Jurnal Ilmiah Wahana Pendidikan, Juli 2023, 9(13), 475-486
DOI:. https://doi.org/10.5281/zenodo.8153212
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Tindak Pidana Penyadapan (*Cyber Espionage*) Menurut Hukum Positif Di Indonesia

Nurazizah, Amirudin, Ufran

Universitas Mataram

Received: 20 Juni 2023
Revised: 29 Juni 2023
Accepted: 03 Juli 2023

Abstract

Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis kriteria penyadapan (cyber espionage) yang berimplikasi tindak pidana dan mengetahui dan menganalisis dasar hukum penyadapan (cyber espionage) menurut hukum positif di indonesia. Penelitian ini merupakan jenis penelitian hukum normatif, dengan menggunakan pendekatan perundang-undang (statute approach), pendekatan konpseptual (conceptual approach). Hasil dari penelitian ini adalah sebagaimana dijelaskan dalam penjelasan Pasal 40 UU No. 36 Tahun 1999 tentang Telekomunikasi, Pasal 31 UU No. 11 Tahun 2008 tentang ITE, dan Pasal 322 ayat 1 sampai ayat 3 UU No. 1 Tahun 2023 tentang KUHP secara tegas menyatakan bahwa penyadapan yang dilakukan dalam bentuk apapun merupakan suatu perbuatan pidana yang berakibat penjatuhan sanksi pidana, dengan kriteria penyadapan itu dilakukan dengan sengaja secara melawan hukum untuk memperoleh informasi/dokumen elektronik milik orang lain. Meskipun penyadapan merupakan suatu perbuatan yang dilarang, namun didalam beberapa peraturan perundang-undangan, penyadapan ini dapat dimungkinkan untuk dilakukan oleh aparat penegak hukum guna mengungkap suatu tindak pidana tertentu berdasarkan undang-undang yang berlaku.

Keywords: *Tindak Pidana, Penyadapan, Hukum Positif*

(*) Corresponding Author: nurazizah10011001@gmail.com

How to Cite: Nurazizah, Amirudin, & Ufran. (2023). Tindak Pidana Penyadapan (Cyber Espionage) Menurut Hukum Positif Di Indonesia. https://doi.org/10.5281/zenodo.8153212

PENDAHULUAN

Perkembangan teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum karena ternyata dalam perkembangannya, internet tersebut membawa sisi negatif, dengan membuka tindakan-tindakan anti sosial dan perilaku kejahatan yang selama ini dianggap tidak mungkin terjadi. Sebagaimana sebuah teori mengatakan *"crime is product of society it self"*,[1] yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas masyarakat, semakin canggih pula kejahatan yang mungkin terjadi pada mayarakat itu.

Awalnya teknologi internet merupakan sesuatu yang bersifat netral dimana teknologi internet diartikan sebagai teknologi yang bebas nilai. Teknologi tidak dapat dilekati sifat baik dan jahatnya, akan tetapi pada perkembangannya kehadiran teknologi menggoda para pihak yang berniat jahat untuk menyalah gunakannya. Sehingga dapat dikatakan teknologi sebagai faktor Kriminologen, faktor yang

[1] Shelly Nicko, Tindak Pidana *Cyber Espionage*, Jurnal Hukum, (Surabaya, ADLN-Perpustakaan, Universitas Airlangga), 2010.

menyebabkan keinginan orang untuk berbuat jahat atau memudahkan terjadinya tindak kejahatan.[2]

Internet sendiri merupakan sarana yang dapat memberikan berbagai macam informasi aktual tajam dan terpercaya dibelahan dunia manapun bahkan banyak dikalangan sekarang sudah banyak yang menggunakan internet sebagai sarana kejahatan yang kita kenal dengan istilah *Cyber Crime. Cyber crime*, merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai alat kejahatan utama.[3] Jenis *cyber crime* yang dirasa membahayakan khalayak dalam aktivitasnya adalah *cyber espionage* yang lazimnya disebut tindakan mata-mata atau pengintaian terhadap suatu data pihak lain.[4] Mengingat internet merupakan media lintas informasi yang berdampak luas, maka akses data yang menyangkut pihak lain patut menjadi perhatian dan dapat menjadi kejahatan yang serius.

