Formosa Journal of Multidisciplinary Research (FJMR)
Vol.1, No. 2,2022: 367-382

Dampak Implementasi Lawfull Interception pada Pemberantasan Tindak Pidana Terorisme

Ade Mulya[1]*, Marzuki Ismail[2], R. Bayu Yuliantoro[3], Heriyanto Kandati[4]
Sekolah Tinggi Ilmu Kepolisian ,DKI Jakarta

ABSTRACT: The terrorism is crime categorized as a serious threat that requires speed of handling with the support of access to accurate and fast information. The Lawful Interception approach that has been accommodated in the latest revised terrorism law has made an important contribution. This is a new way to speed up the investigation of criminal acts of terrorism. The research was conducted qualitatively by studying literature and in-depth interviews with 3 informants. The research focus on law enforcement for criminal acts of terrorism in Indonesia. The results of the research study state that the impact of Lawful Interception has a significant influence in assisting the process of disclosure and investigation of criminal acts of terrorism. However, there is a need for oversight and procedures to guard against potential breaches of privacy.

Keywords: Lawful Interception, Terrorism, Crime, Investigation, Policing

ABSTRAK: Tindak pidana terorisme masuk kategori ancaman serius yang memerlukan kecepatan penanganan dengan dukungan akses informasi yang akurat dan cepat. Pendekatan *Lawful Interception* yang sudah diakomodasi dala m undang undang terorisme hasil revisi terakhir memberikan kontribusi pentin g. Hal ini menjadi jalan baru untuk mempercepat penyelidikan tindak pidana terorisme. Penelitian yang dilakukan secara kualitatif dengan studi literatur dan wawancara mendalam terhadap tiga narasumber. Lokus penelitian pada penegak hukum tindak pidana terorisme di Indonesia. Hasil kajian penelitian menyatakan bahwa dampak *Lawful Interception* mempengaruhi secara signifika n dalam membantu proses pengungkapan dan penyelidikan tindak pidana terorisme. Namun demikian, perlunya pengawasan dan prosedur untuk menja ga potensi pelanggaran privasi

Keywords: Lawful Interception, Terorisme, Tindak Pidana, Penyelidikan, Pemolisian

*Submitted**: 03-06-2022;** Revised: **15-06-2022**; Accepted:**28-06-2022***

Corresponding Author: ademulya838@gmail.com,

DOI prefik: 10.55927
ISSN-E: 2829-8896
https://journal.formosapublisher.org/index.php/fjmr

PENDAHULUAN

Pada penanganan tindak pidana terorisme, penegak hokum mendapatka n tambahan kewenangan dalam bentuk regulasi, yaitu adanya revisi Undang-Undang Terorisme. Terjadi dua kali revisi menjadi Undang-Undang Republik Indonesia Nomor 5 Tahun 2018, Tentang Perubahan Atas Undang Undang No mor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undan g-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang. Revisi Undang-Undang tersebut menjadi landasan hukum yang lebih kuat dalam menjamin perlindungan dan kepastian hukum dalam pemberantasan tindak pidana terorisme. Dalam revisi undang-undang ini, sangat signifikan adanya *Lawful Interception* atau upaya yang legal menurut hukum atau peraturan perundangan untuk mengambil informasi dari komunikasi.

Secara khusus segala bentuk penyadapan dilarang secara hukum kecuali *lawfull interception*. Pada prinsipnya data pribadi dijamin keamanannya. Pada Undang-Undang Nomor 39 Tahun 1999 tentang telekomunikasi, terdapat kata penyadapan, namun tidak ada penjelasannya secara rinci. Pada pasal 40 Undang-Undang tersebut menyebut "*bahwa setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun*". Ini artinya entitas mana saja, termasuk pemerintah, sektor swasta dan warga negara dilarang melakukan tindakan penyadapan.

Model pemolisian pencegahan dan pemberantasan terorisme dengan tiga syarat, yakni: kesiapsediaan sumber daya manusia yang mumpuni dalam merespon ancaman terorisme, adanya integrasi pada pencegahan, pemberantas an dan penegakan hukum, dan kebijakan yang terintegrasi dari pimpinan Polri (Muradi, 2017). Beberapa alasan penting penggunaan *Lawful Interception* untuk penyelidikan tindak pidana terorisme dalam mengungkap, jaringan terorisme, kejahatan dunia *cyber oleh kelompok teror*, pencurian data, peredaran narkotika (diatur dalam Undang-Undang tersendiri), dan berbagai kejahatan yang perlu penanganan khusus. Tindakan penyadapan pada hakikatnya merupakan tinda kan yang dilarang dalam hokum pidana akan tetapi sangat diperlukan (Christia nto, 2011). Perspektif yang kontra dengan *Lawful Interception* dengan alasan privasi, potensi pelanggaran hak asasi manusia, pelanggaran penggunaan saluran komunikasi serta keamanan pribadi. Perlindungan privasi merupakan hak dasar dari hak asasi manusia, karenanya UU perlu mengatur mekanisme tata cara dan saluran komplain secara khusus baik untuk kepentingan penegakan hukum ataupun intelijen. (Ardhiansyah, 2012)

Konsekuensi yang harus dilakukan agensi penegakan hukum, harus adanya kontrol yang akuntabel dari petugas pelaksanaan *Lawful Interception* ini, dengan mendasari ketentuan perundangan yang berlaku. Adanya buku *log* atau buku catatan kegiatan serta otorisasi yang dilakukan oleh pimpinan terhadap pelaksanaan petugas *Lawful Interception* untuk mengungkap kejahatan , melakukan penyelidikan serta membawanya ke pengadilan dengan bukti akurat.

