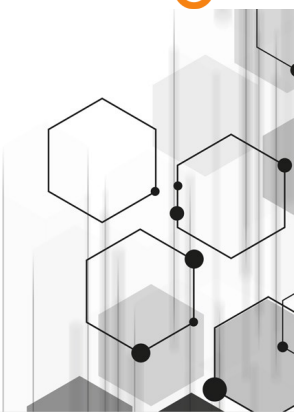
Jurnal Analogi Hukum
Volume 7, Issue 1, 2025, Page 13-22
https://doi.org/10.22225/jah.7.1.2025.13-22

OPEN ACCESS

ISSN ONLINE: 2716-2680 ISSN PRINT: 2716-2672

Jurnal Analogi Hukum

Fakultas Hukum, Universitas Warmadewa
Jl. Terompong 24 Tanjung Bungkak Denpasar Bali, Indonesia
https://www.ejournal.warmadewa.ac.id/index.php/analogihukum/index



Implikasi Penggunaan Alat Sadap *"Zero-Click"* dalam Penanganan Kasus *Cyber Crime*

Dewa Gede Ary Krisna[1] | Ida Ayu Putu Widiati[1] | Ni Made Sukaryati Karma[1]

1. Fakultas Hukum, Universitas Warmadewa

Correspondence address to:
Dewa Gede Ary Krisna, Fakultas Hukum, Universitas Warmadewa
Email address:
arykrisna2001@gmail.com

Abstract—*In Indonesia, technological progress is very rapid, but some people take advantage of this by committing criminal acts. This will have an impact on the protection of personal data. CyberCyber security in the form of wiretapping has a very important role. The formulation of the problem raised is 1) how is the regulation of the use of "zero-clickzero-click" tapping tools in cybercyber crimecrime cases, and 2) how are the implications of the use of "zero-clickzero-click" tapping tools in handling cybercyber crimecrime cases on personal data security? The research conducted is normative juridical, which is a deductive research that begins with analyzing the articles in the governing legislation. The results of the research show that the act of wiretapping is regulated in Article 5 Paragraph (2) and Article 31 Paragraph (3) of the Electronic Information and Transaction Law, there is an expansion of evidence where legally, wiretapping is a legal action. The act of wiretapping is contrary to human rights in the protection of personal data, so the government guarantees data confidentiality for victims which has been regulated in Article 17 of the Minister of Communication and Information Technology Regulation Number: 11/PER/M.KOMINFO/02/2006 relating to Technical Tapping.*

Keywords: *Cybercyber Crimecrime; eavesdropping device; personal data*

1. Pendahuluan

Berdasarkan pada Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Negara Indonesia adalah sebuah negara dengan menjunjung tinggi supremasi hukum. Prinsip-prinsip Pancasila serta ideologi pedoman negara, menjadi landasan sistem hukum di Indonesia. Karena Pancasila adalah dasar negara, maka segala peraturan hukum yang berlaku harus mempunyai landasan hukum di dalamnya. Artinya Pancasila adalah hukum yang berlaku, yang menjadi pedoman bagi negara (Sanusi,M, 2007 : 4). Indonesia adalah negara yang didirikan atas dasar supremasi hukum. Hukum adalah seperangkat peraturan yang dibuat dan diputuskan oleh badan pengatur masyarakat, yang dapat diterapkan pada masyarakat tersebut di lokasi tertentu.

Hukum adalah norma-norma sosial yang memiliki kekuatan untuk memaksa orang untuk mengikuti dan mentaati serta memberikan hukuman (*punishment*) kepada mereka yang memilih untuk tidak mentaati norma-norma tersebut (Wantu, 2015 ; 4). Teknologi yang berkaitan dengan telekomunikasi, media, dan informatika disebut juga dengan istilah telematika, saat ini mengalami kemajuan dengan sangatlah cepat di negara Indonesia. Dalam hal tersebut dibuktikan adanya perluasan infrastruktur informasi global yang telah mengubah pola dan praktik operasional bisnis, termasuk yang dilakukan di pemerintahan, industri, dan perdagangan. Seiring kemajuan umat manusia, ketersediaan alat untuk melakukan tugas sehari-hari seperti penggunaan media elektronik untuk berkomunikasi telah membuat hidup lebih mudah (Jusmadi, 2013 ; 48). Seiring perkembangan zaman hak-hak masyarakat haruslah tetap terpenuhi, dimana hak masyarakat khususnya dalam bidang teknologi termasuk didalam Pasal 28 C aAyat (1) Undang-Undang Dasar Negara Republik Indonesia pada tahun 1945. Jika ditelusuri lebih dalam kedudukan hukum di bidang telematika, maka terlihat jelas bahwa hal tersebut berdampak pada pergeseran masyarakat. Hukum harus digunakan sebagai kerangka kerja untuk mendorong inisiatif perubahan sosial ketika inisiatif tersebut muncul sebagai akibat dari kemajuan di bidang telematika. Oleh karena itu, undang-undang yang diharapkan akan tercipta, apapun bentuknya, harus bersifat mengikat secara hukum bagi pihak-pihak yang terlibat dan tentunya mempunyai sistem hukuman sebagai alat pemaksanya. (Maskun, 2013 ; 10).