Sebelum adanya perkembangan teknologi informasi yang menghadirkan internet sebagai salah satu medianya, dahulu tindakan pengintaian dilakukan secara konvensiaonal, salah satunya adalah penyadapan dengan menggunakan alat perekam biasa, dengan hanya menyadap pembicaraan berbentuk suara sebagai sasarannya. Namun kini, jaringan internet berkecepatan tinggi dengan memanfaatkan berbagai perangkat lunak (*software*) yang dapat di download secara gratis mampu melakukan aksi pengintaian yang salah satunya adalah dengan penyadapan terhadap pihak lawan baik terhadap suara, gambar maupun data sebagai sasarannya, yang kini disebut *cyber espionage*.[5]

Istilah *spyware* atau peranti lunak yang memata-matai pengguna komputer telah lama menjadi kosa kata dunia informasi teknologi. *Spyware* dibuat bukan untuk merusak suatu sistem sebuah komputer, namun digunakan untuk melakukan pengintaian terhadap para pemakai komputer, yang akhirnya akan mengambil data-data pengguna computer, kemudian *spyware* ini akan mengirimkan data-data tersebut kepada si pemilik *spyware*.

Mengingat persoalan yang dihadapi tidak sesederhana penanganan kejahatan komputer biasa, maka tindakan pencegahan suatu kejahatan penyadapan atau pengintaian terhadap informasi khususnya data digital di internet (*cyber espionage*) perlu menjadi perhatian serius. Hal ini juga tidak lepas dari peran hukum khususnya yang berkaitan dengan fungsi hukum pidana adalah melindungi kepentinagn hukum, baik kepentingan hukum orang, warga masyarakat, maupun negara atau pelanggaran oleh siapapun.[6]

Di Indonesia sendiri, dalam perkembangannya tepatnya berkenaan dengan diterbitkannya Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunkasi, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tindakan penyadapan dinyatakan sebagai suatu tindak pidana.

---

[2] Abdul Wahid Dan Mohammad Labil, *Kejahatan Mayantara (cyber Crime)*, Cet 1, Rafika Aditama, Malang, 2005, hlm. 59.

[3] Sutarman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, LaksBang PRESSindo, Jogjakarta, 2007, hlm. 3.

[4] Shelly Nicko, *Op.Cit* , hlm. 16.

[5] https://yuliatwn.cybercrime.wordpress.com, Diakses Pada Tanggal 25 februari 2023

[6] Didik Endro P., Bahan Ajar *Hukum Telematika* , Universitas Airlangga, Genap 2008/2009, hlm. 28.

Perbuatan tersebut diatur dalam Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang menyebutkan bahwa "setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun dan yang melanggar dipidana penjara maksimal 15 tahun penjara". Di dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik penyadapan diatur dalam Pasal 31 ayat (1) menyebutkan bahwa :

"Setiap orang dengan sengaja dan dengan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau elektronik tertentu milik orang lain dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)".

Penyadapan merupakan suatu perbuatan yang dilarang, namun dalam batas-batas dan tujuan tertentu, penyadapan dapat dimungkinkan untuk dilakukan oleh aparat penegak hukum untuk mengungkap suatu tindak pidana tertentu. Hal tersebut diatur dalam Pasal 42 ayat (2) Undang-Undang Telekomunikasi, dan Pasal 31 ayat (3) Undang-Undang Informasi dan Transaksi Elektronik (ITE) memberikan penjelasan bahwa Undang-Undang memperbolehkan tindakan penyadapan kepada Kejaksaan, Kepolisian Negara Republik Indonesai, Penyidik, dan/atau institusi penegak hukum lainnya dalam tindak pidana tertentu yang dilakukan berdasarkan undang-undang yang berlaku.

Dalam kenyataan sekarang ini memang tidak dapat dipungkiri bahwa penyadapan (*cyber Espionage*) merupakan sarana yang sangat membantu para aparatur penegak hukum terutama dalam mengusut kejahatan luar biasa (*extraordinary*) dan membantu menghadapai berbagai bentuk tindak pidana dengan modus baru yang semakin sulit dilacak dan semakin sulit pembuktiannya. Perlu juga difikirkan dan dicari jalan keluar berkaitan dengan sifat penyadapan yang pada dasarnya merupakan suatu tindak pidana, yang dapat menderogasi atau bahkan meniadakan hak privasi sesorang atau hak asasi manusi itu sendiri.

