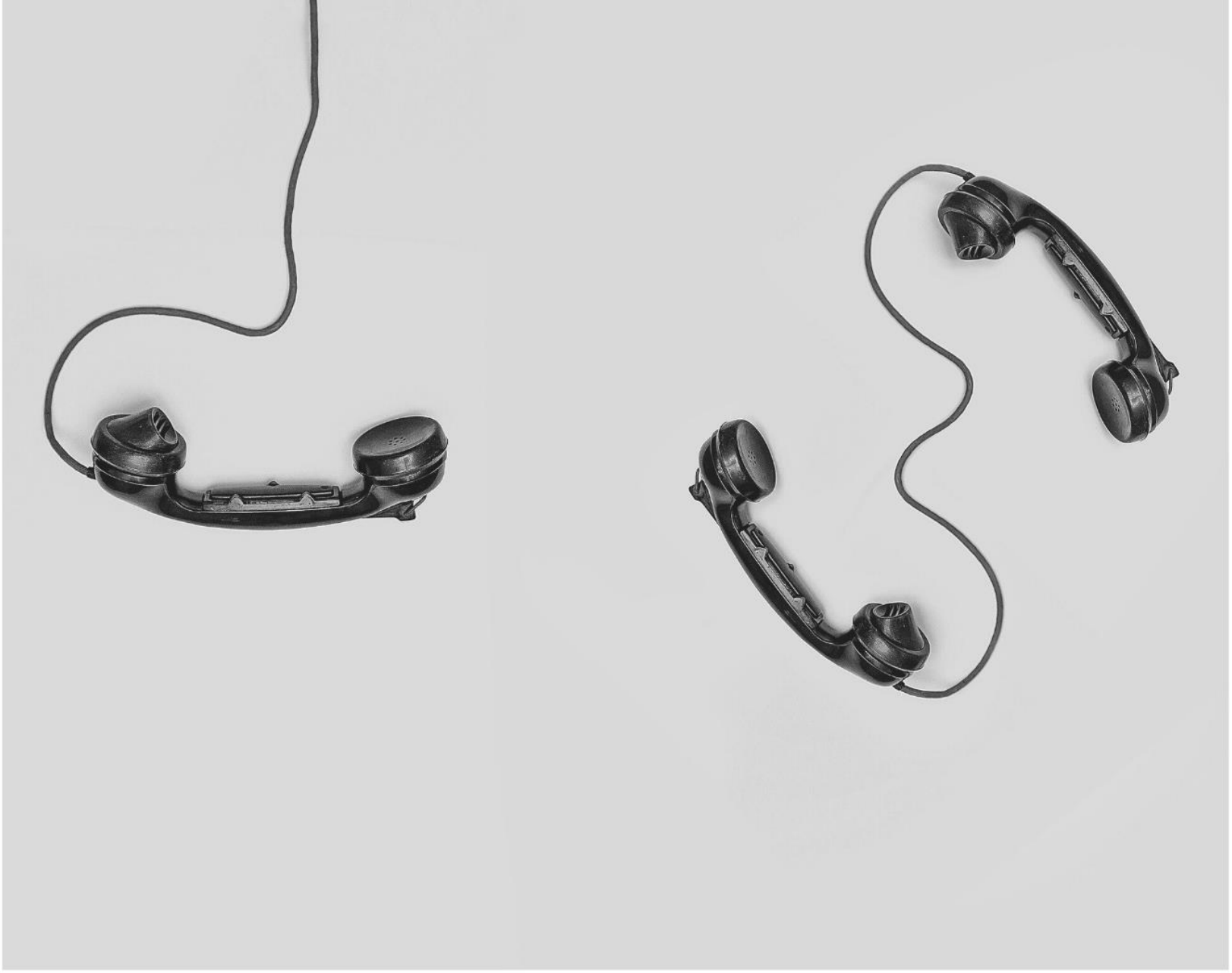

Mengatur Ulang Penyadapan dalam Sistem Peradilan Pidana:

Meninjau Praktik-Praktik Terbaik Pengaturan Penyadapan di Berbagai Negara

Institute for Criminal Justice Reform

Mengatur Ulang Penyadapan dalam Sistem Peradilan Pidana: Meninjau Praktik-Praktik Terbaik Pengaturan Penyadapan di Berbagai Negara

Penyusun:
Iftitahsari

Editor:
Luthfi W. Eddyono

Desain Cover:
Adhigama Andre Budiman

Elemen Visual:
Alex Andrews on Pexels

Diterbitkan oleh:
Institute for Criminal Justice Reform
Jl. Komplek Departemen Kesehatan Nomor B-4 Pasar Minggu, Jakarta Selatan – 12520
Phone/Fax: 021-27807065

ICJRId ICJRID ICJRID perkumpulanicjr

Dipublikasikan pertama kali pada:
Januari 2020

Kami memahami, tidak semua orang memiliki kesempatan untuk menjadi pendukung dari ICJR. Namun jika anda memiliki kesamaan pandangan dengan kami, maka anda akan menjadi bagian dari misi kami untuk membuat Indonesia memiliki sistem hukum yang adil, akuntabel, dan transparan untuk semua warga di Indonesia tanpa membeda-bedakan status sosial, pandangan politik, warna kulit, jenis kelamin, asal-usul, dan kebangsaan.

Hanya dengan 15 ribu rupiah, anda dapat menjadi bagian dari misi kami dan mendukung ICJR untuk tetap dapat bekerja memastikan sistem hukum Indonesia menjadi lebih adil, transparan, dan akuntabel.

Klik taut berikut ini bit.ly/15untukkeadilan

Kata Pengantar

Dalam sistem peradilan pidana, upaya menemukan peristiwa kejahatan termasuk orang yang bertanggungjawab atas peristiwa kejahatan telah melibatkan penggunaan teknologi. Hal juga terkait dengan berkembangnya modus dan cara untuk melakukan kejahatan sehingga diperlukan berbagai upaya yang lebih sistematis untuk membuktikan adanya suatu peristiwa kejahatan dan juga menemukan orang atau sekelompok orang yang perlu untuk dimintai pertanggungjawabannya dalam peristiwa kejahatan tersebut.

Salah satu cara untuk menemukan siapa yang harus bertanggungjawab atas suatu peristiwa kejahatan adalah dengan menggunakan metode penyadapan dan/atau intersepsi. Metode ini menjadi perdebatan hangat di kalangan komunitas hukum khususnya yang berada dalam rumpun sistem peradilan pidana. Selain soal membatasi upaya pelanggaran privasi, namun pada kenyataannya, Indonesia memiliki berbagai hukum, setidaknya 20 aturan, yang mengatur secara singkat tentang hukum acara dan prosedur melakukan penyadapan. Institute for Criminal Justice Reform mengidentifikasi beberapa masalah lain yang mana salah satunya yaitu hukum acara penyadapan di Indonesia belum mampu untuk melindungi pihak-pihak yang berpotensi dirugikan atas tindakan penyadapan yang dilakukan secara sewenang-wenang.

Beragamnya berbagai pengaturan tersebut, dicoba dibenahi oleh Mahkamah Konstitusi melalui Putusan Nomor 5/PUU-VIII/2010 tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap UUD 1945. Putusan tersebut mengamanatkan untuk membentuk satu aturan tunggal tentang mekanisme dan prosedur penyadapan yang berbentuk undang-undang. Putusan tersebut lalu ditindaklanjuti oleh DPR RI dengan membuat RUU Penyadapan.

Riset ini berupaya menggambarkan bagaimana formulasi pengaturan berdasarkan praktik – praktik terbaik di berbagai Negara terkait dengan penyadapan dalam sistem peradilan pidana. Melalui riset, ICJR berharap agar dapat menjadi bahan pengayaan bagi proses perdebatan dalam pembentukan UU penyadapan antara DPR RI dan Pemerintah. ICJR berkeinginan pengaturan penyadapan di masa depan akan memperkuat upaya perlindungan privasi dari tindakan penegakkan hukum yang dilakukan secara sewenang – wenang

Jakarta, Januari 2020

Anggara
Direktur Eksekutif ICJR

Daftar Isi

BAB I

Pendahuluan

1.1. Latar Belakang

Jaminan perlindungan hak atas privasi dalam hukum internasional telah diatur dalam Pasal 17 Konvenan Sipil dan Politik 1976 yang diratifikasi oleh Indonesia melalui Undang-Undang Nomor 12 Tahun 2005. Di Indonesia, perlindungan hak atas privasi baru dikenal luas setelah amandeman UUD 1945, namun sebelumnya ketentuan yang dapat dirujuk salah satu bentuk perlindungan privasi di Indonesia adalah Pasal 551 KUHP.[1] Setelah reformasi, hak atas privasi di Indonesia dijamin perlindungannya secara eksplisit dalam Pasal 28 G ayat (1) UUD 1945[2] dan beberapa peraturan perundang–undangan lainnya. Misalnya, Pasal 32 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia[3], Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi[4], dan Pasal 31 ayat (1) sampai (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[5]. Oleh karena itu, perlindungan privasi telah dijunjung tinggi tidak hanya oleh konstitusi namun juga instrumen hukum nasonal lainnya.

---

1 Pasal 551 KUHP berbunyi sebagai berikut: “Barang siapa tanpa wewenang berjalan atau berkendaraan di atas tanah yang oleh pemiliknya dengan cara jelas dilarang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah.”

2 Pasal 28 G ayat (1) UUD 1945 berbunyi sebagai berikut: ”Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

3 Pasal 32 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia berbunyi sebagai berikut: “Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.”

4 Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi berbunyi sebagai berikut: "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun. “ Kemudian penjelasan Pasal 40 Telekomunikasi disebutkan bahwa: "Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang dimiliki seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang.”

5 Bunyi Pasal 31 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berbunyi adalah sebagai berikut:

(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 apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(3) 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.

Perlindungan hak atas privasi juga telah diatur dalam hukum pidana, yaitu pada Bab XXVII KUHP tentang Kejahatan Jabatan. Ketentuan tersebut mengatur larangan kepada para pejabat yang berwenang untuk melakukan penyadapan, pengawasan, merampas, mendapatkan informasi yang termuat didalam benda-benda yang dapat menyimpan data telekomunikasi seperti surat, telegraph atau isi percakapan telephon. Penyadapan pada dasarnya merupakan pelanggaran hak asasi manusia, namun dalam implementasinya karena hak atas privasi bukan merupakan hak yang tidak dapat dikurangi dalam keadaan apapun, sehingga terdapat kewenangan negara untuk membatasi hak tersebut. Pembatasan tersebut diperbolehkan sepanjang (a) diatur dalam undang-undang, (b) memang sangat dibutuhkan dalam masyarakat demokratis, dan (c) berdasarkan tujuan yang terlegitimasi.[6]

Namun, pengaturan mengenai penyadapan sebagai bentuk intrusi terhadap hak atas privasi tersebut menjadi salah satu topik yang masih mengundang perdebatan di antara kalangan komunitas hukum. Selain dipandang sebagai alat yang efektif untuk mengungkap kejahatan, pada saat yang sama penyadapan juga dipandang sebagai invasi dari negara terhadap hak privasi warganya.[7] Oleh karena memiliki potensi yang besar untuk melanggar HAM, pembahasan mengenai bagaimana penyadapan ini diatur menjadi isu yang sangat penting khususnya bagi para pihak yang terlibat dalam pembuatan kebijakan.

Dalam konteks hukum di Indonesia, penyadapan diatur melalui beragam peraturan perundang–undangan. Pengaturannya tersebar dari tingkat undang-undang hingga pada tingkat peraturan menteri. Oleh karena itu, mekanisme penyadapan dan jangka waktu dilakukannya penyadapan juga sangat beragam, tergantung pada upaya penegakan hukum untuk kejahatan apa dan aturan mana yang dirujuk. Saat ini terdapat setidaknya 20 peraturan perundang-undangan di Indonesia yang mengatur mengenai penyadapan, yaitu di antaranya:

1. Undang-Undang Nomor 5 Tahun 1997 tentang Psikotropika;
2. Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi sebagaimana telah diubah dengan Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-Undang Nomor 31 Tahun 1999;
3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;

---

6 Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, 2009, hal 11.

7 Edmon Makarim, "Analisis terhadap Kontroversi Rancangan Peraturan Pemerintah tentang Cara Intersepsi yang Sesuai dengan Hukum (*Lawful Interception*)", *Jurnal Hukum dan Pembangunan*, tahun ke-40 Nomor 2, 2010, hal. 231.

4. Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan Kedua atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi;
5. Undang-Undang Nomor 18 Tahun 2003 tentang Advokat;
6. Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang;
7. Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika;
8. Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman;
9. Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
10. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara;
11. Undang-Undang Nomor 18 Tahun 2011 tentang Perubahan atas Undang-Undang Nomor 18 Tahun 2004 tentang Komisi Yudisial;
12. Undang-Undang Nomor 13 Tahun 2016 tentang Paten;
13. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
14. Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang;
15. Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Jasa Telekomunikasi;
16. Peraturan Presiden Nomor 50 Tahun 2011 tentang Tata Cara Pelaksanaan Kewenangan Pusat Pelaporan dan Analisis Transaksi Keuangan;
17. Peraturan Menteri Informasi dan Komunikasi Nomor 11/Per/M.Kominfo/02/2006 tentang Teknis Penyadapan terhadap Informasi;
18. Peraturan Menteri Informasi dan Komunikasi Nomor 1 Tahun 2008 tentang Perekaman Informasi untuk Pertahanan dan Keamanan Negara;
19. Peraturan Kepala Kepolisian Republik Indonesia Nomor 5 Tahun 2010 tentang Tata Cara Penyadapan pada Pusat Pemantauan Kepolisian Negara Republik Indonesia;
20. Standar Operasional Prosedur Komisi Pemberantasan Tindak Pidana Korupsi (KPK) tentang Penyadapan;

Ketidaktunggalan pengaturan hukum acara penyadapan di Indonesia membawa dampak yang sangat serius, yakni terbukanya ruang interpretasi di antara para aparat penegak hukum, yakni

kepolisian, kejaksaan, dan KPK misalnya yang pada akhirnya menimbulkan inkonsistensi dalam tataran pelaksanaan,[8] sehingga dalam hal ini juga menunjukkan adanya pelanggaran terhadap asas kepastian hukum dan persamaan di depan hukum (*equality before the law*).[9] Adapun ketentuan-ketentuan mengenai penyadapan sebagaimana tersebar dalam setidaknya 17 peraturan perundang-undangan yang berhasil dihimpun dapat diamati dari tabel perbandingan terhadap lima aspek berikut:[10]

Tabel 1: Pengaturan Mengenai 5 Materi Wajib dalam Penyadapan

No	Peraturan	Pengaturan Mengenai 5 Materi Wajib dalam Penyadapan				
		Otoritas resmi yang memberi izin	**Jaminan Jangka Waktu**	**Pembatasan Penanganan Materi Penyadapan**	**Pembatasan orang yang dapat mengakses**	**Ketersedian mekanisme komplain**
1.	Undang-Undang Nomor 5 Tahun 1997 tentang Psikotropika	Perintah tertulis Kepala Kepolisian Republik Indonesia atau pejabat yang ditunjuknya (Penjelasan Pasal 54)	30 hari, tidak ada pengaturan perpanjangan (Pasal 55 huruf c)	Pembicaraan melalui telepon dan/atau alat telekomunikasi elektronik lainnya yang dilakukan oleh orang yang dicurigai atau diduga keras membicarakan masalah yang berhubungan dengan tindak pidana psikotropika	Tidak ada	Tidak Ada
2.	Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi	Tidak ada	Tidak ada	Tidak ada	Tidak ada	Tidak Ada
3.	Undang-Undang	Tidak ada	Tidak ada	Tidak ada	Tidak ada	Tidak ada

[8] Reda Manthovani, *Penyadapan vs. Privasi*, PT Bhuana Ilmu Populer, Jakarta, 2015, hal. 101.
[9] *Ibid*., hal. 101-102.
[10] Erasmus A.T. Napitupulu dan Maidina Rahmawati, C*atatan Awal terhadap RUU Penyadapan versi Pusat Perancangan Undang-Undang Badan Keahlian DPR RI*, Institute for Criminal Justice Reform, Jakarta, 2018, hal. 8-14.

