

**AKIBAT HUKUM BAGI PELAKU PENYADAPAN ILEGAL (INTERSEPSI) MENURUT UNDANG-UNDANG TELEKOMUNIKASI SERTA UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK<sup>1</sup>**

Oleh: Steve Jelly Walintukan<sup>2</sup>

Dientje Rumimpunu<sup>3</sup>

Rudy R. Watulingas<sup>4</sup>

**ABSTRAK**

Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimana penyadapan menurut hukum dan penyadapan ilegal (intersepsi) menurut peraturan perundang-undangan yang berlaku di Indonesia dan bagaimana akibat hukum bagi pelaku penyadapan ilegal (intersepsi) menurut Undang-Undang Telekomunikasi serta Undang-Undang Informasi dan Transaksi Elektronik, di mana dengan metode penelitian hukum normatif disimpulkan: 1. Penyadapan Menurut Hukum Dan Penyadapan Ilegal (Intersepsi) Menurut Peraturan Perundang-Undangan Yang Berlaku di Indonesia adalah sebagai berikut: Penyadapan atau intersepsi merupakan perbuatan yang dilarang oleh Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dimana pelakunya dapat diancam sanksi pidana. Pengecualian dilakukan terhadap ketentuan larangan penyadapan atau intersepsi itu adalah apabila hal tersebut dilakukan dalam rangka penegakan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang, seperti Komisi Pemberantasan Korupsi. Komisi Pemberantasan Korupsi mempunyai kewenangan untuk melakukan penyadapan termasuk merekam pembicaraan dalam melaksanakan tugas penyelidikan, penyidikan dan penuntutan. Penyadapan merupakan salah satu teknik audit untuk mendapatkan informasi dalam upaya mengungkap kasus ataupun sebagai dasar menetapkan langkah penyelidikan berikutnya. 2. Pelaku penyadapan

ilegal (intersepsi) yang terbukti bersalah akan dikenakan hukuman atau sanksi sesuai Undang-Undang 36 Tahun 1999 Tentang Telekomunikasi dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan pidana penjara maksimal lima belas tahun dan/atau denda paling banyak delapan ratus juta rupiah.

Kata kunci: penyadapan;

**PENDAHULUAN**

**A. Latar Belakang**

Teknologi komunikasi dan informasi yang semakin maju, membuat masyarakat kemudian beralih ke aplikasi *chatting* seperti WhatsApp, Telegram, *Inbox Messenger*, *Direct Message* Instagram dan pelan-pelan meninggalkan pesan teks (SMS). Beberapa fitur (karakteristik khusus) yang terdapat pada *smartphone*, antara lain rekam suara atau video dan *screenshot* (fitur untuk menangkap layar yang bisa diedit atau diubah isinya). Fitur-fitur ini mempunyai kegunaan yang dapat dimanfaatkan dengan baik, namun oleh orang-orang tidak bertanggung jawab disalahgunakan untuk hal-hal negatif (contoh: pornografi, *hacking*, penyadapan dan lain-lain). Salah satu kasus dugaan adanya penyadapan yang cukup menghebohkan di Indonesia, yaitu penyadapan percakapan lewat telepon antara seorang menteri dengan direktur utama salah satu persero.

**B. Rumusan Masalah**

1. Bagaimana penyadapan menurut hukum dan penyadapan ilegal (intersepsi) menurut peraturan perundang-undangan yang berlaku di Indonesia?
2. Bagaimana akibat hukum bagi pelaku penyadapan ilegal (intersepsi) menurut Undang-Undang Telekomunikasi serta Undang-Undang Informasi dan Transaksi Elektronik?

**C. Metode Penelitian**

Jenis penelitian yang digunakan adalah penelitian dengan menggunakan pendekatan secara yuridis normatif.

<sup>1</sup> Artikel Skripsi

<sup>2</sup> Mahasiswa pada Fakultas Hukum Unsrat, NIM. 17071101339

<sup>3</sup> Fakultas Hukum Unsrat, Magister Ilmu Hukum

<sup>4</sup> Fakultas Hukum Unsrat, Doktor Ilmu Hukum

## PEMBAHASAN

### A. Penyadapan Menurut Hukum Dan Penyadapan Ilegal (Intersepsi) Menurut Peraturan Perundang-Undangan Yang Berlaku Di Indonesia

Kasus penyadapan mulai dikenal sekitar tahun 1840-an dengan menggunakan telegraf.<sup>5</sup> Telegraf adalah sebuah mesin atau alat dengan teknologi untuk mengirim serta menerima pesan dari jarak jauh dan biasanya menggunakan morse sebagai kode komunikasi. Salah satu contoh kasus yang terkenal adalah penyadapan pada tahun 1867. Sebuah makelar saham bekerja sama untuk melakukan penyadapan terhadap operator telegraf yang dikirim ke koran di Timur Tengah. Perkembangan berikutnya yang terjadi setelah kasus tersebut, yaitu penyadapan menjadi pembajakan telepon. Hal ini masih terjadi pada era telepon kabel dan berkembang hingga ke zaman digital sekarang ini.