Diperlukannya pembuatan aturan atau standar di bidang telematika karena belum banyaknya peraturan dalam hukum yang dapat mengatur. Definisi tentang teknologi disebutkan dalam peraturan perundang-undangan mengenai teknologi informasi yaitu pada pasal 1 Angka (3) Undang-Undang Nomor 19 Tahun 2016 mengenai perubahan terhadap Undang-Undang Nomor 11 pada tahun 2008 mengenai informasi serta transaksi elektronik. Oleh karena itu, masyarakat meyakini bahwa perkembangan teknologi informasi, khususnya media online*online*, memberikan banyak manfaat, antara lain keamanan, kenyamanan, kecepatan, dan akses terhadap informasi terkini. Kemudahan pengumpulan informasi berkat teknologi tentu saja berdampak signifikan terhadap keamanan informasi pribadi pengguna. Faktanya, ini adalah salah satu peristiwa kebocoran data terbesar dalam sejarah Indonesia. Hal ini terungkap setelah publikasi laporan ahli siber asal Singapura, *Dark Tracer*, tentang pelanggaran data sebanyak 49 ribu situs. *Dark Tracer* juga menyebutkan ada tiga situs web pemerintahan negara Indonesia yang masuk didalam 10 situs paling atas yang banyak mengalami kebocoran data, sebagai contohnya dengan situs dari Ditjen Pajak (*djponlineonline.pajak.go.id*). Dalam hal ini, setiap orang mempunyai kebutuhan mendasar akan perlindungan hukum atas data pribadinya, maka negara sebagai lembaga penentu kebijakan harus menjunjung tinggi hak-hak tersebut. Dimana perlindungan data pribadi yang sudah terdapat di pasal 1 angka (2) Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi. Perkembangan teknologi modern terkadang dapat dimanfaatkan oleh masyarakat untuk tujuan baik dan buruk, seperti memberikan peluang bagi pelaku kejahatan di dalam melaksanakan kejahatan yang ada di dunia maya ataupun media lain yang sering disebut kejahatan siber (*cybercyber crimecrime*) dengan memanfaatkan aktivitas negatif seperti perkembangan tersebut. Kejahatan dunia maya dikenal sebagai kejahatan melalui internet, adalah tindakan apa pun yang tujuannya adalah melakukan kejahatan dengan menggunakan komputer menjadi media yang akan didukung sistem telekomunikasi , seperti sistem nirkabel yang menggunakan antena nirkabel tertentu atau sistem

dial-up. yang menggunakan saluran telepon (Judhariksawan, 2005 ; 12). Dengan demikian, delik formil dan delik materil dapat dilakukan dalam kejahatan komputer. Mengakses komputer orang lain tanpa izin disebut sebagai delik formal, sedangkan merugikan orang lain disebut sebagai delik materiil. Melakukan tindakan penyusupan ke organisasi terkait adalah salah satu cara aparat penegak hukum mencoba menemukan dan mengikuti orang-orang yang bertanggung jawab atas kejahatan jenis baru ini, serta melacak dan menelusuri jaringan organisasi kriminal dan mendokumentasikan rencana pelaku untuk melakukan tindakan kejahatan baru ini (Arief, 2006 ; 25). Maka penyadapan adalah salah satu teknik yang digunakan untuk menemukan sumber bukti ialah satu cara yang dipakai dalam mendapati sumber bukti kejahatan dan melacaknya. Tindakan penyadapan adalah bagian dari usaha alternatif yang boleh dilaksanakan dengan dasar peraturan perundang-undangan, yaitu pada Pasal 18 ayat (3) Undang-Undang Nomor 14 tahun 2008 mengenai Keterbukaan Informasi Publik. Oleh sebab itu, permohonan izin harus diajukan kepada Presiden untuk mengungkapkan informasi yang dibedakan dengan sebagaimana termasuk di dalam ayat (3).

Di Indonesia, sejumlah aparat penegak hukum disinyalir mendatangkan alat penyadap bermetodekan *zero-clickzero-click*. *Zero-clickZero-click* adalah metode penyadapan yang tidak memerlukan Upaya "*click*" dari pengguna perangkat, seperti keyboard komputer. Indonesia Corruption Watch (ICW) memaparkan latar belakang sistem penyadapan "*Zero-ClickZero-click*" (Pegasus) buatan Israel yang akan dimanfaatkan oleh lembaga intelijen dan aparat penegak hukum. ICW mengkhawatirkan alat penyadap pegasus "*Zero Click*" dibawa ke Indonesia akan digunakan di luar sistem hukum, atau dengan kata lain tidak untuk tujuan hukum. Alat penyadap pegasus "*zero-clickzero-click*" juga diperkenalkan Polda Metro Jaya pada tahun 2017 dan 2018. Kesimpulan ini didapat ICW berdasarkan penelusuran yang dilakukan di website serta kesimpulan Konsorsium Indonesia Leaks pada Juli 2023. Ditemukannya kesempatan untuk mendapatkan alat penyadap ini akan membahayakan kelangsungan demokrasi di Indonesia. Pegasus merupakan alat penyadap "*zero-clickzero-click*", artinya alat ini dapat digunakan untuk menguping hanya dengan mengklik dokumen atau tautan tertentu. Menurut penjelasan latar belakang tersebut bisa dilakukan perumusan dua masalah yakni bagaimanakah pengaturan penggunaan alat sadap "*zero-clickzero-click*" dalam kasus *cybercyber crimecrime?* dan bagaimanakah implikasi dari penggunaan alat sadap "*zero-clickzero-click*" dalam penanganan kasus *cybercyber crimecrime* terhadap keamanan data pribadi ?

2. Metode

Pada penelitian yang dilaksanakan ini bersifat hukum normatif, artinya diawali dengan pemeriksaan deduktif terhadap bagian-bagian undang-undang yang membahas masalah tersebut. Penelitian dalam hukum yang berupaya memperoleh informasi normatif mengenai hubungan antara peraturan dan penerapannya dalam praktik maka disebut penelitian dalam hukum yang bersifat normatif. Pada penelitian yang dilaksanakan ini memakai data sekunder atau sumber kepustakaan dikenal dengan penelitian hukum normatif.