	Nomor 36 Tahun 1999 tentang Telekomunikasi					
4.	Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi	Tidak ada	Tidak ada	Tidak ada	Tidak ada	Tidak ada
5.	Undang-Undang Nomor 18 Tahun 2003 tentang Advokat	Tidak ada	Tidak ada	Tidak ada	Tidak ada	Tidak ada
6.	Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang	Izin tertulis Ketua Pengadilan Negeri (Pasal 31 ayat (2))	Paling lama 1 tahun, tidak ada pengaturan perpanjangan (Pasal 31 ayat (2))	Berdasarkan bukti permulaan yang cukup (Pasal 31 ayat (1))	Tidak ada	Tidak ada
7.	Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Diatur dalam undang-undang	Diatur dalam undang-undang	Harus dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lainnya yang kewenangan-nya ditetapkan berdasarkan undang-undang. (penjelasan Pasal 5)	Tidak ada	Tidak ada
8.	Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika	Izin tertulis Ketua Pengadilan Negeri (Pasal 77 ayat (2))	Selama 3 bulan dapat diperpanjang maksimal 3 bulan (Pasal	Berdasarkan bukti permulaan yang cukup (Pasal 77 ayat	Tidak ada	Tidak ada

			77 ayat (1) dan (3))	(1)). Dalam keadaan mendesak bisa tanpa izin Ketua Pengadilan Negeri, dalam jangka waktu 1x24 jam harus meminta izin Ketua Pengadilan Negeri (Pasal 78)		
9.	Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara	Atas perintah kepala Badan Intelijen Negara dengan penetapan pengadilan untuk penyadapan terhadap sasaran (Pasal 32)	Paling lama 6 bulan, dapat diperpanjang sesuai kebutuhannya dalam konteks penyadapan terhadap sasaran (Pasal 32)	Terkait dengan kegiatan tertentu yang mengancam keamanan nasional. Terdapat pembedaan antara penyadapan dengan penyadapan terdahap sasaran.	Hanya digunakan untuk kepentingan Intelijen dan tidak untuk dipublikasikan. (penjelasan Pasal 32)	Tidak ada
10.	Undang-Undang Nomor 18 Tahun 2011 tentang Perubahan Undang-Undang Nomor 18 Tahun 2004 tentang Komisi Yudisial	Tidak ada	Tidak ada	Komisi Yudisial dapat meminta aparat penegak hukum untuk melakukan penyadapan terhadap dugaan pelanggaran kode etik	Tidak ada	Tidak ada

				(pasal 20 ayat (3))		
11.	Peraturan Pemerintah Nomor 19 Tahun 2000 tentang Tim Gabungan Pemberantasan Tindak Pidana Korupsi	Tidak ada	Tidak ada	Tidak ada	Tidak ada	Tidak ada
12.	Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang	Penetapan Ketua Pengadilan Negeri (Pasal 31 ayat (2))	Paling lama 1 tahun, dapat diperpanjang 1 tahun Pasal 31 ayat (3)	Hasil penyadapan bersifat rahasia dan hanya digunakan untuk kepentingan penyidikan Tindak Pidana Terorisme (Pasal 31 ayat (4)	Hasil penyadapan wajib dilaporkan kepada atasan penyidik dan kementerian komunikasi (Pasal 31 ayat (5)	Tidak ada
13.	Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Jasa Telekomunikasi	Permintaan rekaman informasi atas permintaan tertulis Jaksa Agung dan/atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu (Pasal 87)	Tidak ada	Keperluan proses peradilan pidana (pasal 87)	Tidak ada	Tidak ada
14.	Peraturan Menteri	Tidak ada	Tidak ada	Berdasarkan	Terdapat Tim	Tidak ada

	Informasi dan komunikasi Nomor 11 Tahun 2006 tentang Teknis Penyadapan Terhadap Informasi			SOP aparat penegak hukum dan diberitahukan secara tertulis kepada Direktur Jendral Pos dan Komunikasi (Pasal 8 ayat (1))	Pengawas yang terdiri dari penegak hukum dan Direktur Jenderal Pos dan Komunikasi (Pasal 14 ayat (1)) Pasal 17 mengatur kerahasiaan dan larangan menyebarkan informasi penyadapan	
15.	Peraturan Menteri Informasi dan Komunikasi Nomor 1 Tahun 2008 tentang Perekaman Informasi untuk Pertahanan dan Keamanan Negara	Atas permintaan Badan Intelijen Negara kepada penyelenggara telekomunikasi dengan tembusan kepada Menteri (Pasal 5)	Dibebaskan untuk masa waktu tertentu yang dimohonkan (Pasal 89 ayat (1))	Untuk kepentingan pertahanan dan keamanan negara (Pasal 3) Dilaksanakan berdasarkan Standar Operasional Prosedur ("SOP") yang ditetapkan oleh Badan Intelijen Negara sesuai karakteristik kepentingan-nya. (Pasal 9 ayat (1)	Mengatur kerahasiaan dan larangan menyebarkan informasi penyadapan (Pasal 13)	Tidak ada
16.	Peraturan Kepala Kepolisian Republik Indonesia Nomor 5 Tahun 2010 tentang Tata Cara	Kepala Badan Reserse Kriminal (Kabareskrim) Polri ditunjuk oleh Kapolri sebagai	Paling lama 30 hari bisa diperpanjang. Perpanjangan disesuaikan dengan kebutuhan	Hasil penyadapan yang tidak berkaitan dengan pembuktian harus	Mengatur kerahasiaan dan larangan menyebarkan informasi penyadapan (Pasal 21)	Tidak ada

	Penyadapan pada Pusat Pemantauan Kepolisian Negara Republik Indonesia	pejabat yang memberikan izin dimulainya operasi penyadapan. (Pasal 5 ayat (1))	(Pasal 11)	dimusnahkan (Pasal 20)		
17.	Standar Oprasional Prosedur Komisi Pemberantasan Tindak Pidana Korupsi (KPK)	Bersifat rahasia	Bersifat rahasia	Bersifat rahasia	Bersifat rahasia	Bersifat rahasia

Selain dihadapkan dengan masalah beragamnya pengaturan, hukum acara penyadapan di Indonesia juga bermasalah karena telah gagal untuk melindungi pihak-pihak yang berpotensi dirugikan atas tindakan penyadapan yang dilakukan secara sewenang-wenang. Pihak yang menjadi target penyadapan tidak dapat mempertanyakan keabsahan dari prosedural penyadapan yang dikenakan pada dirinya. Kemudian, hasil dari penyadapan yang dijadikan bukti di pengadilan juga sama sekali tidak bisa digugat keberadaannya, karena tidak ada kesatuan mekanisme yang mengaturnya secara jelas dan tegas.

Mahkamah Konstitusi mulai mencoba membenahi persoalan-persoalan yang muncul akibat ketidaktunggalan pengaturan penyadapan tersebut melalui Putusan Nomor 5/PUU-VIII/2010 tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap UUD 1945. Putusan tersebut mengamanatkan untuk membentuk satu aturan tunggal tentang mekanisme dan prosedur penyadapan yang berbentuk undang-undang.[11] Aturan tunggal yang dimaksud setidaknya harus memuat ketentuan-ketentuan mengenai hal-hal berikut:[12]

1) adanya otoritas resmi yang ditunjuk dalam undang-undang seperti atasan atau hakim untuk memberikan izin atau wewenang untuk melakukan, memerintahkan maupun meminta penyadapan;
2) kategori subjek hukum yang diberi wewenang untuk melakukan penyadapan;
3) tujuan penyadapan secara spesifik;

[11] Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap UUD 1945, hal. 61-62.

[12] Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap UUD 1945, hal. 69-70.

4) tata cara penyadapan;
5) adanya jaminan jangka waktu yang pasti dalam melakukan penyadapan;
6) pembatasan penanganan materi hasil penyadapan;
7) pembatasan mengenai orang yang dapat mengakses penyadapan; dan
8) pengawasan terhadap penyadapan.

Selain itu, Pengadilan HAM Eropa juga telah memberikan standar minimum perlindungan yang harus tertuang dalam hukum nasional negara-negara anggotanya terkait pengaturan untuk tindakan-tindakan pengintaian secara rahasia (*secret measures of surveillance*) termasuk dalam hal ini adalah penyadapan. Dalam salah satu putusannya pada 2016, Pengadilan HAM Eropa menyebutkan bahwa negara wajib mengatur hal-hal terkait tata cara penyadapan berikut untuk menghindari penyalagunaan wewenang:[13]

1) sifat tindak pidana yang dapat menimbulkan perintah penyadapan;
2) kategori orang-orang yang dimungkinkan untuk dilakukan penyadapan terhadapnya (target penyadapan);
3) batas waktu penyadapan;
4) prosedur yang harus diikuti untuk memeriksa, menggunakan, dan menyimpan data hasil penyadapan diperoleh;
5) tindakan pencegahan yang harus diambil saat menyerahkan data ke pihak atau otoritas yang lain; dan
6) keadaan di mana rekaman (data hasil penyadapan) dapat atau harus dihapus atau dimusnahkan.

Masing-masing isu tersebut di atas kemudian dapat dikelompokkan dalam enam aspek pokok yang perlu diatur dalam mekanisme atau tata cara penyadapan. Keenam aspek pokok tersebut akan menjadi lingkup penelitian ini, yaitu: (a) proses pemberian ijin dan pelaksanaan penyadapan, (b) persyaratan penyadapan, (c) durasi penyadapan, (e) penanganan data hasil penyadapan, (f) mekanisme pengawasan dalam upaya paksa penyadapan, dan (f) mekanisme permohonan keberatan atau komplain terhadap upaya paksa penyadapan.

Selain itu, sebagaimana diketahui bahwa pada prinsipnya penyadapan merupakan suatu bentuk pembatasan terhadap hak atas privasi, maka pengaturan mengenai penyadapan harus memiliki

[13] European Court of Human Rights Case of Szabó and Vissy v. Hungary Application no. 37138/14 (2016), para 56.

standar perlindungan yang ketat terhadap pembatasan hak atas privasi tersebut. Hal ini penting setidaknya untuk mencapai beberapa tujuan berikut: (a) menjamin agar pembatasan hak atas privasi tidak berlebihan, (b) menghindari dampak penyadapan yang dilakukan secara sewenang-wenang dan melawan hukum, dan (c) menguatkan sistem akuntabilitas dalam penegakan hukum, (d) menghindari legislasi yang hanya bersifat birokratis dalam pengaturan penyadapan. Oleh karena itu, salah satu isu utama yang akan didiskusikan adalah mengenai pembentukan mekanisme perlindungan terhadap pembatasan hak atas privasi dalam upaya paksa penyadapan yang dapat diterapkan melalui ketentuan-ketentuan terkait tujuh aspek yang menjadi lingkup penelitian sebagaimana disebutkan di atas.

Selain itu, berangkat dari Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010, DPR telah mulai menginisiasi pembahasan Rancangan Undang-Undang tentang Penyadapan melalui Badan Legislasi (Baleg). Pembahasan RUU Penyadapan tersebut telah masuk Prolegnas Prioritas sejak 2018 dan berlanjut masuk pada *long list* Prolegnas 2020-2024.[14] Oleh karena itu, penelitian ini diharapkan dapat berkontribusi dalam hal pemberian masukan terkait gambaran pengaturan terkait upaya paksa penyadapan yang sesuai dengan prinsip-prinsip HAM dan yang mempunyai sistem akuntabilitas kuat.

1.2. Pertanyaan Penelitian

Penelitian ini akan mencoba menjawab dua pertanyaan berikut:

1. Bagaimana konsep pembatasan terhadap hak atas privasi pada penyadapan yang dilakukan dalam rangka kepentingan penegakan hukum?
2. Bagaimana mekanisme perlindungan terhadap hak atas privasi dalam upaya paksa penyadapan terkait enam aspek berikut: (a) proses pemberian ijin dan pelaksanaan penyadapan, (b) persyaratan penyadapan, (c) durasi penyadapan, (e) penanganan data hasil penyadapan, (f) mekanisme pengawasan dalam upaya paksa penyadapan, dan (f) mekanisme permohonan keberatan atau komplain terhadap upaya paksa penyadapan?

1.3. Tujuan Penelitian

[14] Dewan Perwakilan Rakyat, *Program Legislasi Nasional 2020-2024*, http://www.dpr.go.id/uu/prolegnas-long-list, diakses pada 5 Januari 2020.

Berdasarkan pertanyaan penelitian di atas, maka penelitian ini mempunyai dua tujuan sebagai berikut:

1. Meninjau konsep pembatasan terhadap hak atas privasi pada penyadapan yang dilakukan dalam rangka kepentingan penegakan hukum.
2. Membentuk mekanisme perlindungan terhadap hak atas privasi dalam upaya paksa penyadapan terkait enam aspek berikut: (a) proses pemberian ijin dan pelaksanaan penyadapan, (b) persyaratan penyadapan, (c) durasi penyadapan, (e) penanganan data hasil penyadapan, (f) mekanisme pengawasan dalam upaya paksa penyadapan, dan (f) mekanisme permohonan keberatan atau komplain terhadap upaya paksa penyadapan.

1.4. Metode Penelitian

Penelitian ini hanya akan menggunakan metode *desk-review* atau peninjauan pustaka. Data yang digunakan antara lain dokumen hukum seperti peraturan perundang-undangan, laporan praktik-praktik penyadapan dari berbagai negara, maupun jurnal-jurnal akademis yang terkait dengan pengaturan penyadapan. Oleh karena penelitian ini menerapkan pendekatan HAM, maka berbagai instrumen HAM internasional maupun regional termasuk *case law* dari Pengadilan HAM Eropa (*European Court of Human Rights* - ECtHR) yang berkaitan dengan aspek-aspek pokok penyadapan yang masuk dalam lingkup penelitian ini juga akan dijadikan sebagai referensi tambahan. Penelitian ini juga akan secara spesifik merujuk pada praktik-praktik negara lain, seperti Inggris, Amerika, dan Australia dalam mengatur penyadapan pada hukum nasional masing-masing negara tersebut.

1.5. Kerangka Penelitian

Penelitian ini tersusun atas empat bab. Bab Pertama berisi pendahuluan yang terdiri dari latar belakang masalah penyadapan dalam kerangka hukum nasional Indonesia dan diikuti dengan pernyataan penelitian, tujuan penelitian, metode penelitian, dan kerangka penelitian secara berurutan. Bab Kedua membahas mengenai konsep penyadapan sebagai bentuk dari upaya paksa yang ditinjau melalui pendekatan hak asasi manusia. Dalam bab ini akan dibahas sedikit pengantar mengenai hak atas privasi serta ulasan mengenai bagaimana penyadapan dilihat sebagai bentuk pembatasan terhadap hak atas privasi.

Bab Ketiga akan menjelaskan mengenai mekanisme perlidungan terhadap hak atas privasi dalam pelaksanaan upaya paksa penyadapan. Bab ini memaparkan secara mendalam mengenai aspek-

aspek yang perlu diperhatikan dalam mengatur penyadapan agar pembatasan terhadap hak atas privasi tidak dilakukan secara berlebihan. Adapun aspek-aspek tersebut terdiri dari proses pemberian ijin, penentuan persyaratan penyadapan, durasi penyadapan, penanganan data hasil penyadapan, mekanisme pengawasan, hingga mekanisme permohonan keberatan. Bab terakhir yakni bab keempat berisi poin-poin simpulan dan rekomendasi yang disaring dari uraian dalam Bab II dan Bab III. Pada bagian akhir penelitian terdapat pula daftar literatur yang digunakan menjadi rujukan penulisan penelitian ini yang terdiri dari buku, jurnal, laporan lembaga, peraturan/kaidan hukum nasional maupun internasional, hingga putusan pengadilan.

BAB II

Peninjauan Konsep Upaya Paksa Penyadapan Melalui Pendekatan Hak Asasi Manusia

Dalam menyusun pengaturan mengenai penyadapan, upaya penyeimbangan terhadap berbagai kepentingan yang terlibat dalam prosesnya mutlak tidak dapat dihindari. Penyadapan sebagai bentuk upaya hukum mengindikasikan dua kepentingan yang sama-sama harus diperhatikan, yaitu kepentingan individu terkait hak atas privasinya serta kepentingan masyarakat umum dalam hal mencegah dan menanggulangi kejahatan dan menjaga keteraturan sosial melalui penegakan hukum. Melalui bab ini, upaya untuk menyeimbangkan dua kepentingan tersebut akan dibahas secara mendalam dengan melihat konsep-konsep dasar yang ditinjau dari pengaturan hukum internasional, yurisprudensi kasus-kasus terkait, serta pengaturan hukum nasional.

2.1. Konsep Hak atas Privasi

Dalam kerangka hukum Indonesia, terdapat tiga instrumen hukum yang menjamin adanya hak atas privasi bagi setiap warga negara, yakni Undang-Undang Dasar 1945 (UUD 1945), Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM), dan Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) yang telah diratifikasi Indonesia melalui Undang-Undang Nomor 12 tahun 2005. Meskipun hak atas privasi hanya dapat dimaknai secara implisit dalam UUD 1945, setidaknya melalui Pasal 28G ayat (1) negara telah mengakui bahwa perlindungan terhadap diri pribadi seseorang dan hak atas rasa aman perlu dijamin supaya mereka bebas dari ketakukan untuk melakukan maupun tidak melakukan sesuatu yang pada dasarnya merupakan hak asasi. Pengakuan terhadap hak atas privasi baru secara tegas dituangkan dalam UU HAM khususnya Pasal 32 yang menyatakan bahwa:

> "*Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundangan*."

Kemudian, dalam kerangka hukum internasional, hak atas privasi salah satunya dijamin dalam ICCPR khususnya Pasal 17 ayat (1) dan (2) yang berbunyi sebagai berikut:

> 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.*
>
> (Terjemahan)

1) Tidak ada seorang pun yang privasi, keluarga, kediaman, atau korespondensinya dapat diintrusi secara sewenang-wenang atau secara tidak sah, maupun diserang kehormatan dan reputasinya secara tidak sah.
2) Setiap orang memiliki hak untuk mendapatkan perlindungan hukum terhadap intrusi atau serangan yang dimaksud tersebut.

Ketentuan tersebut secara tegas melarang segala bentuk intrusi yang dilakukan secara sewenang-wenang atau melawan hukum terhadap privasi seseorang termasuk korespondensinya. Negara harus menjamin adanya perlindungan hukum terhadap pelanggaran hak privasi tersebut. Oleh karenanya, lebih lanjut dalam General Comment No. 16 Pasal 17 ICCPR (HRI/GEN/1/Rev.9 (Vol. I)) tepatnya pada paragraf 8 kemudian ditegaskan bahwa segala bentuk pengintaian baik yang bersifat elektronik maupun bukan, penyadapan atau pengintaian terhadap komunikasi, hingga merekam pembicaraan harus dilarang (*"Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited*").

Perlindungan hak atas privasi dalam ICCPR yang berlaku sejak tahun 1976 tersebut diadopsi dari Pasal 12 Deklarasi Umum PBB tentang Hak Asas Manusia (DUHAM PBB) yang sebelumnya dikeluarkan tahun 1948. Konsep perlindungan terhadap hak atas privasi yang diusung oleh DUHAM PBB memang sangat berpengaruh terhadap perkembangan instrumen-instrumen HAM lainnya termasuk dalam tingkat regional seperti di Eropa. Misalnya, Konvensi Eropa tentang Hak Asasi Manusia (*the European Convention on Human Rights* - ECHR) tahun 1950 juga mengakomodir penghormatan terhadap hak atas kehidupan pribadi, kediaman, serta korespondensi seseorang yang dituangkan dalam ketentuan Pasal 8.

