringan, maka komputer dengan aplikasi tersebut dapat memantau komputer-komputer yang terhubung dalam suatu jaringan[10].

Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, diantaranya proses pembuktian atas suatu tindak pidana (faktor yuridis).

---

[7] http://safirasalsabila.wordpress.com, *Penyadapan Data Pribadi Pengguna Internet yang Dilakukan Melalui Monitoring Aktivitas Komputer*, diakses pada tanggal 05 April 2018

[8] Thor, 2008, *Hacker's Biggest Secret Zero Knowledge Password*, PT. Elex Media Komputindo, Jakarta, hlm. 2

[9] *Ibid,* hlm. 6

[10] http://safirasalsabila.wordpress.com, *Penyadapan Data Pribadi Pengguna Internet yang Dilakukan Melalui Monitoring Aktivitas Komputer*, diakses pada tanggal 05 April 2018

ISBN : 978-623-90705-0-2

Terlebih lagi penggunaan komputer untuk tindak pidana ini memiliki karakter tersendiri atau berbeda dengan tindak pidana yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku dan alat bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer[11].

Teknik umum yang biasa dilakukan oleh seseorang untuk menyadap data pribadi pengguna internet dengan menggunakan program *sniffing tools* yaitu dengan cara memantau suatu jaringan komputer dimana dalam satu jaringan komputer tersebut terhubung dengan banyak komputer. Korban biasanya tidak sadar bahwa aktivitasnya di dalam internet sedang disadap oleh orang lain. Pada dasarnya pelaku memanfaatkan ketidak hati-hatian dari pengguna internet, dengan tujuan untuk mencuri informasi pribadi dari pengguna internet seperti informasi pribadi yang dikirim melalui *email*, dan data pribadi seperti *username* dan *password* dari sebuah *website* yang dimiliki oleh pengguna internet.

Pada awalnya program *sniffing* seperti *etheral, tcpdump, ettercap, dsniff, etherpeak, airopeak* dan lain sebagainya digunakan dengan tujuan yang positif, yaitu untuk mempertahankan jaringan dan sistem agar dapat bekerja secara normal[12]. Biasanya *sniffing tools* digunakan sebagai asisten manajemen jaringan untuk memonitor dan sebagai fitur analisis yang dapat membantu memecahkan masalah jaringan, mendeteksi instruksi, kontrol atau pengawasan jaringan. Namun seiring perkembangan teknologi, perangkat lunak seperti ini mulai dikembangkan untuk kegunaan yang negatif, yaitu untuk mengambil data dan informasi rahasia pengguna internet yang tidak ter-*enkripsi* selama data dan informasi *user* tersebut melintasi suatu jaringan komputer[13].

Program yang dibuat secara khusus untuk memonitoring aktivitas komputer sangat banyak tersebar dan dapat dengan mudah didapatkan oleh seseorang dengan cara men-*download* di internet. Pada dasarnya program monitoring aktivitas komputer merupakan sebuah aplikasi yang digunakan untuk memantau paket data yang bergerak keluar-masuk dalam jaringan komputer kemudian dengan program monitoring aktivitas komputer

---

[11] Puspita Dewi, 2011, *Tindak Pidana Penipuan untuk Memperoleh Informasi Personal (Pishing) Melalui Pengiriman E-Mail*, Unikom, Jakarta, hlm. 38

[12] Firman Nuro, 2018, *Adopsi Enkripsi Jefferson Wheel pada Protokol One-Time Password Authentication untuk Pencegahan Sniffing pada Password E-Mail*, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), Yogyakarta, 2018

[13] http://ryanadisaputra.wordpress.com, *Penyadapan Data Pribadi Pengguna Internet yang Dilakukan Melalui Monitoring Aktivitas Komputer*, diakses pada tanggal 05 April 2018

ISBN : 978-623-90705-0-2

tersebut, paket data yang bergerak keluar-masuk dapat diterjemahkan kembali sehingga dapat dibaca oleh seseorang yang tidak bertanggung jawab tersebut. Tingkat dan ragam kejahatan mengikuti realitas perkembangan kehidupan manusia. Kecendrungan terbukti bahwa semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operasi kejahatan yang terjadi di tengah masyarakat. Hal ini seolah-olah membenarkan suatu *adagium*[14], bahwa dimana ada masyarakat, di situ ada kejahatan[15]. Dengan adanya program monitoring aktivitas komputer, maka akan memunculkan suatu kejahatan baru dimana informasi yang bersifat rahasia dari pengguna internet seperti *password* dan *username* dapat disadap oleh orang yang tidak berkepentingan. Dengan demikian maka seluruh informasi seseorang dalam *website* yang telah dilindungi oleh *password* dan *username* tersebut dapat dicuri oleh orang yang tidak berkepentingan tersebut.