Meskipun prihal penyadapan telah diatur secara tegas dan jelas dalam masing-masing undang-undang sebagaimana telah dikemukakan sebelumnya, namun dalam hal ini masih terdapat kekosongan norma hukum (*recht vacuum*) di bidang penyadapan. Kekosongan hukum tersebut tidak lain dikarenakan masih banyaknya ketidakjelasan mengenai konsep penyadapan, ketidakjelasan mengenai prosedur dan mekanisme penyadapan, atau bahkan terjadi tumpang tindih pengaturan (dualisme norma) sehingga akan menimbulkan ketidakpastian hukum dan tentu akan berpengaruh pada pelaksanaannya. Dikatakan demikian karena di undang-undang yang satu tindak penyadapan dikualifikasikan sebagai suatu tindak pidana, sedangkan di undang-undang lainnya tindak penyadapan justru merupakan kewenangan yang dimiliki oleh aparat penegak hukum untuk mengungkap suatu tindak pidana.

BAHAN DAN METODE

Metode penelitian yang digunakan adalah metode penelitian yuridis normatif, yaitu metode penelitian dengan menggunakan kaidah-kaidah hukum yang ada sebagai apa yang tertulis (*law in books*) dalam peraturan perundang undangan ataupun sebagai kaidah dan norma yang merupakan patokan perilaku manusia yang

dianggap pantas.[7] Penelitian ini mengkaji norma, asas, maupun nilai yang terdapat dalam peraturan Perundang-undangan, yang mencerminkan problematika hukum yang berupa adanya kekosongan norma, kekaburan dan konflik norma, dengan sumber hukum primer, sekunder dan tarsier. Teknik dan alat pengumpulan bahan hukum yang digunakan adalah dengan "*Study Document*" dengan mengadakan penelusuran kepustakaan (*Library Research*), menelusuri, membaca, mempelajari, serta mengkaji berbagai literatur berupa peraturan perundang-undangan, karya tulis, Buku-Buku, pendapat para sarjana, dan para ahli hukum yang berdasarkan pengelompokan yang tepat, berkaitan dengan pokok permasalahan.

HASIL DAN PEMBAHASAN

Perkembangan teknologi yang sedemikian pesat di iringi dengan adaptasi masyarakat terhadap pola perilaku dan kebutuhan yang ada di sisi lain juga melahirkan sebuah modus operandi baru di bidang komunikasi. Berbagai fasilitas yang mempermudah pertukaran informasi di satu sisi memang menguntungkan konsumen pengguna jasa telekomunilcasi namun di sisi lain menciptakan bentuk kejahatan barn yang membutuhkan ketentuan hukum pidana untuk mengantisipasinya. Seperti dijelaskan Sudarto bahwa "hukum pidana atau lebih tepat sistem pidana itu merupakan bagian dari politik kriminil, ialah usaha rasionil dalam menanggulangi kejahatan".[8] Hingga saat ini sudah banyak pengaturan mengenai penyadapan yang tersebar diberbagai undang-undang. Dua diantara ketentuan hukum yang mengatur tentang penyadapan secara khusus, yaitu UU No. 36 Tahun 1999 tentang Telekomunikasi dan UU No. 11 Tabun 2008 tentang Informasi dan Transaksi Eleltronik.

Di dalam UU No. 36 Tahun 1999 tentang Telekomunikasi menjelaskan bahwa segala bentuk pengurangan dan gangguan terhadap kegiatan telekomunikasi mendapatkan larangan keras dalam ketentuan hukum ini, tidak terkecuali penyadapan. Pasal 40 UU No. 36 Tahun 1999 dengan tegas menyatakan "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun." Ketentuan hukum tersebut menyatakan bahwa tindakan penyadapan merupakan tindakan yang dilarang walaupun dilakukan dalam bentuk apapun dan serahasia apapun. Sebagaimana dijelaskan dalam Penjelasan Pasal 40 UU No. 36 Tahun 1999 bahwa, pada dasarnya informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang. Dasar dari pelarangan tindakan penyadapan tidak lain karena memang hak untuk berkomunikasi dan bertukar informasi merupakan hak pribadi yang mendapatkan perlindungan hukum. Uniknya, dalam penjelasan Pasal 40 tersebut diberikan satu definisi tentang penyadapan yaitu "kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara yang tidak sah." Berangkat dari definisi tersebut penyadapan dalam kacamata UU No. 36 Tahun 1999 (secara khusus Pasal 40) dipandang sebagai tindakan yang dilakukan secara sengaja dan

[7]Amiruddin, H Zainal Asikin, "*Pengantar Metode Penelitian Hukum*", (Depok: PT Raja Grapindo Persada), 2020, hlm. 163.