Perlindungan serupa terhadap hak atas privasi juga ditemukan dalam *the Charter of Fundamental Rights of the European Union* (Charter Uni Eropa) yang mulai mengikat secara efektif sejak tahun 2009. Selain menjamin penghormatan terhadap hak atas kehidupan pribadi dan keluarga, kediaman, dan komunikasi melalui Pasal 7, Charter Uni Eropa juga secara tersendiri menjamin adanya hak atas perlindungan terhadap data pribadi pada Pasal 8 yang berbunyi sebagai berikut:

Article 8
Protection of personal data

1) *Everyone has the right to the protection of personal data concerning him or her.*
2) *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3) *Compliance with these rules shall be subject to control by an independent authority.*

(Terjemahan)

1) Setiap orang memilikki hak untuk mendapatkan perlindungan terhadap data pribadinya.
2) Data pribadi tersebut harus dikelola dengan hati-hati untuk tujuan-tujuan tertentu berdasarkan persetujuan orang yang bersangkutan atau berdasarkan tujuan-tujuan yang sah yang diatur dalam peraturan perundangan. Setiap orang memiliki hak untuk mengakses data yang dikumpulkan terkait dirinya dan memiliki hak untuk melakukan koreksi terhadapnya.
3) Kepatuhan terhadap pemenuhan peraturan ini diawasi oleh sebuah badan independen.

Dengan demikian, Charter Uni Eropa memberikan standar pelindungan HAM yang lebih tinggi daripada instrumen HAM yang lain misalnya seperti ECHR. Hak atas perlindungan data pribadi pada umumnya masuk dalam kategori hak atas privasi yang diakomodir melalui penghormatan terhadap kehidupan pribadi dan keluarga, kediaman, serta korespondensi. Dengan menyebutkan secara eksplisit melalui pasal yang terpisah, Charter Uni Eropa dengan demikian seolah-olah dengan sengaja memberikan penekanan atas pentingnya perlindungan terhadap data pribadi sehingga meningkatkan standar perlindungan terhadap hak atas privasi.

Selain itu, Uni Eropa melalui *Directive on Privacy and Electronic Communications (*Directive Nomor 2002/58/EC yang kemudian diamandemen oleh Directive Nomor 2009/136/EC) dan *Data Protection Directive* Nomor 95/46/EC juga memberikan pedoman umum yang sekaligus memberikan standar perlindungan terhadap hak atas privasi bagi negara anggotanya dalam membuat peraturan mengenai penyimpanan data telekomunikasi yang pada prinsipnya bersifat rahasia. Sifat rahasia dari komunikasi elektronik tidak hanya terbatas pada konten komunikasi tersebut tetapi juga pada lalu lintas data, seperti informasi tentang siapa berkomunikasi dengan siapa, kapan dan berapa lama, serta lokasi data seperti dari mana asal data tersebut ketika dalam proses komunikasi.[15]

Dari uraian di atas dapat disimpulkan bahwa konsep hak atas privasi meiliputi hal-hal yang sangatlah luas. Hak atas privasi umumnya dapat melekat pada proses komunikasi hingga pengelolaan data pribadi seseorang. Oleh karenanya, seluruh bentuk intrusi ke dalam wilayah

[15] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Publications Office of the European Union, Luxembourg, 2014, hal. 166.

privat seseorang misalnya dalam percakapan, persuratan, hingga tempat kediamannya merupakan bentuk-bentuk pelanggaran terhadap hak atas privasi.

2.2. Penyadapan Sebagai Bentuk Pembatasan terhadap Hak atas Privasi

2.2.1. Konsep Pembatasan terhadap Hak atas Privasi

Sebagaimana dijelaskan di atas, dalam kerangka hukum di Indonesia hak atas privasi dijamin perlindungannya baik melalui hukum nasional, yaitu UUD 1945 dan UU HAM maupun melalui instrumen hukum internasional seperti DUHAM PBB dan ICCPR. Namun demikian, perlindungan terhadap hak atas privasi tidak sepenuhnya mutlak karena masih dapat dibatasi oleh hal-hal tertentu yang juga diatur dalam hukum-hukum tersebut.

Dalam UUD 1945 misalnya, Pasal 28J ayat (2) menyatakan bahwa:

> '*Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang 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, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis'.*

Kemudian UU HAM juga mengatur pembatasan hak serupa dalam beberapa pasal-pasal berikut, seperti Pasal 70 yang bunyinya sama dengan Pasal 28J ayat (2) UUD 1945 di atas serta Pasal 73 yang pada intinya menyatakan bahwa pembatasan hak dan kebebasan orang lain dilakukan untuk menjamin pengakuan dan penghormatan terhadap hak asasi manusia serta kebebasan dasar orang lain, kesusilaan, ketertiban umum, dan kepentingan bangsa.

Ketentuan mengenai pembatasan hak atas privasi juga kemudian dapat ditemui secara lebih rinci dalam General Comment No. 16 Pasal 17 ICCPR (HRI/GEN/1/Rev.9 (Vol. I)). Penggunaan kata-kata "*unlawful*" (melawan hukum) dan "*arbitrary interferences*" (intrusi yang sewenang-wenang) dalam Pasal 17 ICCPR untuk merujuk pelanggaran terhadap hak atas privasi sebenarnya mengindikasikan bahwa terhadap hak atas privasi pun dapat dilakukan pembatasan yakni sepanjang tindakan intrusi dilakukan dengan cara-cara yang sah secara hukum (*lawful*) dan memang diperlukan dalam keadaan-keadaan tertentu.[16] Legislasi yang mengatur mengenai intrusi yang diperbolehkan

[16] General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) of the International Covenant on Civil and Political Rights (HRI/GEN/1/Rev.9 (Vol. I)), poin 3 dan 4.

terhadap hak atas privasi harus memuat batasan-batasan yang jelas dalam situasi dan kondisi seperti apa hal tersebut dapat diterapkan.[17] Kemudian, otoritas yang mengijinkan tindakan intrusi tersebut juga harus diatur dalam peraturan perundangan.[18] Terakhir, upaya penegakan hukum terhadap insiden terjadinya intrusi yang melawan hukum dan sewenang-wenang, termasuk mekanisme pemulihan bagi yang dirugikan atas insiden tersebut misalnya dengan mengajukan keberatan dan tuntutan ganti rugi, juga harus tersedia sebagai bagian dari mekanisme perlindungan terhadap hak atas privasi.[19]

Selain itu, konsep perlindungan hak atas privasi juga dapat dimaknai dari kerangka hukum internasional yang bersifat regional seperti ditemui di Eropa misalnya, melalui Konvensi Eropa tentang HAM (ECHR), Charter Uni Eropa, beserta legislasi turunannya (*Directive*). Dalam ECHR khususnya Pasal 8 ayat (2) juga menegaskan bahwa negara dilarang melakukan intrusi terhadap hak atas kehidupan pribadi kecuali hanya dalam beberapa hal berikut: jika interferensi tersebut diatur oleh hukum dan memang dibutuhkan dalam kehidupan masyarakat yang demokratis demi keamanan negara dan masyarakat, kesejahteraan ekonomi negara, mencegah kejahatan atau ketidakteraturan, perlindungan terhadap kesehatan dan moral, serta perlindungan terhadap hak dan kebebasan orang lain. Dari ketentuan tersebut dapat ditarik kesimpulan bahwa terdapat tiga bentuk justifikasi yang dapat membatasi pemenuhan hak atas privasi, yaitu (a) penerapannya harus sesuai dengan hukum yang berlaku, (b) dilakukan untuk kepentingan atau tujuan yang sah, dan (c) diperlukan dalam kehidupan masyarakat yang demokratis.

2.2.2. Pengertian Penyadapan

Salah satu bentuk pembatasan terhadap hak atas privasi adalah dilakukannya upaya paksa khusus berupa penyadapan. Penyadapan dapat dikatakan sebagai upaya paksa yang bersifat khusus sebab berbeda dengan jenis-jenis upaya paksa lain seperti penggeledahan dan penyitaan, upaya paksa penyadapan memang tidak dilakukan secara fisik, terlihat, dan terasa namun intrusi atau penerobosan terhadap zona privasi seseorang tetap terjadi yakni melalui pengintaian secara

---

17 General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) of the International Covenant on Civil and Political Rights (HRI/GEN/1/Rev.9 (Vol. I)), para 8.

18 *Ibid.*

19 General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) of the International Covenant on Civil and Political Rights (HRI/GEN/1/Rev.9 (Vol. I)), para 6.

rahasia (*secret surveillance*) terhadap komunikasinya.[20] Istilah yang digunakan dalam bahasa Inggris untuk merujuk tindakan penyadapan juga beragam di antaranya: *interception*, *wiretapping*, *eavesdropping*, dan *electronic surveillance* yang pada dasarnya memiliki makna yang sama dengan letak pembeda yang hanya pada teknis pelaksanaan maupun alat atau teknologi yang digunakan.[21]

Hasil dari kegiatan penyadapan dapat berupa rekaman percakapan, rekaman video, maupun bentuk elektronik lainnya yang kemudian dapat dijadikan sebagai alat bukti untuk kepentingan proses sidang pembuktian di pengadilan.[22] Meskipun demikian perlu dicermati pula bahwa hasil dari tindakan penyadapan tidak selalu berakhir menjadi alat bukti di persidangan. Seperti praktik di Inggris misalnya, penyadapan faktanya lebih banyak digunakan hanya untuk kepentingan pengumpulan informasi yang mana dari informasi tersebut kemudian dimanfaatkan untuk mencari bukti-bukti yang akan diajukan ke persidangan.[23] Namun, apabila hasil dari penyadapan secara langsung akan digunakan sebagai alat bukti yang sah (*admissible*) dalam persidangan, maka seluruh rangkaian kegiatan penyadapan harus memenuhi standar prinsip-prinsip tertentu seperti *legality, legitimate aim, necessity, proportionality,* dan *due process.*[24]

Definisi penyadapan tersebar dalam setidaknya empat undang-undang berikut: (a) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), (b) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), (c) Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika (UU Narkotika), dan (d) Undang-Undang nomor 17 tahun 2011 tentang Intelijen Negara (UU Intelijen Negara). Dalam UU ITE khususnya pada penjelasan Pasal 31 ayat (1) dinyatakan bahwa:

> *"Yang dimaksud dengan 'Intersepsi atau penyadapan' adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi."*

Di sisi lain, UU Intelijen Negara mengadopsi konsep penyadapan yang lebih luas daripada UU ITE karena selain menyebutkan definisi yang sama persis dengan bunyi ketentuan di atas, terdapat pula

---

20 Reda Manthovani, *Op. Cit.,* hal. 231-232.
21 Reda Manthovani, *Op. Cit.,* hal 21-22.
22 Reda Manthovani, *Op. Cit.,* hal. 66.
23 Reda Manthovani, *Op. Cit.,* hal. 259-260.
24 Reda Manthovani, *Op. Cit.,* hal. 66.

penambahan klasula "*termasuk memeriksa paket, pos, surat-menyurat, dan dokumen lain*" dalam Pasal 32 ayat (1).

Berbeda dengan definisi yang diadopsi pada dua undang-undang di atas, definisi penyadapan yang tertera dalam UU Telekomonikasi lebih menekankan pada pemasangan alat penyadapan yang dilakukan dalam rangka mendapatkan informasi secara tidak sah.[25] Kemudian, UU Narkotika juga memberikan penekanan yang berbeda mengenai konsep penyadapan yang dilaksanakan untuk penegakan hukum, dengan menyatakan sebagai berikut:[26]

> "*Penyadapan adalah kegiatan atau serangkaian kegiatan penyelidikan atau penyidikan dengan cara menyadap pembicaraan, pesan, informasi, dan/atau jaringan komunikasi yang dilakukan melalui telepon dan/atau alat komunikasi elektronik lainnya."*

Konsep penyadapan berdasarkan pengertian yang diberikan oleh beberapa undang-undang di atas memang terlihat sangat luas, sebab penyadapan dapat dimaknai sebagai tindakan mencuri dengar, merekam, dan mengambil segala bentuk informasi dengan teknik yang juga tidak terbatas dalam jaringan telekomunikasi. Ide untuk merumuskan konsep penyadapan yang limitatif kemudian sempat muncul dalam rangka untuk memperkuat perlindungan terhadap hak atas privasi, salah satunya misalnya dengan membatasi lingkup penyadapan yang sah (*lawful interception*) hanya untuk telekomunikasi suara.[27] Bentuk-bentuk telekomunikasi lainnya tidak perlu masuk dalam pengertian telekomunikasi yang bisa disadap sehingga hal ini dapat membatasi lingkup obyek penyadapan yang mana dapat menjadi salah satu indikator untuk memperkuat perlindungan hak atas privasi.[28] Namun sejalan dengan perkembangan teknologi yang sangat pesat, pembatasan semacam itu tidak lagi relevan karena penyadapan sangat mungkin dilakukan dengan menggunakan alat-alat yang jangkauannya sangat luas melalui medium yang beragam. Sehingga bentuk-bentuk informasi yang terkumpul tidak dapat hanya dibatasi pada bentuk suara namun juga dimungkinkan dalam bentuk gambar, tulisan, dan lain-lain.

Adapun jenis-jenis jangkauan dari pengintaian terhadap komunikasi antara lain: (a) bersifat individual yang hanya menargetkan pada orang-orang tertentu (*targeted use of offensive*

---

25 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Penjelasan Pasal 40 yang berbunyi sebagai berikut: "*Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah*."

26 Pasal 1 angka 19 Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika.

27 Bert-Jaap Koops, "The Shifting Balance between Criminal Investigation and Privacy: A Case Study of Communications Interception Law in the Netherlands", *Jurnal Information, Communication & Society* Volume 6 Nomor 3, 2018, hal. 379-402.

28 *Ibid.*

technology), (b) bersifat menargetkan orang-orang dalam lingkup tertentu (*targeted and semi-targeted use of mobile phone surveillance*), serta (c) yang bersifat masal yang mencakup jaringan secara luas (*mass surveillance of network activity)*. Umumnya, upaya paksa penyadapan dilakukan melalui dua tipe jangkauan di atas, namun berdasarkan perkembangan teknologi saat ini, penyadapan mungkin pula dilakukan melalui jenis jangkauan ketiga dan ironinya hanya sedikit negara-negara yang mengatur penerapannya dengan jelas.[29]

Dalam merumuskan konsep penyadapan terhadap komunikasi seseorang dengan orang yang lain, jenis-jenis komunikasi yang masuk dalam jangkauan penyadapan tersebut perlu diidentifikasi terlebih dahulu. Misalnya, konsep penyadapan terhadap komunikasi di Amerika dapat dirumuskan dalam tiga jenis komunikasi, yaitu komunikasi melalui kabel, komunikasi lisan atau secara langsung, dan komunikasi elektronik. Komunikasi lisan dapat diindikasikan terjadi melalui pertemuan tatap muka. Kemudian komunikasi melalui kabel mencakup setiap pemindahan yang melibatkan telinga (*aural transfer*) yang dilakukan seluruhnya atau sebagian melalui penggunaan fasilitas untuk transmisi komunikasi dengan bantuan kawat, kabel, atau koneksi sejenis lainnya. Komunikasi melaui kabel tersebut harus mensyaratkan adanya unsur "*aural*", atau diucapkan oleh manusia, dan harus ditransmisikan setidaknya sebagian oleh kabel. Sedangkan yang dimaksud dengan komunikasi elektronik adalah setiap pemindahan tanda, sinyal, tulisan, gambar, suara, data, atau segala bentuk intelijen (*intelligence of any nature*) yang ditransmisikan secara keseluruhan atau sebagian oleh kabel, radio, sistem elektromagnetik, sistem *photoelectronic,* atau sistem *photooptical* yang tidak termasuk dalam komunikasi kabel atau lisan. Dalam perkembangannya, konsep penyadapan di Amerika ini selain diterapkan untuk komunikasi suara, namun juga dapat berlaku untuk intersepsi data. Akan tetapi, Undang-Undang Penyadapan (*Wiretap Act*) hanya berlaku untuk data yang disadap bersamaan melalui transmisi.[30]

Pengadilan HAM Eropa (ECtHR) dengan tegas menyatakan dalam beberapa putusannya bahwa melakukan penyadapan terhadap percakapan di telepon telah melanggar prinsip penghormatan terhadap hak atas kehidupan pribadi, termasuk pula sebagai bentuk interferensi adalah melakukan

---

29 Gus Hosein dan Caroline Wilson Palwo, "*Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*", *Ohio State Law Journal*, Volume 76 Nomor 6, 2013, hal. 1071-1104.

