ANALISIS IMPLEMENTASI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK NOMOR 11 TAHUN 2008 YANG TELAH DIPERBAHARUI PADA UNDANG-UNDANG NOMOR 19 TAHUN 2016 DIKEPOLISIAN NEGARA REPUBLIK INDONESIA DAERAH SUMATERAUTARA

TESIS

OLEH

EDI SUFRAPTO
201801033

PROGRAM STUDI MAGISTER ADMINISTRASI PUBLIK
PROGRAM PASCASARJANA
UNIVERSITAS MEDAN AREA
MEDAN
2024

ANALISIS IMPLEMENTASI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK NOMOR 11 TAHUN 2008 YANG TELAH DIPERBAHARUI PADA UNDANG-UNDANG NOMOR 19 TAHUN 2016 DIKEPOLISIAN NEGARA REPUBLIK INDONESIA DAERAH SUMATERAUTARA

Tesis

Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Magister Administrasi Publik Pada
Pascasarjana Universitas Medan Area

Oleh:

EDI SUFRAPTO
201801033

PROGRAM STUDI MAGISTER ADMINISTRASI PUBLIK
PROGRAM PASCASARJANA
UNIVERSITAS MEDAN AREA
MEDAN
2024

UNIVERSITAS MEDAN AREA
MAGISTER ADMINISTRASI PUBLIK

HALAMAN PENGESAHAN

Judul Tesis	:	**Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016 Di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara**
Nama	:	**Edi Sufrapto**
NPM	:	**201801033**

Menyetujui

Pembimbing I	**Pembimbing II**
Prof. Ir. H. Zulkarnain Lubis, MS., Ph.D	**Dr. Dra. Hj. Nina Siti Salmaniah Siregar, M.Si.**

Ketua Program Studi Magister Administrasi Publik	**Direktur**
Dr. Beby Masitho Batubara, S.Sos., M.AP	**Prof. Dr. Ir. Retna Astuti Kuswardani, MS**

TELAH DI UJI PADA TANGGAL 13 SEPTEMBER 2024

Nama : Edi Sufrapto
NIM : 201801033

Panitia Penguji Tesis :

1. **Ketua : Prof. Dr. Badaruddin, M,Si.**
2. **Penguji Tamu : Prof. Dr. Marlon Sihombing, MA.**
3. **Sekretaris : Dr. Budi Hartono, M.Si.**
4. **Penguji I : Prof. Ir. Zulkarnain Lubis, MS., Ph.D.**
5. **Penguji II : Dr. Nina Siti Salmaniah Siregar, M.Si.**

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tesis dengan Judul Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016 Di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara ini tidak terdapat karya yang pernah diajukan untuk memproleh gelar Magister Ilmu Administrasi Publik di suatu Program Pascasarjana Program Studi Magister Ilmu Administrasi Publik Universitas Medan Area, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh Orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Medan, 01 Oktober 2024

Edi Sufrapto
201801033

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TESIS UNTUK KEPENTINGAN AKADEMI

Sebagai civitas akademik Universitas Medan Area, saya yang bertanda tangan dibawah ini :

Nama	:	Edi Sufrapto
NPM	:	201801033
Program Studi	:	Magister Administrasi Publik
Fakultas	:	Pascasarjana
Jenis karya	:	Tesis

Demi pengembangan Ilmu Pengetahuan, menyetujui untuk memberikan kepada Universitas Medan Area Hak Bebas *Royality Noneksklusif (Non - exclusive Royalty - Free Right)* atas karya ilmiah saya yang berjudul :

Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016 Di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara.
Beserta perangkat yang ada (jika diperluan) dengan Hak Bebas *Non - exclusive Royalty* ini Universitas Medan Area berhak menyimpan, mengalihkan media/ format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas tesis saya.

Dibuat di Medan
Pada Tanggal 01 Oktober 2024
Yang menyatakan

Edi Sufrapto
201801033

ABSTRAK

ANALISIS IMPLEMENTASI UNDANG-UNDANG NFORMASI DAN TRANSAKSI ELEKTRONIK NOMOR 11 TAHUN 2008 YANG TELAH DIPERBAHARUI PADA UNDANG-UNDANG NOMOR 19 TAHUN 2016 DIKEPOLISIAN NEGARA REPUBLIK INDONESIA DAERAH SUMATERAUTARA

Nama : **Edi Sufrapto**
NPM : **201801033**
Program Studi : **Magister Administrasi Publik**
Pembimbing I : **Prof. Ir. H. Zulkarnain Lubis, MS, Ph.D**
Pembimbing II : **Dr. Dra. Hj. Nina Siti Salmaniah Siregar, M.Si**

Undang-undang telah mengatur kejahatan di dunia maya, seperti penyebaran informasi data nasional, pesan penipuan yang membahayakan keselamatan kita, menyebarkan berita bohong untuk menyerang atau menghina orang atau individu melalui media sosial, serta peretasan dan kejahatan dunia maya lainnya. Penelitian ini merupakan implementasi dari pasal khusus tentang Teknologi dan kejahatan dunia maya yang terjadi di dunia maya. Pasal-pasal tersebut berasal dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yaitu pada tanggal 27, 28, 29, dan 31. Penelitian ini dilakukan di Subdit V Kepolisian Daerah Sumatera Utara. Penelitian ini menggunakan metode kualitatif dengan mewawancarai tim c*yber* dari kepolisian Daerah Sumatera Utara. Implementasinya memberikan hal-hal yang positif, tetapi masih memiliki masalah pada pembatasan kebijakan. Peraturan tersebut tidak selalu dapat diimplementasikan tepat sasaran karena perubahan waktu.

Kata Kunci : Undang - Undang ITE, Implementasi, dan *Cyber Crime*

ABSTRACT

ANALYSIS IMPLEMENTATION OF CONSTITUTION OF THE ELECTRONIC INFORMATION AND TRANSACTION REGULATION NUMBER 11Th 2008 THAT HAS BEEN UPDATE INTO REGULATION NUMBER 19Th 2016 AT THE INDONESIAN POLICE DEPARTMEN OF NORTH SUMATRA

Name	***: Edi Sufrapto***
NIM	***: 201801033***
Study Program	***: Master of Science Public Administration***
Adviser I	***: Prof. Ir. H. Zulkarnain Lubis, MS, Ph.D***
Adviser II	***: Dr. Dra. Hj. Nina Siti Salmaniah Siregar, M.Si***

The law had been regulated the crime in the cyberspace, such as the spreading of information of the national data, scamming messages that was harmed our safety, Spreading the hoax news to attacking or insulting peoples or individual through social media, hacking and other cyber crimes. This research is the implementation of specific article about Technology and cyber crime that was occur in the cyberspace. The articles was from Electronic Information and Transaction Law (ITE Law) on 27, 28, 29, and 31. The research was on the Sub-Directorate V of the North Sumatra Police Department. This research was qualitative method by interviewing the Cyber Team of Police Department of Sumatera Utara. The implementation was provides positive things, but still have a problem on policy restriction. The regulations cannot always be implemented on target appropriately due to time changing.

Keywords: ITE Law, Implementation, and Cyber Crime

RIWAYAT HIDUP

Penulis lahir di Medan pada tanggal 31 Oktober 1993 dari Bapak Almarhum Sukatman dan Ibu Hartati Ningsih. Penulis merupakan anak ke empat dari empat bersaudara. Penulis menyelesaikan pendidikan formal di Sekolah Dasar (SD) Persatuan Amal Bakti (PAB) pada tahun 2006, Madrasah Tsanawiyah (MTs) Negeri 3 Medan pada tahun 2009, dan Madrasah Aliyah (MA) Negeri 2 Model Medan pada tahun 2012. Pada tahun 2017 penulis menerima Gelar Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Universitas Medan Area.

Penulis merupakan ASN Kantor Wilayah Kementerian Agama Provinsi Sumatera Utara Jabatan Pelaksana (JP) Analis Sumber Daya Manusia Aparatur. Penulis melaksanakan penelitian Tesis di Kepolisian Daerah Sumatera Utara dengan judul Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016.

KATA PENGANTAR

Dengan mengucapkan Alhamdulillah kehadirat Allah Subhanahu Wata'ala yang telah memberikan hidayah-Nya, sehingga penulis dapat menyelesaikan Tesis ini sebagai salah satu syarat untuk memperoleh gelar Magister Ilmu Administrasi Publik pada program Pascasarjana Universitas Medan Area Medan Sumatera Utara. Adapun judul Tesis ini " Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016 Di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara ".

Dalam pembuatan Tesis ini penulis menyadari bahwa masih jauh dari kesempurnaan, baik dari segi bahasa, penulisan maupun kedalaman materinya, hal ini terjadi disebabkan pengetahuan dan kemampuan penulis masih sangat terbatas serta kurangnya literatur yang berhubungan dengan Tesis ini. Untuk itu penulis sangat mengharapkan kritik dan saran dari berbagai pihak yang bersifat konstruktif demi kesempurnaan Tesis ini.