Pada penyelidikan, data biasanya tersedia dalam volume besar dan beragam, serta menggambarkan fakta individu yang tidak dapat disangkal. Permintaan terhadap data individu adalah contoh data yang sangat baik, karena merupakan pernyataan fakta yang sederhana. Pengumpulan intelijen yang akurat, terperinci, dan tepat waktu menopang pengambilan keputusan penegakan hukum (Nunan et all., 2020). Data tersebut merupakan juga laporan-laporan yang telah ada sebelumnya. Sedangkan informasi dihasilkan ketika serangkaian titik data digabungkan untuk menjawab pertanyaan sederhana. Misalnya, dengan mengikuti contoh data status perkawinan seseorang, maka akan terhubung dengan siapa keluarganya, dan lokasi mereka menikah dan status dalam perkawinan serta pekerjaan atau alamat yang terkait dari perkawinan tersebut. Data yang terkumpul dan terhubung akan menjadi sebuah informasi. Pada akhirnya data dan informasi akan menjadi intelijen, yang membawa proses lebih mendalam dengan "menginterogasi" data dan informasi menjadi intisari atau prediksi yang dapat digunakan untuk pengambilan keputusan. Intelijen tidak pernah menjawab pertanyaan sederhana, melainkan menjawab pertanyaan yang jauh lebih rumit.[1]

Dikaitkan dengan *Lawful Interception,* maka yang dapat menjadi target telah melewati rangkain proses keputusan dan atas pertimbangan bahwa target sangat berbahaya. Dalam menentukan target dengan reduksi dari tahapan peng umpulan intelijen yang menjadi data. Selanjutnya dengan proses pengolahan dan pendalaman menjadi informasi. Pada tahap selanjutnya dilakukan analisis dan menghasilkan intelijen yang menjadi laporan dan bahan pengambilan keputusan. Ilustrasi tentang bagaimana data, informasi dan sampai menjadi intelijen (Demsey, M., 2013) pada gambar berikut.

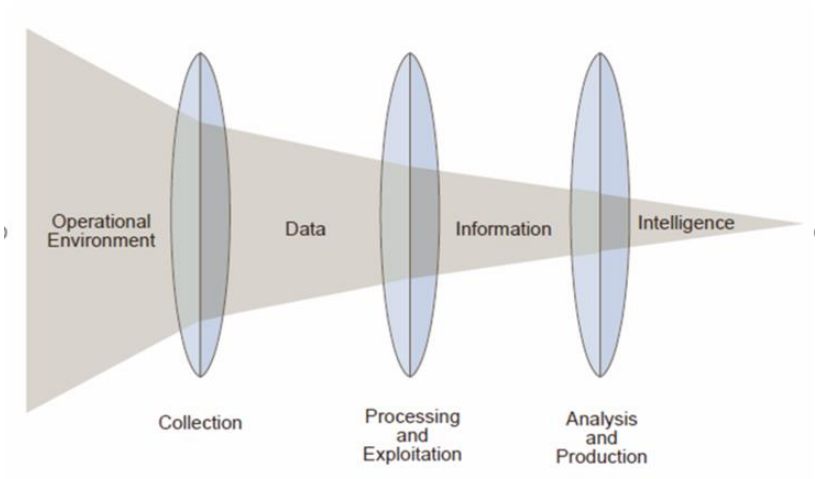

Figure 1 Relation of Data, Information and Intelligence[2] (Dempsey, M. 2013)

Tujuan pada penelitian menemukan nilai kebaruan dari *Lawful Interception* yang melibatkan teknologi dari cara penyelidikan intelijen pada

tindak pidana terorisme yang sebelumnya menggunakan intelijen manusia (*human intelligence*). Intelijen manusia menggunakan cara manual dan proses yang lebih lama serta kapasitas data yang terbatas.

Pada paper ini membahas secara khusus bagaimana teknologi membantu dalam penyelidikan tindak pidana terorisme berbentuk regulasi dalam bentuk Undang-undang. Pada sisi lain, tindakan *lawful interception* mengalami perubahan karena teknologi yang dinamis dan terus berkembang, sehingga tantangan perkembangan teknologi terhadap kondisi target. Namun demikian, peran manusia tetap diperlukan dalam proses *lawful interception.*

TINJAUAN PUSTAKA

Dalam diskursus tentang terorisme tidak ada definisi yang disepakati para pakar. Federal Bureau of Investigation (FBI), Departemen Luar Negeri Amerika serikat dan Departemen Pertahanan AS memiliki perbedaan dalam mendefinisikan terorisme. Sedangkan definisi sebuah kelompok atau organisasi teroris (Hofmen, 2004) didefinisikan sebagai individu yang dikelompokkan atau diorganisasi dengan tujuan berpartisipasi dalam kegiatan yang melanggar hukum yang dirancang untuk mengintimidasi pada populasi sipil atau memaksa pemerintah, atau segmen apa pun darinya, untuk mencapai tujuan politik atau sosial tertentu.[3] Karenanya perlu ada tindakan khusus dalam mencegah dan menanggulangi terorisme, seperti lawful interception untuk mempermudah dan mempercepat dan mengintegrasikan para penegak hukum dan stake holder lainnya.

Sebelumnya, Putusan Mahkamah Konstitusi Nomor 5/PUU-VIII/2010 menyatakan bahwa sejatinya penyadapan (interception) adalah sebuah perbuat an melawan hukum karena tindakan tersebut melanggar privasi orang lain, maka pengaturan penyadapan harus dalam bentuk undang-undang dan UU tersebut akhirnya lahir pada tahun 2018. Pada dasarnya *lawful interception* merupakan kegiatan pengumpulan data dan informasi. Selaras dengan teori intelijen yang dipergunakan, dan merujuk pada Pruckun (2010) intelijen memiliki 4 pengertian, (1) intelijen sebagai aksi atau proses yang dipergunakan untuk menghasilkan pengetahuan, (2) bagian dari pengetahuan yangdihasilkan , (3) organisasi yang berkaitan dengan pengetahuan, seperti organisasi Intelijen, (4) serta laporan atau arahan yang diberikan dalam proses suatu organisasi. Selain itu, pada siklus intelijen memiliki tujuan dan kepentingan organisasinya. Ada empat tahapan yang akan dikerjakan, yaitu penentuan tujuan yang ingin dicapai (*direction/requirement*), pengumpulan data (*collecting*), analisis data (*analyzing*) dan penyampaian intelijen dari hasil analisis kepada user (*disseminat ion*). Teori tersebut dipergunakan pada proses analisis terhadap pelaksanaan *lawfull interception* dalam upaya penyelidikan dengan pengumpulan data (*collecting*).