30 Emily Miskel, *Illegal Evidence: Wiretapping, Hacking, and Data Interception Laws*, State Bar of Texas, Sex, Drugs, & Surveillance, Chapter 12, 2014, hal. 2-3.

perekaman percakapan tersebut, melakukan '*metering*',[31] hingga melakukan registrasi terhadap meta-data dari komunikasi tersebut.[32] Di Jerman, bentuk penyadapan dalam arti intersepsi terhadap telepon dapat dibedakan menjadi dua macam, yaitu: (a) penyadapan secara individual yang menargetkan pada orang atau grup tertentu atau yang bertujuan untuk melakukan intersepsi terhadap komunikasi dari dan pada telepon atau lingkungan kediaman atau bangunan tertentu; dan (b) penyadapan secara strategis dengan melakukan intersepsi pada banyak komunikasi untuk mencari kata kunci atau frasa tertentu.[33]

Kemudian di Australia, intersepsi terhadap komunikasi pada sistem telekomunikasi dimaknai sebagai bentuk merekam dan/atau mendengarkan komunikasi dengan cara apapun ketika komunikasi itu berlangsung tanpa diketahui oleh orang-orang yang sedang melakukan komunikasi tersebut.[34] Lain halnya di Jerman, lingkup penyadapan masuk dalam kategori *monitoring* (pengintaian) terhadap telekomunikasi nirkabel, yaitu telekomunikasi yang tidak melalui saluran telepon secara langsung akan tetapi misalnya melalui koneksi satelit *(Überwachung nicht leitungsgebundener Fernmeldeverkehrsbeziehungen*), dan terhadap persuratan.[35]

2.2.3. Justifikasi terhadap Pembatasan Hak atas Privasi dalam Upaya Paksa Penyadapan

Selain digunakan sebagai bentuk upaya paksa untuk kepentingan penegakan hukum, tindakan penyadapan juga dibenarkan untuk kepentingan intelijen dalam rangka melindungi keamanan nasional. Sedangkan kegiatan penyadapan yang dilakukan diluar kedua konteks tersebut merupakan tindak pidana berdasarkan ketentuan Pasal 430 ayat (2) KUHP, Pasal 40 UU 36/1999 tentang Telekomunikasi, dan Pasal 31 ayat (1) dan (2) UU ITE. Adanya ketentuan pidana tersebut menandakan bahwa pada prinsipnya, penyadapan merupakan tindakan yang terlarang karena melanggar hak atas privasi seseorang dalam berkomunikasi yang dijamin oleh konstitusi dan

---

31 Lingkup *metering* yang termasuk dalam bentuk pelanggaran terhadap Pasal 8 ECHR tentang hak atas kehidupan pribadi dapat dilihat dari European Court of Human Rights Case of Malone v. United Kingdom Application no. 8691/79 (1984) berikut:
"The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8." (para 84)

32 European Court of Human Rights Case of Liberty and Others v. United Kingdom Application no. 58243/00 (2008), para 63.

33 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 3.

34 Telecommunications (Interception and Access) Act 1979, Pasal 6.

35 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 1 ayat (1) angka 1 dan 2 dan Pasal 3 ayat (1).

undang-undang turunannya. Namun, oleh karena hak atas privasi merupakan *derogable rights* atau jenis hak-hak yang memang dapat dibatasi, maka terhadapnya dapat diberikan pengecualian yakni untuk konteks penyadapan terbatas hanya dapat dilakukan dalam rangka penegakan hukum dan pelindungan keamanan nasional.

Penekanan terhadap pembatasan hak atas privasi perlu mendapatkan justifikasi yang kuat khususnya dalam legislasi yang mengatur pembatasan tersebut. Dalam hal untuk mencapai keseimbangan antara perlindungan hak atas privasi dan kepentingan penegakan hukum, perlu penjelasan yang kuat mengapa kewenangan dalam melakukan penyidikan perlu diperluas dengan cara membatasi privasi warga negara seperti yang terjadi dalam upaya paksa penyadapan. Hal ini sangat penting untuk dipertimbangkan karena pembatasan privasi warga negara tidak selalu menjamin adanya tingkat keamanan yang kuat dalam jangka waktu yang lama.[36]

Sejauh mana pembatasan hak atas privasi diperbolehkan dalam konteks upaya paksa penyadapan dapat diatur melalui perumusan justifikasi-justifikasi dalam situasi seperti apa upaya paksa penyadapan dapat dilakukan. Berdasarkan standar perlindungan yang diterapkan di Eropa misalnya dalam konteks penyadapan, terdapat tiga bentuk justifikasi yang akan dijabarkan sebagai berikut.

a. Penerapan yang sesuai dengan hukum yang berlaku mengindikasikan bahwa pengaturan penyadapan harus telah diatur sebelumnya melalui peraturan perundang-undangan yang dapat diakses oleh publik.[37] Pengaturan penyadapan tersebut meliputi seluruh bentuk peraturan yang mengatur mengenai pelaksanaan penyadapan, baik pada level undang-undang hingga peraturan teknis harus dapat diakses oleh publik. Standar ini diterapkan oleh Pengadilan HAM Eropa yang menyatakan pemerintah Inggris melanggar Pasal 8 ECHR dengan tidak menyediakan dokumen pedoman internal pelaksanaan penyadapan secara masal (*internal guidelines and instructions* on *mass surveillance of telecommunication*) kepada publik sehingga warga Inggris tidak dapat memperkirakan sejauh mana bentuk pengintaian terhadap telekomunikasi tersebut dilakukan terhadap mereka.[38]

---

36 Bert-Jaap Koops, *Loc. Cit*.

37 European Court of Human Rights Case of Malone v. United Kingdom Application no. 8691/79 (1984), para 66.

38 European Court of Human Rights Case of Liberty and Others v. United Kingdom Application no. 58243/00 (2008), para 69.

Termasuk dalam bentuk justifikasi penerapan yang sesuai dengan hukum, kondisi-kondisi dimana penyadapan akan mungkin dilakukan juga harus dapat diperkirakan oleh setiap orang.[39] Hal ini tidak berarti bahwa setiap orang harus diberitahu terlebih dahulu bahwa teleponnya akan disadap, namun setidaknya mereka dapat mengetahui dalam situasi seperti apa penyadapan terhadap percakapan telepon mereka dapat dilakukan. Bahkan jika diperlukan, mekanisme konsultasi hukum dalam hal ini juga harus disediakan.

b. Kepentingan/tujuan yang sah biasanya tidak dijabarkan secara rinci dalam putusan-putusan Pengadilan HAM Eropa (ECtHR) karena tidak ditemukan adanya permasalahan mengenai pemenuhannya. Bentuk-bentuk kepentingan/tujuan yang sah yang ditemukan dalam banyak kasus yang diajukan kebanyakan menyangkut keamanan negara, keamanan masyarakat, mencegah tindak pidana, serta tujuan-tujuan lainnya sebagaimana disebutkan dalam Pasal 8 ayat (2) ECHR, yakni untuk kesejahteraan ekonomi negara, perlindungan terhadap kesehatan dan moral, serta perlindungan terhadap hak dan kebebasan orang lain.

c. Syarat "diperlukan dalam kehidupan masyarakat yang demokratis" bermakna bahwa penyadapan merupakan bentuk upaya yang proporsional untuk mencapai tujuan atau kepentingan sah yang dimaksud.[40] Misalnya, dalam proses penyidikan untuk mengungkap tindak pidana, asas proporsionalitas harus dipertimbangkan mengenai apakah upaya paksa penyadapan yang melanggar hak warga negara tersebut telah seimbang dengan kegentingan dari tindak pidana yang diungkap dan apakah ada upaya lain yang dapat digunakan untuk mengungkap tindak pidana tersebut selain menggunakan upaya paksa penyadapan.[41] Beberapa hal berikut dapat digunakan sebagai kriteria untuk menentukan standar pemenuhan asas proporsionalitas:[42]
    1) Adanya suatu tingkat probabilitas yang tinggi bahwa suatu kejahatan serius telah dilakukan atau akan dilakukan;
    2) Alat bukti dari kejahatan tersebut didapat dengan melakukan akses terhadap informasi yang terlindungi;
    3) Teknik penyidikan lain yang ada sudah dilakukan;

---

39 European Court of Human Rights Case of Kruslin v. France Application no. 11801/85 (1990), para 30.
40 European Court of Human Rights Case of Weber and Saravia v. Germany Application no. 54934/00 (2006), para 149.
41 European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015), para 260 dan European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 51.
42 Reda Manthovani, *Op. Cit.,* hal. 125-126.

4) Informasi yang diakses akan digunakan untuk kejahatan yang terkait dan setiap informasi yang telah dikumpulkan namun tidak digunakan tersebut akan dimusnahkan atau dikembalikan;
5) Informasi yang diakses hanya oleh otoritas yang berwenang dan digunakan untuk tujuan sesuai otorisasi yang diberikan.

Bab III

Perlindungan terhadap Hak atas Privasi dalam Upaya Paksa Penyadapan

Sebuah studi yang memperbandingkan hukum acara penyadapan di Indonesia dengan negara-negara seperti Amerika, Australia, Belanda, Inggris, dan Prancis, menunjukkan bahwa sistem penyadapan yang berlaku di Indonesia terbukti paling lemah dalam menerapkan penghormatan terhadap hak asasi manusia sehingga sangat rawan untuk disalahgunakan oleh pihak-pihak tertentu dan untuk kepentingan tertentu.[43] Terlebih dengan sistem yang masih demikian rentannya pun hasil dari penyadapan masih dapat digunakan dan diterima oleh sistem peradilan pidana Indonesia.[44] Oleh karenanya, berbagai mekanisme perlindungan terhadap pembatasan hak atas privasi dalam hukum acara penyadapan perlu dibentuk agar memiliki akuntabilitas yang kuat dan yang dapat mencegah penyalahgunaan wewenang.

Setidaknya terdapat enam aspek utama yang akan ditekankan dalam menyusun mekanisme perlindungan tersebut supaya dapat diatur dalam peraturan perundang-undangan yang mengatur mengenai penyadapan (RUU Penyadapan). Keenam aspek tersebut di antaranya: (a) proses pemberian ijian dan pelaksanaan penyadapan, (b) persyaratan penyadapan, (c) durasi penyadapan, (d) penanganan data hasil penyadapan, (e) mekanisme pengawasan dalam upaya paksa penyadapan, dan (f) mekanisme permohonan keberatan atau komplain terhadap upaya paksa penyadapan.

3.1. Proses Pemberian Ijin dan Pelaksanaan Penyadapan

Berdasarkan standar perlindungan yang ditetapkan oleh Pengadilan HAM Eropa, pihak yang berwenang dalam memberikan ijin pelaksanaan penyadapan idealnya adalah pengadilan.[45] Namun dalam hal penyadapan dilakukan dengan metode *mass surveillance* (pengintaian secarra massal) seperti di Jerman, maka lembaga lainnya juga dapat mengeluarkan ijin penyadapan tersebut sepanjang independensi lembaga yang berwenang memberikan ijin tersebut dapat terjamin. Independensi lembaga yang bersangkutan misalnya dapat terlihat ketika lembaga yang memberi

43 Reda Manthovani, *Penyadapan vs. Privasi*, PT Bhuana Ilmu Populer, Jakarta, 2015, hlm. 230.
44 *Ibid.*
45 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 56.

ijin pelaksanaan penyadapan merupakan lembaga yang terpisah dengan lembaga pelaksana penyadapan.[46]

Praktik di Australia menunjukkan bahwa ijin penyadapan hanya dapat dikeluarkan oleh seorang hakim yang berwenang (*an eligible judge*) atau anggota dari *Administrative Appeals Tribunal* (AAT) yang telah dinominasikan agar dapat mengeluarkan ijin penyadapan. Hakim yang berwenang merupakan hakim yang telah menyatakan kesediaannya secara tertulis untuk menjadi *eligible judge* dan diumumkan oleh Jaksa Agung. Adapun keseluruhan hakim dan anggota ATT yang berwenang tersebut secara nasional hanya berjumlah 89 orang per Desember 2017.[47]

Kemudian dalam hal pengintaian (*surveilance*) di Jerman, ketentuan dalam *the Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications* (*the G10 Act*) menyatakan bahwa ijin untuk mendapatkan surat perintah pelaksanaan pengintaian hanya dapat diajukan oleh kepala atau pejabat pengganti sementara dari institusi berikut*: the Agencies for the Protection of the Constitution of the Federation and the Länder (Bundesamt für Verfassungsschutz; Verfassungsschutzbehörden der Länder)*, Kantor Keamanan Militer *(Amt für Sicherheit der Bundeswehr)*, dan Badan Intelijen Federal *(Bundesnachrichtendienst).* Kemudian, surat perintah akan dikeluarkan oleh otoritas *Supreme Land* jika perkara yang diajukan termasuk dalam yurisdiksi kewenangannya atau oleh Menteri Dalam Negeri dan Pertahanan harus memberikan keputusan untuk menerbitkan atau menolak penerbitan surat perintah dengan alasannya secara tertulis dengan persetujuan *Parliamentary Supervisory Board*.[48] Namun pengaturan terkait pihak-pihak yang terlibat dalam pelaksanaan penyadapan di Jerman mengalami pembaruan melalui penambahan ketentuan dalam *Code of Criminal Procedure* pada 2000 khususnya Pasal 163f yang menyatakan bahwa dalam hal pengintaian dilakukan terhadap tersangka dalam waktu yang lama (lebih dari 24 jam secara terus menerus atau dua hari) maka perintah pelaksanaan penyadapan hanya dapat dikeluarkan oleh kejaksaan untuk maksimal satu bulan dan hanya dapat diperpanjang oleh perintah pengadilan.

Contoh lainnya di Amerika misalnya, berdasarkan *Wiretap Act* penyadapan dilakukan harus berdasarkan ijin pengadilan. Ijin tersebut berlaku untuk semua bentuk penyadapan yang akan

---

46 European Court of Human Rights Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria Application no. 62540/00 (2008), para 87.

47 Department of Home Affairs of the Australian Government, *Annual Report 2016-2017 on Telecommunications (Interception and Access) Act 1979*, Commonwealth of Australia, 2018, hal. 4.

48 The Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 3 ayat (1).

dilakukan aparat penegak hukum, baik yang bersifat individu yang telah ditentukan maupun yang bersifat masal seperti untuk orang-orang dalam lingkungan tertentu dengan menggunakan *IMSI (International Mobile Subscriber Identity) catcher* termasuk pula *mass surveillance.* Dalam hal penyadapan yang dilakukan terhadap target yang bersifat massal tersebut, hakim dalam kasus *Maryland vs. King* di Amerika menolak alasan penyadapan yang hanya semata-mata dilakukan demi kepentingan pengendalian kejahatan secara umum karena alasan tersebut tidak cukup untuk menjustifikasi penyadapan yang beresiko melanggar hak atas privasi orang-orang yang tidak bersalah. Hakim menilai bahwa harus terdapat kepentingan yang lebih genting seperti terdapatnya kepentingan pemerintah yang signifikan misalnya dalam hal memastikan identitas orang-orang yang ditangkap karena diduga telah menjadi pelaku kejahatan.[49]

Melihat praktik tersebut, hakim dalam memberikan ijin penyadapan harus dapat menggali dengan lebih dalam mengenai pertimbangan justifikasi-justifikasi yang diajukan oleh aparat mengenai kegentingan pelaksanaan penyadapan dalam rangka untuk melindungi hak atas privasi warga negara yang terancam dilanggar secara sewenang-wenang. Oleh karena itu, dalam memberikan ijin penyadapan, hakim semestinya harus menghindari upaya-upaya yang hanya sebatas bersifat pengecekan kelengkapan syarat administrasi atau formalitas yang telah tercantum dengan jelas dalam peraturan perundang-perundangan. Di Australia misalnya, sebelum memberikan ijin penyadapan, hakim harus mempertimbangkan 3 hal berikut: (a) tingkat keseriusan dari kejahatan, (b) seberapa besar peran penyadapan dalam membantu proses penyidikan, (c) kemungkinan adanya metode penyidikan lain yang tersedia bagi institusi yang melaksanakan penyidikan.[50] Kemudian di Jerman, permohonan ijin perintah penyadapan yang diajukan oleh otoritas yang melaksanakan penyadapan, misalnya Badan Intelijen Federal, harus menjelaskan alasan-alasan permohonannya secara tertulis terkait sifat, ruang lingkup, dan durasi penyadapan serta harus menjelaskan bagaimana upaya-upaya lain untuk melakukan penyelidikan tidak memiliki peluang untuk berhasil atau akan jauh lebih sulit untuk dilakukan.[51]

Penyadapan juga mungkin dilakukan tanpa didahului ijin dari otoritas yang berwenang, namun perlu dibatasi hanya untuk dilakukan dalam keadaan yang mendesak. Kriteria keadaan yang mendesak pun harus dirumuskan secara limitatif dengan jelas. Di Amerika misalnya, keadaan mendesak hanya terbatas pada situasi-situasi dimana terdapat keadaan bahaya yang dengan segera

---

49 Gus Hosein dan Caroline Wilson Palwo, *Loc. Cit.*

50 Department of Home Affairs of the Australian Government, *Loc. Cit.*

51 The Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 4.

mengancam nyawa atau menimbulkan luka yang serius terhadap seseorang dan kegiatan-kegiatan konspirasi yang mengancam keamanan nasional atau yang menjadi karakteristik kejahatan terorganisasi.[52] Surat ijin perintah penyadapan dalam keadaan mendesak harus dikeluarkan dalam waktu 48 jam dan apabila permohonan ijin tersebut ditolak atau tidak dikeluarkan dalam jangka waktu tersebut maka pelaksanaan penyadapan harus dihentikan dan data hasil penyadapan yang diperoleh selama kurun waktu tersebut dianggap tidak sah.[53] Pelaksanaan penyadapan dalam keadaan mendesak juga seketika harus dihentikan saat tujuan atau informasi yang dicari telah didapatkan meskipun kurun waktu 48 jam tersebut belum berakhir.[54]

3.2. Persyaratan Penyadapan

Sebagaimana telah dijelaskan pada bab sebelumnya, penyadapan merupakan bentuk upaya paksa oleh aparat penegak hukum yang mengurangi pemenuhan hak atas privasi dari warga negara. Oleh karena itu, persyaratan-persyaratan untuk dapat melakukan penyadapan penting untuk diatur seketat mungkin agar dapat memberikan perlindungan dari interferensi yang sewenang-wenang terhadap hak atas privasi tersebut secara maksimal. Dalam hal ini, bentuk-bentuk justifikasi untuk melakukan penyadapan harus disebutkan secara jelas dan *rigid* khususnya melalui rumusan pasal dalam peraturan tentang penyadapan yang komprehensif yang nantinya menjadi sumber rujukan tunggal dalam pelaksanaan penyadapan.