UCAPAN TERIMA KASIH

Dalam penulisan ini, penulis banyak menerima bimbingan dan arahan dari berbagai pihak yang kesempurnaanya itu tidak ternilai harganya. Oleh karenanya dengan kerendahan hati dalam kesempatan ini penulis menyampaikan ucapan terima kasih dan rasa hormat serta penghargaan yang setinggi-tingginya kepada:

1. Yang terhormat, Rektor Universitas Medan Area, Bapak Prof. Dr. Dadan Ramdan, M.Eng, M.Sc,
2. Yang terhormat, Direktur Program Pascasarjana Universitas Medan Area. Ibu Prof. Dr. Ir. Retna Astuti Kusmawardani, MS.
3. Ketua Program Studi Magister Ilmu Administrasi Publik, Ibu Dr. Beby Masitho Batubara, S.Sos, M.AP.
4. Yang terhormat, Bapak Prof. Ir. H. Zulkarnain Lubis, MS, Ph.D, selaku Dosen Pembimbing I Tesis saya yang telah memberikan bimbingan, arahan, dan petunjuk, dalam penyusunan Tesis ini.
5. Yang terhormat, Ibu Dr. Dra. Hj. Nina Siti Salmaniah Siregar, M.Si, selaku Dosen Pembimbing II Tesis saya yang telah memberikan bimbingan, arahan, dan petunjuk, dalam penyusunan Tesis ini.
6. Seluruh Dosen Fakultas Ilmu Sosial dan Ilmu Politik jurusan Administrasi Publik yang namanya tidak dapat saya sebutkan satu per satu, yang telah memberikan ilmu yang sangat berharga.
7. Bapak Aiptu Wesli T Siber Dit Reskrimsus PANIT (Pembantu Unit) 3 POLDASU dan Seluruh pegawai Siber Dit Reskrimsus V.
8. Mama, Abang, Kakak, dan Teman saya, atas kesabaran dan dukungan yang tiada henti serta doanya.

Atas semua ini, kembali penulis menyampaikan doa kehadirat Allah Subhanahu Wata'ala, semogah tulisan ini dapat digunakan sebagai pedoman untuk melaksanakan kegiatan penelitian lanjutan, akhirnya mengharapankan ridho dari Allah Subhanahu Wata'ala, semogah kita memproleh lindungan-Nya.

Medan, 01 Oktober 2024

Penulis

Edi Sufrapto

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi berlangsung dengan pesat sehingga berpengaruh sangat besar dalam kehidupan manusia, bahwa saat ini Teknologi sudah menjadi bagian dampak yang signifikan dalam kehidupan sehari-hari manusia, Teknologi adalah salah satu kebutuhan hidup manusia agar lebih mudah untuk di jalani, Teknologi benar-benar sangat penting membantu kita agar bisa berkomunikasi dengan cepat dan bekerja dengan lancar. Kebutuhan akan Teknologi komunikasi dan Internet untuk mempermudah segala aktivitas, jumlah pengguna Internet di Indonesia meningkat dari separuh penduduk Indonesia ke tingkat yang cukup pesat dan dapat berdampak negatif.

Perkembangan media sosial saat ini juga semakin besar berbagai macam jenis media sosial bisa kita manfaatkan untuk mencari berbagai informasi yang kita dapatkan dengan cepat. Hampir seluruh manusia di dunia bersinggah di dunia maya, berbagai informasi dengan mudah kita dapatkan. Tanpa kita sadari kemudahan yang diberi Teknologi juga rentan terhadap kebocoran informasi, Nomor telepon, email, alamat rumah, dan informasi lainnya yang kita bagi di *flatform* media sosial yang sangat mudah untuk disalah gunakan.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) juga mengatur mengenai penyebaran informasi yang merugikan dan mengancam keamanan nasional, Menyebarkan pesan atau komentar yang bermaksud untuk menyerang, menghina, atau merendahkan kelompok atau individu tertentu. melalui media sosial, serta tindakan hacking dan *cyber crime* lainnya.

Implementasi UU ITE telah dilakukan dengan pembentukan lembaga dan regulasi yang mengawasi pelaksanaan UU ITE, seperti Badan Siber dan Sandi Negara (BSSN) dan Komisi Penyiaran Indonesia (KPI). Namun penggunaan UU ITE kerap menjadi kontroversial karena dapat merugikan kebebasan berpendapat dan berekspresi di media sosial. Oleh karena itu perlu ada evaluasi dan revisi sangat penting untuk menghadapi tantangan yang berkaitan dengan penghinaan dan pencemaran nama baik melalui media sosial. untuk memastikan bahwa penggunaan UU ITE tetap sejalan dengan hak asasi manusia, menurut pendapat Edward III (dalam Subarsono, 2011: 90-92) berpandangan bahwa implementasi kebijakan dipengaruhi oleh empat variabel, yaitu:

1. Komunikasi adalah kunci keberhasilan implementasi kebijakan, di mana para pelaksana harus memahami dengan jelas apa yang harus dilakukan dan siapa yang menjadi target kebijakan. Hal ini bertujuan untuk mengurangi distorsi dalam pelaksanaan kebijakan.
2. Sumber daya, walaupun kebijakan sudah dikomunikasikan dengan baik, jika para pelaksana tidak memiliki sumber daya yang cukup, pelaksanaan kebijakan tidak akan efektif. Sumber daya ini bisa berupa sumber daya manusia, seperti kompetensi pelaksana, maupun sumber daya finansial.
3. Disposisi, yaitu karakter dan sifat yang dimiliki oleh para pelaksana kebijakan, seperti komitmen, kejujuran, dan sikap demokratis. Jika pelaksana memiliki disposisi yang baik, mereka akan menjalankan kebijakan sesuai dengan harapan pembuat kebijakan. Sebaliknya, jika pelaksana memiliki sikap yang berbeda dengan pembuat kebijakan, pelaksanaan kebijakan akan menjadi tidak efektif.
4. Struktur Birokrasi, struktur organisasi yang bertugas mengimplementasikan kebijakan memiliki pengaruh besar terhadap keberhasilan implementasi kebijakan. Aspek yang penting dari struktur organisasi ini adalah Standard Operating Procedure (SOP) dan fragmentasi. Struktur organisasi yang terlalu panjang dapat melemahkan pengawasan dan menyebabkan red-tape, yaitu prosedur birokrasi yang rumit dan kompleks yang membuat aktivitas organisasi menjadi tidak fleksibel.

Percepatan Teknologi Informasi dan Komunikasi (TIK) adalah istilah yang mencakup berbagai teknologi dan sistem yang digunakan untuk mengumpulkan,

menyimpan, mengirim, dan memanipulasi data dalam konteks komunikasi dan informasi. jiuga membuat hubungan dunia tanpa batas dan perubahan sosial, ekonomi dan budaya yang penting berlangsung dengan cepat, Dengan terus berkembangnya teknologi seperti kecerdasan buatan, komputasi awan, dan IoT (Internet of Things), peran TIK di dalam masyarakat dan ekonomi global semakin mendalam dan tidak dapat diabaikan. Hal ini menuntut evaluasi dan regulasi yang cermat untuk memastikan manfaat maksimal dari TIK sambil menjaga keamanan dan integritas informasi.

Teknologi telah memberikan kemudahan bagi manusia untuk berinteraksi dengan masyarakat dalam Komunitas lain. Kejahatan dunia maya merupakan kejahatan yang menggunakan Komputer atau dalam arti sempit setiap perilaku ilegal yang ditujukan dengan sengaja pada perangkat Elektronik yang menargetkan system keamanan Komputer dan data yang diproses oleh system Komputer tersebut atau singkatnya tindak pidana yang dilakukan dengan menggunakan Teknologi yang canggih.

Melihat pentingnya hal ini pemerintah memberikan sebuah kebijakan atau Regulasi dalam memberikan rasa aman kepada masyarakat dalam berselancar di dunia maya membuat pemerintah harus melakukan perbaikan kebijakan agar masyarakat dapat secara bebas dan santun dalam memberikan kebebasan berpendapat. Pentingnya Implementasi dalam melaksanakan kebijakan yang sesuai dengan pedoman yang ada agar terhindar dari ketidak adilan sebagai Hak Asasi Manusia (HAM) dalam memberikan pendapat di ruang digital.