Seluruh informasi intelijen yang diperoleh dari *lawful interception* bersifat rahasia (Gardner, 2017). Artinya distribusi informasi harus terbatas dan semata-

3

mata demi penegakan hukum, sehingga badan badan lain dapat mengembangk an rekomendasi kebijakan untuk meningkatkan kerjasama antara berbagai instansi dalam penanganan terorisme agar memberikan perlindungan kepada masyarakat dengan lebih baik.[4]

Diawali dari tahapan pengumpulan data dan informasi sampai pada tahapan hasil dari *lawful interception* yang berupa isi komunikasi penting yang bisa mengkaitkan dengan content, isi pembicaraan, lokasi, dan koneksi antara jaringan tersebut, dirangkaikan dengan sebuah analisis. Pengambil keputusan perlu menyadari seperti apa situasi di masa depan dan apa yang lebih mungkin terjadi. Prediksi absolut tidak mungkin saat menghadapi situasi yang kompleks. Oleh karena itu, penilaian seperti analisis estimasi, prakiraan, atau analisis masa depan sebagai gantinya (*Pherson & Pherson*, 2013 in *Lars C. Borg*, 2017). Menurut Mahyudin (2016), sejumlah institusi dengan peran intelijen masing masing harus bekerja dalam satu strategi yang sama. Adanya kesadaran bersama bahwa dengan memanfaatkan kemajuan teknologi informasi, khususn ya media sosial dan internet, dapat mencegah kelompok teroris menyebarkan propaganda sekaligus perekrutan kepada siapa saja yang mengakses domain siber.

Seth Harrison menyatakan kebijakan kontraterorisme semakindipolitisas[5]. Bahwa strategi kontra terorisme harus fokus pada akar penyebab teror. Di masa lalu, kebijakan kontra terorisme sebagian besar tidak dipengaruhi wacana politik yang mengganggu. Jika pendekatan teknologi informasi dalam untuk kontra terorisme ingin dilanjutkan, maka menggunakan pendekatan apolitis[6]. Adaptasi teknologi harus dilakukan, karena terus menerus berkembang dan mewajibkan adanya kompatibilitas perangkat, peralatan, komunikasi, protokol, dan koneksitas.

Kegiatan *lawful interception* pada dasarnya upaya untuk mengumpulkan informasi untuk menemukan tindak pidana terorisme dengan mengerjakan tahap tahap dalam pengarahan (*direction/requirement*), pengumpulan data (*collec ting*), analisis data (*analyzing*) dan hasil analisis kepada user (*dissemination*). Hasil dari analisis intelijen dapat digunakan sebagai bukti dalam sidang di pengadilan sebagaimana diatur dalam Undang-Undang Terorisme.

Penelitian sebelumnya di berbagai negara, menggunakan teknologi yang berbasis pada *Lawful Interception* dengan bekerja secara legal antara penegak hukum dengan penyelenggara telekomunikasi atau secara mandiri untuk mendapatkan informasi komunikasi dari target. Hal ini diatur khusus dan mekanisme pengaturan yang telah disepakati. *Lawful Interception* adalah proses membuka akses pada penyedia layanan atau operator jaringan mengumpulkan dan menyediakan komunikasi yang menjadi target atau sasaran baik oleh individu atau entitas kepada pejabat penegak hukum yang telah diatur dalam Undang-Undang. Sebelumnya implementasi *Lawful Interception* diatur oleh

Resolusi Dewan Eropa sejak tanggal 17 Januari 1995 yang menegaskan *Lawful Interception* untuk mencegah kejahatan, termasuk penipuan dan terorisme.

Dalam konteks Indonesia, legalitas terhadap lawful interception diatur pada UU Anti Terorisme Nomor 5 Tahun 2018 pada pasal Pasal 31A menyebutkan:

"Dalam keadaan mendesak penyidik dapat melakukan penyadapan terlebih dahulu terhadap orang yang diduga kuat mempersiapkan, merencanakan, dan/atau melaksanakan Tindak Pidana Terorisme dan setelah pelaksanaannya dalam jangka waktu paling lama 3 (tiga) hari wajib meminta penetapan kepada ketua pengadilan negeri yang wilayah hukumnya meliputi tempat kedudukan penyidik."

Meskipun lawful interception memiliki banyak keunggulan, namun teknologi tidak memiliki tiga kualitas vital pada manusia: (1)pengalaman, (2) nilai dan penilaian. Jadi teknologi menawarkan pelacakan komunikasi teroris dan memprediksi serangan, tapi bukan pengganti penilaian manusia dan teknologi tersebut harus digunakan manusia dengan cermat. (Kumar, 2019).

METODOLOGI

Metode yang digunakan dengan pendekatan penelitian kualitatif, yang spesifikasi penelitian pada *lawful interception* oleh aparat penegak hukum. Teknik pengumpulan data dengan studi literatur dan wawancara mendalam dengan narasmber. Metode analisis yang dipergunakan adalah dampak implementasi *lawfull interception* dan analisis siklus intelijen, bahwa *lawful interception* adalah proses pengumpulan intelijen. Selanjutnya memperlihatkan bagaimana hasil *lawful interception* masuk tahapan proses ke pengadilan sebagai bagian dari pembuktian.

Kerangka berpikir diawali dengan penyelidikan awal terhadap objek, data lapangan, *database* jaringan dan semua *raw data* yang masuk sebagai bahan untuk penyelidikan lanjutan, termasuk laporan dari petugas di lapangan. Dilanjutkan dengan proses *lawful interception.* Selain itu, dapat berupa pengembangan kasus yang masih menyisakan jaringan yang belum terungkap.

HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian menjelaskan *lawwful interception* merupakan upaya pengumpulan intelijen melalui *signal intelligent* yang melalui dua teknis yaitu *communication intelligence* (comint) dan *electronic intelligence* (elint). Pada dasarnya sumber pengumpulan intelijen lainnya menjadi bagian penting dalam mendukung dan konfirmasi selama proses pengumpulan intelijen.