Undang-undang Nomor 11 Tahun 2008 yang mengatur mengenai Informasi dan Transaksi Elektronik di Indonesia, dapat mengakomodasi aturan mengenai penyadapan data pribadi pada pengguna internet. Bermunculannya berbagai bentuk kejahatan melalui media komputer *(cybercrime)*, membuat berbagai negara waspada dengan cara segera menyusun produk hukum *(cyberlaw)*, guna menghadapi masalah yang sedang terjadi dan yang akan datang.

Berdasarkan uraian permasalahan di atas maka penulis tertarik untuk meneliti secara lebih mendalam kedalam bentuk karya ilmiah dengan judul **"TELAAH NORMATIF UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK TERHADAP PENYADAPAN DATA PRIBADI PADA PENGGUNA INTERNET".**

B. Permasalahan

Berdasarkan latar belakang yang diuraikan di atas, maka penulis mengidentifikasikan permasalahan sebagai berikut :

1. Bagaimana Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tindak pidana penyadapan data pribadi pada pengguna internet ?
2. Apa yang menjadi kendala dalam proses penegakan hukum atas penyadapan data pribadi pada pengguna internet?

---

[14] http://kbbi.web.id, *Kamus Besar Bahasa Indonesia*, diakses pada tanggal 12 April 2018

[15] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung, hlm. 8

ISBN : 978-623-90705-0-2

C. Metodologi

Dalam penelitian ini, penulis menggunakan metode pendekatan secara yuridis normatif yaitu metode penelitian hukum yang dilakukan dengan meneliti bahan pustaka atau data sekunder belaka[16] dengan melakukan penafsiran hukum secara gramatikal yaitu penafsiran yang dilakukan terhadap kata-kata atau tata kalimat yang digunakan pembuat undang-undang dalam peraturan perundang-undangan tertentu[17]. Di samping itu dilakukan pula upaya untuk mengkaji dan menguji data dengan menggunakan metode yuridis kualitatif yaitu pendapat para ahli hukum dan data sekunder bahan hukum tersier yaitu berasal dari internet. Pendekatan yuridis normatif dimaksudkan sebagai usaha mendekatkan masalah yang diteliti dengan sifat hukum yang normatif[18].

Adapun yang menjadi sumber data yang diperlukan dalam penelitian ini yaitu data sekunder berdasarkan studi pustaka / studi literatur (*library research*).

D. Pembahasan

Internet *(Interconnection Network)* merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optik, satelit ataupun gelombang frekuensi[19]. Internet berasal dari bahasa latin *"inter"* yang berarti "antara". Internet merupakan jaringan yang terdiri dari milyaran komputer yang ada di seluruh dunia. Internet melibatkan berbagai jenis komputer serta *topology* jaringan yang berbeda. Dalam mengatur integrasi dan komunikasi jaringan, digunakan standar protokol internet yaitu TCP *(Transmission Control Protocol)* / IP *(Internet Protocol)*. TCP *(Transmission Control Protocol)* bertugas untuk memastikan bahwa semua hubungan bekerja dengan baik, sedangkan IP *(Internet Protocol)* bertugas untuk mentransmisikan paket data dari satu komputer ke komputer lainya[20].

Sejarah dan perkembangan internet tidak bisa dilepaskan dari perang dingin antara Uni Soviet (USSR) dan Amerika Serikat yang mulai mengemuka sejak usainya Perang Dunia II. Uni Soviet memulai perang dingin dalam bidang teknologi dengan meluncurkan

---

[16] Soerjono Soekanto dan Sri Mamudji, 2001, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, Rajawali Pers, Jakarta, hlm. 13-14.

[17] http://www.jurnalhukum.com, *Penafsiran Hukum Secara Gramatikal*, diakses pada tanggal 05 April 2018

[18] H. Hilman Hadikusuma, 1995, *Metode Pembuatan Kertas Kerja Atau Skripsi Ilmu Hukum*, CV. Bandar Maju, Bandung, hlm. 60

[19] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, hlm. 59

[20] http://www.termasmedia.com. *Pengertian Internet*, diakses pada tanggal 03 April 2018

 ISBN : 978-623-90705-0-2

Sputnik, satelit bumi buatan yang pertama pada tahun 1957. Sebagai respon atas stimulus yang diberikan oleh Uni Soviet, Amerika Serikat membentuk *Advanced Research Project Agency* (ARPA) pada tahun 1958. Dibentuknya *Advanced Reseacrh Project Agency* (ARPA) menjadikan *Department of Defense* (DoD) Amerika Serikat memimpin dalam pemanfaatan ilmu pengetahuan dan teknologi yang diterapkan untuk kepentingan militer[21].

Secara umum, penyadapan diartikan sebagai proses dengan sengaja mendengarkan dan/atau merekam informasi yang dilakukan dengan sengaja dan tanpa sepengetahuan orang yang bersangkutan[22]. Sementara itu, menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, disebutkan bahwa yang dimaksud dengan intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel seperti pancaran *elektromagnetis* atau radio frekuensi[23].