Pemerintah perlu memberikan kebijakan atau regulasi untuk memberikan rasa aman kepada masyarakat dalam berselancar di dunia maya, namun kebijakan

tersebut juga harus memastikan bahwa kebebasan berpendapat dan berekspresi dapat dijalankan secara bebas dan santun. Dalam hal ini, perlu dilakukan perbaikan kebijakan yang lebih tepat dan sesuai dengan kondisi sosial dan politik yang ada guna memastikan bahwa hak asasi manusia dan kebebasan berekspresi tetap terjaga. Perbaikan kebijakan ini harus melibatkan partisipasi aktif dari berbagai pihak, termasuk masyarakat sipil dan pengguna teknologi informasi, untuk mendapatkan masukan yang lebih komprehensif dan responsif terhadap kebutuhan masyarakat secara luas.

> Menurut Iman Amanda Permatasari dan Junior Hendri Wijaya, "anggapan mengenai ketidakjelasan dan multitafsir tidak lagi muncul pada pasal 45 dan 46 yang berhubungan dengan pasal 27, yang hanya menjelaskan tentang hukuman pidana penjara dan denda bagi pelanggar pasal 27, 28, dan 29. Pemerintah mencoba menyelesaikan masalah tersebut dengan merevisi Undang-Undang, yaitu Undang-Undang Informasi dan Transaksi Elektronik No. 19 Tahun 2016" (2019: 36). Sedangkan menurut Yosephus Mainake dan Luthvi Febryka Nola, "pasal 27 ayat (1) dan (3) dinilai multitafsir karena tidak ada batasan yang jelas terkait pengaduan kesusilaan, penghinaan, dan pencemaran nama baik. Orang yang merasa tersinggung dengan pernyataan orang lain dapat merasa terhina. Pasal 28 ayat (2) UU ITE tidak menyebutkan apakah ketentuan mengenai SARA dalam pasal tersebut merupakan delik biasa atau delik aduan. Ketentuan ini juga multitafsir karena tidak ada batasan yang jelas terkait ketentuan mengenai SARA. Pasal 29 UU ITE terkait ancaman kekerasan dan menakut-nakuti. Permasalahan dalam pasal ini adalah klausula menakut-nakuti. UU ITE tidak memberikan rumusan yang jelas terkait tindakan menakut-nakuti" (2020:3).

Untuk mencegah interpretasi yang salah dari Undang-Undang Informasi dan Transaksi Elektronik (ITE), Surat Keputusan Bersama menetapkan standar untuk pelaksanaan kebijakan publik, terutama dalam hal memberikan perlindungan kepada masyarakat yang terjerat oleh UU ITE dan berharap penegakan hukum terkait UU ITE tidak menimbulkan interpretasi yang salah lagi.

Menteri komunikasi dan informasi, Kejaksaan Agung Republik Indonesia dan Kepolisian Republik Indonesia menerbitkan Surat Keputusan Bersama

pedoman Implementasi Pasal-Pasal tertentu dalam Undang-Undang Informasi dan Elektronik. Pentingnya pelaksanaan Surat Keputusan Bersama untuk melindungi jerat Pasal-Pasal yang dapat merugikan masyarakat memberikan hal positif untuk menciptakan rasa aman dalam memberikan kebebasan dalam berpendapat.

> Undang-Undang Informasi dan Transaksi Elektronik (ITE) awalnya bertujuan menjaga agar ruang digital Indonesia tetap bersih, sehat, beretika, dan produktif. Namun, implementasi UU tersebut tidak boleh menimbulkan rasa ketidakadilan. Presiden Joko Widodo meminta Kepala Kepolisian Negara Republik Indonesia (Kapolri) untuk meningkatkan pengawasan agar implementasi dan penegakan UU ITE berjalan secara konsisten, akuntabel, dan menjamin rasa keadilan di masyarakat. Kepala Negara menyampaikan pandangannya bahwa belakangan ini banyak masyarakat saling membuat laporan dengan menjadikan UU ITE sebagai salah satu rujukan hukum, yang sering kali membuat proses hukum dianggap kurang memenuhi rasa keadilan (kominfo.go.id).

Pernyataan tersebut menunjukkan kekhawatiran mengenai pelaksanaan Undang-Undang Informasi dan Transaksi Elektronik (ITE) di Indonesia. Presiden Joko Widodo menyatakan bahwa menjaga ruang digital tetap bersih, sehat, beretika, dan produktif sangat penting. Namun, dia juga mengingatkan bahwa implementasi UU ITE harus dilakukan tanpa menimbulkan rasa ketidakadilan di masyarakat. Presiden secara khusus meminta Kepala Kepolisian Negara Republik Indonesia (Kapolri) untuk meningkatkan pengawasan agar penegakan UU ITE dapat berjalan konsisten, akuntabel, dan menjamin rasa keadilan. Ada kekhawatiran bahwa banyaknya laporan masyarakat yang merujuk pada UU ITE dapat mengakibatkan proses hukum yang dianggap tidak adil.

Dalam situasi seperti ini, pentingnya menjaga keseimbangan antara penegakan hukum dan perlindungan hak asasi manusia menjadi perhatian utama. Dalam menerapkan UU ITE, pemerintah harus memastikan bahwa kebebasan berekspresi dan hak privasi warga negara dihormati, dan bahwa penggunaan

undang-undang tersebut tidak disalahgunakan untuk membungkam kritik atau merugikan individu secara tidak adil. Pernyataan Presiden menunjukkan kesadaran terhadap potensi penyalahgunaan UU ITE dan pentingnya menjaga keseimbangan antara penegakan hukum dan keadilan.

Sumber data yang digunakan adalah sumber data primer. Data didapatkan dari pengumpul data secara langsung, menurut Sugiyono (2012:188) Data primer yaitu suber data yang langsung memberikan data kepada pengumpul data. Sumber-sumber tersebut seperti wawancara, survei, dan observasi. Namun pengumpulan data menggunakan teknik Dokumentasi, yang berarti bahwa data dikumpulkan dari sumber yang memiliki dokumentasi, seperti buku, jurnal, berita, dan internet dengan asumsi bahwa data tersebut relevan dengan topik penelitian yang dilakukan penulis.

1.2 Perumusan Masalah

1. Seberapa baik pelaksanaan Implementasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Wilayah Hukum Sumatera Utara ?
2. Adakah kendala dalam melakukan Implementasi Pasal 27, 28, 29, dan 31 Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik?

1.3 Pembatasan Masalah

Pembatasan masalah pada penelitian ini adalah pada pelaksanaan pasal tertentu tentang *cyber crime* yang terjadi di ruang digital dengan menjalankan Implementasi pasal 27, 28, 29, dan 31 Undang – Undang Informasi dan Transaksi Elektronik yang dilakukan Subditrektorat V Kepolisian Daerah Sumatera Utara.

1.4 Manfaat Penelitian

Penelitian penulisan tesis dengan judul "Analisis Implementasi Pasal Tertentu Dalam Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus Kepolisian Negara Republik Indonesia Daerah Sumatera Utara) " ada dua manfaat yang kiranya diharapkan dapat diproleh, yaitu sebagai berikut:

a. Manfaat Teoritis

Dari segi teoritis, penelitian ini mempunyai tujuan untuk memberikan Analisis Implemntasi mengenai kebijakan Teknologi dan Transaksi Elektronik di Indonesia, memberikan gambaran bagaimana ketentuan Undang-Undang yang berlaku berjalan sesuai dengan kebijakan yang berlaku.

b. Manfaat Praktis

Dari sisi praktis peneliti berharap dapat memberikan masukan dalam hal pelaksanaan Undang-Undang secara baik dan tidak lagi timbul kerugian masyarakat karena terhadap Undang-Undang Informasi dan Transaksi Elektronik. penelitian ini diharapkan akan terwujudnya suatu penerapan Undang-Undang yang diimplikasikan sesuai dengan kebijakan yang berlaku dan untuk menjawab

tantangan Informasi dan Transaksi Elektronik yang semangkin meningkat di Indonesia.

BAB II

TINJAUAN PUSTAKA

2.1 Analisis Kebijakan Publik

Pelaksanaan kebijakan publik memberikan hal yang positif bagi keberlangsungan banyak pihak dalam memenuhi Hak dan Kewajiban sebagai warganegara yang baik, kebijakan publik atau regulasi tidak salamanya dapat di Implementasikan secara tepat sasaran dikarenakan perkembangan jaman yang semangkin berkembang. Teknologi memberikan perubahan pada kebijakan secara nyata dan harus mendapat evaluasi kembali untuk di analisis secara menyeluruh untuk memberikan dampak yang baik dan tidak terjadi kesalah pahaman dalam melaksanakan tugas pemerintahan.

Pelaksanaan kebijakan publik dapat memberikan banyak manfaat bagi keberlangsungan banyak pihak dalam memenuhi hak dan kewajiban sebagai warga negara yang baik, namun kebijakan publik juga harus diimplementasikan secara tepat sasaran dan harus selalu menyesuaikan dengan perkembangan jaman yang semakin berkembang. Hal ini dapat menjadi tantangan dalam pelaksanaan pebijakan publik, karena tuntutan dan kebutuhan masyarakat terus berubah seiring dengan perkembangan zaman.