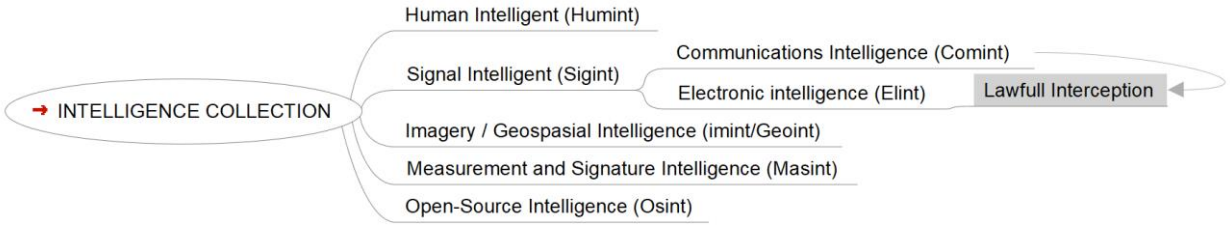

Figure 2 : Posisi *Lawfull Interception* sebagai proses dalam *Intelligence Collection* (Bagan diolah oleh penulis)

Penguatan dalam Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme yang fokus pada implementasi praktis Teknologi Informasi dan Komputer (TIK) melalui *Lawful Interception*-nya lebih cepat daripada metode investigasi manual yang cenderung lambat. Gagasan TIK adalah alat pengumpulan intelijen yang memiliki tempat penting dalam pemolisian modern. Hal ini mengidentifikasi bahwa yang paling efektif penggunaan TIK didasarkan pada kerangka kerja proaktif dan tidak pasif menunggu. (*Mitchell Congram & Peter Bell, 2010*).

Perubahan secara teknis dari penyelidikan manual berubah kepada penyadapan secara legal atas dukungan TIK berdasarkan hukum pada tabel sebagai berikut :

Tabel 1 : Perbedaan penyelidikan manual dengan *lawfull interception*.[7]

Penyelidikan Manual	**Penyelidikan Lawful Interception**
Kemampuan intelijen manusia	Penggunaan teknologi penyadapan *European Telecommunications Standards Institute* (ETSI) atau *European Telecommunications Standards Institute* (Calea)
Sumber Daya Manusia lebih banyak	Sumber Daya Manusia teknis untuk *surveillance*
Unit taktis dengan peralatan bergerak	Unit taktis dan stasioner
Informasi cenderung parsial teknis intelijen dan kegiatan rutin	Informasi komprehensif dengan ijin pengadilan
Bertujuan analisis informasi dan laporan intelijen	Bertujuan membawa sebagai bukti di pengadilan
Analisis yang dilakukan untuk laporan intelijen	Analisis yang dilakukan bertujuan untuk menemukan fakta dan pembuktian di pengadilan

Standar baku yang ada pada penyadapan yang dilakukan mengacu pada dua standar, yaitu (1). *European Telecommunications Standards Institute (ETSI),* berlok asi di negara Prancis, dan (2). *Communications Assistance for Law Enforcement Act (Calea*), berlokasi di Amerika Serikat. Tentu saja, standar mana yang dipergunakan aparat penegak hukum merupakan rahasia yang harus dijaga demi pelaksanaan tugas dan menghindari kerawanan yang tidak perlu atau efek merugikan.

Standar dalam tindakan penyadapan yang dilakukan bertujuan untuk penyesuaian perangkat komunikasi sasaran agar menjadi kompatibel terhadap pelaksanaan *Lawful Interception*. Pada komunikasi internet, maka sarana yang dapat dilakukan *Lawful Enforcement* antara lain : akses ke internet itu sendiri, kegiatan berselancar di dunia maya, penggunaan email, group email, media chat berbasis internet, akun yang dipergunakan untuk login, aplikasi pada percakapan (chat) Facebook atau *market place*, penggunaan komunikasi melalui Voip, pemindahan file melalui File Transfer Protocol (FTP), telnet, bluetooth, aplikasi *sharing* antara *handphone* dengan laptop atau komputer. Berkaca pada infrastruktur yang berbeda-beda dan protokol komunikasi yang berbeda akan menambah kompleksitas pelaksanaan terhadap saluran komunikasi yang diamankan dengan *Virtual Private Network* (VPN). Hal demikian merupakan tantangan yang menyulitkan dilakukannya *lawful interception*, sehingga perlu pengembangan teknik dan akses legal untuk membukanya.

Penyelidikan yang dilakukan dengan menggunakan cara manual menyebabkan lamanya waktu dalam mengungkap jaringan terorisme di Indonesia. Penggunaan teknologi dalam penanggulangan terorisme sangat penting. Hal ini untuk mendapatkan pembuktian di pengadilan dengan memanfaatkan *lawful interception.* Terlihat bagaimana dampak perubahan yang terjadi antara penggunaan penyelidikan secara manual dengan penyelidikan melalui *lawful Interception.*

Melakukan *profiling* terhadap target sasaran, dan mencari informasi komunikasi yang dipergunakan. Pada saat ini sarana komunikasi yang sering digunakan adalah telepon selular, radio *handy talky*, dan telepon kabel. Masing-masing memiliki karateristik tersendiri. Apabila sasaran menggunakan telepon selular, maka dapat ditemukan nomor telepon selular dan dapat dilakukan proses selanjutnya. *Lawfull Interception* dilakukan dengan prosedur yang ketat. Kontra dari *lawfull interception* ini adalah *Encrypted Communication* dan berbagai algoritma encryption yang menyebabkan komunikasi tersebut menjadi tidak dapat didengarkan karena seperti suara sinyal (*noise*). Pada *short message service* (sms), perlindungan komunikasi dengan menggunakan beberapa algoritma untuk mengacak data menjadi tidak dapat dibaca yang tidak memiliki makna. (Seth & Rajan, 2011).

Segala bentuk ancaman terorisme harus diperhitungkan dengan mengukur ancaman, dirumuskan dan kodefikasi relevansi. Analisis ancaman bertujuan untuk mengukur tingkat ancaman sehingga dapat dilakukan upaya mengurangi tingkat ancaman menjadi lebih rendah dan mengurangi bahaya. Untuk dapat mengetahui ancaman terorisme perlu memperhatikan komponen dari ancaman yang menurut Prunckun (2002), yaitu adanya kenginan dan

tindakan dari seseorang atau organisasi yang dapat membahayakan keamanan. Selanjutnya dilakukan upaya deteksi (untuk persiapan dalam *lawful interception*), dengan tujuan mencapai kesiapan dalam melakukan antisipasi dan penindakan dengan cara mengidentifikasi sesuai dengan prinsip dari deteksi[8] (Prunckun, 2002: 43), antara lain :