Penyadapan telepon dimulai setelah ditemukannya alat perekam percakapan telepon pada tahun 1890-an. Awalnya, komunikasi suara jarak jauh dilakukan secara eksklusif oleh sistem pertukaran sirkuit. Pertukaran percakapan telepon akan menghubungkan kawat untuk membentuk sirkuit berkesinambungan dan memutuskannya ketika panggilan berakhir. Bell Labs pada tahun 1965 mengembangkan sistem komunikasi telepon terkomputerisasi pertama yang menggantikan teknik penyadapan standar.

Penyadapan telepon pertama kali dilakukan melalui kawat yang secara fisik disisipkan melalui saluran antara operator dan pengguna telepon, dimana sinyalnya akan dibawa menuju alat pendengar sekaligus perekam. Penyadapan telepon baru-baru ini dipasang di tempat saluran penyadap yang menangani percakapan masuk. Penyadapan telepon secara resmi dikontrol secara ketat di beberapa negara untuk menjaga privasi.

Penyadapan telepon memerlukan persetujuan pengadilan dan hanya disetujui apabila penyadapan tersebut bertujuan untuk mendeteksi tindakan kriminal atau kegiatan subversif (gerakan dan usaha atau rencana untuk menjatuhkan kekuasaan yang sah

dengan menggunakan cara di luar undang-undang) yang menghalangi penegakan hukum. Penyadapan telepon yang ilegal atau tidak sah dianggap sebagai tindak pidana karena bertentangan dengan undang-undang.

Beberapa negara seperti Jerman, pengadilannya akan menyetujui penyadapan ilegal tanpa persetujuan pihak lain, meskipun yang bersangkutan dan disadap tersebut juga dapat mengajukan tuntutan. Negara seperti Amerika Serikat, badan intelijen federal di bawah undang-undang Pengawasan Intelijen Asing, bisa mendapatkan persetujuan untuk melakukan penyadapan dari Pengadilan Pengawasan Intelijen Asing Amerika Serikat atau yang dalam keadaan tertentu dapat juga disetujui oleh Kejaksaan Agung tanpa melalui pengadilan.<sup>6</sup>

Banyak cara dapat dilakukan untuk memonitor percakapan telepon seseorang. Salah satu pihak dapat merekam percakapan, baik dengan bantuan alat rekam ataupun melalui komputer yang memiliki perangkat lunak perekam panggilan. Perekaman baik yang dilakukan terbuka ataupun terselubung, dapat terjadi melalui beberapa cara berikut ini:<sup>7</sup>

1. Manual.
2. Otomatis dengan mendeteksi suara pada saluran telepon.
3. Otomatis setiap kali panggilan telepon diputus.

Telepon seluler mempunyai sejumlah masalah keamanan privasi. Pemerintah, penegak hukum dan badan intelijen di beberapa negara tertentu menggunakan telepon seluler untuk melakukan penyadapan. Teknologinya, antara lain dengan mengaktifkan mikrofon pada telepon seluler dari jarak jauh untuk mendengarkan percakapan sementara berlangsung di dekat orang yang memegang telepon seluler tersebut.

Telepon seluler juga sering digunakan untuk mengumpulkan data lokasi. Telepon seluler begitu dihidupkan, lokasi geografisnya dapat ditentukan dengan mudah (baik saat sedang digunakan atau tidak) melalui teknik yang dikenal sebagai multilaterasi. Teknik ini mampu menghitung perbedaan waktu yang dibutuhkan

<sup>5</sup> Kristian dan Gunawan, Y. 2013. *Sekelumit Tentang Hukum Penyadapan Dalam Hukum Positif Di Indonesia*. Bandung: Nuansa Aulia. Hlm. 22.

<sup>6</sup> Wikipedia. 2012. *Penyadapan Telepon* [https://id.wikipedia.org/wiki/Penyadapan\\_telepon](https://id.wikipedia.org/wiki/Penyadapan_telepon) Diakses tanggal 9 November 2021.

<sup>7</sup> *Ibid*.

oleh sinyal dari menara seluler untuk mencapai telepon seluler pemiliknya.

Salah satu contoh kasus penyadapan telepon yang berasal dari negara lain, yaitu Yunani, dimana sepanjang tahun 2004-2005 terdapat lebih dari seratus nomor telepon seluler yang sebagian besar dimiliki oleh pejabat pemerintah dan Pegawai Negeri Sipil, telah disadap secara ilegal. Pemerintah Yunani menyatakan, bahwa penyadapan ini dilakukan oleh badan intelijen asing untuk alasan keamanan terkait dengan penyelenggaraan Olimpiade Athena pada tahun 2004. Penyadapan dilakukan dengan cara mengaktifkan *lawful interception* dari operator seluler.