Oleh karena itu, perlu adanya monitoring secara terus-menerus terhadap pelaksanaan kebijakan publik agar dapat dilakukan secara tepat dan sesuai dengan tuntutan dan kebutuhan masyarakat. Selain itu, partisipasi aktif dari masyarakat dalam pelaksanaan kebijakan publik juga sangat penting untuk memastikan bahwa kebijakan tersebut benar-benar bermanfaat bagi masyarakat secara luas.

Menurut William N. Dunn "*Prospective policy analysis involves the*

production and transformation of knowledge before prescriptions are made. …“ (2018 : 10). Analisis kebijakan prospektif menggunakan metode yang berfokus pada masa depan untuk memahami dan merencanakan implikasi kebijakan yang mungkin terjadi. Analisis kebijakan prospektif harus mempertimbangkan tren dan perkembangan terkini dalam produksi dan transformasi pengetahuan. Ini dapat mencakup perkembangan teknologi, perubahan sosial, dan dinamika pasar terkait dengan sektor tersebut.

Melibatkan produksi dan transformasi pengetahuan memerlukan pemahaman mendalam tentang literatur dan penelitian terkini di bidang tersebut. Review literatur dapat membantu mengidentifikasi pengetahuan yang ada dan potensi perubahan yang mungkin terjadi di masa depan. Identifikasi berbagai kebijakan yang mungkin diimplementasikan dilakukan analisis dampak untuk masing-masing kebijakan alternatif untuk memahami konsekuensi dan implikasinya. Penggunaan model dan simulasi dapat membantu menggambarkan bagaimana kebijakan tertentu dapat mempengaruhi Globalisasi. Ini dapat mencakup pemodelan skenario yang berbeda untuk mengevaluasi hasil yang mungkin.

Identifikasi potensi risiko dan ketidakpastian yang terkait dengan implementasi kebijakan tertentu. Penilaian risiko akan membantu merencanakan langkah-langkah mitigasi yang diperlukan. Melibatkan masyarakat dan pemangku kepentingan lainnya dalam proses pengambilan keputusan dapat membantu memperoleh perspektif yang lebih luas dan mendapatkan masukan yang dapat memperkaya analisis kebijakan. Setelah kebijakan diimplementasikan, perlu dilakukan pemantauan dan evaluasi berkelanjutan untuk melihat bagaimana kebijakan tersebut memengaruhi produksi dan transformasi pengetahuan. Hal ini

memungkinkan penyesuaian kebijakan sesuai dengan perubahan kondisi atau hasil yang muncul.

Dari pembahasan diatas pentingnya kebijakan untuk dapat dianalisis secara *prospective* agar memberikan gambaran yang baik terhadap kebijakan, pentingnya menganalisis Kembali regulasi atau sebuah kebijakan agar tidak terjadi multitafsir dalam meimplelementasikanya. Pelaksanaan Implementasi kebijakan Undang-Undang Nomor 16 tahun 2016 merupakan salah satu contoh yang telah di perbaharui pada Undang-Undang Nomor 11 tahun 2008 dalam perkembangan nya ada beberapa aspek kebijakan yang harus di rubah dikarenakan perkembangan dunia maya di era globalisasi ini.

> Menurut William N. Dunn dalam Dr. Riant Nugroho " analisis kebijakan adalah aktivitas intelektual dan praktis yang ditujukan untuk menciptakan, secara kritis menilai, dan mengomunikasikan pengetahuan tentang dan dalam proses kebijakan. analisis kebijakan adalah ilmu sosial Terapan yang menggunakan beberapa metode Pengkajian multi pelajaran dalam konteks argumentasi dan debat politik untuk menciptakan, secara kritis menilai, dan mengkomunikasikan pengetahuan yang relevan…" (Dr. riant Nugroho 2011 : 269 -270).

Penggunaan berbagai metode dan pendekatan multi-pelajaran dalam analisis kebijakan menunjukkan kompleksitasnya dan kebutuhan untuk memahami berbagai aspek dari isu kebijakan. Dengan melakukan analisis ini dalam konteks argumentasi dan debat politik, tujuannya adalah untuk menciptakan, mengevaluasi secara kritis, dan mengkomunikasikan pengetahuan yang relevan. Semua ini diarahkan untuk mendukung pengambilan keputusan kebijakan yang lebih baik. Dalam konteks ini, analisis kebijakan bukan hanya suatu kegiatan akademis, tetapi juga menjadi suatu alat untuk membentuk opini dan mendukung pengambilan keputusan kebijakan yang lebih baik. Proses ini melibatkan penyusunan dan

komunikasi temuan analisis kebijakan sehingga dapat memberikan kontribusi yang signifikan dalam menyusun dan mengevaluasi kebijakan publik.

Pelaksanaan Implementasi haruslah disertai dengan ilmu yang tepat guna tercapainya suatu kebijakan secara prospektif dalam memberikan kebijakan tersebut, ini dapat dilihat diatas apa yang telah dikatakan oleh Wiliam N. Dunn tentang bagaimana cara menganalisis sebuah kebijakan yang mengkaitkan antara politik dan metodelogi kajian multi pelajaran yang konteks antara argumen dan debat politik untuk menciptakan sebuah regulasi. Pentingnya menganalisis kebijakan dengan pendekatan metodologi kajian multi-pelajaran yang melibatkan konteks dari argumen dan debat politik.

Kajian Implementasi	**Keterangan**
Ilmu yang tepat guna	Implementasi kebijakan harus didasarkan pada Ilmu yang relevan dan tepat guna hal ini mencakup pengetahuan dan metodologi yang diperlukan untuk memahami konteks kebijakan, serta memastikan bahwa tindakan yang diambil sesuai dengan tujuan yang diinginkan.
Prospektif	Implementasi kebijakan harus diarahkan pada pencapaian hasil yang diinginkan di masa depan hal ini menekankan pada perencanaan yang matang dan strategi jangka panjang agar kebijakan dapat memberikan dampak positif dalam jangka waktu yang lebih luas.

Analisis Kebijakan	William N. Dunn menyoroti pentingnya menganalisis kebijakan dengan menggunakan pendekatan multi-pelajaran. Ini mencakup pemahaman mendalam tentang konteks politik dan penggunaan metodologi yang beragam untuk memahami implikasi dan potensi dampak dari kebijakan yang diusulkan.
Konteks Argumen dan Debat Politik	Kebijakan seringkali merupakan hasil dari proses politik yang melibatkan berbagai argumen dan debat. Oleh karena itu, implementasi kebijakan harus mempertimbangkan konteks politik tersebut agar dapat menghasilkan regulasi yang lebih baik dan dapat diterima oleh masyarakat.
Revisi Kebijakan	Pemahaman bahwa kebijakan tidak bersifat statis, melainkan dinamis, adalah kunci untuk kesuksesan implementasi. Proses revisi perlu diintegrasikan, memungkinkan penyesuaian kebijakan seiring berjalannya waktu dan berubahnya kondisi sosial, ekonomi, dan politik.

Tabel 1 Kajian Implementasi

Pentingnya keterlibatan Ilmu dan pendekatan analisis yang komprehensif dalam implementasi kebijakan membantu memastikan bahwa kebijakan tersebut tidak hanya sesuai dengan keinginan politik, tetapi juga dapat memberikan dampak positif dalam praktiknya. Pelaksanaan sebuah kebijakan atau yang sering disebut dengan Implementasi sering sekali terjadi ketidakselarasan antara pembuat

kebijakan dan yang menjalankan kebijakan tersebut, hal inilah yang menyebabkan pentingnya menganalisis Kembali sebuah regulasi untuk menentukan arah sebuah kebijakan, peran penting masyarakat dalam melaksanakan kebijakan publik haruslah mendapatkan tempat untuk berargumentasi agar tidak terjadi kesalah pahaman antara pemerintah dan masyarakat.

> Pentingnya peran pemerintah dalam melaksanakan sebuah kebijakan, menurut Tachjan, bahwasanya "… Peran pemerintah atau administrator publik memegang posisi yang sangat penting dalam proses pembuatan kebijakan. Fungsi sentral dari pemerintah adalah menyiapkan, menentukan dan menjalankan kebijakan atas nama dan untuk keseluruhan masyarakat di daerah kekuasaannya (Hoogerwerf, 1983 : 9). Menurut Easton (1971 : 129) pemerintah sebagai "authorities in a political system", yaitu para penguasa dalam suatu sistem politik yang terlibat masalah sehari-hari dan merupakan tanggungjawabnya " (2006 : 14).