3.2.1. Jenis tindak pidana yang dapat diungkap melalui penyadapan

Dalam menentukan kondisi-kondisi dimana penyadapan dapat dilakukan, membuat kategorisasi berdasarkan jenis kejahatan memang dapat dibenarkan oleh Pengadilan HAM Eropa. Kategorisasi tersebut harus disebutkan dengan jelas dalam peraturan perundang-undangan, meskipun tidak diwajibkan untuk menyebutkan satu per satu bentuk tindak pidananya; Penyebutan kisaran ancaman hukuman atau pemberian gambaran umum mengenai jenis tindak pidana (misalnya, tindak pidana yang mengancam keamanan negara atau yang mengarah pada serangan teroris) juga telah cukup memenuhi standar perlindungan yang ditetapkan oleh Pengadilan HAM Eropa.[55]

---

52 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2518 para 7 (a).
53 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2518 para 7 (b).
54 *Ibid*.
55 European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015), para 247 dan European Court of Human Rights Case of Szabó and Vissy v. Hungary Application no. 37138/14 (2016), para 64.

Di Eropa, penyadapan terhadap telepon diperbolehkan untuk dipergunakan sebagai salah satu metode investigasi khusus dalam penanganan kejahatan tertentu seperti korupsi, *cybercrime*, terorisme, dan kejahatan serius lainnya. Hal ini terlihat dari beberapa konvensi yang mengatur mengenai penanganan kejahatan tertentu misalnya *the Council of Europe Criminal Law Convention on Corruption*) dan *the Budapest Convention on Cybercrime* yang memberikan kewenangan untuk dilakukan penyadapan dalam menangani kasus-kasus tersebut.

Selain bertujuan untuk memberikan perkiraan kepada setiap orang bahwa hak atas kehidupan pribadi mereka dapat dikurangi, adanya penyebutan yang spesifik terkait jenis-jenis tindak pidana tersebut juga bertujuan untuk membatasi jumlah tindak pidana apa saja yang dapat diungkap melalui penyadapan. Hal ini terlihat dari putusan Pengadilan HAM Eropa terhadap negara Moldova yang menyatakan adanya pelanggaran terhadap Pasal 8 ECHR karena upaya paksa penyadapan dapat dilakukan terhadap lebih dari 50% tindak pidana yang diatur dalam KUHP Moldova.[56]

Namun, praktik di Jerman menunjukkan bahwa negara tersebut memberikan daftar kejahatan secara spesifik yang mana upaya paksa penyadapan dapat dilakukan dalam Pasal 3 *the Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications* (*the G 10 Act*). Tujuan pelaksanaan penyadapan dalam ketentuan tersebut adalah untuk mengumpulkan informasi yang diperlukan agar dapat dengan segera mengidentifikasi dan menghindari bahaya-bahaya tertentu dari:

a. serangan bersenjata terhadap Republik Federal Jerman;
b. serangan teroris jaringan internasional di Republik Federal Jerman;
c. perdagangan senjata internasional dalam lingkup ketentuan *Control of Weapons of War Act* dan pelarangan perdagangan barang eksternal, program dan teknologi terkait pengelolaan data dalam kasus-kasus yang sangat penting;
d. impor obat-obatan dalam jumlah besar secara illegal ke dalam wilayah Republik Federal Jerman;
e. pemalsuan uang (*Geldfälschung*) yang dilakukan di luar negeri;
f. pencucian uang dalam konteks kejahatan yang tercantum dalam poin c sampai e.

Selain itu, beberapa jenis kejahatan lainnya juga masuk dalam daftar kejahatan yang mana dapat dilakukan upaya paksa penyadapan dalam pencegahan, penyelidikan, hingga penuntutannya, yaitu:

---

56 European Court of Human Rights Case of Iordachi v. Moldova Application no. 25198/02 (2009), para 44.

pengkhianatan tingkat tinggi terhadap perdamaian atau keamanan negara, kejahatan yang mengancam tatanan demokrasi, keamanan eksternal Negara atau keamanan pasukan sekutu yang berbasis di Republik Federal Jerman, pembentukan asosiasi teroris, pembunuhan, perampokan, pemalsuan kartu pembayaran atau cek, penipuan yang berkaitan dengan subsidi ekonomi, penyusupan orang asing, serta produksi, impor dan perdagangan obat-obatan terlarang.[57]

Pengaturan di Australia, penyadapan hanya dapat diterapkan dalam proses penyidikan terhadap kejahatan yang serius yakni yang diancam dengan pidana minimal tujuh tahun penjara. Adapun misalnya bentuk-bentuk kejahatan tersebut antara lain pembunuhan, penculikan, kejahatan narkotika yang serius, terorisme, kejahatan yang melibatkan pornografi anak, tindak pidana pencucian uang, dan kejahatan-kejahatan yang terorganisir. Namun demikian, masih terdapat pengecualian terhadap kejahatan-kejahatan yang meskipun diancam di bawah tujuh tahun penjara, yakni ketika terdapat unsur penggunaan sistem telekomunikasi misalnya dalam kejahatan-kejahatan yang terkait konspirasi atau *collusion*. Upaya penyadapan dirasa sangat dibutuhkan dan menjadi kunci pengungkapan kejahatan tersebut sehingga penggunaan metode penyadapan tersebut masih diperbolehkan.[58]

Dari praktik negara-negara di atas dalam mengatur hukum acara penyadapan dapat terlihat bahwa penyadapan tidak digunakan dalam investigasi setiap jenis tindak pidana, sehingga menjadi wajar jika penyadapan tidak perlu dianggap sebagai metode utama atau bahkan satu-satunya metode dalam mengungkap kejahatan. Pembatasan terhadap jenis-jenis tindak pidana yang dapat dilakukan penyadapan dalam pengungkapannya memang perlu dilakukan untuk menghindari pembatasan terhadap hak atas privasi yang berlebihan. Misalnya, penyadapan hanya dapat dilakukan terhadap kejahatan atau tindak pidana yang memiliki dampak buruk dan meluas bagi kehidupan bermasyarakat, berbangsa, dan bernegara serta tindak pidana-tindak pidana yang bersifat rumit atau kompleks dalam pengungkapan dan pembuktiannya.[59]

3.2.2. Kategori Orang-orang yang Berpotensi Menjadi Target Penyadapan

---

57 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 3 ayat (3).

58 Department of Home Affairs of the Australian Government, *Op. Cit.,* hal. 2.

59 Kristian dan Yopi Gunawan, *Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia*, Nuansa Aulia, Bandung, 2013, hal. 262.

Ketentuan mengenai persyaratan penyadapan dalam peraturan perundang-undangan juga penting untuk menjabarkan kategori orang-orang yang berpotensi menjadi target penyadapan. Penjabaran kategori orang-orang tersebut harus secara rinci. Pengadilan HAM Eropa misalnya memberikan standar bahwa selain tersangka atau terdakwa, definisi terkait "orang-orang yang terlibat dalam tindak pidana" harus dijelaskan dengan detil siapa-siapa saja yang dapat masuk dalam kategori tersebut.[60] Orang-orang yang dapat masuk dalam kategori tersebut antara lain setiap orang yang mempunyai informasi tentang adanya tindak pidana atau setiap orang yang mempunyai informasi lain yang relevan tentang kasus pidana meskipun mereka tidak terlibat dalam tindak pidana tersebut.[61] Selanjutnya, dalam permohonan ijin penyadapan nantinya daftar nama-nama orang yang masuk dalam kategori tersebut harus disebutkan dengan alasan yang mendasari mengapa mereka menjadi target penyadapan.

Kemudian, dalam kurun waktu tertentu setelah penyadapan selesai dilakukan, orang-orang yang menjadi target penyadapan tersebut harus diberikan pemberitahuan bahwa telekomunikasi mereka telah disadap. Hal ini penting untuk mencegah upaya paksa penyadapan yang dilakukan secara berlebihan dan tidak efektif.

Dalam sebuah kasus pada Pengadilan HAM Eropa, Bulgaria dinyatakan telah melakukan pelanggaran terhadap Pasal 8 ECHR karena telah gagal memberikan perlindungan yang memadai terhadap potensi penyalahgunaan wewenang pada pelaksanaan penyadapan. Hal ini terjadi karena peraturan penyadapan di Bulgaria tidak mengakomodasi ketentuan mengenai pemberitahuan bagi orang-orang yang pernah disadap bahwa mereka pernah menjadi target penyadapan. Akibatnya, orang yang pernah menjadi target penyadapat tersebut tidak akan pernah bisa mengetahui bahwa mereka pernah diintai dan tidak dapat mengajukan pengaduan mengenai interferensi yang dilakukan secara melawan hukum terhadap hak atas kehidupan pribadi mereka.[62]

Selain itu, dalam kasus Bulgaria di atas kemudian diketahui bahwa banyak terjadi penyalahgunaan dan penggunaan upaya penyadapan dinilai telah berlebihan. Dari total 10.000 surat perintah untuk melakukan pengintaian rahasia (*the system of secret surveillance*) dalam kurun waktu 24 bulan

60 European Court of Human Rights Case of Iordachi v. Moldova Application no. 25198/02 (2009), para 44.
61 European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015), para 245.
62 European Court of Human Rights Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria Application no. 62540/00 (2008), para 90-94.

(belum termasuk penyadapan pada telepon untuk total populasi kurang dari 8 juta penduduk), hanya sekitar 267-269 yang akhirnya digunakan dalam proses peradilan.[63]

Sebagai kebalikannya, praktik yang cukup baik diterapkan di Jerman misalnya. Komisi G10 yang merupakan lembaga pengawas independen untuk pelaksanaan penyadapan memiliki kewenangan untuk memutuskan apakah seseorang yang menjadi target penyadapan harus diberitahu tentang upaya paksa penyadapan yang telah dilakukan terhadapnya.[64] Pengadilan HAM Eropa menyatakan bahwa ketentuan tersebut, sebagaimana ditafsirkan oleh Mahkamah Konstitusi Federal, secara efektif telah memastikan orang-orang yang menjadi target penyadapan untuk dapat diberikan pemberitahuan dalam hal pemberitahuan tersebut dimungkinkan tanpa menghalangi tujuan dari pembatasan terhadap kerahasiaan isi komunikasi.[65]

Oleh karena itu, sistem perlindungan untuk mencegah penggunaan upaya paksa penyadapan yang berlebihan dan tidak efektif harus dibentuk, yakni salah satunya dengan memberikan pemberitahuan kepada orang-orang yang pernah menjadi target penyadapan setelah proses penyadapan selesai. Pemberitahuan tersebut perlu dilakukan dengan tanpa mengurangi esensi dari tujuan pelaksanaan penyadapan itu sendiri. Dengan demikian, orang-orang yang pernah menjadi target penyadapan tersebut juga mempunyai kesempatan untuk meninjau keabsahan penyadapan yang pernah dilakukan terhadapnya.[66]

3.3. Durasi Penyadapan

Tidak ada standar yang baku dalam hukum HAM internasional yang mengatur mengenai durasi penyadapan. Pengadilan HAM Eropa bahkan menyerahkan kepada masing-masing negara anggotanya untuk menentukan berapa lama maksimal penyadapan dapat dilakukan karena hal tersebut dapat bergantung pada kompleksitas serta durasi investigasi pada kasus yang bersangkutan.[67] Namun, Pengadilan hanya memerintahkan agar terdapat evaluasi berkala

---

63 *Ibid.*

64 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 5 ayat (5) dan Pasal 9 ayat (3).

65 European Court of Human Rights Case of Weber and Saravia v. Germany Application no. 54934/00 (2006), para 136.

66 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 57.

67 European Court of Human Rights Case of Kennedy v. the United Kingdom Application no. 26839/05 (2010), para 161.

mengenai perlu tidaknya penyadapan untuk dilanjutkan serta terdapat pengaturan mengenai persyaratan perpanjangan dan kondisi-kondisi dimana penyadapan harus diakhiri.[68]

Praktik di Inggris misalnya, berdasarkan Pasal 9 ayat (6) *Regulation of Investigatory Powers Act 2000* (RIPA) perintah penyadapan yang tidak diperpanjang berlaku untuk 5 hari kerja atau untuk 3 bulan, sedangkan perpanjangannya dapat dilakukan untuk maksimal 3 bulan atau 6 bulan. Namun tidak ada pembatasan mengenai berapa jumlah perpanjangan perintah penyadapan. Terhadap hal tersebut, Pengadilan HAM Eropa menyatakan bahwa mekanisme perpanjangan perintah penyadapan yang tidak terbatas tersebut dapat diperbolehkan mengingat kompleksitas perkara dan durasi penyelidikan kasus yang sedang ditangani dapat berbeda-beda, namun harus diimbangi dengan adanya prosedur perlindungan (*safeguard mechanism*) yang cukup dapat menjamin pencegahan proses perpanjangan perintah penyadapan dari kesewenang-wenangan.[69]

Berdasarkan ketentuan dalam RIPA, pihak yang mengajukan perpanjangan perintah penyadapan harus mengajukan permohonan kepada Sekretaris Negara (*Secretary of State*) untuk memberikan perkembangan informasi terbaru dan menilai urgensi operasi penyadapan hingga saat ini. Selain itu, alasan-alasan sebagaimana disebutkan dalam Pasal 5 ayat (3) RIPA (untuk kepentingan keamanan nasional atau untuk mencegah/mendeteksi kejahatan atau untuk melindungi kepentingan ekonomi negara) terkait mengapa surat perintah penyadapan tetap diperlukan harus diuraikan secara khusus. Lebih lanjut, berdasarkan Pasal 9 ayat (3) RIPA, Sekretaris Negara berkewajiban untuk membatalkan suatu surat perintah ketika ia mengganggap bahwa surat perintah tersebut tidak lagi diperlukan untuk tujuan sebagaimana disebutkan dalam Pasal 5 ayat (3) RIPA. Adanya kewenangan dari Sekretaris Negara untuk membatalkan surat perintah untuk upaya penyadapan yang tidak lagi dianggap layak untuk dilanjutkan, dalam praktiknya mengindikasikan bahwa pihak pelaksana penyadapan harus menempatkan perintah penyadapan untuk selalu dapat dilakukan review atau penilaian secara berkala. Dengan demikian, ketentuan mengenai durasi, prosedur perpanjangan, hingga pembatalan perintah penyadapan dalam hukum Inggris telah diatur secara jelas sehingga telah tersedia standar perlindungan yang cukup untuk mencegah pelanggaran HAM dalam upaya paksa penyadapan.

---

68 European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015), para 250.

69 European Court of Human Rights Case of Kennedy v. the United Kingdom Application no. 26839/05 (2010), para 161.

Prosedur yang serupa juga diberlakukan di Australia. Berdasarkan ketentuan Pasal 49 ayat (3) dalam *Telecommunications (Interception and Access)* (TIA) *Act 1979* menyatakan bahwa penyadapan dapat diterapkan untuk 45 hari atau 90 hari. Kemudian untuk penghitungan durasi perpanjangan ijin penyadapan menggunakan batas-batas waktu tertentu yaitu setelah 90 hari, setelah 150 hari, dan setelah 180 hari sejak surat perintah pertama diterbitkan. Namun pada dasarnya, ijin penyadapan di Australia dapat dicabut sewaktu-waktu sepanjang kondisi-kondisi yang mendasari dilakukannya penyadapan sudah tidak ditemukan. Dalam hal ini, pimpinan institusi terkait yang melaksanakan penyadapan berwenang untuk mencabut ijin penyadapan secara tertulis berdasarkan Pasal 57 TIA Act 1979.

Sedangkan untuk praktik di Jerman, jangka waktu pelaksanaan penyadapan yang harus dicantumkan dalam surat perintah penyadapan dapat diberikan untuk maksimal tiga bulan. Durasi ini masih dapat diperpanjang selama tiga bulan sepanjang syarat-syarat berlakunya surat perintah tersebut masih terpenuhi.[70]

3.4. Penanganan Data Hasil Penyadapan

Dari penjabaran sejauh ini dapat diketahui bahwa pada prinsipnya penyadapan merupakan merupakan perbuatan yang dilarang namun hal tersebut dapat dilakukan sepanjang untuk kepentingan penegakan hukum yang diatur melalui peraturan perundang-undangan. Kemudian proses dari penyadapan tersebut akhirnya akan menghasilkan kumpulan data yang terkait dengan komunikasi seseorang dengan pihak lain baik yang diperoleh melalui percakapan telepon, transmisi jaringan internet, dan lain sebagainya. Oleh karena proses penyadapan termasuk di dalamnya pengelolaan data hasil penyadapan merupakan kegiatan yang rentan terhadap penyalagunaan dan kesewenang-wenangan dalam membatasi hak atas privasi seseorang, maka pembatasan-pembatasan mengenai bagaimana data tersebut disimpan dan diakses menjadi aspek yang sangat penting pula untuk diatur dalam peraturan perundangan yang mengatur mengenai penyadapan.

Pengaturan tentang penyadapan dalam hal ini juga harus memuat ketentuan mengenai perawatan data hasil penyadapan. Ketentuan tersebut dapat melingkupi beberapa hal berikut, yakni (a) tempat dan proses penyimpanan data yang diperoleh dari proses penyadapan, (b) mekanisme

70 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 5.

perlindungan keaslian data tersebut, (c) kapan data tersebut harus dimusnahkan dan tindakan apa yang harus diambil untuk memastikan data tersebut benar-benar telah dimusnahkan, (e) siapa yang dapat mengakses data tersebut, serta (f) kepada siapa dan dalam kondisi seperti apa data tersebut dapat diberikan kepada pihak ketiga. Secara umum, informasi mengenai hal-hal tersebut akan dibahas dalam dua subbab berikut, yaitu mekanisme penyimpanan data hasil penyadapan dan pembatasan akses terhadap data hasil penyadapan.