Kasus lain pada tahun 2007, yaitu peretasan telepon oleh salah satu tabloid internasional terhadap selebritas, politikus dan keluarga kerajaan. Kasus tersebut menimbulkan kemarahan masyarakat dan sponsor tabloid mulai melakukan pemboikotan. Aksi pemboikotan tersebut menyebabkan tabloid internasional bersangkutan yang dimaksud ditutup setelah 168 tahun terbit. Kasus penyadapan telepon selanjutnya melibatkan seorang mantan kepala negara yang dalam pengakuannya menyebutkan, bahwa dia bertanggung jawab atas penyadapan telepon warga negaranya dengan alasan keamanan dari teroris untuk memudahkan penangkapan.<sup>8</sup>

Menurut Kamus Besar Bahasa Indonesia, menyadap adalah mendengarkan (merekam) informasi (rahasia, pembicaraan) orang lain dengan sengaja tanpa sepengetahuan orangnya. Merekam, yaitu memindahkan suara (gambar, tulisan) ke dalam pita kaset, piringan dan sebagainya.<sup>9</sup> Penyadapan secara khusus diatur dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang kemudian disebut dengan istilah intersepsi.

Penjelasan pasal demi pasal Angka 5 Pasal 31 Ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyebutkan, bahwa yang dimaksud dengan

intersepsi atau penyadapan adalah sebagai berikut: “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.”

Beberapa istilah yang berkaitan dengan penjelasan pasal di atas, antara lain:

1. Informasi Elektronik

Satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *teletype* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang telah diolah dan memiliki arti serta dapat dipahami oleh orang mampu memahaminya.

2. Dokumen Elektronik

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 tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna maupun arti serta dapat dipahami oleh orang mampu memahaminya.

3. Sistem Elektronik

Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.

Berbagai istilah penyadapan dalam bahasa Inggris, yaitu sebagai berikut:

1. *Bugging*<sup>10</sup>

Sebuah bentuk dari pengawasan elektronik berupa pembicaraan atau kemungkinan menangkap secara elektronik, mendengar

<sup>8</sup> *Ibid.*

<sup>9</sup> Kamus Besar Bahasa Indonesia.

<sup>10</sup> Gardner, B. A. 2004. *Black Law Dictionary*. ST. Paul: Thomson, hlm. 7.

atau merekam, biasanya dengan diam-diam, mendengar diam-diam dengan perangkat elektronik.

2. *Eavesdropping*<sup>11</sup>

Tindakan mendengar secara diam-diam terhadap pembicaraan pribadi orang lain tanpa sepengetahuannya.

3. *Wiretapping*<sup>12</sup>

Elektronik atau mesin untuk mendengar pembicaraan secara diam-diam, biasanya dilakukan oleh penegak hukum di bawah izin pengadilan untuk mendengar pembicaraan pribadi.

Objek penyadapan (*lawful interception*) meliputi layanan komunikasi yang menggunakan atau melintasi *network operator*, *access operator* dan/atau layanan internet melalui *service provider*. Layanan internet merupakan akses ke internet itu sendiri dan layanan-layanan yang menggunakan internet. Tindakan penyadapan yang dilakukan mengacu pada dua standar, yaitu:<sup>13</sup>

1. *European Telecommunication Standards Institute* (ETSI) yang berbasis di Perancis.
2. *Communications Assistance for Law Enforcement Act* (Calea) yang berbasis di Amerika Serikat.

Tindakan merekam belum tentu sama dengan menyadap, karena realita berupa suara atau kejadian yang direkam ke dalam satu tape recorder maupun kamera bukanlah data elektronik, Informasi Elektronik maupun Dokumen Elektronik. Mengacu pada definisi-definisi di atas, maka dapat dikatakan bahwa menyadap lebih luas dari maknanya daripada merekam. Menyadap dilakukan salah satunya dengan jalan merekam, namun secara diam-diam (tanpa sepengetahuan orang yang disadap). Hal ini dapat dibedakan dari merekam, dimana bisa saja orang atau objek yang direkam itu tahu bahwa dirinya sedang direkam.<sup>14</sup>

Penyadapan atau intersepsi merupakan perbuatan yang dilarang oleh Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dimana pelakunya dapat diancam sanksi pidana. Pengecualian dilakukan terhadap ketentuan larangan penyadapan atau intersepsi itu adalah apabila hal tersebut dilakukan dalam rangka penegakan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

Salah satu institusi penegak hukum yang berwenang menurut undang-undang untuk melakukan penyadapan atau intersepsi adalah Komisi Pemberantasan Korupsi. Komisi Pemberantasan Korupsi mempunyai kewenangan untuk melakukan penyadapan termasuk merekam pembicaraan dalam melaksanakan tugas penyelidikan, penyidikan dan penuntutan. Penyadapan merupakan salah satu teknik audit untuk mendapatkan informasi dalam upaya mengungkap kasus ataupun sebagai dasar menetapkan langkah penyelidikan berikutnya.