1. Identifikasi peristiwa yang menjadi tujuan teroris. Tujuannya menemukan rencana umum atau target yang ditentukan oleh kelompok teroris, termasuk dengan memperhatikan kondisi perkembangan dinamika dunia dan isu yang berkembang. Kisaran suara dari berbagai pihak dapat dijadikan analisis sementara terhadap ancaman teroris.
2. Identifikasi orang-orang yang dapat melakukan serangan. Setiap orang-orang yang terlibat dalam aksi terorisme sebelumnya perlu dilakukan analisis dan pemantauan. Laporan intelijen dianalisis terkait dengan tujuan penyerangan. Identifikasi terhadap calon pelaku serangan teror ini sangat penting, dan dengan pendekatan *lawful interception* sehingga akan memungkinkan untuk mendeteksi dinamika kelompok dan desas-desus yang berkembang sampai kepada fakta-fakta perbuatan.
3. Identifikasi organisasi yang terlibat dan mendukung serangan. Dari *database* organisasi yang sudah terkumpul dan anggota dari organisasi tersebut, termasuk lokasi, pergerakan dan peran dalam organisasinya. Posisinya sekarang dan aktivitas yang akan dilakukan dapat diperhitungkan dengan melaksanakan indentifikasi organisasi.
4. Identifikasi berdasarkan tempat dan ketertarikan wilayah. Sebagaimana kelompok teror dalam jaringan dan juga dalam sel, memiliki ketertarikan pada wilayah tertentu atau pembagian wilayah. Kita kenal ada Mujahidin Indonesia Timur yang beroperasi dan berpusat di Poso Sulawesi Tengah dan Sekitarnya. Selain itu dikenal sebagai Mujahidin Indonesia Barat dengan wilayah mereka pada Jawa Barat, Lampung dan sebagian besar wilayah Sumatera.
5. Mengumpulkan semua fakta yang menunjukkan bahwa seseorang akan melakukan serangan (*attack*). Pada setiap tahapan dalam melakukan serangan adanya persiapan, sehingga dengan melakukan *law inforcement* dari hasil *Lawful Interception* tersebut dapat dideteksi setiap pergerakan persiapan kelompok terorisme tersebut, termasuk individunya.

Dengan menggunakan pendekatan deteksi tersebut, akan mempersempit fokus sasaran deteksi dan memudahkan dalam melakukan *lawfull interception.* Pada prosesnya akan menghadapi situasi kelompok jaringan atau group komunikasi yang menghubungkan antara satu dengan lainnya. Pelaksanaan *lawfull interception* harus memiliki target yang khusus.

Dampak implementasi *Lawfull Interception* dari hasil penelitian dapat ditabulasi sebagai berikut :

Indikator	Dampak Implementasi
Waktu mengungkap kasus	Lebih cepat
Deteksi ancaman	Ancaman lebih cepat terdeteksi
Locus ijin pengadilan pada wilayah kantor penyidik	Birokrasi yang lebih cepat
Tradisional dan nontradisional	Nontradisional melibatkan teknologi
Waktu pelaksanaan lawfull interception	1 (satu) tahun dan dapat diperpanjang 1 (satu) tahun
Sarana komplain	Melalui pengadilan
Kerja sama dengan stake holder	Mudah dengan payung hukum UU

Tabel 2 : Dampak implementasi *Lawfull Interception*

Penyelidikan tindak pidana terorisme memiliki kemajuan yang sangat baik. Pada pasal 31 Undang Undang Nomor 5 Tahun 2018 memberikan akses penyad apan (*Lawful Interception*) terhadap penyelidikan tindak pidana terorisme. Hal ini, memberikan keleluasaan dan payung hukum dalam pelaksanaan tugas penyelidikan oleh penegak hukum pada tindak pidana terorisme ini. Penyidik dalam pelaksanaan tugas *lawful interception* wajib melaporkan semua aktivitas penyadapan kepada atasannya dan tembusan ke Kementerian Komunikasi dan Informatika.

Dari hasil wawancara dengan narasumber 1, 2, dan 3 yang dilakukan selama penelitian dalam periode waktu antara Maret 2022 sampai dengan Juni 2022 ditemukan bahwa penyadapan dilakukan dengan peralatan khusus denga n mekanisme kontrol ketat yang harus dijalankan. Adapun hasil wawancara dapat klasifikasikan sebagai berikut :

1. Penggunaan peralatan penyadapan sudah dilakukan dengan memperhatik an berbagai aspek keamanan dan juga tingkat prioritas dari tujuan pelaksanaan kegiatan baik penyelidikan (sebagai upaya menemukan tindak pidana) maupun dalam penyidikan dalam upaya mengungkap kasus dan membawa ke pengadilan.
2. Dampak implementasi *lawful interception* secara umum meliputi (1) penyadapan aktif , yaitu penyadapan yang dilakukan secara langsung, (2) Penyadapan semi aktif, dan (3) Penyadapan pasif. Namun ciri khas yang penting adalah adanya akses legal yang dilindungi dengan undang-undang untuk akses terhadap informasi komunikasi sasaran.
3. Mekanisme kontrol dilakukan sesuai dengan prosedur yang dijalankan. Bahwa penyadapan yang dilakukan oleh aparat penegak hukum, harus berdasarkan atas peraturan dalam tingkat Undang-Undang dan hal ini sudah dimuat dalam Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme. Mekanisme komplain kepada pengadilan dimana proses pembuktian terhadap tersangka dilakukan.
4. Adanya penyidik yang terlatih dalam melakukan tugas *lawful interception* serta dengan adanya perintah (*warrant*) yang jelas dan tujuan serta proses pencatatan yang tertib. Karena sifatnya yang rahasia dan khusus, maka

hasil apapun dari *lawful interception* bersifat rahasia sampai nantinya dibuka di pengadilan.