I. Pengaturan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Terhadap Tindak Pidana Penyadapan Data Pribadi Pada Pengguna Internet

Perkembangan teknologi informasi yang sangat pesat di Indonesia, menuntut masyarakat untuk dapat menyesuaikan diri dengan perubahan-perubahan yang terjadi sebagai dampak dari kemajuan teknologi informasi tersebut. Teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global, perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial budaya, ekonomi dan pola penegakan hukum yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena disatu sisi teknologi informasi tersebut telah memberikan kontribusi bagi peningkatan kesejahteraan kemajuan dan peradaban manusia, sedangkan disisi lainnya teknologi informasi juga menjadi sarana yang sangat efektif untuk melakukan perbuatan melawan hukum[24].

---

[21] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, hlm. 61

[22] *Ibid*, hal 180.

[23] http://zelously.blogspot.com, *Definisi dari Penyadapan*, diakses pada tanggal 04 April 2018

[58] Israel Fanny, 2011, *Analisis Hukum Mengenai Tanggung Jawab Operator Seluler Terhadap Pelanggan Seluler Terkait Spam*, Unikom, Jakarta, hlm. 47

ISBN : 978-623-90705-0-2

Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, diantaranya proses pembuktian atas suatu tindak pidana (faktor yuridis). Terlebih lagi penggunaan komputer untuk tindak pidana ini memiliki karakter tersendiri atau berbeda dengan tindak pidana yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku dan alat bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer[25].

Pada dasarnya setiap kegiatan atau aktivitas manusia dapat diatur oleh hukum. Hukum dipersempit pengertiannya menjadi peraturan perundang-undangan yang dibuat dan dilaksanakan oleh negara[26], begitu pula aktivitas kejahatan dunia maya yang menjadikan internet sebagai sarana utamanya. Dalam kaitan dengan teknologi informasi khususnya dunia maya, peran hukum adalah melindungi pihak-pihak yang lemah terhadap eksploitasi dari pihak yang kuat atau berniat jahat, disamping itu hukum dapat pula mencegah dampak negatif dari ditemukannya suatu teknologi baru.

Di Indonesia, pengaturan khusus mengenai kejahatan dunia maya atau *cybercrime* telah ditetapkan menjadi Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik itu sendiri disusun sedemikian rupa sebagai upaya pemerintah dalam pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin, kemudian sebagai bentuk dari upaya penegakan hukum menyangkut tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan teknologi informasi disertai sanksi pidananya termasuk untuk tindakan *carding, hacking, dan cracking*[27].

Pengaturan yang menyangkut intersepsi atau penyadapan tertuang dalam Pasal 31 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tersebut, yaitu[28] :

---

[25] Puspita Dewi, 2008, *Tindak Pidana Penipuan Untuk Memperoleh Informasi Personal (Phising) Melalui Pengiriman E-Mail*, Unikom, Jakarta, hlm. 38

[26] Firman Nuro, 2010, *Analisis Hukum Tentang Penyadapan Data Pribadi Pengguna Internet Melalui Monitoring Aktivitas Komputer*, Unikom, Jakarta, hlm. 53

[27] *Ibid*, hlm. 55

[28] Siswanto Sunarso, 2009, *Hukum Informasi dan Transaksi Elektronik*, PT. Rineka Cipta, Jakarta, hlm. 104

ISBN : 978-623-90705-0-2

Ayat (1) :
"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain."

Ayat (2) :
"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau elektronik yang tidak bersifat publik, dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun, maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang di transmisikan."

Pasal tersebut diatas merupakan landasan hukum atau perlindungan hukum bagi para pengguna internet dari tindakan penyadapan yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain secara melawan hukum. Unsur yang terkandung dalam Pasal 31 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) adalah[29] :

1. Setiap orang;
2. Dengan sengaja dan tanpa hak, atau melawan hukum;
3. Melakukan intersepsi atau penyadapan atas:
   a. Informasi elektronik dan/atau dokumen elektronik;
   b. Transmisi informasi elektronik dan/atau elektronik yang tidak bersifat publik;
   c. Dalam suatu komputer dan/atau sistem elektronik;
   d. Milik orang lain;
   e. Yang tidak atau menyebabkan perubahan, penghilangan, penghentian, informasi elektronik dan/atau dokumen elektronik yang sedang di transmisikan.

Pengertian setiap orang disini, selain ditafsirkan sebagai individu juga badan hukum yang berbadan hukum sesuai ketentuan perundang-undangan. Pengertian dengan sengaja dan tanpa hak, dapat ditafsirkan sebagai perbuatan yang bertentangan dengan undang-undang dan tindakan melalaikan yang diancam hukuman. Adapun perbuatan yang dilarang oleh undang-undang *(wederrechtelijk)* ini adalah melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik, yang tidak bersifat publik, dalam

[29] *Ibid*, hlm. 104

ISBN : 978-623-90705-0-2

suatu komputer dan/atau sistem elektronik milik orang lain, yang tidak atau menyebabkan perubahan, penghilangan, penghentian, informasi elektronik dan/atau dokumen elektronik yang sedang di transmisikan. Delik ini adalah delik formil atau delik dengan perumusan formil, yakni delik yang dianggap telah sepenuhnya terlaksana dengan dilakukannya suatu perbuatan yang dilarang oleh undang-undang, dan tidak perlu dibuktikan akibat dari perbuatan yang dilarang tersebut[30].