Rekaman hasil penyadapan tidak serta merta dapat menjadi alat bukti tersendiri dalam hukum pidana, namun informasi yang diperoleh dapat dijadikan petunjuk dalam Kitab Undang-Undang Hukum Acara Pidana. Hal ini karena dari hasil penyadapan tersebut, hakim memperoleh kejelasan mengenai terjadinya tindak pidana korupsi.<sup>15</sup> Penyidik dalam memproses tindak pidana khusus menurut Pasal 83 Ayat (3) Undang-Undang Nomor 8 Tahun 1981 Tentang Kitab Undang-Undang Hukum Acara Pidana, dapat melakukan penyadapan dengan izin dari Ketua Pengadilan Negeri.

Pemberian kewenangan penyadapan kepada Komisi Pemberantasan Korupsi ditujukan untuk melaksanakan tugas penyelidikan, penyidikan dan penuntutan terhadap Tindak Pidana Korupsi. Komisi Pemberantasan Korupsi berwenang untuk melakukan penyadapan dan merekam pembicaraan, terutama dalam menjangkau pelaku Tindak Pidana Korupsi. Beberapa kasus

<sup>11</sup> *Ibid*, hlm. 551.

<sup>12</sup> *Ibid*, hlm. 1631.

<sup>13</sup> Rachmad, A. 2016. *Legalitas Penyadapan Dalam Sistem Peradilan Pidana Indonesia*. Jurnal Hukum Samudra Keadilan. Volume 11, Nomor 2, hlm. 241-242.

<sup>14</sup> Pramesti, T. J. A. 2017. *Perbedaan Menyadap Dan Merekam*.

<https://www.hukumonline.com/klinik/detail/ulasan/lt566f607210efa/perbedaan-menyadap-dan-merekam> Diakses tanggal 9 November 2021.

<sup>15</sup> Anggraeni, R. 2010. *Penggunaan Hasil Penyadapan Sebagai Alat Bukti Petunjuk Dalam Perkara Tindak Pidana Korupsi*. Jurnal Yudisial, Volume III, No. 2, hlm. 186.

penyadapan dilakukan terhadap seseorang setelah Komisi Pemberantasan Korupsi mendapatkan laporan, bahwa adanya dugaan penyalahgunaan keuangan dan perekonomian negara dari masyarakat.

Pelaksanaan penyadapan dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2019 Tentang Perubahan Kedua Atas Undang-Undang Nomor 30 Tahun 2002 Tentang Komisi Pemberantasan Tindak Pidana Korupsi diatur pada Pasal 12B sampai dengan Pasal 12 D yang berbunyi sebagai berikut:

*Pasal 12B*

- 1) *Penyadapan sebagaimana dimaksud dalam Pasal 12 Ayat (1), dilaksanakan setelah mendapatkan izin tertulis dari Dewan Pengawas.*
- 2) *Untuk mendapatkan izin sebagaimana dimaksud pada Ayat (1) dilaksanakan berdasarkan permintaan secara tertulis dari Pimpinan Komisi Pemberantasan Korupsi.*
- 3) *Dewan Pengawas dapat memberikan izin tertulis terhadap permintaan sebagaimana dimaksud pada Ayat (2) paling lama 1x24 (satu kali dua puluh empat) jam terhitung sejak permintaan diajukan.*
- 4) *Dalam hal Pimpinan Komisi Pemberantasan Korupsi mendapatkan izin tertulis dari Dewan Pengawas sebagaimana dimaksud pada Ayat (3), penyadapan dilakukan paling lama 6 (enam) bulan terhitung sejak izin tertulis diterima dan dapat diperpanjang 1 (satu) kali untuk jangka waktu yang sama.*

*Pasal 12C*

- 1) *Penyelidik dan penyidik melaporkan penyadapan sebagaimana dimaksud dalam Pasal 12 Ayat (1) yang sedang berlangsung kepada Pimpinan Komisi Pemberantasan Korupsi secara berkala.*
- 2) *Penyadapan sebagaimana dimaksud dalam Pasal 12 Ayat (1) yang telah selesai dilaksanakan harus dipertanggungjawabkan kepada Pimpinan Komisi Pemberantasan Korupsi dan Dewan Pengawas paling lambat 14 (empat belas) hari kerja terhitung sejak Penyadapan selesai dilaksanakan.*

*Pasal 12D*

- 1) *Hasil penyadapan sebagaimana dimaksud dalam Pasal 12 Ayat (1) bersifat rahasia*

*dan hanya untuk kepentingan peradilan dalam Pemberantasan Tindak Pidana Korupsi.*

- 2) *Hasil penyadapan yang tidak terkait dengan Tindak Pidana Korupsi yang sedang ditangani Komisi Pemberantasan Korupsi wajib dimusnahkan seketika.*
- 3) *Dalam hal kewajiban sebagaimana dimaksud pada Ayat (2) tidak dilaksanakan, pejabat dan/atau orang yang menyimpan hasil penyadapan dijatuhi hukuman pidana sesuai dengan ketentuan peraturan perundang-undangan.*