[8] Sudarto, Hukum Pidana dan Perkembangan Masyarakat: Kajian terhadap Pembaharuan Hukum Pidana, Sklar Baru, Bandung, 1983, hlm. 31.

melawan hukum dengan tujuan untuk mendapatkan informasi melalui pemasangan alat sadap pada jaringan telekomunikasi. Artinya perbuatan tersebut dilakukan memang dengan tujuan untuk merugikan pihak lain dan sangat berbahaya bagi kepentingan publik. Pasal 56 UU No. 36 Tahun 1999 menegaskan ancaman sanksi bagi pelaku penyadapan *illegal* ini dengan pidana penjara maksimal 15 tahun. Secara eksplisit, Pasal 40 jo. Pasal 56 UU No. 36 Tahun 1999 menegaskan satu bentuk tindak pidana di bidang telekomunikasi yaitu tindak pidana penyadapan.

Berdasarkan beberapa ketentuan hukum diatas tarnpak jelas bahwa UU No. 36 Tahun 1999 pada prinsipnya menekankan perlindungan hak atas informasi dan pengamanan yang sangat ketat atas kerahasiaan informasi konsumen. Bentuk pengecualian pun sebenarnya merupakan ketentuan yang bersifat permisif dan sangat dibatasi dalam pelaksanaannya karena dinilai melanggar hak pribadi orang lain.

Undang-Undang ini memiliki jangkauan yurisdiksi tidak sematamata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Dalam kehidupan bermasyarakat, berbangsa, dan bernegara, hak dan kebebasan melalui penggunaan dan pemanfaatan Teknologi Informasi tersebut dilakukan dengan mempertimbangkan pembatasan yang ditetapkan dengan undangundang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilainilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis. UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undangundang pertama di bidang Teknologi.

Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi ujung tombak yang meletakkan dasar pengaturan di bidang pemanfaatan Teknologi Informasi dan Transaksi Elektronik, walaupun dalam kenyataannya, selama pelaksanaan dari UU ITE mengalami beberapa masalah. Kesatu, terhadap UndangUndang ini telah diajukan beberapa kali uji materiil di Mahkamah Konstitusi dengan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, Nomor 2/PUUVII/2009, Nomor 5/PUU-VIII/2010, dan Nomor 20/PUU-XIV/2016. Berdasarkan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008 dan Nomor 2/PUU-VII/2009, tindak pidana penghinaan dan pencemaran nama baik dalam bidang Informasi Elektronik dan Transaksi Elektronik bukan semata-mata sebagai tindak pidana umum, melainkan sebagai delik aduan.

Mengingat penggunaan transaksi elektronik ini terus meningkat, maka sangat diperlukan panyaring hukum untuk mengaturnya, untuk itulah UU ITE menjadi urgent (penting) dan mendesak untuk segera diimplementasikan. UU ITE ini diharapkan memberikan manfaat, guna menjamin kepastian hukum bagi masyarakat yang melakukan transaksi elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan

melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi. Landasan hukum bagi pemanfaatan teknologi informasi dan transaksi elektronik serta segala sesuatu yang mendukung penyelenggarannya yang dapat pengakuan hukum di dalam dan di luar pengadilan.