3.4.1. Mekanisme Penyimpanan Data Hasil Penyadapan

Sebelum membahas mengenai mekanisme penyimpanan data hasil penyadapan, setidaknya perlu diklarifikasi terlebih dahulu mengenai bentuk-bentuk data apa saja yang dimaksud sebagai data hasil penyadapan. Data hasil penyadapan khususnya terhadap komunikasi dapat dikategorikan dalam tiga jenis berikut: [71]

a) Data yang berisi konten percakapan yang berlangsung selama komunikasi, yang mana bersifat sangat rahasia;
b) Data yang diperlukan untuk membentuk dan melangsungkan komunikasi atau yang biasa disebut '*traffic data*', misalnya informasi mengenai siapa yang dihubungi, kapan komunikasi berlangsung, dan durasi komunikasi;
c) Data mengenai lokasi dari perangkat komunikasi yang digunakan atau yang biasa disebut '*location data*' yang biasanya juga dapat terlihat dari '*traffic data*'. Jenis data ini pada saat yang sama juga dapat menunjukkan lokasi dari pengguna perangkat komunikasi serta menunjukkan informasi tentang data diri pengguna.

Di Inggris, Pasal 15 ayat (3) RIPA mensyaratkan bahwa materi penyadapan dan data komunikasi terkait, serta salinan apa pun yang terbuat dari bahan atau data, harus dimusnahkan segera setelah tidak ada lagi alasan untuk menyimpannya sebagaimana diperlukan Pasal 5 ayat (3) RIPA yaitu untuk kepentingan keamanan nasional, untuk mencegah/mendeteksi kejahatan, atau untuk melindungi kepentingan ekonomi negara. Data hasil penyadapan harus ditinjau atau diperiksa pada interval tertentu untuk memastikan bahwa alasan pembenaran untuk menyimpan data tersebut tetap valid. Selain ketiga jenis data tersebut, Pasal 4.18 *the Interception of Communications Code of Practice* yang disusun oleh Sekretaris Negara di Inggris juga mengamanatkan agar beberapa jenis informasi terkait pelaksanaan upaya paksa penyadapan, misalnya kapan penyadapan dimulai dan

[71] European Union Agency for Fundamental Rights, *Op. Cit.,* hal. 167-168.

dihentikan, surat perintah penyadapan dan seluruh perpanjangannya, maupun alasan penolakan pemberian perintah atau perpanjangan perintah penyadapan, yang juga perlu disimpan dengan baik agar dapat diakses sewaktu-waktu untuk keperluan pengawasan yang dilakukan oleh Komisioner Penyadapan Komunikasi (*the Interception of Communications Commissioner*).

Terkait dengan pemusnahan data hasil penyadapan, Prinsip 2.2 yang diusulkan oleh Komite Menteri-Menteri Dewan Eropa dalam *Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector* (Rekomendasi Komite Menteri-Menteri Dewan Eropa) menyatakan bahwa dalam hal data hasil penyadapan tidak langsung dihapus dan akan terus disimpan, maka orang-orang yang data terkait diri mereka dikumpulkan tanpa sepengetahuannya (orang yang telah menjadi target penyadapan) harus diberi tahu bahwa data tersebut masih disimpan segera setelah tidak ada lagi hal-hal yang mungkin dapat menghambat upaya pencegahan dan penanggulangan kejahatan atau keteraturan publik. Namun dalam hal mekanisme penyadapan yang digunakan bersifat pengintaian massal sehingga melibatkan data dari banyak individu, maka upaya pemberitahuan tersebut dapat dilakukan ketika secara praktis dimungkinkan.[72]

Kemudian dalam Prinsip 7 dalam *Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector* juga diatur bahwa evaluasi secara berkala terhadap data hasil penyadapan yang disimpan perlu untuk dilakukan agar dapat diketahui apakah penyimpanan tersebut masih diperlukan dalam rangka mencegah dan menanggulangi kejahatan atau untuk menjaga keteraturan sosial. Selain itu, termasuk dalam proses evaluasi tersebut adalah memeriksa kualitas data yang disimpan.

Dalam ketentuan hukum Jerman misalnya, jika data hasil penyadapan tidak lagi diperlukan untuk mencapai tujuan yang ditentukan dan jika data tersebut tidak harus dikirim ke otoritas lain, maka data tersebut harus dihancurkan dan dihapus atau setidak-tidaknya, akses terhadap data hasil penyadapan tersebut harus diblok.[73] Proses pemusnahan data tersebut harus dilakukan di bawah pengawasan seorang anggota staf yang memenuhi syarat untuk menduduki lembaga yudisial dan

---

72 Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

73 The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 3 ayat (6)-(7) dan Pasal 7 ayat (4).

setiap tindakan penghancuran dan penghapusan harus dicatat dalam arsip.[74] Verifikasi atau pengecekan terhadap data hasil penyadapan dilakukan setiap enam bulan sekali untuk menentukan apakah data tersebut memenuhi kriteria untuk dimusnahkan dan dihancurkan.[75]

3.4.2. Pembatasan Akses terhadap Data Hasil Penyadapan

Salah satu pihak yang harus diberikan hak untuk mendapatkan akses terhadap data hasil penyadapan adalah orang-orang yang menjadi target penyadapan. Sistem hukum acara penyadapan di Amerika misalnya memungkinkan bagi orang yang menjadi target penyadapan untuk mengajukan permohonan kepada hakim agar mendapat akses berupa salinan sebagian dari data hasil penyadapan terhadapnya.[76] Pemberian akses tersebut juga harus dilakukan dalam waktu yang wajar dan tanpa penundaan yang tak beralasan (*undue delay*).[77]

Sejalan dengan hal tersebut, maka akses terhadap data hasil penyadapan juga wajib diberikan kepada tersangka/terdakwa dalam hal hasil penyadapan tersebut digunakan sebagai alat bukti dalam proses peradilan. Selain karena target penyadapan memang berhak untuk mengakses data hasil penyadapan sebagaimana dijelaskan sebelumnya, namun terdapat pula kepentingan yang lebih mendesak jika target penyadapan tersebut berstatus sebagai tersangka/terdakwa, yakni untuk kepentingan menyusun pembelaan di persidangan serta untuk menjamin adanya keseimbangan proses penuntutan (*equality of arms*). Pengadilan HAM Eropa juga menegaskan dalam memperlakukan data hasil penyadapan sebagai alat bukti di persidangan, maka prinsip yang berlaku adalah prinsip umum yang mewajibkan kedua belah pihak (penuntut umum dan tersangka) untuk saling memberikan akses agar dapat memeriksa bukti yang diajukan oleh masing-masing pihak dalam rangka menjamin terlaksananya prinsip *fair trial* dan bahwa tersangka/terdakwa setidaknya juga perlu diberitahu dan ikut dilibatkan dalam proses pembuatan

---

74 *Ibid.*

75 *Ibid.*

76 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2518 para 8 (d).

77 Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies), Prinsip 6.

keputusan mengenai pemberian maupun penolakan akses terhadap data hasil penyadapan tersebut dalam proses pra-sidang.[78]

Namun di sisi lain, pembatasan akses memang perlu dilakukan supaya data hasil penyadapan dapat terjaga integritasnya secara fisik dan kerahasiaannya secara konten. Akses terhadap data hasil penyadapan harus terbatas untuk petugas tertentu sehingga kemungkinan adanya kontak dengan data atau pengubahan data yang dilakukan tanpa ijin dapat dicegah. Apabila terdapat pelanggaran dalam hal ini maka pemberian sanksi pidana yang proporsional juga dapat diterapkan.[79]

Pengaturan di Jerman misalnya menentukan hanya otoritas-otoritas tertentu saja yang dapat diberikan akses (*transmission*) terhadap data hasil penyadapan setelah mendapat persetujuan dari Komisi G10 (salah satu anggota yang mempunyai kualfikasi untuk menduduki lembaga yudisial) sepanjang dibutuhkan oleh otoritas tersebut untuk menjalankan tugas-tugas mereka. Adapun otoritas-otoritas tersebut diantaranya adalah *the Offices for the Protection of the Constitution of the Federation and of the Länder*, *the Military Counter-Intelligence Service, the Customs Investigation Office (Zollkriminalamt)*, kejaksaan, dan instansi kepolisian tertentu.[80] Kemudian, setiap agenda penyerahan data hasil penyadapan kepada otoritas-otoritas tersebut harus ditulis dalam arsip.

Selain itu, Pengadilan HAM Eropa dalam kasus *Kennedy v. The United Kingdom* juga menyatakan bahwa pemberian akses terhadap alat bukti, dalam hal ini adalah data hasil penyadapan, bukanlah termasuk hak yang absolut.[81] Sebab, dalam sistem adversarial sekalipun misalnya, hak tersebut perlu juga diseimbangkan dengan kepentingan untuk menjaga keamanan nasional dan untuk menjaga kerahasiaan metode penyidikan tindak pidana.[82] Dengan demikian, pemberian akses terhadap data hasil penyadapan pada prinsipnya perlu dinyatakan secara tegas sebagai hak, dan jika terdapat kondisi-kondisi dimana pengecualian perlu dilakukan, maka ketentuan lebih lanjut juga harus dirumuskan untuk mengatur hal tersebut dengan jelas.

3.5. Mekanisme Pengawasan dalam Upaya Paksa Penyadapan

78 European Court of Human Rights Case of Natunen v. Finland Application no. 21022/04 (2009), para 39 dan para 48.
79 Reda Manthovani, *Op. Cit.,* hal. 224 dan hal. 298.
80 The Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 3 ayat (5).
81 European Court of Human Rights Case of Kennedy v. the United Kingdom Application no. 26839/05 (2010), para 187-191
82 *Ibid*.

Selain memastikan bahwa terdapat kontrol terhadap pelaksanaan penyadapan pada tahap sebelum pelaksanaan, Pengadilan HAM Eropa juga menegaskan bahwa kontrol tersebut harus tersedia saat pelaksanaan maupun setelah pelaksanaan penyadapan selesai.[83] Hal ini penting untuk memastikan agar setiap adanya dugaan pelanggaran terhadap pelaksanaan penyadapan dapat terdeteksi, tidak hanya sebatas ketika terdapat pengaduan dari pihak yang dirugikan. Mengingat tidak ada pemberitahuan terkait pelaksanaan penyadapan kepada targetnya, maka sangat mungkin jika pengaduan terhadap dugaan pelanggaran tidak akan pernah ditemukan.

Oleh karena itu, pihak yang menjadi pengawas pelaksanaan penyadapan harus diberikan akses terhadap semua dokumen dan informasi mengenai proses penyadapan tersebut dari pihak yang melaksanakan penyadapan.[84] Adapun detail informasi yang harus diberikan kepada badan pengawas penyadapan misalnya mengenai deskripsi setiap informasi/dokumen yang diperoleh atau yang terkait, siapa petugas yang menguasai informasi/dokumen tersebut, tujuan penyimpanan, jenis-jenis data yang ada di dalamya, dan siapa saja pihak-pihak yang mendapat pemberitahuan mengenai informasi/dokumen tersebut.[85]

Di Amerika Serikat, beban untuk memberikan pelaporan pelaksanaan penyadapan sebanyak satu kali dalam setahun diberikan kepada hakim, Jaksa Agung, dan Direktur Administrasi Pengadilan Amerika Serikat (*Director of Administration Office of the United States Courts.* Masing-masing hakim yang memberikan, memperpanjang, dan menolak ijin penyadapan menyerahkan laporannya kepada Direktur Administrasi Pengadilan Amerika Serikat setiap bulan Januari; Jaksa Agung untuk diberikan kepada Direktur Administrasi Pengadilan Amerika Serikat setiap bulan Maret; dan (c) Direktur Administrasi Pengadilan Amerika Serikat (*Director of Administration Office of the United States Courts*) untuk diberikan pada Kongres setiap bulan Juni.[86]

Laporan yang diberikan oleh Direktur Administrasi Pengadilan Amerika Serikat kepada Kongres merupakan laporan lengkap hasil analisis terhadap data yang diberikan dalam laporan hakim maupun Jaksa Agung, antara lain terkait jumlah permohonan untuk melakukan penyadapan serta

---

83 European Court of Human Rights Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria Application no. 62540/00 (2008), para 84.

84 European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015), para 281.

85 Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

86 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2519 para 1-3.

jumlah surat perintah yang memberikan ijin maupun menolak ijin atau perpanjangan ijin penyadapan.[87] Data tersebut diperoleh dari laporan yang diserahkan baik oleh hakim maupun Jaksa Agung.

Laporan yang disusun oleh hakim setidaknya harus memuat informasi sebagai berikut:[88]

a) fakta bahwa surat ijin atau surat perpanjangan ijin diberikan;
b) bentuk pemberian ijin atau perpanjangan ijin (termasuk hal-hal khusus yang terkait dengan pemberian ijin atau perpanjangan ijin);
c) fakta bahwa ijin atau perpanjangan ijin telah ditolak atau telah diberikan dengan diterapkan sebagaimana mestinya atau diterapkan dengan pengubahan tertentu;
d) durasi pelaksanaan penyadapan yang diperintahkan dalam surat ijin, serta jumlah dan durasi setiap perpanjangan ijin;
e) jenis kejahatan yang tercantum dalam surat ijin, perpanjangan ijin, atau dalam penerapannya;
f) identitas petugas atau apparat penegak hukum dan institusi yang melaksanakan perintah penyadapan dan identitas orang yang memberikan ijin penyadapan; dan
g) deskripsi fasilitas yang digunakan untuk melaksanakan penyadapan atau tempat dimana penyadapan dilakukan.

Sedangkan informasi yang harus dijabarkan dalam laporan Jaksa Agung antara lain:[89]

a) informasi yang diberikan oleh hakim sebagaimana tercantum dalam poin (a) hingga (g) di atas sehubungan dengan setiap permohonan untuk mendapatkan surat ijin atau perpanjangan ijin yang dibuat selama satu tahun kalender sebelumnya;
b) deskripsi umum dari pelaksanaan penyadapan berdasarkan surat ijin atau perpanjangan ijin tersebut, yang meliputi: (i) perkiraan sifat dan frekuensi komunikasi yang berisi hal-hal yang memberatkan (*incriminating*) yang disadap, (ii) perkiraan sifat dan frekuensi komunikasi lainnya yang disadap, (iii) perkiraan jumlah orang-orang yang komunikasinya disadap, (iv) jumlah surat ijin yang terdapat enkripsi dan apakah enkripsi tersebut mencegah petugas atau aparat penegak hukum untuk mendapatkan teks komunikasi sebagaimana diperintahkan dalam surat ijin tersebut, dan (v) perkiraan sifat, jumlah, dan biaya dari tenaga kerja dan sumber daya lain yang digunakan dalam proses penyadapan;

87 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2519 para 3.
88 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2519 para 1.
89 The Omnibus Crime Control and Safe Streets Act 1968, Title III Section 2519 para 2.

c) jumlah penangkapan yang dihasilkan dari pelaksanaan penyadapan yang dibuat berdasarkan ijin atau perpanjangan ijin tersebut, dan jenis kejahatan yang mana dilakukan penangkapan terhadap tersangkanya tersebut;
d) jumlah kasus yang disidangkan dari hasil penyadapan;
e) jumlah mosi/gerakan untuk menekan yang dibuat sehubungan dengan penyadapan tersebut, dan jumlah yang diberikan atau ditolak (*the number of motions to suppress made with respect to such interceptions, and the number granted or denied*);
f) jumlah putusan bersalah yang dihasilkan dari hasil penyadapan dan jenis kejahatan dari kasus yang diperoleh putusan bersalah tersebut, dan penilaian umum tentang pentingnya pelaksanaan penyadapan tersebut; dan
g) informasi yang diperlukan oleh paragraf (b) sampai (f) dari ayat ini sehubungan dengan ijin atau perpanjangan ijin yang diperoleh pada satu tahun kalender sebelumnya.

Kemudian untuk praktik di Inggris misalnya, terdapat pula komisi khusus yakni *the Interception of Communications Commissioner* (Komisioner Penyadapan Komunikasi) yang bertugas sebagai pengawas. Berdasarkan Pasal 59 *Regulation of Investigatory Powers Act* (RIPA) 2000, Komisioner tersebut diwajibkan untuk membuat laporan setiap akhir tahun dan saat-saat tertentu jika diminta terkait pelaksanaan penyadapan untuk dilaporkan kepada Perdana Menteri yang kemudian diteruskan ke Parlemen.

Namun beberapa rekomendasi untuk penguatan sistem pengawasan pada Parlemen (*parliamentary oversight*) di Inggris juga didorong. Misalnya, dalam laporan yang disusun oleh Komisioner tersebut harus memuat data statistik yang detil mengenai kondisi-kondisi dan hasil dari penggunaan upaya penyadapan sehingga Komite pada Parlemen yang melakukan evaluasi di parlemen dapat menilai aspek proporsionalitas dari tindakan upaya penyadapan tersebut. Parlemen juga diharapkan dapat mempunyai wewenang untuk investigasi dugaan adanya pelanggaran terkait upaya penyadapan yang dilakukan dalam rangka keamanan nasional. Pemotongan rantai akuntabilitas melalui Perdana Menteri semestinya juga dapat dipotong sehingga Komisioner dapat memberikan laporan tahunannya langsung kepada Komite khusus yang ditunjuk pada Parlemen.[90]

[90] Ian Brown, *Regulation of Converged Communications Surveillance*, Oxford Internet Institue of the University of Oxford, Oxford, 2009, hal. 20-21.