3. Hasil Penelitian Dan Pembahasan

Pengaturan Penggunaan Alat Sadap "Zero-ClickZero-click" Dalam Kasus CyberCyber CrimeCrime

Penegakan hukum yang ada saat ini telah berkembang sebagai akibat dari kemajuan teknologi. Aparat penegak hukum harus mempunyai cara alternatif yang lebih efisien dalam menjalankan tugasnya guna mencegah tindakan kejahatan. Salah satu contoh yaitu penggunaan alat penyadapan oleh penegak hukum di Indonesia. Dimana tindakan mendengarkan, merekam, mengubah, mencegah, dan/atau merekam perpindahan data elektronik pribadi melalui jaringan kabel komunikasi atau jaringan nirkabel dikenal dengan istilah penyadapan. Alat sadap adalah alat yang digunakan untuk merekam, mendengarkan, mengubah, mengalihkan, menghentikan, dan mencatat informasi serta dokumen elektronik yang tidak ditujukkan untuk dikonsumsi. Alat sadap

merujuk pada alat yang digunakan untuk merekam, mendengar, membelokkan , memblokir, mengubah ataupun merekam transmisi data elektronik serta dokumen yang tidak mempunyai sifat *public* baik melalui jaringan kabel telekomunikasi ataupun jaringan dengan nirkabel, seperti frekuensi radio ataupun radiasi elektromagnetik yang dikenal dengan alat sadap. Alat penyadapan "*zero-clickzero-click*" adalah sebuah teknik penyadapan yang bekerja tanpa pengguna atau perangkat komputer perlu mengklik untuk mengaktifkan alat tersebut. Alat penyadapan "zero-click*zero-click*" adalah perangkat elektronik yang digunakan untuk secara ilegal dan melanggar hak pribadi orang lain, menyadap dokumen atau informasi elektronik dari komputer atau sistem elektronik lainnya. Perangkat ini memanfaatkan kelemahan dalam layanan pesan singkat (SMS) yang memungkinkan terjadinya intruksi hanya dengan menerima pesan tanpa memerlukan interaksi atau meminta persetujuan pengguna, mekanisme penyadapan "zero-click*zero-click*" sangat membahayakan. Dengan tujuan yakni agar mendapatkan kendali secara penuh terhadap sistem operasi yang ada di perangkat seluler, yakni baik secara *jailbreakjaikbreak* (untuk perangkat *Apple iOS*) ataupun *rootingrooting* (untuk perangkat Android). Keamanan bawaan sistem operasi Android atau iOS dihilangkan dengan rooting*rooting* dan jailbreak*jaikbreak*. Biasanya, kedua pendekatan tersebut memerlukan perubahan konfigurasi sistem dan "meretas" komponen penting untuk memungkinkan eksekusi kode yang disesuaikan.

Cara kerja "*zero-clickzero-click*" biasanya sangat terfokus dan menggunakan teknik-teknik canggih, hal ini dapat menimbulkan akibat yang sangat negatif, yaitu target tidak menyadari bahwa ada masalah dengan peralatan jaringan elektronik mereka. Strategi umum yang digunakan oleh mereka yang melakukan penyadapan adalah mencoba membujuk korban yang dituju untuk mengklik link atau file yang telah disusupi dengan memasang file penyadapan di komputer, tablet, atau ponsel mereka. Namun demikian, dengan menggunakan teknik penyadapan "*zero-clickzero-click*", perangkat penyadap dapat dipasang pada perangkat tersebut tanpa korban harus *mengclick* tautan apa pun. *Black's Law Dictionary* mengemukakan mengenai alat sadap yaitu *Wiretapping is a covert electronic method of listening in on phone conversations*. Hal ini menunjukkan kegiatan penyadapan adalah praktik mendengarkan percakapan telepon orang lain untuk menguping pembicaraan seseorang secara elektronik ketika aparat penegak hukum telah mengambil upaya dengan izin atau perintah dari pengadilan setempat (Garner, 2005 ; 11). Berikutnya definisi alat sadap oleh ETSI (*European Telecommunication Standard Institute*) mengemukakan mengenai alat sadap yaitu (*lawful interception*) adalah tindakan penyadapan yang dilakukan oleh operator jaringan, penyedia akses, atau penyedia layanan untuk memastikan bahwa data selalu tersedia untuk dipakai penegak hukum pada sebuah kasus. (Gunawan, 2018 ; 184-185). Dasar hukum dalam tindakan penyadapan yang dilaksanakan aparat penegak hukum terdapat pada Pasal 31 aAyat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik. Dimana dalam penjelasan Pasal 31 aAyat (3) dapat diartikan bahwasannya penyadapan diperbolehkan jika maksud di balik penggunaan alat penyadap tersebut adalah untuk menegakkan hukum di Indonesia. Dalam kasus ini, tindakan dapat diambil atas permintaan resmi dari polisi, kantor kejaksaan, atau aparat penegak hukum. Menurut penjelasan undang-undang yang dapat mengatur tentang tindakan sebuah penyadapan dalam tindak pembuktian.