5. Kerja sama yang dilakukan aparat penegak hukum dengan penyelenggara jasa telekomunikasi dengan menggunakan protokol komunikasi serta dengan dilengkapi peralatan. Pada konteks tersebut, karena nyata dinyatakan dalam Undang-Undang, maka yang menjadi sasaran dari *lawful interception* dapat dibuka dan diberikan kepada penyidik, demikian juga sebaliknya apabila bukan sasaran dalam penyelidikan, maka sama sekali tidak boleh dibuka datanya.
6. Hasil *lawful interception* dapat menemukan informasi yang terbungkus dengan enkripsi, baik *end to end encryption* maupun *full device encrytion*[9], sehingga perlu upaya lanjutan untuk membuka agar terbaca atau terdengar informasi hasil *lawful interception* tersebut (Graham, 2016). Karena hasilnya tidak hanya dalam bentuk suara, namun juga data, file, suara, folder, informasi berupa teks atau gambar, jejak atau lokasi, pergerakan dalam wilayah dan sebagainya, maka perlu proses lanjutan seperti analisis lanjutan.
7. *Lawful interception* dapat dipergunakan untuk melakukan pencegahan dala m konteks kesiapsiagaan nasional, kontra radikalisasi dan deradikalisasi dengan BNPT yang mengoordinasikan antarpenegak hokum dalam penang gulangan terorisme hingga mengoordinasikan program pemulihan korban.

Lawful interception dalam rangkaian penyelidikan terhadap sasaran dan target dalam komunikasi yang melewati radio, telepon, internet dan alat komunikasi lainnya, dilakukan dengan rentang waktu paling lama satu tahun dan dapat diperpanjang selama 1 (satu) tahun. Rentang waktu tersebut relatif cukup dengan waktu penyelidikan untuk membuka jaringan teror sampai ke akar-akarnya. Mulai dari tahap persiapan, perencanaan, dan pelaksanaan penindakan tindak pidana terorisme. Penyidik memiliki kesempatan untuk mengendus sasaran dari mulai tahap kelompok teroris ini merencanakan, sehingga dapat dicegah dan ditanggulangi dengan baik.

Klausul penting, bahwa permintaan ijin kepada pengadilan pada wilayah kedudukan penyidik, dan bukan pada *locus* dari target. Artinya ada perluasan yurisdiksi dimanapun targetnya, maka cukup satu kantor pengadilan saja, untuk mengajukan ijin *lawful interception* tersebut, sehingga akan memudahkan dalam proses permintaan ijin kepada pengadilan pada *locus* kedudukan penyidik bukan kedudukan target.

Dukungan terhadap penindakan terorisme juga muncul dari penerapan *E-Policing*dapat mengatasi berbagai isu-isu kerawanan yang makin berkembang seperti terorisme, kondisi keamanan lintas, batas negara, keamanan wilayah maritim, spionase, HAM Internasional, dan senjata pemusnah massal[10]. Upaya penegak hukum dalam melaksanakan tugas tersebut, merupakan juga tugas pemolisian penegakan hukum terhadap teroris, maka sangat relevan dengan pemolisian berkontribusi pada penanganan tindak pidana terorisme (Chryshna

nda, 2020). Selain itu, peranBadan Nasional Penanggulangan Terorisme (BNPT) sebagai organ negara yang secara luas mengkoordinasikan setiap upaya penanggunangan terorisme. Namun Istiqomah (2013) menyebut bahwa UU anti teror baru berpotensi terjadinya pelanggaran HAM dibandingkan dengan UU Anti Teror milik Filipina.

Sebelumnya, tercatat bahwa cara manual yang digunakan kelompok terorisme dalam berkomunikasi sangat tradisional dengan menggunakan kurir, yaitu pesan yang disampaikan melalui orang per orang. Dikutip dari Hasani dan Naipospos (2012) bahwa peran kurir Noordin M. Top sebagai berikut:

" ….Allen yang dikontak oleh Joko sahabat dekatnya, sudah bergabung dengan kelompok Noordin M. Top, dan bertugas menjadi kurir Noordin menggantikan *Lutfi Haidaroh* alias *Ubeid* yang ditangkap polisi karena terlibat kasus Bom Kuningan 2004. Allen menjadi kurir dengan motor yang dipinjam dari Joko untuk digunakan menjemput Noordin M. Top yang itu jadi buronan teroris di Indonesia".[11]

Pada kutipan tersebut, kurir yang bertugas mendistribusikan informasi, serta logistik dan keperluan pada kelompok tersebut secara manual dan bukan dengan perangkat komunikasi. Ini menjadi tantangan juga dalam penyelidikan.

Sebelum berlakunya Undang-Undang Pemberantasan Terorisme, Ketua Panja rancangan Undang-Undang Antiterorisme Muhammad Syafii (*Kompas,* Rabu 26 Juli 2017) sebelum UU disahkan menyatakan bahwa penyadapan dapat dilakukan dalam keadaan mendesak dengan dilengkapi dua alat bukti yang cukup dapat dilakukan tanpa ijin pengadilan terlebih dahulu. Tiga hal yang yang dimaksud dalam keadaan mendesak ini, akan diatur dalam Pasal 31a revisi Undang-Undang Antiterorisme. Tiga syarat menyadap sebelum meminta izin pengadilan ini adalah: (1) bahaya maut atau luka fisik yang serius dan mendesak, (2) pemufakatan jahat untuk melakukan tindak pidana terhadap keamanan negara, (3) dan/atau pemufakatan jahat yang merupakan karakteristik tindak pidana terorganisasi.

Perlu diingat bahwa penyadapan (*Lawful Interception*) berdasarkan aturan hukum sehingga berbeda dengan penyadapan intelijen. Tidak ada satupun penyadapan dalam konteks *Lawful Interception* yang dapat dikerjakan tanpa melalui prosedur yang berlaku.

Bahwa hasil dari *lawful interception* apabila tidak terkait dengan sasaran sebagaimana target hasil dari *lawaful interception* yang telah dilakukan dengan tindakan: (1) menjadi file intelijen dan untuk kepentingan intelijen dan bukan untuk bukti di pengadilan, (2) File tersebut sebagai database pendukung yang dapat dibuka untuk dan hanya semata-mata untuk kepentingan penyelidikan, (3), Semua rekaman yang tidak terkait dengan upaya penyelidikan, harus dimusnahkan. Setiap file apapun, yang bukan merupakan relevansi harus dibuang. Sebagai contoh : file hasil *lawful interception* terkait dengan bisnis atau soal rumah tangga dan bukan merupakan tindak pidana terorisme, maka harus hentikan dan dihapus.

Database informasi intelijen yang telah terkumpul baik dari agen-agen di lapangan maupun dari berbagai inputan informasi yang masuk, dilakukan analisis sehingga jaringan serta arah komunikasi terhadap target, akan membua t terang suatu jaringan[12].