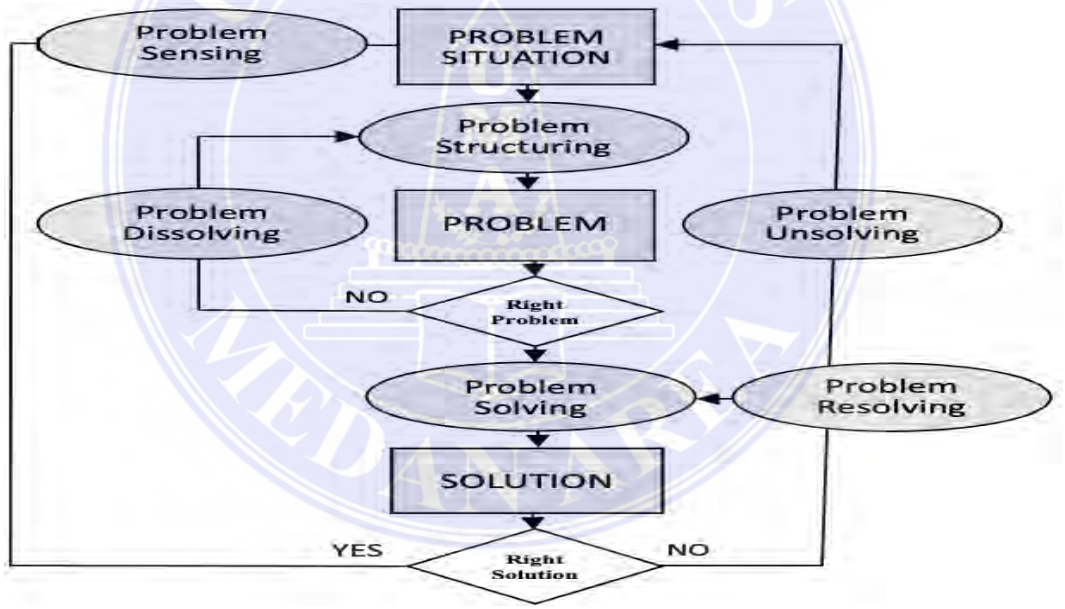
Suatu kebijakan publik yang berkualitas harus memuat tidak hanya pemikiran atau pendapat manajer publik, tetapi juga pandangan publik sebagai badan perwakilan kepentingan publik. Oleh karena itu, tugas pokok administrator publik memiliki hubungan yang sangat erat dengan kepentingan publik, oleh karena itu ia harus mengurusi masalah, kebutuhan, dan persyaratan yang ada di lingkungannya. Pengelola negara, sebagai aktor politik, merupakan bagian dari sistem kebijakan publik.

> Menurut William N. Dunn " *Policy problems are unrealized needs, values, or opportunities for improvement. Informa- tion about the nature, scope, and severity of a problem is produced by applying the policy-analytic procedure of problem structuring. Problem structuring, which is a phase of inquiry in which analysts compare, contrast, and evaluate competing formulations of a problem, is among the most important procedures performed by analysts. Problem structuring is a central guidance system that affects the success of other phases of policy analysis. Analysts seem to fail more often because they solve the wrong problem than because they get the wrong solution to the right problem* " (2017 : 70).

Proses ini membantu analis memahami sifat, ruang lingkup, dan kompleksitas suatu masalah sebelum mencari solusi, Strukturasi masalah memungkinkan analis untuk mendapatkan pemahaman yang mendalam tentang

masalah tertentu, dengan membandingkan dan mengevaluasi formulasi masalah yang berbeda, analis dapat mengidentifikasi aspek-aspek kunci dan faktor-faktor yang terlibat.

Kebijakan merupakan keputusan tentang sejumlah atau serangkaian pilihan yang saling terkait yang bertujuan untuk mencapai suatu tujuan, analisis kebijakan sering digambarkan sebagai pendekatan pemecahan masalah, gambaran pemecahan masalah secara keliru menunjukkan bahwa analisis dapat berhasil mengidentifikasi, mengevaluasi, dan mengusulkan solusi untuk suatu masalah tanpa menginvestasikan banyak waktu dalam perumusan masalah. Menurut William N. Dunn ada beberapa Proses struktur permasalahan :



Gambar 1 Proses Struktur Permasalahan (2017 : 71)

Menurut Gambar 1 oleh Willian N. Dunn, Pemecahan masalah jarang dimulai dengan masalah yang dinyatakan dengan jelas, kecemasan dan tanda-tanda kecemasan yang menyebar ini tidak sepenuhnya merupakan masalah, melainkan situasi masalah, mengacu pada keadaan "keyakinan tidak stabil" yang kita alami ketika memahami suatu situasi, membingungkan dan tidak jelas perlunya tindakan.

Sebaliknya, masalah politik adalah produk dari penerapan metode penataan masalah pada situasi masalah. Masalah adalah elemen situasi masalah yang telah ditarik dari situasi oleh struktur masalah.

Konfigurasi dan pemecahan masalah analisis kebijakan mencakup metode penataan masalah serta metode pemecahan masalah. Metode penataan masalah memberikan pelengkap metodologis untuk teori kebijakan. Metode penataan masalah adalah metametode, yaitu metode pemecahan masalah "tentang" atau "lanjutkan". Menurut William N. Dunn ada beberapa metode analisis yaitu :

1. *Forecasting. Forecasting methods are used to produce knowledge about expected policy outcomes…. which are based on the judgments of experts, are useful in identifying expected outcomes of science and technology policies.*
2. *Prescription. Methods of prescription are employed to create knowledge about preferred policies....The spreadsheet goes beyond the identification of expected policy outcomes by expressing consequences in terms of monetary benefits and costs...*
3. *Monitoring. Methods of monitoring are employed to produce knowledge about observed policy outcomes...*
4. *Evaluation. Evaluation methods are used to produce knowledge about the value or utility of observed policy outcomes and their contributions to policy performance* (2017 : 8).

Dengan mempertimbangkan keempat langkah ini, organisasi dapat mengoptimalkan strategi kebijakan mereka dengan membangun pada kekuatan internal, mengatasi kelemahan, memanfaatkan peluang eksternal, dan merespons secara efektif terhadap ancaman. Hal ini membantu meningkatkan kemungkinan keberhasilan pelaksanaan kebijakan dan mencapai tujuan yang diinginkan. Bahwasaannya ada metode yang harus dijalankan untuk memecahan masalah yang melibatkan analisis ulang masalah terstruktur dengan benar untuk mengurangi kesalahan, di sisi lain, pemecahan masalah melibatkan pengabaian solusi

berdasarkan rumusan masalah yang salah dan kembali ke masalah terstruktur untuk mencoba menghasilkan masalah yang benar.

Melihat regulasi yang digunakan pada Undang-Undang Informasi dan transaksi elektronik (ITE) No 11 tahun 2008 yang semesti mana telah dirubah sebahagian pasal dengan Undang-Undang No 19 tahun 2016 memecahkan permasalahan pada pasal karet, sehingga pemerintah menganalisis Kembali regulasi tersebut dan membuat sebuah Surat Keputusan Bersama (SKB) dan melakukan Revisi Pasal 27 dan 28.

2.2 Evaluasi Kebijakan Publik

Evaluasi kebijakan publik terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) penting sebagai respons terhadap perkembangan teknologi informasi dan komunikasi. Langkah ini melibatkan penilaian dampak dan efektivitas regulasi, dengan fokus pada aspek perlindungan hak asasi manusia, penegakan hukum, perlindungan data pribadi, ketentuan kriminalisasi, kebebasan pers, partisipasi masyarakat, kesiapan aparat penegak hukum, kesesuaian dengan teknologi terkini, pengawasan berkala, dan dampak sosial-ekonomi. Evaluasi tersebut bertujuan untuk memastikan bahwa UU ITE tetap relevan, melindungi hak individu, dan mampu mengakomodasi dinamika dalam dunia digital.

Kebijakan memainkan peran penting ketika mempertimbangkan bahwa proses kebijakan yang dibangun dengan model kebijakan yang berbeda memerlukan desain dan alat pemantauan yang berbeda dan dibuat. Analisis kebijakan diperlukan untuk menghasilkan informasi dan pengetahuan serta untuk mengembangkan metode menganalisis kebijakan yang diperlukan untuk memastikan bahwa rancangan kebijakan secara kompatibel dengan proses kebijakan secara keseluruhan.