Izin untuk menggunakan perangkat penyadapan "*zero-clickzero-click*" dianggap sebagai upaya untuk menjaga dan mencapai tujuan yang jauh lebih besar tanpa mengorbankan hak-hak mereka yang diduga melakukan kejahatan yang berdampak pada wilayah yang luas dan terkoordinasi. Hal ini perlu dibentuk dan didasarkan pada HAM. Dikarenakan kebebasan dalam berkomunikasi serta memperoleh informasi dijelaskan dalam Pasal 28F serta Pasal 28G aAyat (1) UUDNRI 1945. Maka oleh sebab itu, Tindakan penyadapan dapat digunakan untuk menemukan aktivitas kriminal berdasarkan aturan hukum tertentu. (*lex specialis derogat legi generali*). Tindakan penyadapan adalah perbuatan dapat diterima di mata hukum untuk diajukan sebagai bukti di pengadilan. Hal tersebut tertuang pada Pasal 5 aAyat (2) Undang-Undang Nomor 19 Tahun 2016 mengenai Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi serta Transaksi Informasi Elektronik. Dimana pada penjelasan Pasal 5 aAyat (2) memuat mengenai peningkatan dari sebuah alat bukti dengan merujuk pada tindakan kasus penyadapan dari penyidik saat penanganan kasus tindakan pidana *cybercyber crimecrime*, dimana alat bukti dengan maksud seperti informasi secara

elektronik ataupun dokumen elektronik ataupun hasil dari cetakannya dimana hal ini menjadi alat bukti hukum yang sah. Tindakan penyadapan hanya diperbolehkan jika dilakukan sesuai dengan undang-undang hukum terkait dan dibatasi untuk digunakan oleh aparat penegak hukum. Dimana alat penyadap itu sendiri terbagi menjadi *interface, monitoring centre*, serta *link transmission*. (Hiariej, 2012 ; 79). *Interface* disiapkan oleh penyelenggara ahli teknologi, selanjutnya *monitoring centre* ataupun *link transmission* dipersiapkan aparat penegak hukum dengan mana tindakan ini dibawah pengawasan POLRI selaku aparat penegak hukum. Selanjutnya dalam mencari atau memecahkan sebuah petunjuk dalam penanganan kasus tindak pidana *cybercyber crimecrime* dengan menggunakan alat sadap dimana definisi serta dasar hukumnya terdapat pada Pasal 188 aAyat (1) Undang-Undang Nomor 8 Tahun 1981 mengenai Hukum Acara Pidana. Dengan ini, pada Pasal 5 ayat (2) UU ITE menunjukkan bahwasannya alat bukti petunjuk, seperti informasi lisan, disampaikan, dan diamankan secara elektronik, menggunakan perangkat elektronik atau perangkat yang sama, dan informasi, seperti data atau informasi apa pun yang direkam yang bisa untuk dilihat, didengar, dibaca ataupun dapat digunakan untuk mengumpulkan alat bukti petunjuk. yang dapat menggunakan suatu sarana, baik seperti suara, peta, tulisan, gambar, huruf, foto, angka ataupun perforasi dengan tertulis diatas benda yang fisik apapun kecuali kertas ataupun dicatat dengan elektronik.

Dalam Pasal 284 ayat (2) Undang-Undang Nomor 8 Tahun 1981 mengenai Hukum Acara Pidana mengkaji pengecualian terhadap persyaratan KUHAP dengan berhubungan pada penuntutan pidana melalui tindak pidana tertentu yang dimana memuat peraturan khusus. Dengan demikian Undang-Undang ini memungkinkan hukum dalam pidana tertentu, seperti berhubungan antara perbuatan hukum dimana mencakup penyadapan dalam penyelidikan, dapat dikecualikan terhadap aturan yang ditetapkan dalam hukum pada acara pidana. Memberi wewenang ekstra atau khusus untuk penyidik dalam melaksanakan tugas penyidikannya.

Penyadapan hanya boleh dilakukan ketika adanya indikasi ancaman yang ditujukan kepada negara. Hal ini dinyatakan pada Pasal 42 aAyat (2) Undang-Undang Nomor 36 Tahun 1999 mengenai Telekomunikasi. Maka penjelasan Pasal 42 aAyat (2) dapat diartikan bahwa pencatatan informasi dapat dikabulkan apabila permintaan penyidik memenuhi syarat berupa. Pertama, keterangan yang diperoleh atas dengan suatu proses di peradilan tindak pidana dengan mencakup proses penyidikan, lalu penuntutan serta persidangan serta ancaman hukuman mati atau lima tahun penjara. Kedua, informasi tersebut antara lain harus berupa rekaman percakapan antara pihak-pihak yang berkomunikasi melalui telepon. Sebagai perpanjangan dari pembuktian selama persidangan, penyadapan dikendalikan secara independen berdasarkan undang-undang yang tersebar di dalam peraturan perundang-undangan dan tidak tercakup dalam KUHP saat ini. Peraturan penyadapan memberikan kewenangan kepada aparat penegak hukum untuk menyelidiki jenis aktivitas ilegal tertentu, termasuk penyalahgunaan narkoba, terorisme, perdagangan manusia, dan korupsi. Banyak undang-undang, termasuk UU mengenai informasi serta transaksi elektronik serta tindakan pidana tertentu, yang memiliki peraturan mengenai penyadapan di negara Indonesia. Demikian adanya perluasan alat bukti dengan telah disebutkan di Pasal 5 aAyat (2) Undang-Undang Nomor 19 Tahun 2016 mengenai Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi serta Transaksi Informasi Elektronik bisa menjadi dasar hukum yang dipegang oleh aparat penegak hukum untuk berlangsungnya tindak penyadapan untuk penanganan kasus *cybercyber crimecrime* maka oleh sebab itu, di Negara Indonesia dalam pengaturan tentang tindak penyadapan ada di sebagian undang-undang.