Selain itu, sistem pengawasan otomatis untuk melakukan penyelidikan lebih lanjut terhadap pelaksanaan penyadapan yang tidak biasa juga perlu diterapkan sehingga Komisioner dapat secara otomatis mendapatkan hasil audit terkait riwayat penyadapan terhadap komunikasi dan riwayat akses terhadap data hasil komunikasi seketika saat upaya penyadapan mulai dilaksanakan.[91] Sistem yang bersifat automatis tersebut juga dapat dilengkapi dengan fasilitas yang bisa mengidentifikasi keabsahan pemberian ijin perintah penyadapan yang bersifat formil (misalnya dengan memeriksa keaslian cap pengadilan), sehingga pelanggaran terhadap tertib administrasi peradilan dapat dicegah dan kepercayaan publik dapat ditingkatkan dengan menekankan bahwa upaya penyadapan yang sewenang-wenang tidak terjadi.[92]

Dalam sebuah laporannya, Komisioner Penyadapan Komunikasi di Inggris bahkan pernah menyampaikan beberapa pelanggaran yang terjadi saat pelaksanaan penyadapan. Selain menjabarkan masalah pelanggaran yang terjadi, Komisioner juga menjelaskan bagaimana mekanisme pertanggungjawaban dan langkah penyelesaian atas pelanggaran tersebut. Adapun kutipan laporan dari Komisioner tersebut adalah sebagai berikut:

> *"2.10 Twenty-four interception errors and breaches have been reported to me during the course of 2007. This is the same number of errors reported in my first Annual Report (which was for a shorter period) and is a significant decrease in the number reported by my predecessor. I consider the number of errors to be too high. By way of example, details of some of these errors are recorded below. It is very important from the point of view of the public that I stress that none of the breaches or errors were deliberate, that all were caused by human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. The most common cause of error tends to be the simple transposition of numbers by mistake e.g., 1965 instead of 1956. The examples that I give are typical of the totality and are anonymous so far as the targets are concerned. Full details of all the errors and breaches are set out in the Confidential Annex."*

(Terjemahan)

"Terdapat dua puluh empat kesalahan dan pelanggaran dalam pelaksanaan penyadapan yang telah dilaporkan kepada saya selama tahun 2007. Jumlah tersebut adalah jumlah kesalahan yang sama yang dilaporkan dalam Laporan Tahunan pertama saya (untuk periode yang lebih pendek) dan merupakan penurunan yang signifikan dibanding dengan jumlah yang dilaporkan oleh Komisioner pendahulu saya. Namun saya menganggap jumlah kesalahan

91 *Ibid.*

92 *Ibid.,* hal. 23.

masih terlalu tinggi. Sebagai contoh, detail dari beberapa kesalahan ini dicatat di bawah ini. Dari sudut pandang publik, saya perlu tekankan bahwa tidak ada pelanggaran atau kesalahan yang disengaja, semua itu disebabkan oleh kesalahan manusia atau kesalahan prosedur atau oleh masalah teknis dan dalam setiap kasus baik ketika penyadapan terlaksana maupun tidak terlaksana, data hasil penyadapan seketika dihancurkan segera setelah ditemukannya kesalahan. Penyebab kesalahan yang paling umum adalah kesalahan penulisan angka yang sederhana secara tidak sengaja, seperti penulisan 1965 yang seharusnya tertulis 1956. Contoh-contoh yang saya berikan adalah tipikal dari keseluruhan yang ada dan bersifat anonim sejauh ini karena menyangkut kepentingan target. Detail lengkap dari semua kesalahan dan pelanggaran tertulis dalam Lampiran yang bersifat rahasia."

Dengan dibukanya informasi terkait indikasi pelanggaran yang terjadi dan proses penyelesaiannya menandakan bahwa sistem akuntabilitas yang diterapkan di Inggris dalam pelaksanaan penyadapan cukup tinggi. Meskipun beberapa informasi terkait hal tersebut juga tetap dapat dirahasiakan untuk pertimbangan tertentu. Pemberian klarifikasi dan koreksi atas kesalahan sebagaimana diuraikan dalam laporan yang cukup transparan dari pihak pengawas tersebut dirasa dapat meningkatkan tingkat kepercayaan publik terhadap setiap tindakan upaya paksa khususnya penyadapan yang dilakukan oleh aparat penegak hukum.

Kemudian, pengawasan juga tidak mesti dibatasi hanya dalam hal pelaksanaan penyadapan. Dalam hal penanganan hasil penyadapan, sistem pengawasan yang efektif juga perlu dibentuk khususnya pada proses pemberian akses terhadap data hasil penyadapan kepada pihak-pihak tertentu. Akses tidak boleh diberikan jika tidak disertai dengan ketersediaan mekanisme pengawasan misalnya melalui pengadilan yang independen dan bersifat publik.[93]

Mekanisme pengawasan yang serupa dengan Inggris juga ditemukan di Australia. Pengawasan dilakukan berdasarkan sistem pelaporan yang dilakukan secara rutin oleh otoritas-otoritas tertentu. Ketentuan mengenai sistem pelaporan terkait pelaksanaan upaya paksa penyadapan diatur dalam Pasal 93 hingga 104 *Telecommunications (Interception and Access) Act 1979*. Selain mekanisme pelaporan, beberapa mekanisme *check and balances* lainnya juga ditemukan ditemukan

[93] Joel Reidenberg, "The Data Surveillance State in Europe and the United States", *49Wake Forest Law Review*, 2014, hal. 606.

pada sistem di Australia, sehingga secara umum, bentuk-bentuk mekanisme pengawasan yang diterapkan di Australia antara lain:[94]

a) Kepala institusi pelaksana penyadapan memberikan salinan dari setiap surat perintah penyadapan telekomunikasi kepada Sekretaris Departemen Dalam Negeri (*Secretary of Home Affairs*);
b) Institusi pelaksana penyadapan membuat laporan kepada *Minister of the Crown of that State*, dalam waktu tiga bulan dari surat perintah yang tidak lagi berlaku, yang merinci penggunaan informasi yang diperoleh dari penyadapan;
c) Sekretaris Departemen Dalam Negeri (*Secretary of Home Affairs*) untuk memelihara Daftar Umum (*General Registry*) yang melingkupi rincian semua surat perintah penyadapan terhadap telekomunikasi. Sekretaris Dalam Negeri harus memberikan Daftar Umum kepada *Minister of the Crown of that State* untuk diperiksa setiap tiga bulan;[95]
d) Sekretaris Dalam Negeri mencatat perincian surat perintah penyadapan terhadap telekomunikasi yang kasusnya tidak mencapai tahap penuntutan dalam waktu tiga bulan sejak waran berakhir Daftar Khusus (*Special Registry*). Daftar Khusus juga diberikan kepada *Minister of the Crown of that State* untuk diperiksa;[96]
e) Pengawasan oleh *Commonwealth Ombudsman* yang berupa inspeksi dan pelaporan.
f) Penyusunan laporan tahunan oleh *Minister of the Crown of that State.*

Lain halnya di Jerman, terdapat dua macam sistem pengawasan terhadap pelaksanaan penyadapan yang dikenal yaitu, pengawasan oleh parlemen (*Board of Parliamentary Members)* dan pengawasan oleh komisi khusus pelaksanaan penyadapan yang bersifat independen (*G 10 Commission*). Komisi G 10 yang terdiri dari seorang Kepala (yang harus berkualifikasi untuk menduduki lembaga yudisial) dan dua penilai (*assessors*) menyusun peraturan dan prosedur operasionalnya secara mandiri dengan persetujuan *Board of Parliamentary Members* yang telah berkonsultasi dengan Pemerintah.[97] Komisi G10 memegang peranan yang cukup signifikan dalam pelaksanaan penyadapan karena, Menteri yang menerbitkan surat perintah penyadapan dalam prakteknya, kecuali dalam keadaan mendesak, selalu menanyakan persetujuan Komisi terlebih dahulu, bahkan Pemerintah juga berencana untuk merevisi undang-undang terkait supaya

94 Department of Home Affairs of the Australian Government, *Op. Cit.,* hal. 23.
95 Telecommunications (Interception and Access) Act 1979, Pasal 81A-81B.
96 Telecommunications (Interception and Access) Act 1979, Pasal 81C-81D.
97 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 21.

menjadikan prosedur tersebut sebagai kewajiban.[98] Di sisi lain, Menteri tersebut juga harus melaporkan setiap perinth penyadapan yang dikeluarkannya setiap bulan kepada Komisi G10,[99] sedangkan pengawasan oleh parlemen dilkukan dalam bentuk pemberian laporan rutin dari Menteri terkait yang mengeluarkan ijin penyadapan. *Board of Parliament* yang terdiri dari lima anggota gabungan antara kelompok oposisi dan pemerintah, setidaknya setiap enam bulan sekali harus menerima laporan pelaksanaan dari undang-undang terkait penyadapan (*the G10 Act*).[100]

3.6. Mekanisme Permohonan Keberatan terhadap Upaya Paksa Penyadapan

Pembentukan mekanisme untuk mengajukan keberatan merupakan perwujudan dari prinsip *due process* yang menghendaki adanya tahapan berupa tata cara yang terbuka dan dapat diuji oleh pihak-pihak terkait untuk memastikan pemenuhan prinsip-prinsip perlindungan hak asasi manusia.[101] Adanya mekanisme pengujian terhadap upaya paksa dilandasi oleh kemungkinan terjadinya *human error* dalam proses penanganan perkara, sehingga ketika mekanisme *challenge* tersebut tersedia, maka proses peradilan pidana dapat menjadi terkendali dan terhindar dari penyalahgunaan kekuasaan maupun sifat otoriter serta aparat juga dapat didorong agar lebih berhati-hati untuk meminimilasir dan mencegah terjadinya kesalahan.[102]

Belanda merupakan salah satu negara yang menganut sistem *due process* dengan menerapkan pengujian keabsahan perolehan alat bukti yang didapat dari mekanisme upaya paksa seperti penggelehan, penyitaan, dan termasuk penyadapan dalam rangka untuk melindungi hak atas privasi warga negaranya. Ketentuan mengenai keabsahan perolehan alat bukti tersebut diatur dalam Pasal 359a *Wetboek van Strafvoordering* (KUHAP) yang menjabarkan tiga konsekuensi terhadap pelanggaran hukum acara perolehan alat bukti sebagai berikut:

a) Pengadilan dapat mengurangi hukuman secara proporsional sesuai dengan tingkat keseriusan pelanggaran yang dilakukan apabila kerugian yang dihasilkan dari penyimpangan tersebut dapat dikompensasi melalui mekanisme ini;
b) Pengadilan dapat mengecualikan alat bukti yang dimaksud; dan

---

98 *Ibid.*
99 The Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 1 ayat (9).
100 The Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act), Pasal 1 ayat (9) angka 1 dan the Rules of Procedure of the Bundestag, poin 12.
101 Reda Manthovani, *Op. Cit.,* hal. 135.
102 *Ibid.*

c) Penuntutan dinyatakan ditolak (*inadmissible)* jika pelanggaran tersebut menjadikan perkara tidak dapat diadili berdasarkan prinsip-prinsip hukum acara pidana yang berlaku.

Hal lainnya yang dapat dijadikan landasan untuk mengajukan komplain misalnya terkait dengan alasan penolakan pemberian akses data hasil penyadapan. Sebagaimana disebutkan di atas bahwa orang yang menjadi target penyadapan mempunyai hak untuk mendapatkan akses terhadap data hasil penyadapan yang dilakukan terhadapnya. Rekomendasi Komite Menteri-Menteri pada Majelis Eropa kemudian mengamanatkan agar pemberian akses tersebut untuk tetap dapat dibatasi sehingga masih terdapat kemungkinan bahwa permohonan tersebut akan ditolak melalui pemberitahuan tertulis yang berisikan alasan-alasan penolakannya. Penolakan hanya dapat dilakukan atas dasar bahwa hal tersebut memang sangat diperlukan untuk kepentingan proses hukum atau untuk melindungi hak dan kebebasan orang lain. Terhadap keputusan tersebut, orang yang menjadi target penyadapan harus diberikan kesempatan untuk dapat mengajukan perlawanan kepada badan pengawas atau badan lain yang independen untuk memeriksa kembali apakah dasar penolakan sudah tepat.[103]

Di Inggris, segala bentuk komplain yang terkait dengan pelaksanaan penyadapan dapat diajukan kepada sebuah *Tribunal* atau pengadilan yang mempunyai kewenangan khusus untuk memeriksa dugaan pelanggaran terhadap pemenuhan hak asasi manusia, yaitu *IPT- Investigatory Powers Tribunal*. Pasal 65 *Regulation of Investigatory Powers Act 2000* (RIPA) menjabarkan hal-hal apa saja yang termasuk dalam kewenangan mengadili pengadilan tersebut, yakni ketika terjadi pelanggaran terhadap prosedur-prosedur yang diantaranya terkait dengan pemberian, perubahan, perpanjangan perintah penyadapan; penanganan hasil penyadapan, pemasangan alat penyadapan, serta kewajiban pemberitahuan pelaksanaan penyadapan.

Dalam melakukan pemeriksaan atas pengaduan oleh individu, IPT memiliki akses terhadap data hasil penyadapan serta informasi terkait pelaksanaan penyadapan yang bersifat rahasia. Berdasarkan Pasal 68 ayat (2) RIPA, IPT memiliki kewenangan untuk meminta Komisioner Penyadapan Komunikasi agar dapat memberikan bantuan dalam bentuk apa pun yang dianggapnya sesuai termasuk memberikan kewenangan kepada IPT untuk meminta akses terhadap semua dokumen yang dianggapnya relevan kepada seluruh pihak yang terlibat dalam proses pemberian

[103] Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies), Prinsip 6.5 dan Prinsip 6.6.

ijin hingga pelaksanaan perintah penyadapan. Dalam hal IPT mengabulkan permohonan pemohon, Pasal 67 ayat (7) RIPA memberikan kewenangan bagi IPT untuk dapat membatalkan perintah penyadapan, memerintahkan pemusnahan data hasil penyadapan, dan memerintahkan pembayaran kompensasi atau ganti rugi (lihat paragraf 80 di atas).

Pengadilan HAM Eropa tidak membatasi bentuk-bentuk "*effective remedy*" yang hanya mengacu pada otoritas pengadilan.[104] Segala bentuk pemulihan (*remedy*) apapun dapat diadopsi sepanjang mekanisme tersebut dapat seefektif mungkin diterapkan untuk kasus-kasus penyadapan yang sifat pelaksanaannya adalah rahasia, sehingga otomatis terdapat keterbatasan-keterbatasan tertentu dalam proses penyelesaian kasusnya.[105] Misalnya di Jerman, tidak ada pengadilan khusus seperti IPT di Inggris yang dapat menangani keberatan yang secara spesifik terkait pelaksanaan penyadapan. Akan tetapi, terdapat sebuah komisi khusus yang bertugas mengawasi pelaksanaan penyadapan dan menerima pengaduan terkait keabsahan pelaksanaan penyadapan, yaitu *G10 Commission*. Selain itu, orang-orang yang merasa dirugikan juga dapat mengajukan keberatan kepada *Federal Constitutional Court* atas pelanggaran Konstitusi/*Basic Law* (meskipun sangat jarang ditemukan karena hanya untuk keadaan luar biasa) atau mengajukan gugatan kepada *Civil Court* untuk mengklaim kerugian dan menuntut ganti rugi atas pelaksanaan penyadapan yang melanggar peraturan yang berlaku.[106]

104 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 67.
105 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 69.
106 European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978), para 71.

Bab IV
Simpulan dan Rekomendasi

4.1. Simpulan

Konstitusi menentukan bahwa hak atas privasi merupakan *derogable rights* yang diatur secara eksplisit dalam Pasal 28G ayat (1) UUD 1945 yang meliputi hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta hak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu. Oleh karenanya, pembatasan terhadap hak tersebut dapat dilakukan sepanjang mendapat justifikasi-justifikasi yakni: (a) penerapannya dilakukan sesuai dengan undang-undang yang telah ditentukan (*rule of law*), (b) dilakukan untuk tujuan yang sah (*legitimate* aim) seperti untuk menjaga ketertiban/keteraturan sosial dan keamanan nasional, dan (c) diperlukan dalam kehidupan masyarakat yang demokratis secara proporsional.

Penerapan penyadapan yang termasuk dalam salah satu metode *secret surveillance* (pengintaian secara rahasia) terhadap komunikasi seseorang merupakan bentuk pembatasan terhadap hak atas privasi. Pada prinsipnya, penyadapan merupakan tindak pidana karena melanggar hak asasi manusia namun terdapat pengecualian-pengecualian ketika penyadapan dapat digunakan secara terbatas yakni untuk kepentingan penegakan hukum dan kepentingan intelijen.

Dalam konteks penegakan hukum, penyadapan termasuk dalam kategori upaya paksa yang bersifat khusus dalam sistem peradilan pidana. Sehingga, hasil dari penyadapan memungkinkan untuk dijadikan alat bukti dalam persidangan, meskipun tidak selalu demikian sebab dalam beberapa kasus hasil penyadapan bisa jadi masih berupa informasi awal yang kemudian digunakan sebagai petunjuk untuk mencari alat bukti yang lain. Ketika data hasil penyadapan digunakan secara langsung sebagai alat bukti di persidangan, maka prinsip-prinsip umum hukum acara pembuktian yang terkait dengan keabsahan perolehan alat bukti hingga akses terhadap alat bukti berupa data hasil penyadapan wajib diberlakukan dalam seluruh rangkaian pelaksanaan penyadapan.

Namun, hukum acara penyadapan di Indonesia masih menghadapi masalah serius terkait inkonsistensi peraturan yang berujung pada pelanggaran terhadap asas kepastian hukum dan persamaan didepan hukum akibat tidak adanya peraturan tunggal yang mengatur tentang

penyadapan secara komprehensif. Sejauh ini, terdapat setidaknya 20 peraturan perundang-undangan yang mengatur mengenai penyadapan yang mana masing-masing peraturan tersebut memiliki prosedur yang berbeda-beda, misalnya dalam hal penentuan durasi penyadapan hingga mekanisme permohonan ijin dan perpanjangannya. Bahkan, terdapat pula masalah tidak adanya transparansi terkait peraturan tentang prosedur penyadapan dari salah satu institusi aparat penegak hukum yang semestinya dapat diakses oleh publik agar dapat dinilai tingkat akuntabilitasnya dalam implementasi peraturan tersebut.

Isu penting lainnya yang juga gagal diakomodir oleh keduapuluh peraturan perundangan tersebut adalah terkait dengan pengelolaan data hasil penyadapan, di antaranya mengenai: prosedur untuk memeriksa, menggunakan, dan menyimpan data yang diperoleh; tindakan pencegahan yang harus diambil saat mengomunikasikan data ke pihak lain; dan keadaan-keadaan dimana data yang diperoleh dapat atau harus dihapus/dimusnahkan. Kemudian, terkait dengan mekanisme keberatan maupun pengawasan yang efektf dalam pelaksanaan upaya penyadapan juga belum tersedia.