Penegasan mengenai delik aduan dimaksudkan agar selaras dengan teori kepastian hukum dan rasa keadilan masyarakat. Berdasarkan Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010, Mahkamah Konstitusi berpendapat bahwa kegiatan dan kewenangan penyadapan merupakan hal yang sangat sensitif karena di satu sisi merupakan pembatasan hak asasi manusia, tetapi di sisi lain memiliki aspek kepentingan hukum. Oleh karena itu, pengaturan (regulation) mengenai legalitas penyadapan harus dibentuk dan diformulasikan secara tepat sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Di samping itu, Mahkamah berpendapat bahwa karena penyadapan merupakan pelanggaran atas hak asasi manusia sebagaimana ditegaskan dalam Pasal 28J ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, sangat wajar dan sudah sepatutnya jika negara ingin menyimpangi hak privasi warga negara tersebut, negara haruslah menyimpanginya dalam bentuk undang-undang dan bukan dalam bentuk peraturan pemerintah. Berdasarkan Putusan Mahkamah Konstitusi Nomor 20/PUUXIV/2016, Mahkamah Konstitusi berpendapat bahwa untuk mencegah terjadinya perbedaan penafsiran terhadap Pasal 5 ayat (1) dan ayat (2) UU ITE, Mahkamah menegaskan bahwa setiap intersepsi harus dilakukan secara sah, terlebih lagi dalam rangka penegakan hukum. Oleh karena itu, Mahkamah dalam amar putusannya menambahkan kata atau frasa "khususnya" terhadap frasa "Informasi Elektronik dan/atau Dokumen Elektronik". Bahwa putusan tersebut akan mempersempit makna atau arti yang terdapat di dalam Pasal 5 ayat (1) dan ayat (2) UU ITE agar tidak terjadi penafsiran, guna memberikan kepastian hukum keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti perlu dipertegas kembali dalam Penjelasan Pasal 5 UU ITE.

Perbuatan yang dilarang dalam Undang-Undang baik UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 27 UU Nomor 11 Tahun 2008 tentang ITE.

Terkait dengan penyadapan, UU No. 11 Tahun 2008 juga memberikan pengaturan secara khusus dalam Pasal 31. Ketentuan hukum Pasal 31 mengatur 2 (dua) bentuk larangan yaitu tindakan penyadapan atas dokurnen elektronik dan tindakan penyadapan atas transmisi informasi elektronik, tennasuk di dalamnya berakibat perubahan terhadap dokumen elektronik. Ketentuan Pasal 31 dan Pasal 32 UU ITE sama-sama mengatur tentang tindak pidana penyadapan. Perbedaannya, pada Pasal 31 ayat (1) UU ITE mengatur tindak pidana penyadapan secara umum sedangkan Pasal 32 ayat (2) UU ITE mengatur tindak pidana penyadapan yang dilakukan pada transmisi informasi elektronik/dokumen elektronik.

Keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik. Ketentuan pidana yang diatur dalam Undang-Undang

Nomor Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Ketentuan mengenai penggeledahan, penyitaan, penangkapan, dan penahanan yang diatur dalam UU ITE menimbulkan permasalahan bagi penyidik karena tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik begitu cepat dan pelaku dapat dengan mudah mengaburkan perbuatan atau alat bukti kejahatan. Karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja,

Dalam rangka melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik, diperlukan penegasan peran Pemerintah dalam mencegah penyebarluasan konten ilegal dengan melakukan tindakan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum agar tidak dapat diakses dari yurisdiksi Indonesia serta dibutuhkan kewenangan bagi penyidik untuk meminta informasi yang terdapat dalam Penyelenggara Sistem Elektronik untuk kepentingan penegakan hukum tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik. Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya cybercrime. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet). Aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusiinstitusi penegak hukum di daerah yang belum didukung dengan jaringan Internet.

Penyidikan tindak pidana di bidang informasi berdasarkan UU ITE diatur dalam Pasal 42 UU Nomor 11 Tahun 2008 tentang ITE menyatakan Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pengaturan Pasal 43 berdasarkan Undang-Undang Nomor Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan:

1. Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.
2. Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap

privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

3. Penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.
4. Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.
5. Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
b. memanggil setiap Orang atau pihak lainnya untuk didengar dan diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi
f. Elektronik;melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundangundangan;
h. membuat suatu data dan/atau Sistem Elektronik yang terkait tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik agar tidak dapat diakses;
i. meminta informasi yang terdapat di dalam Sistem Elektronik atau informasi yang dihasilkan oleh Sistem Elektronik kepada Penyelenggara Sistem Elektronik yang terkait dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;
j. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik; dan/atau
k. mengadakan penghentian penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan hukum acara pidana

6. Penangkapan dan penahanan terhadap pelaku tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.
7. Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) dalam melaksanakan tugasnya memberitahukan dimulainya penyidikan kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia. Dalam hal penyidikan sudah selesai, Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) menyampaikan hasil penyidikannya kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.
8. Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk

berbagi informasi dan alat bukti sesuai dengan ketentuan Peraturan perundang-undangan.