Berdasarkan rumusan unsur-unsur diatas, maka perbuatan yang dilakukan oleh *sniffer* sudah memenuhi unsur objektif dan unsur subjektif sebagaimana yang terdapat dalam Pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan demikian, Pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dapat diterapkan terhadap tindak pidana penyadapan data pribadi pada pengguna internet.

Selanjutnya dalam Pasal 31 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ditegaskan :

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan."

Pasal 31 ayat (2) tersebut menegaskan untuk melarang siapa saja yang secara sengaja dan tanpa hak untuk melakukan intersepsi atau penyadapan atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik. Tidak bersifat publik disini mengandung arti yaitu pribadi dalam arti informasi elektronik atau dokumen elektronik tersebut milik pribadi orang lain.

Intersepsi yang dilakukan baik menyebabkan adanya perubahan, penghilangan maupun penghentian informasi atau dokumen elektronik yang sedang ditransmisikan, mempunyai maksud yaitu, menegaskan bahwa intersepsi atau penyadapan yang dilakukan dalam bentuk apapun maka intersepsi atau penyadapan tersebut sudah bertentangan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, khususnya Pasal 31 ayat (2) yang selanjutnya bagi pelaku akan dikenakan sanksi pidana

---

[30] *Ibid*, hlm. 105

ISBN : 978-623-90705-0-2

sesuai dengan ketentuan pidana yang telah di atur dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tersebut.

Sanksi pidana yang berkaitan dengan intersepsi atau penyadapan, diatur dalam BAB XI Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai ketentuan pidana yaitu Pasal 47, yang menyatakan :

> Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Pada hakikatnya, tindakan penyadapan merupakan suatu perbuatan yang berpotensi melanggar atau bahkan meniadakan hak pribadi atau hak privasi seseorang atau sekelompok orang yang disadap, karena suatu informasi yang disadap tentu bukanlah informasi yang bersifat umum, melainkan suatu informasi yang bersifat rahasia *(confidential information)*[31].

Seseorang yang telah melakukan intersepsi atau penyadapan, dalam hal ini penyadapan data pribadi pada pengguna internet yang merupakan perbuatan seseorang dengan tanpa hak dan secara melawan hukum karena telah melewati batas-batas wilayah pribadi orang lain untuk memperoleh data pribadi orang lain seperti *password* dan *username* akun seseorang dalam suatu situs internet, maka sangat relevan untuk dikenakan sanksi sesuai dengan sanksi pidana yang telah tercantum dalam BAB XI Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengenai ketentuan pidana khususnya pada Pasal 47 tersebut.

Korban yang mengalami kerugian atas tindakan penyadapan khususnya penyadapan data pribadi yang umumnya merupakan pengguna internet dapat pula melakukan tindakan hukum terhadap pelaku penyadapan atau *sniffer* tersebut dengan menempuh proses hukum melalui lembaga peradilan umum secara perdata, yaitu berdasarkan pada Pasal 1365 BW dimana penyadapan data pribadi pada pengguna internet tersebut merupakan perbuatan yang dapat dikategorikan sebagai perbuatan melawan hukum *(Onrechtmatigedaad)* sebagaimana ditentukan dalam Pasal 1365 BW yang menyatakan bahwa :

> Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut.

---

[31] Kristian dan Yopi Gunawan, 2013, *Sekelumit Tentang Penyadapan Dalam Hukum Positif Di Indonesia,* Nuansa Aulia, Bandung, hlm. 51

ISBN : 978-623-90705-0-2

Berdasarkan isi Pasal 1365 BW, suatu perbuatan dapat dianggap perbuatan melawan hukum bilamana memenuhi unsur-unsurnya, dimana unsur-unsur tersebut yaitu[32] :

1. Perbuatan melanggar hukum;
2. Unsur kesalahan (ada sebuah niat);
3. Adanya kerugian (kerugian materil);
4. Hubungan sebuah akibat/kausal antara point 1, 2, dan 3.

Penerapan ketentuan Pasal 1365 BW dilakukan dengan cara melakukan penafsiran hukum ekstensif[33] yaitu memperluas arti kata perbuatan melawan hukum itu sendiri, tidak hanya yang terjadi dalam dunia nyata, tetapi juga dimungkinkan perbuatan melawan hukum yang terjadi di dunia maya, dalam hal ini intersepsi atau penyadapan data pribadi pada pengguna internet. Selain itu, dapat pula diterapkan Pasal 1365 BW dengan melakukan konstruksi hukum analogi yaitu dengan cara membandingkan antara perbuatan melawan hukum yang dilakukan di dunia nyata dengan dunia maya, sehingga pada akhirnya unsur-unsur perbuatan melawan hukum sebagaimana disyaratkan tetap dapat terpenuhi. Walaupun pada prakteknya muncul kesulitan-kesulitan dalam penerapannya, namun tetap diharapkan perbuatan melawan hukum yang terjadi harus tetap mendapat sanksi secara hukum sehingga tidak ada kekosongan hukum.