Penyadapan yang dilakukan oleh Komisi Pemberantasan Korupsi mengikuti *Standard Operational Procedure* yang didasarkan pada keputusan komisi tersebut. Proses penyadapan oleh Komisi Pemberantasan Korupsi cukup ketat. Setiap tahun, pelaksanaan penyadapan oleh Komisi Pemberantasan Korupsi akan diaudit oleh tim khusus yang dibentuk berdasarkan Peraturan Menteri Komunikasi dan Informasi Nomor 11/PERM.KOMINFO/02/2006 Tentang Teknis Penyadapan Terhadap Informasi.<sup>16</sup>

Penyadapan dapat dikelompokkan menjadi empat jenis, antara lain:<sup>17</sup>

1. *Penyadapan pasif (passive interception)*  
Tindakan penyadapan yang dilakukan secara tidak langsung dengan cara membaca data atau tidak diotorisasi.
2. *Penyadapan aktif (active interception)*  
Tindakan penyadapan secara langsung dan disertai dengan tindakan mengubah data yang tidak diotorisasi.
3. *Penyadapan semi aktif.*
4. *Penyadapan yang merupakan penggabungan antara penyadapan aktif dan pasif.*

Teknik yang digunakan dalam implementasi penyadapan Komisi Pemberantasan Korupsi adalah penyadapan aktif dan semi aktif. Kebanyakan penyadapan yang dilakukan adalah dengan mengimplementasikan penggabungan teknik aktif dan pasif. Penyadapan di Indonesia dilakukan sesuai dengan Peraturan Menteri Komunikasi dan Informasi Nomor 11/PERM.KOMINFO/02/2006 Tentang Teknis

<sup>16</sup> *Ibid*, hlm. 187.

<sup>17</sup> Kristian dan Gunawan, Y., *Op. Cit.*, hlm. 205.

Penyadapan Terhadap Informasi.<sup>18</sup> Sedikitnya terdapat enam macam bentuk penyadapan, yaitu sebagai berikut.<sup>19</sup>

1. Penyadapan telepon kabel  
Praktik ini dilakukan dengan memasang alat pada telepon jaringan berbasis kabel dan melibatkan teknologi yang mendukung segala aktivitas penyadapan informasi di jaringan telepon tetap atau kabel (*Public Switched Telephone Network/PSTN*).
2. Pemantauan telepon seluler  
Ini adalah bentuk penyadapan terhadap informasi yang dikirimkan melalui jaringan telepon seluler.
3. Pemantauan internet  
Bentuk intersepsi komunikasi ini berupa tindakan menangkap data yang di dunia maya (*cyber space*) dalam perjalanannya menuju tujuan akhir (contohnya, data yang dikirim ke alamat email tertentu). Praktik ini bersifat *omnipresent* karena dapat dilakukan dan terjadi di manapun dalam dunia maya.
4. Pemantauan video teknologi  
Intersepsi video yang paling umum saat ini adalah *Closed-Circuit Television* (CCTV) yang dipasang pada tempat-tempat tertentu untuk merekam aktivitas apapun dalam jangkauannya. Teknologi CCTV mampu menganalisis bagian-bagian terkecil dari subjek yang direkam, seperti perekaman biometrik terhadap wajah, bahkan kornea mata.
5. Pemantauan lokasi *Global Positioning System* (GPS)  
Pelacakan lokasi melibatkan penggunaan perangkat lunak tertentu untuk mencatat dan melaporkan secara visual informasi yang tertangkap dalam jaringan.
6. Penerabas komunikasi  
Praktik ini melibatkan tindakan dengan menanamkan perangkat lunak, seperti

*malware* tertentu ke dalam sebuah perangkat komunikasi untuk mengambil semua informasi yang tersimpan di dalamnya.

Berikut beberapa kasus penyadapan paling fenomenal yang pernah terjadi di Indonesia:<sup>20</sup>

1. Kasus penyadapan kepala negara bersama sembilan petingginya yang pelakunya diduga berasal dari negara lain. Hal ini menyebabkan hubungan Indonesia dengan negara tersebut memanas. Kasus tersebut menyebabkan duta besar Indonesia untuk negara bersangkutan dipulangkan. Negara bersangkutan yang dimaksud menolak untuk melakukan permintaan maaf atas kasus tersebut.
2. Kasus penyadapan seorang gubernur dari salah satu provinsi di Indonesia. Tiga alat sadap ditemukan di rumah dinas gubernur tersebut.
3. Kasus penyadapan seorang wakil rakyat dengan petinggi salah satu perusahaan terbesar di Indonesia.
4. Kasus penyadapan seorang tokoh ternama dengan salah satu organisasi keagamaan terkait pernyataan sikap mengenai dugaan penistaan agama.