Melihat rumusan diatas dapat digaris bawahi beberapa unsur penting dalam tindakan penyadapan, yaitu unsur "dengan sengaja", unsur "tanpa hak atau melawan hukum" dalam melakukan intersepsi. Hal yang menarik dari rumusan diatas yang menekankan unsur subyektif berupa kesengajaan dalam bentuk kesengajaan sebagai suatu maksud (*opzet als oogmerk*). Artinya bentuk kesalahan yang dimiliki pelaku merupakan kesalahan yang memang pelaku menghendaki dan dapat membayangkan hasil dari perbuatannya tersebut sehingga syarat *willen en wetens* terpenuhi. Faisal Thayib sebagaimana dikutip Go Lisanawati mengakategorikan penyadapan dalam Pasal 31 UU ITE sebagai computer related crime dalam bentuk *illegal interception*." [9] Sebagai sebuah tindak pidana yang dilarang karena memang dilakukan tanpa ijin dan merugikan kepentingan orang lain. Tindakan penyadapan dalam ruang lingkup Pasal 31 UU 1TE merupakan tindakan yang benarbenar dilarang karena memang merupakan tindakan yang berbahaya bagi pengguna sistem komputer. Penyadapan juga diatur secara jelas di dalam UU No 1 Tahun 2023 tentang KUHP, yaitu di dalam Pasal 322 ayat 1 sampai ayat 3 secara tegas menyatakan bahwa penyadapan yang dilakukan dalam bentuk apapun merupakan suatu perbuatan pidana yang berakibat penjatuhan sanksi pidana.

Penyadapan selain dikategorikan sebagai suatu tindak pidana, namun juga suatu kebolehan dalam hal-hal tertentu bagi aparat penegak hukum guna mengungkap suatu tindak pidana tertentu. Undang-undang tersebut sebagai berikut

1. *Bab XXVII KUHP Belanda tentang Kejahatan Jabatan, Pasal 430-434.*
   Norma yang terdapat pada Primer kedua KUHP justru melarang pejabat yang berwenang melakukan penyadapan dan/atau pemantauan atau memperoleh informasi dan/atau memberikan kepada pihak lain terkait informasi yang telah didapatkan, contohnya isi percakapan telepon atau telegrap. Walaupun aturan tentang objek telekomunkasi itu sangatlah sederhana akan tetapi melihat dimana saat menyusun KUHP ini teknologi yang ada saat ini belum secanggih sebagaimana hari ini.[10]
2. *Undang-Undang Nomor 5 Tahun 1997 tentang Psikotropika.*
   Pada UU tersebut telah diatur proses penyadapan penyidik pada konteks investigasi kriminal yang berkaitan pada psikotropika. Hukum yang berkaitan dengan penyadapan dijelaskan dalam BAB XIII tentang Investigasi dimana memberi kekuasaan kepada polisi agar dapat melakukan penyadapan.
3. *Undang-Undang Nomor 31 tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi.*
   Pada UU kali ini, wewenang Spionase ditempatkan pada penjelasaan terhadap UU yang berkaitan pada wewenang penyelidik, pemeriksaan disidang pengadilan dan penuntutan. Point penjelasan dalam Pasal 26 ialah "Kewenangan penyidik dalam

[9]Go Lisnawati, "*Mengurai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Dimensi Pembangunan Cyber Law*", Jurnal Mika, Vol. 12 Nomor 1 Juli 2D09, hlm. 96

[10]R. Soesilo. *Kitab Undang-undang Hukum Pidana (KUHP) serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*, (Bogor: Politea, 1994), hlm. 290-293, Pasal 430-434.

Pasal ini termasuk wewenang untuk melakukan penyadapan (wiretapping)".