Suatu perbuatan dapat dikatakan perbuatan melawan hukum apabila perbuatan tersebut memang melanggar peraturan perundang-undangan, bertentangan dengan kesusilaan dan ketertiban umum. Meskipun demikian, suatu perbuatan yang telah dikategorikan sebagai perbuatan melawan hukum ini harus dapat dipertanggungjawabkan apakah mengandung unsur kesalahan atau tidak[34].

Pasal 1365 BW tidak membedakan kesalahan dalam bentuk kesengajaan *(opzet-dolus)* dan kesalahan dalam bentuk kurang hati-hati *(culpa)*, dengan demikian hakim harus dapat menilai dan mempertimbangkan berat ringannya kesalahan yang dilakukan sesorang dalam hubungannnya dengan perbuatan melawan hukum ini, sehingga dapat ditentukan ganti kerugian yang seadil-adilnya.

Adapun perbuatan yang dianggap sebagai perbuatan melawan hukum, namun tidak dapat dituntut sebagai perbuatan melawan hukum, yaitu apabila perbuatan tersebut

---

[32] Riduan Syahrani, 1992, *Seluk-Beluk dan Asas-Asas Hukum Perdata*, Alumni, Bandung, hal 273.
[33] http://kuliahhukum-rozieq.blogspot.com, *Penafsiran Hukum*, diakses pada tanggal 22-04-2018
[34] http://wonkdermayu.wordpress.com, ***Tinjauan Hukum Mengenai Perbuatan Melawan Hukum Dalam Transaksi Jual Beli Melalui Internet (E-Commerce) Dihubungkan dengan Buku III KUH Perdata***, diakses pada tanggal 13 April 2014 pukul 03:20 WIB.

ISBN : 978-623-90705-0-2

dilakukan dalam kcadaan darurat, kcadaan mcmaksa *(overmacht)*[35], karcna pcrintah kepegawaian atau salah sangka yang dapat dimaafkan. Namun dalam hal ini, pengecualian tersebut tidak berlaku bagi pelaku karena pelaku melakukannya dengan sengaja untuk mencari keuntungan. Apabila unsur kesalahan dalam suatu perbuatan melawan hukum dapat dibuktikan, maka pelaku penyadapan atau *sniffer* harus bertanggung jawab atas kerugian yang disebabkan perbuatannya tersebut.

Perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 BW ini dapat digunakan sebagai dasar untuk mengajukan ganti kerugian atas perbuatan yang dianggap melawan hukum karena telah menyebabkan kerugian kepada pengguna internet baik kerugian secara materiil maupun immaterial.

II. Kendala Dalam Proses Penegakkan Hukum Terhadap Penyadapan Data Pribadi Pada Pengguna Internet

Dalam ruang siber pelaku pelanggaran seringkali menjadi sulit dijerat karena hukum dan pengadilan Indonesia tidak memiliki yuridiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum bersifat transnasional tetapi akibatnya justru memiliki implikasi hukum di Indonesia[36].

Dalam hukum internasional, dikenal 3 (tiga) jenis yuridiksi, yaitu:[37]

1. Yuridiksi untuk menetapkan Undang-Undang;
2. Yuridiksi untuk penegakkan hukum;
3. Yuridiksi untuk menuntut.

Semakin tingginya kejahatan dengan menggunakan media internet sebagai sarananya pada saat ini yang meliputi berbagai jenis kejahatan contohnya yaitu penipuan kartu kredit, penipuan perbankan, *defacing*, *cracking*, *hacking*, *crading*, transaksi seks, judi *online* dan terorisme dengan korban yang sudah melintasi batas-batas teritorial dari suatu wilayah negara pada saat ini, merupakan salah satu permasalahan yang cukup rumit yang harus dihadapi oleh aparat penegak hukum dalam suatu wilayah negara.

Adapun teori yang berlaku di Amerika Serikat untuk menentukan *locus delicti* atau tempat kejadian perkara suatu tindakan *cybercrime* adalah sebagai berikut[38] :

---

[35] Purwahid Patrik, ***Dasar-Dasar Hukum Perikatan***, Mandar Maju, Bandung, 1994, hal 82.

[36] Ahmad Mujahid Ramli, 2010, *Cyberlaw dan Haki dalam Sistem Hukum Indonesia*, PT. Refika Aditama, Bandung, Hlm. 19

[37] *Ibid,* hlm. 20

[38] Darrel Menthe, *Jurisdiction in Cyberspace : A Theory of International Space,* sumber: www.hukumonline.com, diakses pada tanggal 22-04-2018

ISBN : 978-623-90705-0-2

1. *Theory of the Uploader and the Downloader*

   Teori ini menekankan bahwa dalam dunia *cyber* terdapat dua hal utama yaitu *uploader* (pihak yang memberikan informasi kedalam *cyberspace*) dan *downloader* (pihak yang mengakses informasi).