Oleh karena itu, sebuah peraturan yang komprehensif dalam bentuk undang-undang menjadi sangat genting untuk segera dirumuskan agar dapat dijadikan sebagai acuan tunggal dalam setiap pelaksanaan tindakan penyadapan baik yang digunakan dalam rangka kepentingan penegakan hukum maupun kepentingan intelijen. Peraturan tentang penyadapan tersebut perlu dirumuskan sedemikian rupa untuk menentukan koridor pembatasan hak atas privasi dapat dilakukan untuk memenuhi tujuan-tujuan berikut: menjaga ketertiban/keteraturan sosial melalui penegakan hukum maupun menjaga keamanan nasional melalui kerja-kerja intelijen.

4.2. Rekomendasi

Dalam merumuskan pengaturan tentang penyadapan, setidaknya enam aspek berikut perlu diperhatikan agar pembatasan terhadap hak atas privasi dipastikan masih berada dalam spektrum yang proporsional serta akuntabilitasnya juga dapat terjamin:

1) **Mengenai proses pemberian ijin dan pelaksanaan penyadapan.** Ketentuan mengenai bilamana pemberian ijin penyadapan dapat diberikan termasuk mekanisme perpanjangannya harus dicantumkan secara spesifik dalam undang-undang, sehingga, lingkup diskresi dari

kewenangan pihak pemberi ijin dalam menentukan dalam keadaan apa dan seberapa lama perintah penyadapan diberlakukan akan dapat diperkirakan (*foreseeable*).

Selain itu, perlu juga dipastikan bahwa dalam penerapannya nanti, mekanisme pemberian ijin maupun memperpanjang ijin penyadapan bukan hanya sekedar "*rubber stamp*" atau dengan kata lain hanya melihat kelengkapan syarat administrasi secara formal. Oleh karenanya, penilaian serta analisis secara kualitatif mengenai alasan dan tingkat kegentingan tiap-tiap kasus juga wajib dilakukan, misalnya dengan mempertanyakan seberapa signifikan kontribusi diterapkannya penyadapan dalam pengungkapan kasus tersebut dan apakah metode investigasi lainnya telah digunakan.

Lembaga yang memberi ijin juga tidak boleh merangkap sebagai lembaga pelaksana penyadapan demi menjaga independensi. Dalam hal ini misalnya otoritas untuk memberikan ijin penyadapan diberikan kepada hakim sedangkan jaksa sebagai pelaksana penyadapan dan yang bertanggung jawab mengumpulkan alat bukti adalah pihak yang mengajukan permohonan ijin.

2) **Mengenai persyaratan penyadapan.** Persyaratan-persyaratan untuk dapat melakukan penyadapan penting untuk diatur seketat mungkin agar pembatasan terhadap hak atas privasi tidak dilakukan secara berlebihan. Setidaknya dua hal berikut perlu menjadi pertimbangan dalam merumuskan persyaratan penyadapan: (a) jenis-jenis tindak pidana; dan (b) kategori orang-orang yang berpotensi menjadi target penyadapan.

Pembatasan terhadap jenis-jenis tindak pidana menjadi penting untuk memberikan pesan bahwa penyadapan tidak perlu diterapkan untuk semua jenis kasus dan harus selalu menjadi pilihan paling terakhir untuk digunakan sebagai metode investigasi sehingga tidak akan dianggap sebagai satu-satunya metode dalam mengungkap perkara. Penyadapan harus dibatasi hanya untuk mengungkap jenis kejahatan atau tindak pidana yang memiliki dampak buruk dan meluas bagi kehidupan bermasyarakat, berbangsa, dan bernegara serta tindak pidana-tindak pidana yang bersifat rumit atau kompleks dalam pengungkapan dan pembuktiannya.

Kemudian, definisi terkait orang-orang yang berpotensi menjadi target penyadapan juga harus dijabarkan karena bisa jadi penyadapan tidak hanya terbatas untuk diterapkan pada tersangka/terdakwa dalam perkara pidana. Selain untuk membatasi agar penyadapan tidak diterapkan terhadap komunikasi sembarang orang, hal ini juga penting agar publik dapat mengetahui dalam hal seperti apa komunikasi dalam zona privat mereka dapat diintervensi. Selain itu, pemberitahuan bagi orang-orang yang pernah disadap bahwa mereka pernah menjadi target penyadapan juga perlu dilakukan sepanjang pemberitahuan tersebut tidak menghalangi tujuan dari pembatasan terhadap kerahasiaan isi komunikasi yang menjadi esensi pelaksanaan penyadapan. Ketika publik dapat menyadari bahwa mereka berpotensi menjadi target penyadapan serta ditambah dengan adanya sistem pemberitahuan tersebut, maka orang-orang yang pernah menjadi target penyadapan akhirnya mempunyai kesempatan untuk dapat meninjau keabsahan pembatasan hak atas privasi melalui penyadapan yang pernah dilakukan terhadap komunikasinya.

3) **Mengenai durasi penyadapan.** Tidak ada standar baku terkait jangka waktu penyadapan maupun berapa kali ijin penyadapan dapat diperpanjang karena perlu mempertimbangkan tingkat kompleksitas kasus per kasus. Namun mekanisme perlindungan dari perintah penyadapan yang sewenang-wenang perlu dibentuk salah satunya misalnya dengan memerintahkan agar pihak pelaksana penyadapan dapat menempatkan perintah penyadapan untuk selalu dapat dilakukan *review* atau penilaian secara berkala, atau jika perlu, surat perintah tersebut juga dapat dimungkinkan untuk dicabut sewaktu-waktu ketika syarat-syarat pelaksanaan penyadapan tidak lagi terpenuhi. Dengan demikian, ketika mengeluarkan surat perintah pemberian ijin maupun perpanjangan ijin penyadapan perlu juga ditegaskan bahwa jika tujuan penyadapan telah tercapai (misalnya informasi yang dicari telah didapatkan) maka pelaksanaan penyadapan harus seketika dihentikan meskipun belum mencapai tenggat batas waktu yang diberikan dalam surat perintah tersebut. Sebaliknya, jika jangka waktu sebagaimana tertera dalam surat perintah tersebut dihabiskan, maka perlu terdapat justifikasi mengapa pelaksanaan penyadapan tersebut memakan waktu yang maksimal dan tidak dapat diselesaikan sesegera mungkin. Sebab dalam pelaksanaan penyadapan, prinsip utama yang perlu dijunjung dalam hal ini adalah agar pembatasan terhadap hak atas privasi dapat ditekan seminimal mungkin.

4) **Mengenai penanganan data hasil penyadapan.** Masalah utama yang wajib diatur yang berkaitan dengan penanganan data hasil penyadapan adalah mengenai mekanisme penyimpanan data dan pembatasan akses terhadap data tersebut. Mekanisme penyimpanan data hasil penyadapan setidaknya harus memuat: (a) tempat dan proses penyimpanan data yang diperoleh dari hasil penyadapan, (b) mekanisme perlindungan keaslian data selama penyimpanan tersebut, (c) kapan data tersebut harus dimusnahkan, (d) prosedur pemusnahan data hasil penyadapan. Pemeriksaan rutin secara periodik perlu dilakukan untuk menilai apakah data hasil penyadapan masih perlu untuk disimpan dan untuk memastikan bahwa data yang ada merupakan data yang terdaftar. Pembentukan sistem pengarsipan yang terorganisir dengan baik dan aman merupakan kunci utama dalam mengatur mekanisme penyimpanan data hasil penyadapan.

   Kemudian, selain otorisasi untuk mengakses data hasil penyadapan hanya diberikan kepada petugas-petugas tertentu, namun pemberian akses terhadap data hasil penyadapan pada prinsipnya perlu dinyatakan secara tegas sebagai hak terutama bagi pihak-pihak yang menjadi target penyadapan. Apabila terdapat kondisi-kondisi dimana akses tersebut tidak memungkinkan untuk diberikan, maka ketentuan lebih lanjut mengenai bentuk-bentuk pengecualian tersebut juga harus dirumuskan dengan jelas. Sehingga, dalam hal permohonan untuk mendapatkan akses ditolak, maka penolakan tersebut disertai dengan alasan-alasan yang telah dinyatakan dalam ketentuan pengecualian yang dimaksud.

5) **Mengenai mekanisme pengawasan dalam upaya paksa penyadapan.** Sistem pengawasan untuk upaya paksa penyadapan perlu dibentuk yang meliputi seluruh rangkaian pelaksanaan penyadapan mulai dari proses awal yakni pemberian ijin hingga proses akhir yakni pemusnahan data hasil penyadapan. Sistem pengawasan dalam bentuk *judicial oversight* maupun *parliamentary oversight* perlu diterapkan secara efektif. Namun, oleh karena rangkaian proses pelaksanaan penyadapan yang panjang dan membutuhkan tingkat keamanan yang mumpuni karena bersinggungan dengan data hasil penyadapan yang sensitif, maka badan pengawas yang memiliki SOP dan bertugas khusus secara *real time* juga akan sangat dibutuhkan. Selain adanya kepentingan untuk meningkatkan akuntabilitas, pelanggaran hak atas privasi yang sangat rentan terjadi dalam pelaksanaan *secret surveillance* seperti penyadapan akan dengan lebih mudah untuk dideteksi sehingga dapat

dicegah dan diminimalisir ketimbang hanya mengandalkan sistem pengawasan yang bersifat *post facto*.

6) **Mengenai mekanisme permohonan keberatan.** Terhadap pelaksanaan upaya paksa penyadapan yang tidak sesuai dengan prosedur, pihak-pihak yang berpotensi dirugikan (tidak hanya terbatas jika pihak yang dirugikan merupakan tersangka/terdakwa dalam perkara pidana) perlu disediakan untuk mengajukan keberatan dan menuntut ganti kerugian. Terlebih jika perihal keberatan berkaitan dengan masalah perolehan alat bukti dalam hal data hasil penyadapan diajukan sebagai alat bukti ke persidangan. Ketentuan ini perlu secara tegas dinyatakan dalam peraturan tentang hukum acara penyadapan.

Daftar Pustaka

Buku

Emily Miskel, 2014. *Illegal Evidence: Wiretapping, Hacking, and Data Interception Laws, State Bar of Texas, Sex, Drugs, & Surveillance*, Chapter 12.

Erasmus A.T. Napitupulu dan Maidina Rahmawati, 2018. *Catatan Awal terhadap RUU Penyadapan versi Pusat Perancangan Undang-Undang Badan Keahlian DPR RI*. Institute for Criminal Justice Reform, Jakarta.

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

Reda Manthovani, 2015. *Penyadapan vs. Privasi*. PT Bhuana Ilmu Populer. Jakarta.

Jurnal

Bert-Jaap Koops, 2018. "*The Shifting Balance between Criminal Investigation and Privacy: A Case Study of Communications Interception Law in the Netherlands*". *Jurnal Information, Communication & Society*, Volume 6 Nomor 3.

Edmon Makarim, 2010. "Analisis terhadap Kontroversi Rancangan Peraturan Pemerintah tentang Cara Intersepsi yang Sesuai dengan Hukum *(Lawful Interception)". Jurnal Hukum dan Pembangunan*, tahun ke-40 Nomor 2.

Gus Hosein dan Caroline Wilson Palwo, 2013. "*Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques". Ohio State Law Journal* Volume 76 Nomor 6.

Ian Brown, 2009. *Regulation of Converged Communications Surveillance*. Oxford Internet Institue of the University of Oxford. Oxford.

Joel Reidenberg, 2014. "*The Data Surveillance State in Europe and the United States". 49Wake Forest Law Review*.

Laporan Lembaga

Department of Home Affairs of the Australian Government, 2018. *Annual Report 2016-2017 on Telecommunications (Interception and Access) Act 1979*. Commonwealth of Australia.

European Union Agency for Fundamental Rights. 2014. *Handbook on European Data Protection Law*. Publications Office of the European Union. Luxembourg.

Human Rights Council. 2009. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*.

Peraturan

Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) of the International Covenant on Civil and Political Rights (HRI/GEN/1/Rev.9 (Vol. I)).

Telecommunications (Interception and Access) Act 1979.

The Act of on Restrictions on the Secrecy of the Mail, Post and Telecommunications (the G 10 Act).

The Omnibus Crime Control and Safe Streets Act 1968.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika.

Putusan Pengadilan

Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 tentang pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap UUD 1945.

European Court of Human Rights Case of Klass and Others v. Germany Application no. 5029/71 (1978).

European Court of Human Rights Case of Malone v. United Kingdom Application no. 8691/79 (1984).

European Court of Human Rights Case of Kruslin v. France Application no. 11801/85 (1990).

European Court of Human Rights Case of Weber and Saravia v. Germany Application no. 54934/00 (2006).

European Court of Human Rights Case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria Application no. 62540/00 (2008).

European Court of Human Rights Case of Liberty and Others v. United Kingdom Application no. 58243/00 (2008).

European Court of Human Rights Case of Iordachi v. Moldova Application no. 25198/02 (2009).

European Court of Human Rights Case of Natunen v. Finland Application no. 21022/04 (2009).

European Court of Human Rights Case of Kennedy v. the United Kingdom Application no. 26839/05 (2010).

European Court of Human Rights Case of Roman Zakharov v. Russia Application no. 47143/06 (2015).

European Court of Human Rights Case of Szabó and Vissy v. Hungary Application no. 37138/14 (2016).

Laman

Dewan Perwakilan Rakyat, Program Legislasi Nasional 2020-2024, http://www.dpr.go.id/uu/prolegnas-long-list. Diakses pada 5 Januari 2020.

Profil Penulis

Iftitahsari, menempuh pendidikan sarjana hukum di Universitas Gadjah Mada, kemudian menyelesaikan pendidikan master Crime and Criminal Justice di Leiden University, Belanda, saat ini berkarya sebagai peneliti di ICJR.

Profil Editor

Luthfi Widagdo Eddyono adalah peneliti di Mahkamah Konstitusi. Beliau mendapatkan pendidikan sarjana hukum internasional Universitas Gadjah Mada (2005) dan master hukum tata negara Universitas Indonesia (2009). Luthfi aktif pada Center for Democratization Studies. Pernah magang dan riset di High Court of Australia dan Federal Court of Australia dalam program Indonesia-Australia Legal Development Facility (IALDF) pada tahun 2009 dan mengikuti Legislative Fellows Program yang diadakan United States of America (USA) Department of State dan American Council of Young Political Leaders (ACYPL) di Washington DC dan negara bagian Washington pada tahun 2010. Pada tahun 2015, beliau terpilih menjadi Asia Young Leader for Democracy 2015 oleh Taiwan Foundation for Democracy. Pada tahun 2018, beliau menjadi salah satu partisipan Recharging Program (Pro curia) di Hague University, Belanda. Beliau juga aktif menulis dalam berbagai media cetak dan online. Buku yang pernah ditulis di antaranya: *Penyelesaian Sengketa Kewenangan Lembaga Negara oleh Mahkamah Konstitusi* (Insignia Strat: 2013), *Memaknai Konstitusionalisme Indonesia* (Penerbit Aura: 2018), dan *Hak Asasi Manusia dan Hukum Internasional di Indonesia* (Rajagrafindo: 2019).

Profil ICJR

Institute for Criminal Justice Reform, disingkat ICJR, merupakan lembaga kajian independen yang memfokuskan diri pada reformasi hukum pidana, reformasi sistem peradilan pidana, dan reformasi hukum pada umumnya di Indonesia.

Salah satu masalah krusial yang dihadapi Indonesia pada masa transisi saat ini adalah mereformasi hukum dan sistem peradilan pidananya ke arah yang demokratis. Di masa lalu hukum pidana dan peradilan pidana lebih digunakan sebagai alat penompang kekuasaan yang otoriter, selain digunakan juga untuk kepentingan rekayasa sosial. Kini saatnya orientasi dan instrumentasi hukum pidana sebagai alat kekuasaan itu dirubah ke arah penopang bagi bekerjanya sistem politik yang demokratis dan menghormati hak asasi manusia. Inilah tantangan yang dihadapi dalam rangka penataan kembali hukum pidana dan peradilan pidana di masa transisi saat ini.

Dalam rangka menjawab tantangan tersebut, maka diperlukan usaha yang terencana dan sistematis guna menjawab tantangan baru itu. Suatu grand design bagi reformasi sistem peradilan pidana dan hukum pada umumnya harus mulai diprakarsai. Sistem peradilan pidana seperti diketahui menduduki tempat yang sangat strategis dalam kerangka membangun *the Rule of Law*, dan penghormatan terhadap hak asasi manusia. Sebab demokrasi hanya dapat berfungsi dengan benar apabila ada pelembagaan terhadap konsep *the Rule of Law*. Reformasi sistem peradilan pidana yang berorientasi pada perlindungan hak asasi manusia dengan demikian merupakan "*conditio sine quo non*" dengan proses pelembagaan demokratisasi di masa transisi saat ini.

Langkah-langkah dalam melakukan transformasi hukum dan sistem peradilan pidana agar menjadi lebih efektif memang sedang berjalan saat ini. Tetapi usaha itu perlu mendapat dukungan yang lebih luas. Institute for Criminal Justice Reform (ICJR) berusaha mengambil prakarsa mendukung langkahlangkah tersebut. Memberi dukungan dalam konteks membangun penghormatan terhadap the Rule of Law dan secara bersamaan membangun budaya hak asasi manusia dalam sistem peradilan pidana. Inilah alasan kehadiran ICJR.

Sekretariat: Jl. Komplek Departemen Kesehatan Nomor B-4, Pasar Minggu, Jakarta Selatan – 12520

Phone/Fax: 02127807065 **Email:** infoicjr@icjr.or.id

ICJRId ICJRID ICJRID perkumpulanicjr