Pada pelaksanaan kegiatan yang dilakukan pada organisasi penegak hukum dalam melakukan *Law Enforcement* atau sering disebut sebagai *Law Enforcement Agency (LEA).* Secara spesifik di Indonesia sebagaimana Undang-Undang dilaksanakan oleh Polri dan organ strukturnya pada Densus 88 Anti Teror yang diberikan otorisasi yang sah berdasarkan hukum nasional, untuk meminta tindakan intersepsi dan menerima hasil intersepsi. Penggunaan Fasilitas pada LEA yang berupa Pemantauan Penegakan Hukum (*Law Enforcement Monitoring Facility / LEMF*) dengan tujuan transmisi untuk hasil intersepsi yang berkaitan dengan objek intersepsi tertentu. Pada standar prosedur yang dilakukan, maka harus ada otorisasi yang memberikan ijin. Otorisasi Sah (*Lawful Authorization*) dalam hal ini adalah pengadilan lokasi penyidik, yang berupa izin diberikan kepada LEA dalam kondisi tertentu, untuk mencegat atau mengambil informasi telekomunikasi tertentu dan membutuhkan kerjasama dari penyelenggara jasa telekomunikasi, operator internet, dan operator saluran radio, serta sarana komunikasi lainnya. Koneksi jaringan dan fungsi protokol khusus yang diperlukan untuk pengiriman produk intersepsi dari fungsi mediasi atau fungsi pengiriman ke LEMF. Kondisi sasaran menyangkut dengan subjek intersepsi, termasuk lokasi dan informasi dari pihak-pihak yang terlibat dalam komunikasi tersebut.

Pada komunikasi dengan menggunakan email, maka perlu ada adanya elemen jaringan yang berkedudukan sebagai "*Point of Presence*" (POP) untuk menerima dan menyimpan dan meneruskan e-mail atas nama pengguna surat terdaftar di server yang dipergunakan. Pada email publik, maka adanya akses yang diberikan kepada penegak hukum atas permintaan yang sudah diterima secara legal. Fungsi Mediasi (*Mediation Function/MF*) diperlukan untuk menjebatani mekanisme informasi antara penyedia akses atau penyedia layanan dan proses serah terima dalam sebuah aplikasi antar muka. Dengan layanan internet, maka perlu adanya kerja sama dan akses dengan Penyelenggara Jasa Telekomunikasi (*network operator*), yaitu penyelenggara infrastruktur telekomunikasi publik yang memungkinkan penyampaian komunikasi dengan paket data internet, jaringan nir kabel, serta dengan sinyal alat optik atau dengan elektromagnetik lainnya. Hasil dari *lawful interception* tersebut termasuk isi komunikasi yang diteruskan oleh penyedia akses atau operator jaringan atau penyedia layanan ke *Law Enforcement Agency (*LEA) yaitu penegak hukum.

KESIMPULAN DAN REKOMENDASI

Bahwa cara pemberantasan terorisme yang tertuang dalam Undang-Undang Nomor 5 Tahun 2018 *lawful interception* pada penyidikan tindak pidana terorisme merupakan terobosan baru, yang dapat dipergunakan untuk memperbaiki secara kelembagaan dalam penanganan terorisme. Tantangan penanggulangan terorisme menjadi sangat tinggi, karena perkembangan dari teknologi yang terus berubah. Keuntungan yang dapat diperoleh dengan *lawful interception* ini, sebagai upaya untuk memanggulangi terorisme ini tidak sebatas pada upaya penyelidikan dari komunikasi yang bersifat elektronik saja, namun semua media apapun yang dapat dipergunakan sebagai sarana komunikasi.

Dengan terbukanya cara *lawful interception* pada pemberantasan tindak pidana terorisme ini, maka jaringan kelompok teroris menjadi jalan untuk mengelabui para penyidik untuk upaya melawan *lawful interception* ini. Dengan perkataan lain, bahwa upaya dan tindakan *lawful interception* semaksimal mungkin tindakan rahasia secara teknis dan dapat dipertanggungjawabkan secara tepat dalam koridor hukum yang berlaku.

Untuk mendukung *lawful interception*, perkembangan industri keamanan dan Aparatur Penegak Hukum Pemerintah, masih terus mencoba menstandaris asikan pengolahan secara teknis. Hal ini berlaku secara umum di seluruh negara, karena adanya perbedaan dalam infrastruktur komunikasi. Tetapi secara teknis,sebagian besar *lawful interception* yang dilakukan mengimplement asikan penggabungan teknis yang komprehensif, baik sarana komunikasi telepon, internet, paket data, email dan lain-lain. Selain itu, dengan bekerja sama dengan penyelenggara telekomunkasi, termasuk penyelenggara jasa internet serta *flatform* lainnya, untuk diberikan akses secara legal dan bertanggung jawab terhadap target, termasuk kelompok simpatisan dan jaringan teroris.

PENELITIAN LANJUTAN

Penelitian ini memiliki keterbatasan pada jumlah narasumber dan kompl eksitas serta peran berbagai pihak dalam pemberantasan tindak pidana terorisme yang secara khusus dapat dilakukan dengan *lawful interception*. Peneli tian lebih lanjut dapat dengan melakukan studi perbandingan pelaksanaan atau praktek *lawful interception* dalam penanganan tindak pidana terorisme di berbag ai Negara yang menghadapi problematika yang sama dan tantangan problematika perkembangan teknologi.

DAFTAR PUSTAKA

----, Technical Report, Lawful Interception (LI); *Concepts of Interception in a Generic Network Architecture*, ETSI TR 101 943 V2.2.1 (2006-11)

Ardhiansyah, Wellza., (2012), Tesis, "Tindakan penyadapan pada hakikatnya merupakan tindakan yang dilarang dalam hukum pidana akan tetapi merupakan tindakan yang sangat diperlukan dalam proses penegakan hukum terutama terkait kejahatan yang sulit dibuktikan", Jakarta: Universitas Indonesia.

Borg , Lars C. (2017). *Improving Intelligence Analysis: Harnessing Intuition and Reducing Biases by Means of Structured Methodology*, The International Journal of Intelligence, Security, and Public Affairs, 19:1, 2-22.