Tugas aparat penegak hukum dalam penyadapan hanya sebatas menyelidiki keabsahan perintah penugasan dari putusan pengadilan, sehingga walaupun mempunyai kewenangan untuk melakukan penyadapan, namun tidak diperbolehkan melakukan tindakan sewenang-wenang selama proses yang tidak diperbolehkan melalui ketentuan yang berlaku. Hal ini dijelaskan pada dijelaskan pada Pasal 14 dan Pasal 15 Peraturan Menteri komunikasi dan informatika dengan nomor No. 11/PER/M.KOMINFO/020/2006 berkaitan Teknis Penyadapan. Penggunaan informasi dan dokumen bentuk elektronik menjadi alat bukti untuk di dalam pengadilan mempunyai landasan hukum yang jelas dan berkembang dalam pembuktian penyadapan melalui penggunaan alat perekam dan pencatatan hasil setelah Undang-Undang Nomor 19 tahun 2016

mengenai Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Dengan dinilai dapat lebih memberi kepastian dalam hukum serta cangkupan berlakunya yang lebih luas lagi. Pemakaian alat perekam serta pencatatan hasil dalam praktek hukum yang dimana menjadi bagian dari sebuah proses yakni *pro justitia* dalam perkara suatu pidana. *Implikasi dari penggunaan alat sadap "zero-clickzero-click" dalam penanganan kasus cybercyber crimecrime terhadap keamanan data pribadi.* Banyak pakar hukum yakni baik praktis maupun akademis, percaya bahwasannya penyadapan melanggar hak asasi manusia, sehingga penggunaan alat penyadapan zero click untuk menemukan dan mengadili pelaku kejahatan menjadi persoalan serius. Dimana ketentuan HAM yang telah termasuk pada Pasal 28F serta Pasal 28G. dalam UUDNRI memberikan penanganan terhadap hak pribadi dijelaskan pada pasal 17 Undang-Undang Nomor 12 Tahun 2005 mengenai Pengesahan *International Covenant on Civil and Political Rights* (Kovenan Internasional mengenai Hak-Hak Sipil serta Politik). Penyadapan sangat bertentangan dengan Pasal 65 aAyat (1) Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi dimana merupakan pelanggaran hukum jika siapapun mengakses atau mengumpulkan informasi pribadi tentang orang lain tanpa izin demi keuntungan diri sendiri ataupun orang lainnya, karena hal ini bisa membahayakan subjek informasi pribadinya. Perlindungan data pribadi mungkin akan terkena dampak dari penyadapan, khususnya terkait keamanan dan kerahasiaan informasi. Tentu saja, menyadap komunikasi termasuk menggunakan informasi pribadi orang lain, yang melanggar aturan privasi dan perlindungan data mengingat betapa pentingnya hal tersebut di era teknologi saat ini. tindakan untuk melindungi subjek hukum dari keputusan sewenang-wenang dan aktivitas melanggar hukum adalah perlindungan hukum, seperti penyadapan, pencurian, dan *cybercyber crimecrime*. Salah satu jenis perlindungan hak asasi manusia yang sangat penting dalam membela hak-hak masyarakat adalah perlindungan hukum, dan perlindungan hukum ditujukan kepada seluruh elemen masyarakat untuk memberikan kebebasan terhadap segala hak yang diatur dalam peraturan yang ada.

Berdasarkan Pendapat dari Philipus M. Hadjon, terdapat dua jenis perlindungan dalam hukum yakni sebagai berikut: pertama, perlindungan hukum dengan preventif, dengan memberi waktu kepada penegak hukum untuk mengumpulkan bukti sebelum akhirnya pemerintah memutuskan bentuk yang pasti. Bertujuan untuk menunda terjadi sebuah tindakan seperti pertikaian. Jenis perlindungan hukum yang kedua adalah perlindungan hukum dengan represif, yaitu jenis dari perlindungan dalam hukum dengan lebih memfokuskan kepada penyelesaian (Budiartha, 2016 ; 138). Pada konsep dari perlindungan hukum untuk korban terdapat asa yang dipakai menjadi sebuah dasar berpikir dalam perlindungan hukum untuk korban tindak kejahatan yakni Asas Manfaat yang dimana selain membantu korban kejahatan merasa lebih aman, perlindungan untuk korban tindak kejahatan pun bermanfaat juga untuk masyarakat umum, terkhusus pada hal inisiatif untuk menurunkan tingkat kejahatan dan membangun ketertiban umum.

Asas keadilan yakni tidak tergantung pada pangkat atau golongan dalam memberikan perlindungan hukum yang adil terhadap korban tindak sebuah pidana yang tepat pada peraturan undang-undang yang berlaku. Asas keseimbangan adalah keseimbangan antara hukuman yang dijatuhkan kepada pelaku dan perbuatan pelaku harus dicapai ketika memberikan perlindungan hukum bagi korban. Dan asas kepastian yaitu kepastian hukum sangat penting dalam penerapan undang-undang bagi perlindungan korban karena undang-undang tersebut menetapkan batasan tentang bagaimana yang bisa dilaksanakan oleh pribadi serta memberikan hukuman bagi mereka yang melanggarnya, sehingga membuat penyerang enggan untuk melakukan penyerangan dan melindungi korban dalam prosesnya. (Kardiyasa, 2020 ; 80)