#### **B. Akibat Hukum Bagi Pelaku Penyadapan Ilegal (Intersepsi) Menurut Undang-Undang Telekomunikasi Serta Undang-Undang Informasi Dan Transaksi Elektronik**

Penyadapan merupakan perbuatan yang dilarang oleh hukum sebagaimana tercantum dalam Pasal 40 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi yang berbunyi: "*Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.*"

Penyadapan secara umum dilarang oleh undang-undang karena melanggar hak privasi seseorang. Penyadapan dapat menyebabkan kehidupan seseorang terancam kebebasannya dan berada dalam keadaan takut, karena kemerdekaan pribadinya dirampas. Setiap orang mempunyai hak atas kebebasan privasi

<sup>18</sup> Hasanah, H. 2018. *Penggunaan Hasil Penyadapan Komisi Pemberantasan Korupsi (KPK) Sebagai Alat Bukti Dalam Mengungkap Dan Menyelesaikan Perkara Tindak Pidana Korupsi*. <https://fh.unram.ac.id/wp-content/uploads/2018/07> Diakses tanggal 9 November 2021.

<sup>19</sup> Panji, A. 2018. *Rini-Sofyan Diduga Disadap, Pakar Jelaskan 6 Bentuk Penyadapan*. <https://kumparan.com/kumparantech/rini-sofyan-diduga-disadap-pakar-jelaskan-6-bentuk-penyadapan/full> Diakses tanggal 7 November 2021.

<sup>20</sup>Kukuh, T. 2017. *4 Kasus Penyadapan Ilegal Paling Fenomenal, SBY 2 Kali Jadi Korban*. <https://www.jawapos.com/nasional/politik/06/02/2017/4-kasus-penyadapan-ilegal-paling-fenomenal-sby-2-kali-jadi-korban/> Diakses tanggal 7 November 2021

masing-masing, bebas dari rasa takut dan lainnya, sebagaimana tercantum dalam Pasal 28F dan Pasal 28G Ayat (1), Undang-Undang Dasar 1945 amandemen ke empat yang berbunyi: *Pasal 28F "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungannya, serta berhak untuk memperoleh, memiliki, menyimpan mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia."*

*Pasal 28G Ayat (1) Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."*

Pernyataan tersebut didukung oleh Pasal 14 dan Pasal 21 Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia yang berbunyi: *Pasal 14 "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi yang diperlukan untuk mengembangkan pribadi dan lingkungan sosialnya. Setiap orang juga berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia."*

*Pasal 21 "Setiap orang berhak atas keutuhan kehidupan pribadinya, baik jasmani maupun rohani, sehingga tidak boleh menjadi objek penelitian tanpa persetujuan darinya."*

Penyadapan juga bertentangan dengan Pasal 17 *International Covenant on Civil and Political Rights* (Kovenan Internasional Hak-Hak Sipil dan Politik) yang menyatakan, bahwa:

- 1) *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
- 2) *Everyone has the right to the protection of the law against such interference or attacks.*

Berdasarkan rumusan tersebut, terlihat jelas bahwa setiap orang tidak dapat dijadikan atau diperlakukan sewenang-wenang atas kerahasiaan pribadi, keluarga, rumah tangga atau hubungan surat menyurat dan tidak boleh dicemari kehormatan serta nama baiknya.

Sebaliknya, setiap orang berhak atas perlindungan hukum terhadap campur tangan atau pencemaran demikian.<sup>21</sup>

Komentar Umum Nomor 16 mengenai Pasal 17 Pasal 17 Kovenan Internasional Hak-Hak Sipil dan Politik yang disepakati oleh Komite Hak Asasi Manusia Perserikatan Bangsa-Bangsa pada persidangan ke dua puluh tiga tahun 1988, memberikan komentar terhadap materi muatan pasal tersebut, dimana pada poin 8 dinyatakan:<sup>22</sup>

*"Bahwa integritas dan kerahasiaan korespondensi harus dijamin secara de jure dan de facto. Korespondensi harus diantarkan ke alamat yang dituju tanpa halangan dan tanpa dibuka atau dibaca terlebih dahulu. Pengamatan (surveillance), baik secara elektronik maupun lainnya, penyadapan telepon, telegram dan bentuk-bentuk komunikasi lainnya, serta perekaman pembicaraan harus dilarang."*

Dua ketentuan hukum yang secara khusus mengatur tentang teknologi dalam kaitannya dengan komunikasi, yaitu Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.<sup>23</sup> Larangan penyadapan dapat dikecualikan apabila diatur dalam undang-undang demi kepentingan penegakan hukum, sebagaimana tercantum dalam Pasal 31 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang menyatakan: *"Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2) intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan Undang-Undang."*

Penyadapan dikatakan tidak melanggar Hak Asasi Manusia, apabila dilakukan demi kepentingan pengungkapan kasus. Pelanggaran Hak Asasi Manusia dengan kata lain terjadi apabila hasil penyadapan tersebut digunakan

<sup>21</sup> Kristian dan Gunawan, Y., *Op. Cit.*, hlm. 239.