2. *Theory of Law of the Server*

   Dalam pendekatan ini, penyidik memperlakukan *server* dimana halaman *web* secara fisik berlokasi tempat mereka dicatat atau disimpan sebagai data elektronik.

3. *Theory of International Space*

   Menurut teori ini, *cyberspace* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama.

Yang berwenang untuk melakukan penyidikan menyangkut masalah *cybercrime,* khususnya penyadapan data pribadi pada pengguna internet ini adalah institusi POLRI, yang mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Salah satu upaya pemerintah dalam menekan tingkat kejahatan dunia maya atau *cybercrime* tersebut yaitu dengan menyusun dan mengesahkan suatu peraturan perundang-undangan yang secara khusus mengatur mengenai kejahatan dunia maya atau *cybercrime* yang termasuk di dalamnya membahas mengenai intersepsi atau penyadapan, dalam hal ini penyadapan data pribadi pada pengguna internet yang merupakan salah satu bentuk dari *cybercrime*.

Indonesia sendiri yang merupakan salah satu negara dengan tingkat kejahatan *cybercrime* yang cukup tinggi telah mengesahkan suatu peraturan perundang-undangan yang secara khusus mengatur mengenai seluruh kegiatan dalam dunia maya khususnya bagi permasalahan yang menyangkut *cybercrime* yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Meskipun tidak mencakup semua aktivitas di dunia maya, namun dengan adanya Undang-Undang Informasi dan Transaksi Elektronik dirasa membawa angin segar bagi para penegak hukum dalam menghadang laju kejahatan yang dilakukan para *cracker* yang semakin banyak muncul di dunia siber *(cyberspace).*

ISBN : 978-623-90705-0-2

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini mempunyai 13 Bab dan 54 Pasal di dalamnya yang mengatur berbagai kegiatan dunia *cyber* serta menerapkan asas-asas diantaranya yaitu[39] :

1. Asas ekstra teritorial
2. Asas kepastian hukum
3. Asas manfaat
4. Asas kehati-hatian
5. Asas itikad baik, dan
6. Asas netral teknologi.

Tetapi, lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini belum didukung dengan peraturan yang mengatur tentang hukum formilnya. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengacu pada prinsip pengaturan dengan metode sintesis hukum materiil dan *lex informatica*. Yaitu strategi pembentukan pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik tersebut dilakukan dengan cara menetapkan prinsip-prinsip pembentukan dan pengembangan teknologi informasi, yang isinya antara lain sebagai berikut[40]:

1. Mengikuti keunikan *cyberspace*;
2. Melibatkan unsur-unsur masyarakat, pemerintah, swasta, dan profesional serta perguruan tinggi;
3. Mendorong peran sektor swasta;
4. Mendorong peran masyarakat, swasta, pemerintah, kelompok profesi, dan perguruan tinggi;
5. Peran dan tanggung jawab pemerintah terhadap kepentingan publik;
6. Aturan hukum yang bersifat preventif, derektif, dan futuristik yang tidak bersifat restriktif;
7. Mendorong harmonisasi dan uniformitas hukum regional dan internasional; dan
8. Melakukan pengkajian terhadap peraturan yang berkaitan langsung atau tidak langsung dengan munculnya persoalan-persoalan hukum akibat perkembangan teknologi informasi.

---

[39] Firman Nuro, *Opcit*, hlm. 63

[40] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknolog*i, Citra Aditya Bakti, Bandung, hlm. 224

ISBN : 978-623-90705-0-2

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana Pasal 183 menyatakan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali dengan sekurang-kurangnya dua alat bukti yang sah sehingga hakim memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Berdasarkan Pasal 183 KUHAP tersebut dapat diketahui bahwa peradilan di Indonesia menuntut sekurang-kurangnya harus ada dua alat bukti yang sah untuk menjatuhkan pidana terhadap seseorang yang terkait dalam suatu kasus. Sedangkan alat bukti yang dimaksud adalah alat bukti sebagaimana diatur dalam pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yaitu terdiri dari :

1. Keterangan saksi

   Dalam Pasal 185 ayat (1) KUHAP disebutkan bahwa keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan dalam persidangan. Berdasarkan penjelasan KUHAP dinyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain. Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia lihat sendiri dan dialami sendiri dengan menyebut alasan dari pengetahuannya itu.

2. Keterangan ahli

   Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Selanjutnya penjelasan Pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga telah diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah pada waktu ia menerima jabatan atau pekerjaan. Menurut teori hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya.