4. *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.*
   Tidak hanya Mengatur persoalan UU penyadapan, UU ini juga telah memberikan kekuasaan kepada pemilik layanan teknologi tersebut untuk dapat memberi suata data catatan komunikasi sebagai bukti pengguna layanan atau untuk tujuan Peradilan Tindak Pidana seperti yang telah ditentukan oleh Undang-undang dan peraturan.
5. *Perppu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme.*
   Perppu Nomor 1 Tahun 2002 tersebut menetapkan kekuasaan terhadap penyidik agar dapat menyadap akan tetapi pada konteks investigasi criminal terorisme. Writetaping hanya dapat dilaksanakan ketika ada suatu izin yang di berikan oleh ketua Pengadilan sebagaimana telah diberikan kurung waktu selama maksimal 1 tahun.
6. *Undang-Undang Nomor 18 Tahun 2003 Mengenai Advokat*.
   Pada aturan UU ini telah mengatur sebagaimana kemerdekaan seorang Advokat agar dapat dilindungi oleh segala tindakan writetapping ketika mereka sedang berkomunikasi dengan klien mereka. Undang-undang Advokat ini menjelaskan bahwa seorang Advokat itu mempunyai wewenang atas keprivasian hubungannya terhadap kliennya, juga perlindungan akan file dan dokumen yang dia sita ataupun inspeksi.
7. *Udang-Undang Nomor 21 Tahun 2003 Tentang Pemberantasan Tindak Pidana Perdagangan Orang*.
   Pada peraturan Perundang-undangan kali ini telah memberikan wewenang terhadap penyidik agar dapat melakukan wiretapping sebagaimana yang telah melakukan criminal perdagangan orang wiretapping dapat diaktualkan ketika jenis criminal itu berlandaskan bukti awal yang kuat dan dengan izin dari kepala Pengadilan.
8. *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.*
   Dimana Peraturan Perundang-undang ini pada dasarnya melarang adanya pelaksanaan pengadaan informasi elektronik dan / atau data elektronik. Ketika terdapat suatau penyimpangan dari itu maka wiretapping dapat prinsipnya melarang pelaksanaan pengadaan informasi elektronik dan / atau data elektronik. Adapun penyimpangan dari ketentuan ini dimana penyadapan bisa digunakan pada konteks penegakan hukum dengan syarat permintaan polisi, lembaga penegak hukum dan / atau jaksa penuntut umum lainnya atau telah ditentukan berlandaskan Hukum.
9. *Undang-Undang Nomor 35 tahun 2009 tentang Tindak Pidana Narkotika.*
   Undang-undang ini memberi wewenang kepada penyelidik (BNN) Badan Narkotika Nasional untuk melakukan penyadapan yang terkait dengan penyalahgunaan dan peredaran gelap narkotika dan prekursor narkotika setelah terdapat bukti awal yang cukup.
10. *Undang-Undang Nomor 8 Tahun 2919 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.*
    Berdasarkan peraturan ini dikatakan bahwa dalam rangka mencegah dan meberantas tindak pidana pencucian uang, Pusat Pelaporan dan Analisis Transaksi (PPATK) dapat merekomendasikan kepada instansi penegak hukum yaitu penyidik TPPU, untuk melakukan intersepsi atau penyadapan atas informasi elektronik/dokumen elektronik.

11. *Undang-Undang Nomor 46 Tahun 2009 tentang Pengadilan Tindak Pidana Korupsi.*
    Berdasarkan peraturan ini, dikatakan bahwa penyadapan dapat dilakukan dan hasil dari penyadapan akan dianggap sebagai alat bukti yang sah di pengadilan apabila penyadapan yang dilakukan sesuai dengan hukum yang berlaku, dan sesuai dengan prosedur dan tata cara yang telah ditentukan oleh undang-undang.