Selain dari kacamata teknokratis, pengawasan kebijakan juga bisa dibaca dari pelaksanaan yang telah di jalankan sesuai dengan aturan yang dibuat. Seperti pemangku kepentingan dalam membuat proses kebijakan publik. Bagi para aktor ini, mereka yang tertarik untuk memulai atau mengakhiri suatu kebijakan, proses dan hasil pengawasan harus di evaluasi secara baik. Menurut Bingham dan Felbinger dalam Dr. Riant Nugroho membagi evaluasi kebijakan menjadi empat jenis, yaitu :

1. Evaluasi proses, yang fokus pada bagaimana proses Implementasi suatu kebijakan.
2. Evaluasi impak, yang fokus pada hasil akhir suatu kebijakan.
3. Evaluasi kebijakan, yang menilai hasil kebijakan dengan tujuan yang direncanakan dalam kebijakan pada saat di rumuskan.
4. Meta evaluasi, yang merupakan evaluasi terhadap berbagai hasil atau temuan evaluasi dari berbagai kebijakan yang terkait (2011 : 676).

Dari pembahasan Riant Nugroho membagi evaluasi kebijakan menjadi empat jenis yang memberikan pendekatan yang komprehensif dalam menilai dan memahami keberhasilan suatu kebijakan. Berikut adalah penjelasan singkat mengenai masing-masing jenis evaluasi:

1. Evaluasi Proses:

   Fokus : Menilai bagaimana proses implementasi suatu kebijakan dilakukan.

   Tujuan : Memastikan bahwa langkah-langkah pelaksanaan kebijakan berjalan sesuai dengan rencana dan prosedur yang telah ditetapkan.

2. Evaluasi Impak:

   Fokus : Menilai hasil akhir atau dampak yang dihasilkan oleh suatu kebijakan.

Tujuan : Mengukur apakah kebijakan tersebut mencapai tujuan yang diinginkan dan dampaknya terhadap masyarakat atau target yang dituju.

3. Evaluasi Kebijakan:

Fokus : Menilai hasil kebijakan dengan tujuan yang direncanakan saat kebijakan dirumuskan.

Tujuan : Mengukur sejauh mana kebijakan mencapai sasaran yang telah ditentukan dan apakah sesuai dengan visi dan misi yang diinginkan.

4. Meta Evaluasi:

Fokus : Evaluasi terhadap berbagai hasil atau temuan evaluasi dari berbagai kebijakan yang terkait.

Tujuan : Memberikan pandangan komprehensif terhadap sejumlah kebijakan dan mengevaluasi efektivitas keseluruhan kebijakan yang diterapkan.

Dengan membagi evaluasi kebijakan ke dalam empat jenis ini, Riant Nugroho memberikan kerangka kerja yang dapat membantu pemerintah atau organisasi untuk memahami dan meningkatkan pelaksanaan kebijakan mereka. Sedangkan menurut *Howlet dan Ramesh* dalam Dr. Riant Nugroho mengelompokkan evaluasi menjadi tiga, yaitu :

1. Evaluasi administratif mengkaji berbagai aspek seperti anggaran, efisiensi, dan biaya dari proses kebijakan pemerintah yang mencakup:
a. Evaluasi usaha, menilai input program yang dikembangkan oleh kebijakan.
b. Evaluasi kinerja, menilai output program yang dikembangkan oleh kebijakan.
c. Evaluasi kecukupan kinerja atau efektivitas, menilai apakah program dijalankan sesuai rencana.
d. Evaluasi efisiensi, menilai biaya program dan efektivitas biayanya.
e. Evaluasi proses, menilai metode yang digunakan organisasi dalam melaksanakan program..

2. Evaluasi yudisial terkait dengan keabsahan hukum tempat kebijakan diterapkan, termasuk kemungkinan pelanggaran konstitusi, sistem hukum, etika, aturan administrasi negara, hingga hak asasi manusia.
3. Evaluasi politik menilai sejauh mana kebijakan publik yang diterapkan diterima oleh konstituen politik.

Penilaian Implementasi kebijakan sama yang dilakukan sehubungan dengan penjelasan di atas bahwa penting untuk melaksanakan penilaian kebijakan agar memiliki strategi yang berarti bagi kelangsungan pemerintahan. Ketika kegiatan pengawasan didefinisikan sebagai kegiatan yang dirancang untuk memastikan bahwa proses kebijakan tidak menyimpang dari desain yang digariskan, kegiatan penilaian menilai efektivitas kebijakan dalam mencapai tujuan kebijakan yang diinginkan.

Dalam mengImplementasikan kebijakan yang akan dievaluasi, beberapa isu perlu dievaluasi berdasarkan hasil dari kegiatan kebijakan. seperti kebijakan Undang-Undang Informasi dan Transaksi Elektronik yang telah di evaluasi sesuai dengan tuntutan perkembangan masyarakat dan aturan hukum kebijakan tentang Informasi dan Transaksi berbasis elektronik dilakukan perubahan dalam Undang-Undang Nomor 11 tahun 2008 yang diubah dengan Undang-Undang Nomor 19 tahun 2016 atas Pasal tertentu.

> Menurut Aqsa Rahardian "timbulnya pro kontra dari Implementasi Undang-Undang Informasi dan Transaksi Elektronik ini memunculkan opini tersendiri dari masyarakat" (2019:2). Isu-isu dalam kebijakan ini berkaitan dengan penyampaian informasi, komunikasi, dan transaksi secara elektronik, terutama bukti dan isu-isu yang berkaitan dengan kebijakan yang akan dilaksanakan.

Kebijakan dapat dianggap sebagai proses bagaimana diImplementasikan dalam urutan langkah demi langkah, tetapi dalam praktiknya proses-proses ini tumpang tindih dan saling terkait satu sama lain. Menurut Thomas R. Thomas R Dye ada beberapa Proses pembuatan kebijakan yaitu :

Steps	***Process***	***Activity***	***Participants***
1	*Problem Identification*	*Publicizing societal problems Expressing demands for government action*	*Mass media Interest groups Citizen initiatives Public opinion*
2	*Agenda Setting*	*Deciding what issues will be decided, what problems will be addressed by government*	*Elites, including president, Congress Candidates for elective office Mass Media*
3	*Policy Formulation*	*Developing policy proposals to resolve issues and ameliorate problems*	*Think tanks President and executive office Congressional committees Interest groups*
4	*Policy Legimition*	*Selecting a proposal Developing political support for it Enacting it into law Deciding on its consitutionslity*	*Interest groups President Congtess Court*
5	*Policy Implementation*	*Budgeting and appropriations Organizing departments and agencies Providing payments or services Levying taxes*	*President and White House staff Executive departments and agencies Independent agencies and government corporations*
6	*Policy Evaluation*	*Reporting outputs of government programs Evaluating impacts of policies on target and nontarget groups Proposing changes and "reforms"*	*Executive departements and agencies Congressional oversight committees Mass media Think tanks*

Tabel 2 Proses Pembuatan Kebijakan (2015 : 26)

Pembuatan kebijakan merupakan proses yang kompleks dan berjenjang, memerlukan pemahaman mendalam terhadap berbagai tahapan yang dapat membentuk dasar kerangka kerja umum. Thomas R Thomas R Dye, seorang ahli dalam studi kebijakan, telah mengidentifikasi beberapa tahap kunci dalam proses ini, sementara tetap memberikan ruang untuk variasi yang mungkin terjadi berdasarkan konteks politik dan lembaga yang terlibat. Salah satu tahapan awal yang dikenal adalah identifikasi masalah. Thomas R Thomas R Dye menyoroti

pentingnya langkah ini sebagai fondasi pembuatan kebijakan. Pada tahap ini, para pemangku kepentingan melakukan analisis mendalam untuk mengidentifikasi isu-isu yang memerlukan perhatian dan tindakan. Ini bisa melibatkan berbagai metode penelitian, seperti survei masyarakat, analisis data, atau konsultasi dengan ahli terkait.

Dalam memahami bahwa sifat dan tingkat kompleksitas masalah dapat bervariasi, tergantung pada konteks dan karakteristik lembaga yang terlibat. Setelah identifikasi masalah, tahap berikutnya dalam proses pembuatan kebijakan adalah penetapan agenda. Pada langkah ini, para pemangku kepentingan dan pembuat kebijakan bekerja bersama untuk menentukan prioritas dan urgensi dari isu-isu yang telah diidentifikasi.

Negosiasi dan komunikasi yang efektif antara berbagai pihak menjadi kunci dalam membentuk agenda yang dapat diterima oleh semua pihak terlibat. Proses selanjutnya, yang ditekankan oleh Thomas R Thomas R Dye, adalah pengembangan kebijakan, ini melibatkan perumusan strategi dan solusi untuk mengatasi masalah yang diidentifikasi sebelumnya. Pembuat kebijakan akan mempertimbangkan berbagai opsi, menganalisis dampak potensial, dan melibatkan para ahli untuk memastikan kebijakan yang dihasilkan efektif dan dapat diimplementasikan. Meskipun Thomas R Thomas R Dye memberikan kerangka kerja umum untuk proses pembuatan kebijakan, ia juga mengakui bahwa proses ini tidak bersifat kaku.