<sup>22</sup> Pasal 17 Kovenan Internasional Hak-Hak Sipil dan Politik.

<sup>23</sup> Christianto, H. 2016. *Tindakan Penyadapan Ditinjau Dari Perspektif Hukum Pidana*. Jurnal Hukum, Volume V, Nomor 2, hlm. 95.

untuk kepentingan di luar penegakkan hukum. Komisi Pemberantasan Korupsi adalah lembaga utama yang bergerak untuk menangani kasus-kasus Tindak Pidana Korupsi yang ada di Indonesia. Aktivitas penyadapan sangat penting bagi Komisi Pemberantasan Korupsi dalam mengungkap kasus-kasus tersebut.

Keberhasilan Komisi Pemberantasan Korupsi dalam membongkar kasus Tindak Pidana Korupsi, demikian identik dengan keberhasilan penyadapan terhadap percakapan yang dilakukan oleh para pelaku. Selama Komisi Pemberantasan Korupsi melakukan penyadapan demi kepentingan hukum dan pengungkapan kasus pidana, maka hal tersebut bukanlah pelanggaran terhadap Hak Asasi Manusia. Penyadapan memang tidak dapat dilakukan oleh sembarang orang, kecuali dengan alasan yang dibenarkan hukum. Hal ini karena banyak orang yang melakukan penyadapan dengan maksud-maksud jahat.<sup>24</sup>

Penyadapan adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi yang bertujuan untuk mendapatkan informasi dengan cara tidak sah. Informasi yang dimiliki oleh seseorang pada dasarnya adalah hak pribadi dan harus dilindungi, sehingga penyadapan harus dilarang. Penyadapan atau intersepsi ini termasuk sebagai perbuatan yang dilarang, namun kecuali dilakukan oleh pihak berwenang sesuai aturan peundang-undangan sebagaimana dijelaskan oleh Pasal 31 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik berikut ini:

- (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.*
- (2) *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.*

(3) *Ketentuan sebagaimana dimaksud pada Ayat (1) dan Ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.*

(4) *Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada Ayat (3) diatur dengan undang-undang.*

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 Ayat (1) atau Ayat (2) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik di atas, akan dipidana dengan pidana penjara paling lama sepuluh tahun dan/atau denda paling banyak delapan ratus juta rupiah. Berikut uraian pasal-pasal berkaitan dengan penyadapan atau intersepsi beserta sanksi-sanksinya menurut Undang-Undang 36 Tahun 1999 Tentang Telekomunikasi dan juga Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik:

1. Undang-Undang 36 Tahun 1999 Tentang Telekomunikasi

*Pasal 40*

*"Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."*

Sanksinya, antara lain:

*Pasal 56*

*"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 Tahun."*

2. Undang-Undang Nomor Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-

---

<sup>24</sup> Sidabukke, S. *Tinjauan Kewenangan Penyadapan Oleh KPK Dalam Perspektif Hak Asasi Manusia*  
<http://repository.ubaya.ac.id/133/1/Makalah%20Penyadapan%20KPK.pdf> Diakses tanggal 10 November 2021.



Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

*Pasal 31 Ayat (1) dan Ayat (2)*

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.*

2) *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.*

Sanksinya: *Pasal 47 "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)."*

*Pasal 52 Ayat (4) "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga."*

Penyadapan merupakan perbuatan yang melanggar hukum dan para pelakunya dapat dijerat dengan sanksi pidana, baik berupa penjara maupun denda. Pihak yang merasa dirugikan akibat penyadapan atau intersepsi tidak sesuai hukum atau aturan undang-undang berlaku, juga dapat melaporkan perbuatan tersebut kepada instansi terkait, yaitu kepolisian.

## **PENUTUP**

### **A. Kesimpulan**

1. Penyadapan Menurut Hukum Dan Penyadapan Ilegal (Intersepsi) Menurut Peraturan Perundang-Undangan Yang Berlaku di Indonesia adalah sebagai berikut:

Penyadapan atau intersepsi merupakan perbuatan yang dilarang oleh Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dimana pelakunya dapat diancam sanksi pidana. Pengecualian dilakukan terhadap ketentuan larangan penyadapan atau intersepsi itu adalah apabila hal tersebut dilakukan dalam rangka penegakan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang, seperti Komisi Pemberantasan Korupsi. Komisi Pemberantasan Korupsi mempunyai kewenangan untuk melakukan penyadapan termasuk merekam pembicaraan dalam melaksanakan tugas penyelidikan, penyidikan dan penuntutan. Penyadapan merupakan salah satu teknik audit untuk mendapatkan informasi dalam upaya mengungkap kasus ataupun sebagai dasar menetapkan langkah penyelidikan berikutnya.

2. Pelaku penyadapan ilegal (intersepsi) yang terbukti bersalah akan dikenakan hukuman atau sanksi sesuai Undang-Undang 36 Tahun 1999 Tentang Telekomunikasi dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dengan pidana penjara maksimal lima belas tahun dan/atau denda paling banyak delapan ratus juta rupiah.