KESIMPULAN DAN SARAN

Tindak penyadapan dapat dikatakan sebagai cara untuk mendengar atau merekam suatu informasi secara objek dengan sembunyi-sembunyi dan penyadapan itu sendiri adalah bagian dari proses, suatu tindakan atau penyadapan. Dapat di artikan sebagai aktivitas mendengar (merekam) informasi (privasi) atau percakapan yang objeknya diaktualkan tanpa melihat dampak dari orang yang menjadi objek tersebut. Tindak pidana penyadapan sendiri diatur dalam Pasal 40 UU No, 36 Tahun 199 tentang Telekomunikasi, Pasal 31 UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), dan Pasal 322 ayat 1-3 UU No 1 Tahun 2023 tentang KUHP. Pengaturan tentang penyadapan yang diperbolehkan kepada aparat penegak hukum guna mengungkap suatu tindak pidana tertentu diatur dalam beberapa peraturan seperti, Bab XXVII KUHP Belanda tentang Kejahatan Jabatan, Pasal 430-434, Undang-Undang Republik Indonesia Nomor 5 Tahun 1997 tentang Psikotropika, Undang-Undang Nomor 31 tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi, Undang-Undang No 36 Tahun 1999 Tentang Telekomunikasi, Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang Nomor 18 Tahun 2003 Mengenai Advokat, Udang-Undang No 21 Tahun 2003 Tentang Pemberantasan Tindak Pidana Perdagangan Orang, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 35 tahun 2009 tentang Tindak Pidana Narkotika, Undang-Undang Nomor 8 Tahun 2919 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-Undang Nomor 46 Tahun 2009 tentang Pengadilan Tindak Pidana Korupsi.

SARAN

Perlu adanya formulasi kebijakan khusus yang mengatur lebih komprehensif mengenai konsep penyadapan, batasan-batasan tindak penyadapan, dan kriteria apa saja yang menjadi dasar penyadapan itu berakibat pidana. Mengingat pengaturan di berbagai undang-undang terkait tindak pidana penyadapan masih terdapat ketidaksesuaian (inkonsistensi) dalam pengkualifikasian suatu bentuk tindak pidana. Oleh karena itu perlu adanya perubahan atau penerbitan perundang-undangan oleh Presiden bersama DPR RI yang spesifik atau khusus terkait dengan ruang lingkup (nomenklatur) tindak pidana penyadapan sehingga tidak terjadi tumpang tindih pengaturan (dualisme norma) di dalam pelaksanaannya.

REFRENSI

Abdul Wahid Dan Mohammad Labil, 2005, *Kejahatan Mayantara (cyber Crime)*, Cet 1, Rafika Aditama, Malang.

Amiruddin, H Zainal Asikin, 2020, "*Pengantar Metode Penelitian Hukum*", (Depok: PT Raja Grapindo Persada).

Didik Endro P., Bahan Ajar *Hukum Telematika* . Universitas Airlangga, Genap 2008/2009

Go Lisnawati, "*Mengurai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Dimensi Pembangunan Cyber Law*", Jurnal Mika, Vol. 12 Nomor 1 Juli 2009

R. Soesilo. *Kitab Undang-undang Hukum Pidana (KUHP) serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*, 1994, (Bogor: Politea,), hal. 290-293, Pasal 430-434.

Shelly Nicko, Tindak Pidana *Cyber Espionage,* Jurnal Hukum, 2010 (Surabaya, ADLN-Perpustakaan, Universitas Airlangga).

Sudarto, *Hukum Pidana dan Perkembangan Masyarakat*, 1993, Kajian terhadap Pembaharuan Hukum Pidana, Sklar Baru, Bandung.

Sutarman, *Cyber Crime, Modus Operandi dan Penanggulangannya*, 2007, LaksBang PRESSindo, Jogjakarta.

Indonesia, *Undang-Undang Republik Indonesia Nomor 5 Tahun 1997 tentang Psikotropika.*

Indonesia, *Undang-Undang Nomor 31 tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi.*

Indonesia, *Undang-Undang No 36 Tahun 1999 Tentang Telekomunikasi*.

Indonesia, *Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme.*

Indonesia, *Undang-Undang Nomor 18 Tahun 2003 Mengenai Advokat.*

Indonesia, *Udang-Undang No 21 Tahun 2003 Tentang Pemberantasan Tindak Pidana Perdagangan Orang*.

Indonesia, *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.*

Indonesia, *Undang-Undang Nomor 35 tahun 2009 tentang Tindak Pidana Narkotika.*

Indonesia, *Undang-Undang Nomor 8 Tahun 2919 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.*

Indonesia, *Undang-Undang Nomor 46 Tahun 2009 tentang Pengadilan Tindak Pidana Korupsi.*

Indonesia, *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undnag-Undang Hukum Pidana.*