Variasi dalam tahapan dan urutan proses dapat terjadi tergantung pada konteks politik dan karakteristik lembaga yang terlibat. Proses ini dapat melibatkan iterasi dan penyesuaian sepanjang waktu sesuai dengan perubahan situasional atau

pemahaman yang lebih baik terhadap isu-isu yang dihadapi. Dengan demikian, pemahaman terhadap tahap atau proses dalam pembuatan kebijakan, seperti yang diidentifikasi oleh Thomas R Thomas R Dye, memberikan landasan yang kuat bagi para pembuat kebijakan dan pemangku kepentingan untuk merancang kebijakan yang responsif, kontekstual, dan efektif dalam menanggapi Era Globalisasi.

2.3 Analisis Evaluasi Kebijakan Undang-Undang Informasi Dan Transaksi Elektronik

Pelakasanaan Undang-Undang Informasi dan Transaksi Elektronik harus dilaksanakan secara tepat sesuai dengan peraturan yang berlaku serta turunan dari pelaksanaan Undang-Undang ini agar tidak terjadinya multitafsir dalam menjaga ruang digital di Indonesia. Menurut Mahmud Md "… Pedoman Implementatif yang ditandatangani tiga menteri dan satu pimpinan lembaga setingkat menteri bisa berjalan dan bisa memberikan perlindungan yang lebih maksimal kepada masyarakat. Ini dibuat setelah mendengar dari para pejabat terkait, dari kepolisian, Kejaksaan Agung, Kominfo, masyarakat, LSM, Kampus, korban, terlapor, pelapor, dan sebagainya, semua sudah diajak diskusi, inilah hasilnya," tegas Mahfud Md usai menyaksikan penandatanganan di Kantor Kemenko Polhukam RI, Jakarta, Rabu (23/06/2021)" (kominfo.go.id).

Dalam pelaksanaan kebijakan masyarakat berhak memantau terlaksananya ruang digital, peran msyarakat juga akan merubah arah pelaksanaan regulsi untuk di rubah atau di revisi guna memberikan jawaban tantangan kedepan. Undang-Undang Informasi dan Transaksi Elektronik telah dilakukan perubahan pada pasal tertentu yang menjadi permasalahan di kalangan masyarakat. Pemerintah telah melakukan perumusan masalah terkait Pasal-Pasal karet yang membuat masyarakat menjadi rugi dengan adanya pasal tersebut, Adapun pasal yang dimaksud adalah

pasal pada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (kominfo.go.id) yang terlampir pada lampiran I.

Perubahan Undang-Undang terjadi karena Undang-Undang terdahulu belum sepenuhnya memberikan regulasi terhadap perubahan ruang digital yang semangkin canggih, adanya sebuah alat pendukung guna memberikan kesaksian terhadap Implementasi tersebut. Tantangan di dunia maya harus di awasi dengan baik untuk menjaga keamanan ruang Digital di Indonesia, melihat banyaknya aktivitas yang dilakukan masyarakat.

Menurut Media Elektronik Republika "Presiden Joko Widodo (Jokowi) membuka ruang untuk merevisi UU ITE. Jokowi menilai ada Pasal-Pasal karet yang bisa ditafsirkan secara berbeda oleh setiap individu. Berikut sejumlah kasus terkait Undang-Undang Informasi dan Transaksi Elektronik dari tahun 2008-2021:

No	Tahun	Kasus	Sumber
1.	2008	Kasus kritikan Prita Mulyasari terhadap RS OMNI Batavia.	Republika.co.id
2.	2008	Roy Suryo ditetapkan sebagai tersangka karena dituduh melakukan pencemaran nama baik terhadap Farhat Abbas melalui SMS.	nasional.tempo.com
3	2010	Prita Mulyasari divonis bebas setelah sempat ditahan dan dihukum karena dituduh melakukan pencemaran nama baik terhadap RS Omni Internasional	nasional.kompas.com
4	2011	Benny Handoko alias Benhan ditetapkan sebagai tersangka karena dituduh melakukan penghinaan terhadap Presiden Susilo Bambang Yudhoyono melalui Twitter	tekno.kompas.com
5.	2013	Farhat Abbas dilaporkan terkait kasus rasisme terhadap Basuki Tjahaja Purnama	Republika.co.id

		terkait isi Twiter. Kasus selesai setelah dimediasi.	
6.	2014	Ridwan Kamil melaporkan Kemal Septian terkait penghinaan Kota Bandung. Baiq Nuril Maknun, mantan Pegawai Guru Honorer tata usaha SMAN 7 Mataram dilaporkan H. Muslim terkait Pasal 27 ayat 1 Undang-Undang Informasi dan Transaksi Elektronik (ponigrafi). Sempat ditahan polisi, Baiq Nuril Bebas setelah mendapat amnesti dari presiden.	Republika.co.id
7.	2016	Harry Tanoesoedibjo melaporkan Prasetyo ke Bareskim karena dianggap mencemarkan nama baik. Thony Saut Situmorang yang saat itu menjabat sabagai wakil Komisi Pemberantasan Korupsi dilaporkan Ade Irfan Pulungan ke Polisi karena dianggap mencemarkan nama baik HMI. Muannas Alaidid yang melaporkan Buni Yani kemudian divonis penjara 1,5 tahun. Buni Yani melaporkan Guntur Romli terkait kasus video Basuki Tjahaja Purnama yang menyinggung Surat Al-maidah. Basuki Tjahaja Purnama (Ahok) terjerat kasus penistaan Agama. Ahok kemudian divonis 2 tahun penjara . Ridwan Hanafi melaporkan Sri Bintang Pamungkas terkait ujaran kebencian.	Republika.co.id
8.	2017	Kaesang dilaporkan oleh Muhammad Hidayat S karena video unggahannya dianggap mengandung ujaran kebencian dan penodaan Agama, kasus kemudian dihentikan. Aris Budiman yang kala itu menjabat sebagai Dirdik Komosi Pemberantasan Korupsi melaporkan Novel Baswedan terkait isi email yang dianggap menghina. Muannas Alaidid melaporkan Jon Riah Ukur (Jonru Ginting) terkait ujaran kebencian. Jonru kemudian divonis 1.5 tahun penjara.	Republika.co.id

9.	2018	Ratna Sarumpaet terjerat kasus penyebaran kabar bohong. Ratna Sarumpaet kemudian divonis 2 tahun penjara.	bbc.com
10.	2019	Artis Fairuz A Rafiq melaporkan Galih Ginanjar, Pablo Benua dan Rey utami terkait kasus "bau ikan asin". Setya Novanto melaporkan Emerson Yuntho terkait kasus pencemaran nama baik.	Republika.co.id
11.	2020	Ustadz Maher dilaporkan Waluyo Wasis Nugroho karena dianggap menghina Habib Luthfi Bin Yahya. Ustadz Maher meninggal sakit dalam tahanan. Musisi I Gede Ary Astina alias Jerinx atau JRX dilaporkan terkait ujaran kebencian terhadap Ikatan Dokter Indonesia (IDI). Denny Siregar dilaporkan karena dianggap menghina santri.	Republika.co.id
12.	2021	Ambroncius Nababan ditetapkan sebagai tersangka terkait dugaan Tindakan rasis terhadap Natalius Pigai. KNPI melaporkan Abu Janda ke Bareskrim Polri, terkait unggahan di Medsos bermuatan SARA.	Republika.co.id

Tabel 3 Kasus Terkait Undang-Undang Informasi Dan Transaksi Elektronik

Kebijakan peraturan Undang-Undang terkait dengan Informasi dan Transaksi Elektronik menuai pro dan kontra untuk segerah dilakukan revisi keseluruhan isi dari Undang-Undang tersebut. banyak juga yang memberi tanggapan perlunya segerah melakukan revisi kembali Undang-Undang Informasi dan Transaksi Elektronik agar tidak terjadi mulitafsir.

Dengan adanya ketidak nyamanan ini pemerintah terus melakukan perbaikan kebijakan publik untuk memberikan rasa aman, bebas, dan sesuai dengan Hak Asasi Manusia dalam memberikan pendapat, sehingga pemerintah dalam hal ini memberikan sebuah pedoman Implementasi yang berkaitan dengan Pasal-Pasal karet. Adapun Implementasi tersebut tertuang dalam Surat Keputusan Bersama

yang terlampir pada lampiran II tentang Pedoman Implementasi Atas Pasal Tertentu Dalam Undang - UndangNomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomo 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (kominfo.go.id)

2.4 Implementasi Kebijakan Publik

Implementasi kebijakan publik merujuk pada serangkaian tindakan yang dilakukan untuk menerapkan atau menjalankan kebijakan yang telah diambil sebelumnya. Proses implementasi ini melibatkan langkah-langkah konkret untuk mengubah keputusan kebijakan menjadi tindakan nyata di lapangan. Implementasi kebijakan publik adalah fase pelaksanaan dan operasionalisasi keputusan-keputusan kebijakan yang telah diambil oleh pemerintah atau lembaga terkait. Langkah-langkah ini mencakup serangkaian tindakan konkret yang dirancang untuk memastikan bahwa kebijakan yang telah dirumuskan dapat dijalankan dengan efektif di tengah masyarakat. Menurut Van Meter dan Van Horn (dalam Budi Winarno, 2008:146-147) mendefinisikan implementasi kebijakan publik sebagai tindakan-tindakan dalam keputusan-keputusan sebelumnya.