### **B. Saran**

1. Undang-undang mengenai penyadapan sebaiknya diberi batasan yang jelas, karena masih terdapat beberapa perbedaan yang tidak semuanya bisa dipahami oleh orang. Contohnya, mengenai istilah menyadap dan merekam yang dianggap masyarakat sama tapi interpretasinya berbeda. Hal ini perlu dilakukan agar tidak ada salah tafsir mengenai undang-undang tersebut

yang di kemudian hari dapat dimanfaatkan oleh pihak-pihak tertentu untuk menjerat orang lain, terutama apabila ada niat atau maksud jahat terselubung di dalamnya. Sosialisasi mengenai kewenangan Komisi Pemberantasan Korupsi berkaitan dengan penyadapan atau intersepsi dalam rangka penyidikan untuk membantu pengungkapan kasus Tindak Pidana Korupsi diperlukan agar tidak ada salah pengertian antara masyarakat dengan komisi tersebut, mengingat kegiatan menyadap dianggap sebagian masyarakat adalah pelanggaran terhadap hak asasi dan informasi pribadi seseorang.

2. Akibat hukum berupa sanksi pidana dan denda terhadap pelaku penyadapan atau intersepsi ilegal harus tegas agar ada efek jera, karena dapat mengancam kebebasan dan hak privasi seseorang atau bahkan kelompok apabila dilakukan tidak sesuai dengan hukum. Arahan untuk para penegak hukum juga diperlukan dalam melakukan penyidikan, karena kasus penyadapan tidak sembarang dilakukan oleh orang lain selain yang berwenang menurut hukum atau dalam hal ini Komisi Pemberantasan Korupsi.

#### DAFTAR PUSTAKA

- Ali, A. 2008. Menguak Tabir Hukum. Jakarta: Ghalia Indonesia.
- \_\_\_\_\_. 2012. Menguak Teori Hukum Dan Teori Peradilan. Jakarta: Kencana.
- Anggraeni, R. 2010. Penggunaan Hasil Penyadapan Sebagai Alat Bukti Petunjuk Dalam Perkara Tindak Pidana Korupsi. Jurnal Yudisial.
- Christianto, H. 2016. Tindakan Penyadapan Ditinjau Dari Perspektif Hukum Pidana. Jurnal Hukum.
- Gardner, B. A. 2004. Black Law Dictionary. ST. Paul: Thomson.
- Kristian dan Gunawan, Y. 2013. Sekelumit Tentang Hukum Penyadapan Dalam Hukum Positif Di Indonesia. Bandung: Nuansa Aulia.
- Marzuki, P. M. 2009. Pengantar Ilmu Hukum. Jakarta: Kencana.
- Mertokusumo, S. 2003. Mengenal Hukum. Yogyakarta: Liberty.
- \_\_\_\_\_. 2010. Mengenal Hukum Suatu Pengantar. Yogyakarta: Universitas Atma Jaya.
- Prodjodikoro, W. 1986. Asas-asas Hukum Pidana di Indonesia. PT. Eresco: Bandung.
- Rachmad, A. 2016. Legalitas Penyadapan Dalam Sistem Peradilan Pidana Indonesia. Jurnal Hukum Samudra Keadilan.
- Said, N. A. Aspek-Aspek Sosiologik Sistem Hukum Nasional. Jurnal Dinamika.
- Soeroso, R. 2011. Pengantar Ilmu Hukum. Jakarta: Sinar Grafika.
- #### SUMBER-SUMBER LAIN
- Arifiyadi, T. 2013. Hukum Merekam Menggunakan Kamera Tersembunyi (Hidden Camera). <https://www.hukumonline.com/klinik/detail/ulasan/lt508a38edc9c87/hukum-merekam-menggunakan-kamera-tersembunyi-hidden-camera>
- Hasanah, H. 2018. Penggunaan Hasil Penyadapan Komisi Pemberantasan Korupsi (KPK) Sebagai Alat Bukti Dalam Mengungkap Dan Menyelesaikan Perkara Tindak Pidana Korupsi. <https://fh.unram.ac.id/wp-content/uploads/2018/07>
- Kemp, S. 2020. Digital 2020: Indonesia. <https://datareportal.com/reports/digital-2020-indonesia>
- Kukuh, T. 2017. 4 Kasus Penyadapan Ilegal Paling Fenomenal, SBY 2 Kali Jadi Korban. <https://www.jawapos.com/nasional/politik/06/02/2017/4-kasus-penyadapan-ilegal-paling-fenomenal-sby-2-kali-jadi-korban/>
- Panji, A. 2018. Rini-Sofyan Diduga Disadap, Pakar Jelaskan 6 Bentuk Penyadapan. <https://kumparan.com/kumparantech/rini-sofyan-diduga-disadap-pakar-jelaskan-6-bentuk-penyadapan/full>