Alat penyadapan "*zero-clickzero-click*" adalah program yang digunakan dalam kasus kejahatan dunia maya yang berupaya mengumpulkan semua data pada sistem target kejahatan dunia maya. Metode penyadapan "*zero-clickzero-click*" biasanya hanya menghasilkan satu panggilan tidak terjawab di perangkat. dimana alat penyadapan "*zero-clickzero-click*" dapat menyelesaikan operasi penyadapan hanya dengan satu panggilan tidak terjawab. di mana peretas sama sekali tidak menyadari bahwa program spionase "*zero-clickzero-click*" telah menguasai alat komunikasi korban. Tidak ada persyaratan untuk masukan ke perangkat pengguna karena alat penyadap ini beroperasi

berdasarkan teori kerentanan "*zero-clickzero-click*". Di Indonesia penyadapan merupakan proses penggunaan alat sadap untuk aparat penegak hukum dalam menangani kasus tindakan pidana *cybercyber crimecrime*. Penyadapan mempunyai banyak sebuah istilah, terdapat sebutan seperti *wiretapping* serta adapun yang menyebutnya *lawful interception*. Pada Tindak penyadapan dapat dilaksanakan dengan mengarah kepada dua buah standar internasional yakni: *European Telecommunications Standards Institute* (ETSI) serta *Communications Assistance for Law Enforcement Act*. Menurut ETSI, penyadapan adalah praktik penyadapan sah yang digunakan oleh operator jaringan, penyedia akses, dan penyedia layanan (NWP/AP/SvP) untuk memastikan bahwa data selalu tersedia untuk digunakan oleh fasilitas kontrol penegakan hukum. Tidak ada peraturan yang khusus yang dapat melarang penyadapan telepon di negara Indonesia, sebab bukanlah termasuk anggota dari *European Telecommunication Standard*, Secara dasar, negara Indonesia hanyalah melaksanakan pengamatan serta pengkajian terkait dengan standar serta sistematika dalam penyadapan yang ETSI keluarkan , menjadi bahan pembelajaran dalam pembentukan peraturan mengenai tindak penyadapan. Kegiatan penyadapan secara garis besar dapat dikategorikan menjadi empat bentuk utama, yaitu sebagai berikut: penyadapan pasif atau (*Passive Interception*) khususnya kegiatan penyadapan yang dilaksanakan dengan tersembunyi yakni membaca sebuah data ataupun tanpa izin, lalu penyadapan aktif atau (*Active Interception*) yaitu tindak penyadapan secara langsung dikombinasikan menggunakan modifikasi data dari pelanggaran hukum, Selanjutnya penyadapan semi aktif yaitu tindakan penyadapan di mana orang yang melakukannya mempunyai akses atau mencatat informasi yang diberikan atau diterima oleh pihak lain meskipun mereka tidak berpartisipasi aktif dalam proses komunikasi yang disadap, dan penyadapan gabungan diantara penyadapan secara aktif serta penyadapan secara pasif. Dalam tindak penyadapan ini melibatkan penggunaan berbagai teknik penyadapan, seperti penyadapan pasif, di mana informasi diamati tanpa intervensi langsung, dan penyadapan aktif, di mana penyadap berpartisipasi aktif dalam proses komunikasi. (Gunawan, 2013 ; 208-209).

Indonesia sendiri, Tindakan penyadapan telah diatur dalam Peraturan Menteri Komunikasi dan Informasi dengan Nomor 11/PERM.KOMINFO/02/2006 mengenai Teknis Penyadapan Terhadap Informasi. Selanjutnya Tindakan penyadapan dari aparat penegak hukum perlu berlandaskan asas kepastian hukum itu sendiri hal ini dimuat pada Pasal 2 Peraturan Menteri Komunikasi dan Informasi dengan Nomor: 11/PER/M.KOMINFO/02/2006 mengenai Teknis Penyadapan. Selain itu, perlu digaris bawahi bahwa penyadapan hanya bisa dilaksanakan penegak hukum dengan menggunakan teknik ataupun peralatan penyadapan sebuah informasi tertentu, serta hanya diperbolehkan jika dilakukan tepat pada peraturan undang-undang yang ada. Selanjutnya penegak hukum harus memasang dan mengoperasikan instrumen dan/atau alat penyadap tersebut pada perangkat perangkap di stasiun pemantauan pusat. Tatacara penyadapan kemudian diatur melalui Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 5 Tahun 2010 mengenai Tata Cara Penyadapan Pada Pusat Pemantauan Kepolisian Negara Republik Indonesia termuat dalam 4 buah bagian utama yaitu. Penyidik harus mengajukan permohonan tertulis untuk melakukan operasi penyadapan yang termasuk nomor laporan polisi, sinopsis dugaan tindakan pidana dan pasalnya, penjelasan maksud dan tujuan operasi, serta alasan dilakukannya operasi dalam penyadapan dengan memuat informasi yang diperlukan. Kemudian nomor telepon atau nama peralatan komunikasi tambahan kemudian diserahkan dan selanjutnya diikuti dengan sinopsis singkat identitas target dalam operasi penyadapan telepon. Dalam jangka waktu pelaksanaan penyadapan akan sesuai dengan peraturan yang ditentukan dalam undang-undang. Surat pernyataan perlu ditandatangani penyidik yang menyatakan bahwasannya yang menjadi tindakan penyadapan akan menjadi sasaran penyadapan adalah orang yang patut sekiranya membuat ataupun sedang melakukan, atau ikut serta dalam tindakan pidana, harus diajukan bersama permohonan penyadapan. *Provisioning* merupakan langkah awal dalam operasi penyadapan antara Mabes polri yang menyediakan jasa komunikasi yang merupakan pemilik nomor telepon ataupun pengenal lain dari perangkat telekomunikasi yang dituju. Kegiatan penyadapan yang dilaksanakan dengan mempertimbangkan penting serta mendesak harus dilakukan pelaporan pada Badan *Reserse* Kriminal Kepolisian dalam waktu selambat-lambatnya 1x24 jam ketika mendapat izin instansi tersebut untuk memastikan apakah operasinya dapat dilanjutkan atau tidak.