Christianto, Hwian, (tanpa tahun),Tindakan Penyadapan ditinjau dari Perspektif Hukum Pidana, Dosen Fakultas Hukum Universitas Surabaya, Jawa Timur, Email: hwall4jc@yahoo.co.id

Congram , Mitchell & Bell, Peter (2010) *Laying the Groundwork for the Successful Deployment of Communication Interception Technology (CIT) in Modern Policing*, Journal of Policing, Intelligence and Counter Terrorism, 5:1, 9-27, DOI: 10.1080/18335300.2010.9686938.

Deflem , Mathieu (Ed).(2004). *Terrorism And Counter-Terrorism:Criminological Perspectives*. Department of Sociology. University of South Carolina, USA.

Dempsey, M. 2013. Joint intelligence. Joint Publication, 2–0.

Dwilaksana, Chryshnanda. (2020). *Bagimu Negeri Untuk Semakin Mencintai Indonesia*. Jakarta : YPKIK (Yayasan Pengembangan Kajian Ilmu Kepolisian)

Gardner, Jeffrey & Riedel, Eric. (2017). *A Duty to Share: The Opportunities and Obstacles of Federal Counterterrorism Intelligence Sharing with Nonfederal Fusion Centers*. 10.13140/RG.2.2.29633.45923.

Graham, Robert. (2016). *"How Terrorists Use Encryption," CTC Sentinel,* Vol. 9.6, 2016, https:// ctc.usma.edu/posts/how-terrorists-use-encryption.

Harrison, Seth. "*Evolving Tech, Evolving Terror*", research intern with the Transnational Threats Project at CSIS. Sumber :

Hasani , Ismail & Naipospos, Bonar Tigor (Editor). (2012). *Dari Radikalisme Menuju Terorisme: Studi Relasi Dan Transformasi Organisasi Islam Radikal Di Jawa Tengah & D.I. Yogyakarta*. Jakarta : Pustaka Masyarakat Setara

Herold, Rebecca. (2011). *Managing an Information Security and Privacy Awareness and Training Program*, USA, CRC Press

Hoffman, Bruce. (2017). *Inside Terrorism, Third Edition*. New York. Columbia University Press, https://www.csis.org/npfp/evolving-tech-evolving-terror, tanggal akses 8 Maret 2022.

Istiqomah, Milda. (2013). *Perbandingan Hukum Pengaturan Tindakan Penyadapan (Wiretapping) di Indonesia dan Filipina*. Arena Hukum Volume 6, Nomor 1, April 2013, Halaman 1-151..Fakultas Hukum Universitas Brawijaya, Jl. Mayjen Haryono 169, Malang, email: milda.istiqomah@ub.ac.id

Kbarek, Leonard J.F., & Patiran , Andarias. (2012). *Analisis Pengaruh Pelatihan Terhadap Kinerja Personil Pada Satuan Detasemen Khusus 88 Anti Teror Polda Papua*, (*Jurnal Fokus Ekonomi*), Vol. 7 No. 1 Juni 2012 : 83 – 92

Kumar, Narender. (2019). Use of Modern Technology to Counter Terrorism.

Mahyudin, Emil. (2016). *Tantangan Intelijen Dalam Kontra-Terorisme di Indonesia: Suatu Pandangan*, Departemen Hubungan Internasional Universitas Padjadjaran email: emil.mahyudin@unpad.ac.id, Journal of International Studies, e-ISSN 2503-443X Volume 1, No. 1, November 2016 (23-35) doi:10.24198/intermestic.v1n1.3

Muradi, (2017), "Polri dan UU Anti Teror Baru, Jurnal Ilmu Kepolisian", Edisi 089, Agustus-Oktober 2017.

Nunan, J., Stanier, I., Milne, R., Shawyer, A., & Walsh, D. (2020). "Source Handler perceptions of the interviewing processes employed with informants. Journal of Policing, Intelligence and Counter Terrorism", 15(3), 244-262.

Prunckun, Hank. (2002). *Counterintelligence Theory and Practice*. United Kingdom: Rowman & Littlefield Publisher, Inc

Seth, Shashi Mehrotra & Mishra, Rajan, (2011), "Comparative Analysis Of Encryption Algorithms For Data Communication", International Journal of Computer Science and Technology (IJCST) Vol. 2, Issue 2, June 2011

Shaffan, Ahmad Mafud. (2018). *Respons Indonesia terhadap Kasus Penyadapan Australia*, Journal of International Relations, Volume 4, Nomor 2, 2018, hal. 285-294, Online di http://ejournal-s1.undip.ac.id/index.php/jihi

Škrtić , Dražen. (2016). (Ministry of Interior Republic of Croatia), *Lawful Interception: European Union Legal, Framework*, https://www.researchgate.net/publication/275462294

Smith, Megan J."Correctional Agencies Receive Assistance From the Law Enforcement Analysis Facility", (Megan J. Smith, LEAF technical administrator, coordinates statistical information regarding technology success and is the facility technical writer), www.nlectc.org/nlectcne tanggal akses 9 Mei 2022

Zeiger, Sara.(2016). *Melemahkan Narasi Ekstremis Brutal di Asia Tenggara Sebuah Panduan Praktis*. Canberaa: Alhedayah, (naskah lanjutan dari *Australia's Regional Summit To Counter Violent Extremism* (Cve)

Peraturan

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 5 Tahun 2010 Tentang Tata Cara Penyadapan Pada Pusat Pemantauan Kepolisian Negara Republik Indonesia

Undang-Undang Nomor 5 Tahun 2018 Tentang Perubahan Atas 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.

Website/Presentation :

Ihsanuddin, Kompas.com, "Pasal-Pasal Penting yang Perlu Anda Tahu dalam UU Antiterorisme", sumber: https://nasional.kompas.com/read/2018/05/26/10190871/pasal-pasal-penting-yang-perlu-anda-tahu-dalam-uu-antiterorisme?page=all, (diakses pada 10 Mei 2022)

Tirto.id, "*4 Point dalam UU Terorisme yang baru yang berpotensi bermasalah*", sumber :https://tirto.id/4-poin-dalam-uu-terorisme-baru-yang-berpotensi-jadi-masalah-cLcW, (diakses pada 15 Mei 2022)

Jaya Baloo, Presentation: "*Lawful Interceptionof IP Traffic : The European Context*", email: Jaya@baloos.org