3. Surat

   Sebagai alat bukti diatur dalam Pasal 187 KUHAP. Menurut komentar KUHAP yang disusun oleh M. Karjadi dan R. Soesilo, Pasal 187 membedakan atas empat macam surat, yaitu[41] :

---

[41] Darsono, *Tinjauan Yuridis terhadap Pencurian Dana Nasabah Bank Melalui Internet Dihubungkan dengan Pasal 362 Kitab Undang-Undang Hukum Pidana Juncto Undang-Undang Nomor 11 Tahun 2008*

ISBN : 978-623-90705-0-2

a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, didengar, dilihat atau dialaminya sendiri, disertai dengan alasan tentang keterangan itu;
b. Surat yang dibuat menurut peraturan undang-undang atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukan bagi pembuktian sesuatu hal atau keadaan;
c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau keadaan yang diminta secara resmi dari padanya; dan
d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

4. Petunjuk

   Pasal 188 ayat (1) KUHAP memberi definisi petunjuk sebagai perbuatan, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya. Selanjutnya Pasal 188 ayat (3) KUHAP dinyatakan bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif dan bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan keseksamaan berdasarkan hati nuraninya.

5. Keterangan terdakwa

   Menurut Pasal 189 ayat (1) KUHAP adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri dan alami sendiri. Keterangan terdakwa tidak perlu sama dengan pengakuan, karena pengakuan sebagai alat bukti mempunyai syarat, yaitu :

   a. Mengaku ia yang melakukan delik yang didakwakan; dan
   b. Mengaku ia bersalah.

Yang sering dipermasalahkan antara lima jenis alat bukti tersebut adalah keterangan ahli, dalam hal ini adalah ahli komputer. Masalahnya adalah apakah setiap orang yang mahir mengoperasikan komputer dapat dikategorikan sebagai ahli komputer. Dalam

---

tentang Informasi dan Transaksi Elektronik, Sumber: http://elib.unikom.ac.id, diakses pada tanggal 25 April 2018

ISBN : 978-623-90705-0-2

KUHAP sendiri tidak terdapat penjelasan mengenai apakah yang dimaksud dengan keterangan ahli dan siapakah yang dimaksud dengan ahli. Padahal keterangan saksi ahli *(expert testimony)* merupakan salah satu ciri peradilan modern.

Untuk mengantisipasi kendala menyangkut alat bukti yang sah yang merupakan salah satu unsur yang harus ada dalam persidangan dalam tindak pidana *cybercrime*[42], dalam hal ini penyadapan data pribadi pada pengguna internet menunjuk pada Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa : Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah.

Berdasarkan Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatas, bahwa Informasi Elektronik merupakan alat bukti hukum yang sah, meliputi informasi elektronik dan/atau dokumen elektronik, dan/atau hasil cetakannya. Ketentuan ini merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia[43]. Dalam pengertiannya, Informasi Elektronik adalah salah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, surat elektronik, telegram, teleks, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sedangkan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk *analog, digital, elektromagnetik, optikal*, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tapi tidak terbatas pada tulisan, suara, gambar, peta rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Kemudian Pasal 5 ayat (2) menyebutkan :

> 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.

---

[42] Firman Nuro, *Opcit*, hal 69.

[43] Siswanto Sunarso, 2009, *Hukum Informasi dan Transaksi Elektronik*, Rineka Cipta, Jakarta, hlm. 50

ISBN : 978-623-90705-0-2

Jadi, pada dasarnya setiap dokumen elektronik dan/atau informasi elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah dimana hal tersebut merupakan perluasan dari alat bukti yang sah menurut hukum acara yang telah berlaku di Indonesia.

Pada perkara *cybercrime* alat bukti yang digunakan adalah alat bukti yang mengandung unsur dari teknologi dan informasi dimana dalam dunia teknologi dan informasi banyak hal-hal yang bersifat digital atau elektronik. Oleh karena itu kejahatan yang terjadi dalam ranah *cybercrime* juga akan menghasilkan alat bukti yang bersifat digital atau elektronik[44].

Di Indonesia sendiri terdapat putusan pengadilan yaitu Putusan Mahkamah Agung Republik Indonesia Nomor 9/KN/1999, yang dalam putusannya hakim menerima hasil *print out* sebagai alat bukti surat. Kemudian kasus pidana yang diputus di Pengadilan Negeri Jakarta Timur mengetengahkan bukti *Email (Elektronic Mail)* sebagai salah satu alat bukti. Setelah mendengar keterangan ahli bahwa dalam transfer data melalui *Email* tersebut tidak terjadi tindakan manipulatif, hakim memvonis terdakwa dengan hukuman satu tahun penjara karena terbukti telah melakukan tindakan cabul berupa penyebaran tulisan dan gambar[45]. Hal ini merupakan perkembangan baru yang tepat untuk diikuti oleh hakim-hakim dalam memutus perkara *cyber*.

Memang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tidak sembarang informasi elektronik atau dokumen elektronik dapat dijadikan alat bukti yang sah. Suatu informasi elektronik atau dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan Sistem Elektronik yang sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan persyaratan minimum sebagaimana dimaksud dalam Pasal 7 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik[46].

Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang merupakan perluasan dari Pasal 184 Kitab Undang-Undang Hukum Acara Pidana sudah sangat relevan untuk dijadikan dasar hukum

---

[44] Fh.unpad.ac.id, *Studi KasusTerhadap Putusan Pengadilan Negeri Kota Bandung Nomor 622./PID.B/2013/PN.BDG Tentang Prostitusi Online Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,* diakses pada tanggal 21-04-2018

[45] Michael Barama, 2011, *Elektronik Sebagai Alat Bukti Dalam Cybercrime,* Karya Ilmiah Universitas Sam Ratulangi, Manado, hlm. 28-29

[46] http://www.hukumonline.com, *Perluasan Alat Bukti Hukum yang Sah dalam Undang-Undang Informasi dan Transaksi Elektronik,* diakses pada tanggal 22-04-2018

ISBN : 978-623-90705-0-2

menyangkut alat bukti yang sah dalam persidangan yang menyangkut kejahatan *cybercrime* dalam hal ini penyadapan data pribadi pada pengguna internet yang bertentangan dengan Pasal 31 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Cybercrime yang pada prosesnya menggunakan teknologi tinggi, jangkauannya sangat luas serta pelaku rata-rata mempunyai intelektualitas yang tinggi dan mempunyai komunitas tersendiri, sehingga untuk pembuktiannya memerlukan penyidik yang mengerti bidang tersebut.

Adapun salah satu faktor yang menghambat dalam proses penyidikan untuk penanganan kasus *cybercrime* antara lain adalah sebagai berikut :

1. Kurangnya pengetahuan tentang komputer;
2. Pengetahuan dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas;
3. Faktor sistem pembuktian yang menyulitkan para penyidik.

E. Kesimpulan Dan Saran

Berdasarkan pembahasan pada bab-bab sebelumnya, maka penulis dapat menarik simpulan sebagai berikut :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tindak pidana penyadapan data pribadi pada pengguna internet berdasarkan yaitu tertuang dalam Pasal 31 ayat (1) dan (2). Pasal tersebut merupakan landasan hukum bagi para pengguna internet dari tindakan penyadapan yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain.
2. Kendala dalam penegakkan hukum terhadap penyadapan data pribadi pada pengguna internet yaitu dalam upaya pembuktian, keterangan para ahli, dan masalah yuridiksi peradilan, dimana hukum suatu negara tidak dapat menjangkau pelaku kejahatan diluar negaranya.

Berdasarkan kesimpulan yang telah diuraikan diatas, maka Perlu diatur secara terperinci mengenai tata cara intersepsi atau penyadapan pada Pasal 31 ayat 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, agar tidak terjadi kesalahan teknis penyadapan yang mengakibatkan kerugian bagi seseorang

ISBN : 978-623-90705-0-2

berkaitan dengan privasi orang tersebut. Karena kegiatan intersepsi atau penyadapan tersebut sudah bertentangan dengan hak seseorang untuk mendapatkan privasi dalam wilayah pribadi orang lain.

Daftar Pustaka

Buku-Buku

Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum,* PT. Citra Aditya Bakti, Bandung, 2004.

Abdul Wahid & Mohammad Labib, *Kejahatan Mayantara (Cybercrime),* Refika Aditama, Bandung, 2005.

Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* PT. Citra Aditya Bakti, Bandung, 2002.

Ahmad Mujahid Ramli, *Cyberlaw dan Haki dalam Sistem Hukum Indonesia,* PT. Refika Aditama, Bandung, 2010.

Firman Nuro, *Adopsi Enkripsi Jefferson Wheel pada Protokol One-Time Password Authentication untuk Pencegahan Sniffing pada Password E-mail,* Seminar Nasional Aplikasi Teknologi Informasi (SNATI), Yogyakarta, 2010.

H. Hilman Hadikusuma, *Metode Pembuatan Kertas Kerja atau Skripsi Ilmu Hukum,* CV. Bandar Maju, Bandung, 1995.

Israel Fanny, *Analisis Hukum mengenai Tanggung Jawab Operator Seluler terhadap Pelanggan Seluler Terkait Spam,* Unikom, Jakarta, 2011.

Kristian & Yopi Gunawan, *Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia,* Nuansa Aulia, Bandung, 2013.

Michael Barama, *Elektronik sebagai Alat Bukti dalam Cybercrime,* Karya Ilmiah Universitas Sam Ratulangi, Manado, 2011.

Purwahid Patrik, *Dasar-dasar Hukum Perikatan,* Mandar Maju, Bandung, 1994.

Puspita Dewa, *Tindak Pidana Penipuan untuk Memperoleh Informasi Personal (Pishing) melalui Pengiriman E-mail,* Unikom, Jakarta, 2001.

Riduan Syahrani, *Seluk Beluk dan Asas-asas Hukum Perdata,* Alumni, Bandung, 1992.

Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik,* PT. Rineka Cipta, Jakarta, 2009.

Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat),* Rajawali Peers, Jakarta, 2001.

Thor, *Hacker's Biggest Secret Zero Knowledge Password,* PT. Elex Media Komputindo, Jakarta, 2008.