Polri menginformasikan kepada Ketua Tim Pengawasan tentang tujuan operasi penyadapan

di bagian Pelaksanaan Pengawasan Balai Pengawasan Kalakhar. Sasaran yang telah disadap kemudian dibagikan kepada anggota pemantau oleh tim pemantau. Kemudian anggota tim pemantau wajib mendengarkan, membaca serta mendokumentasikan dari setiap aspek percakapan yang target operasi penyadapan laksanakan. Jika mereka menemukan informasi yang relevan, mereka harus segera melaporkan kepada tim pemantau. Tim pemantau memberitahukan kepada penyidik yang mengajukan permintaan pokok-pokok informasi yang dicari. Pada Kalakhar Pusat dari pemantauan polri hanyalah memberi produk hasil dari penyadapan untuk penyidik dengan identitas yang termasuk didalam surat permohonan penyadapan yang berhak menerima produk penyadapan dari Mabes Polri. Selain itu, penyidik tidak diperbolehkan meminta akses terhadap seluruh rekaman temuan operasi penyadapan, kecuali semua rekaman pertukaran pesan singkat yang berkaitan dengan aktivitas ilegal. Jika porsi percakapan ataupun pesan secara singkat yang nantinya dipakai menjadi alat bukti dinilai tidak adanya kaitan pada perilaku ilegal yang ditonton, maka Pusat Pengawasan Kalakhar kemudian diberi wewenang untuk menolak memenuhi permintaan penyidik. Bareskrim Polri berhak mengambil keputusan akhir atas segala perselisihan yang mungkin timbul antara penyidik dan Mabes Polri Kalakhar terkait permintaan rekaman operasi penyadapan. Badan *Reserse* Kriminal Polri sebagai pengawas mengawasi seluruh kegiatan operasional, kecuali yang berkaitan dengan penyadapan barang, guna menjamin tanggung jawab dan transparansi dalam pelaksanaan operasi penyadapan. Kalakhar Pusat Pemantauan Polri menyerahkan temuan peretasan oleh penyidik yang ditunjuk dalam surat permohonan izin penyadapan dapat menjadi satu-satunya penerima rekaman suara, SMS, transkrip percakapan serta peta jaringan telekomunikasi berisi informasi yang diminta. Sesuai peraturan hukum, hasil penyadapan tersebut bersifat pribadi dan dapat dijadikan alat bukti. Penyidik yang telah memperoleh seluruh rekaman dialog yang berkaitan perbuatan kejahatan cyber*cyber*, tidak diperkenankan mendapatkan produk penyadapan dan mencari seluruh rekaman hasil kegiatan penyadapan. Sebaliknya, hasil peretasan yang tidak ada hubungannya oleh tujuan pembuktian wajib dihilangkan. Untuk mencegah penyalahgunaan wewenang yang berujung pada pelanggaran hak asasi manusia, maka proses dan teknik peretasan oleh aparat penegak hukum yang berwenang perlu tepat pada ketetapan dalam hukum yang ada.

Penyidik kepolisian yang memeriksa suatu tindak pidana wajib tetap dalam kewenangannya, memperhatikan fakta-fakta yang ada, dan mempertimbangkannya. Ada beberapa hal yang harus dipastikan serta diperhatikan pada proses penyidikan tindakan pidana yakni cyber*cyber* crime*crime* dengan dimana diuraikan sebagai berikut berupa: Asas praduga tak bersalah dalam hal ini dijunjung tinggi oleh penyidik kepolisian, memberikan kesempatan kepada agar memahami hak dan wewenang selama di dalam proses penyidikan. serta pelaku juga diberi kesempatan untuk menjaga integritas dirinya sebagai manusia tanpa harus melanggar HAM dimana hal ini harus dijunjung dan dilindungi oleh setiap orang (Trimarlina, 2019 ; 414). Maka oleh sebab itu, demi menjamin perlindungan HAM dalam konteks perlindungan data pribadi masyarakat, pemerintah menerbitkan peraturan pemerintah berkaitan tata cara dalam melakukan tindak penyadapan menggunakan alat sadap *"zero-clickzero-click"* dalam penanganan kasus *cybercyber crimecrime* yaitu Peraturan Menteri Komunikasi dan Informatika dengan Nomor : 11/PER/ M.KOMINFO/02/2006 mengenai Teknis Penyadapan Terhadap Informasi dimana dijelaskan pada Pasal 1 Angka 9 yang menjelaskan mengenai sahnya suatu penyadapan. Pemerintah juga menjamin kerahasiaan data bagi korban yang mengalami penyadapan dalam kepentingan berlangsungnya proses persidangan tindak pidana *cybercyber crimecrime* hal ini kemudian dijelaskan pada pasal 17 Peraturan Menteri Komunikasi dan Informatika dengan Nomor : 11/PER/ M.KOMINFO/02/2006 mengenai Teknis Penyadapan. Selanjutnya Putusan mentri di atas dipertegas lagi melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik yang dimana demi menjaga kerahasiaan data pribadi dalam proses penyadapan disebutkan pada Pasal 43 aAyat (2).

Demi menjaga keamanan dalam penyelenggaraan perkara pidana yang sedang berlangsung, pemerintah menjamin kerahasiaan barang bukti penyadapan. Untuk menghindari potensi penyalahgunaan kemampuan penyadapan dan pencatatan dalam proses penanganan perkara, hal ini berupaya untuk menjaga perlindungan data pribadi masyarakat yang terkandung dalam hak asasi setiap orang. Oleh karena itu, apabila penyadapan dilakukan untuk membantu untuk

terungkapnya sebuah kasus, maka dianggap tidak melanggar HAM. Bilamana temuan dari tindak penyadapan dipergunakan untuk tujuan selain penegakan hukum, maka terjadilah pelanggaran hak asasi manusia. Semua orang yang terlibat menyadari pentingnya peran penyadapan dalam membantu penyidik menemukan bukti kejahatan dunia maya. Ketika penyidik berhasil menemukan bukti kejahatan *cybercyber crimecrime*, maka aparat penegak hukum berhasil mendengarkan obrolan para pelaku kejahatan. Hal tersebut bukanlah merupakan sebuah pelanggaran dalam hak asasi manusia selama penyidik penegak hukum menggunakan penyadapan untuk tujuan yang sah dan menemukan kasus pidana.

Selain memiliki dampak negatif terkait tindakan penyadapan terhadap keamanan informasi pribadi seseorang saat menangani kasus kejahatan dunia maya dengan alat penyadapan "*zero-clickzero-click*", penggunaan alat penyadapan ini untuk kasus pidana juga memberikan dampak positif yang justru membantu penyidik dalam menyelesaikan kejahatan. baik Tindakan yang berhubungan dengan pidana umum maupun pidana khusus. Sahnya tindakan penyadapan haruslah berdasarkan hukum (*Lawful Interception*) dalam transaksi dengan elektronik, dengan menyatakan bahwasannya penyadapan dibolehkan sebagai rangka dalam penegakan hukum terhadap permintaan dari kepolisian, kejaksaan ataupun instansi penegak hukum yang lain dengan ditentukan menurut undang-undang.

Maka oleh sebab itu penyadapan memberikan dampak yang sangat signifikan terhadap perlindungan data pribadi penyadapan menggunakan alat penyadap *"zero-clickzero-click"* memberikan peluang terjadinya suatu kejahatan *cybercyber* yang berupa pelanggaran privasi, kemungkinan terjadinya penyalahgunaan data oleh aparat penegak hukum yang melakukan penyadapan serta paling berbahaya yaitu terjadinya penjualan data pribadi korban. Pemerintah telah memberikan berbagai upaya melalui peraturan perundang-undangan dimana hal ini demi mencegah terjadinya pelanggaran ham dalam proses penyadapan dalam penanganan kasus *cybercyber crimecrime* berlangsung. Saat ini peran serta pemerintah disini sangatlah penting dan berarti dengan dibuatnya peraturan pemerintah yang bertujuan untuk menghindari terjadinya kebocoran data yang telah di sadap serta menjaga kerahasiaan bagi orang yang di sadap. Karena perlindungan data pribadi merupakan hak asasi manusia setiap orang miliki yang tidak dapat diganggu oleh siapapun.

4. Simpulan

Pengaturan penggunaan alat sadap "*zero-clickzero-click*" dalam kasus *cybercyber crimecrime* dimana dilihat dari sudut definisi alat sadp merujuk pada alat bukti dan *zero click* sendiri merujuk pada sebuah konsep dalam penggunaan alat sadap. Alat bukti yang dimaksud disini merupakan alat bukti dengan elektronik serta dokumen berbentuk elektronik lainnya yang dimana di pasal 5 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik dimana terdapat peningkatan alat bukti digunakan digunakan sebagai acuan untuk penyidik saat pembuktian saat persidangan berlangsung. Serta dasar hukum proses penyidik melakukan peretasan diatur pada Pasal 31 ayat (3) Undang-undang Informasi dan Transaksi Elektronik dijelaskan penyadapan yang dilaksanakan sebagai rangka dalam penegakan hukum terhadap permintaan dari kepolisian, jaksa ataupun institusi penegak hukum yang lain dengan ditentukan menurut perundang-undangan dari pernyataan ini membuat perbuatan peretasan sebagai perbuatan yang tidak melakukan pelanggaran dalam hukum beserta alat buktinya bisa digunakan dalam Tindakan pembuktian saat berlangsungnya persidangan.

Daftar Pustaka

Arief, B. N. (2006). Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia. Jakarta: Rajawali Pers.

Budiartha, I. N. (2016). *Hukum Outsourcing : Konsep Alih Daya Bentuk Perlindungan Dan Kepastian Hukum.* Malang: Setara Press Kelompok Intrans publishing.

Garner, B. A. (2005). *Black's Law Dictionary.* West: Thompson.

Gunawan, K. d. (2013). *Sekelumit Tentang Hukum Penyadapan Dalam Hukum Positif Di Indonesia.* Bandung: Nuansa Aulia.

Hiariej, E. O. (2012). *Teori dan Hukum Pembuktian.* Jakarta: Erlangga.

I Made Kardiyasa, A. S. (2020). Sanksi Pidana Terhadap Ujaran Kebencian (Hate Speech). *Jurnal Analogi Hukum, Volume 2, Nomor 1.* , 80.

Judhariksawan. (2005). *Pengantar Hukum Telekomunikasi.* Jakarta.: Rajawali Press.

Jusmadi, D. d. (2013). Konvergensi Telematika, Arah Kebijakan dan Pengaturannya Dalam Tata Hukum Indonesia. *Yustisia Volume 2, Nomor 3.* , 48.

Komang Dara Trimarlina, I. N. (2019). Implementasi Perlindungan Hak Asasi Manusia Terhadap Pemeriksaan Dalam Proses Penyidikan. *Jurnal Analogi Hukum, Volume 1, Nomor 3.*, 414.

Maskun. (2013). *Kejahatan Siber (CyberCyber CrimeCrime): Suatu Pengantar.* Jakarta: Kencana.

Sanusi, M. A. (2007). *Konvergensi Hukum & Teknologi Informasi.* Jakarta: The Indonesian Research.

Wantu, F. M. (2015). *Pengantar Ilmu Hukum.* Gorontalo: Reviva Cendekia.