Van Meter dan Van Horn dikenal sebagai peneliti yang memberikan kontribusi dalam pemahaman mengenai implementasi kebijakan. Menurut mereka, implementasi kebijakan publik dapat didefinisikan sebagai serangkaian tindakan yang dilakukan untuk menerapkan kebijakan yang telah diambil sebelumnya. Dalam konteks ini, tindakan-tindakan tersebut mencakup berbagai langkah konkret yang bertujuan untuk mengubah keputusan kebijakan menjadi realitas di lapangan.

Definisi tersebut menekankan bahwa implementasi bukan hanya sebatas pada tahap perumusan kebijakan, tetapi melibatkan langkah-langkah pelaksanaan

yang konkret setelah keputusan diambil. Dengan kata lain, implementasi mencakup sejumlah kegiatan yang harus dilakukan untuk menjalankan kebijakan tersebut.

Penting untuk dicatat bahwa implementasi kebijakan publik dapat melibatkan berbagai pihak, mulai dari aparat pemerintah yang terlibat langsung dalam pelaksanaan, hingga pihak-pihak masyarakat yang dapat dipengaruhi oleh kebijakan tersebut. Oleh karena itu, implementasi kebijakan memerlukan koordinasi yang baik, alokasi sumber daya yang tepat, dan pemantauan yang cermat untuk memastikan bahwa kebijakan dapat dijalankan sesuai dengan tujuan yang diinginkan. Adapun makna implementasi menurut Daniel A. Mazmanian dan Paul Sabatier (1979) sebagaimana dikutip dalam buku Solihin Abdul Wahab (2008: 65), mengatakan bahwa:

> "Implementasi adalah memahami apa yang senyatanya terjadi sesudah suatu program dinyatakan berlaku atau dirumuskan merupakan fokus perhatian implementasi kebijaksanaan yakni kejadian-kejadian dan kegiatan-kegiatan yang timbul sesudah disahkannya pedoman-pedoman kebijaksanaan Negara yang mencakup baik usaha-usaha untuk mengadministrasikannya maupun untuk menimbulkan akibat/dampak nyata pada masyarakat atau kejadian-kejadian".

Implementasi kebijakan, sebagaimana dijelaskan oleh Daniel A. Mazmanian dan Paul Sabatier yang dikutip dalam buku Solihin Abdul Wahab (2008: 65), merujuk pada suatu proses pemahaman terhadap peristiwa-peristiwa yang benar-benar terjadi setelah suatu program atau kebijakan dinyatakan berlaku atau dirumuskan. Fokus utama implementasi kebijakan adalah pada kejadian-kejadian dan kegiatan-kegiatan yang muncul setelah pedoman-pedoman kebijakan negara disahkan.

Dalam konteks ini, implementasi kebijakan mencakup pelaksanaan nyata dari kebijakan tersebut di lapangan. Proses ini mencakup berbagai peristiwa dan

aktivitas yang timbul setelah kebijakan diumumkan atau disahkan. Dengan demikian, penting untuk memahami dampak dan dinamika yang terjadi selama pelaksanaan kebijakan, termasuk tantangan dan perubahan yang mungkin terjadi di tingkat pelaksanaan. Implementasi kebijakan juga melibatkan pemantauan, evaluasi, dan penyesuaian sesuai keadaan yang berkembang.

Penting untuk memiliki pemahaman menyeluruh terhadap dampak dan dinamika yang terjadi selama pelaksanaan kebijakan. Ini mencakup pemahaman terhadap berbagai tantangan yang mungkin muncul serta potensi perubahan di tingkat pelaksanaan. Implementasi kebijakan tidak hanya sebatas pada pengenalan kebijakan itu sendiri.

Dengan memahami dinamika, mengidentifikasi tantangan, dan mengakui kemungkinan perubahan selama pelaksanaan kebijakan, pemerintah atau lembaga terkait dapat menciptakan strategi yang lebih efektif dan responsif terhadap keadaan yang berkembang. Pemantauan, evaluasi, dan penyesuaian yang terus-menerus menjadi kunci kesuksesan dalam mencapai tujuan kebijakan. Terdapat beberapa teori dari beberapa ahli mengenai implementasi kebijakan, yaitu:

Teori George C. Edward III (dalam Subarsono, 2011: 90-92 berpandangan bahwa implementasi kebijakan dipengaruhi oleh epat variabel, yaitu:

a) Komunikasi: Keberhasilan dalam penerapan kebijakan mengharuskan para pelaksana untuk memahami dengan jelas tugas yang harus dilakukan dan sasaran yang hendak dicapai. Informasi ini harus disampaikan kepada kelompok sasaran (target group) dengan baik agar mengurangi kesalahan dalam pelaksanaan kebijakan.
b) Sumber Daya: Meski kebijakan telah dikomunikasikan dengan jelas dan konsisten, implementasi tidak akan efektif jika para pelaksana kekurangan sumber daya. Sumber daya ini mencakup sumber daya manusia, seperti kompetensi pelaksana, dan sumber daya finansial.
c) Disposisi: Disposisi mencakup watak dan karakteristik pelaksana kebijakan, seperti komitmen, kejujuran, dan sifat demokratis. Pelaksana dengan disposisi yang baik cenderung menjalankan kebijakan sesuai

harapan pembuat kebijakan. Sebaliknya, perbedaan sikap atau pandangan antara pelaksana dan pembuat kebijakan dapat menghambat efektivitas implementasi.

d) Struktur Birokrasi: Struktur organisasi yang bertugas melaksanakan kebijakan memiliki dampak signifikan terhadap penerapan kebijakan tersebut. Aspek penting dari struktur organisasi meliputi Standard Operating Procedure (SOP) dan fragmentasi. Struktur yang terlalu kompleks dapat melemahkan pengawasan dan menciptakan prosedur birokrasi yang rumit (red-tape), yang mengurangi fleksibilitas organisasi.

Menurut pandangan Edwards (dalam Budi Winarno, 2008: 181) sumber-sumber yang penting meliputi, Sumber Daya Manusia yang memadai serta keahlian-keahlian yang baik untuk melaksanakan tugas-tugas kinerja, wewenang dan fasilitas-fasilitas yang diperlukan untuk menerjemahkan usul-usul di atas guna melaksanakan pelayanan-pelayanan publik yang prima di tengah masyarakat. Menurut Struktur Birokrasi Edwards (dalam Budi Winarno, 2008: 203) terdapat dua karakteristik utama, yakni Standard Operating Procedures (SOP) dan Fragmentasi:

> "SOP atau prosedur kerja dasar berkembang sebagai respons internal terhadap keterbatasan waktu dan sumber daya pelaksana serta keinginan untuk keseragaman dalam operasional organisasi yang kompleks dan tersebar luas. Sementara itu, fragmentasi muncul dari tekanan eksternal terhadap unit-unit birokrasi, seperti komite legislatif, kelompok kepentingan, pejabat eksekutif, konstitusi negara, dan sifat kebijakan yang mempengaruhi organisasi birokrasi pemerintah.".

SOP atau *Standard Operating Procedure* adalah serangkaian prosedur kerja atau langkah-langkah yang telah ditetapkan untuk membimbing para pelaksana dalam menjalankan tugas-tugas mereka dengan konsisten dan efisien. Pengembangan SOP dilakukan sebagai respons internal terhadap keterbatasan waktu dan sumber daya para pelaksana, serta keinginan untuk mencapai keseragaman dalam operasional organisasi yang kompleks dan tersebar.

Di sisi lain, fragmentasi dalam konteks ini merujuk pada pengaruh dari tekanan-tekanan eksternal yang berasal dari unit-unit birokrasi di luar organisasi. Faktor-faktor tersebut dapat mencakup komite-komite legislatif, kelompok kepentingan, pejabat eksekutif, konstitusi negara, dan sifat kebijakan yang memengaruhi struktur dan operasi organisasi birokrasi pemerintah.

Dengan adanya fragmentasi, organisasi birokrasi mungkin menghadapi tantangan dalam menjaga kohesivitas dan kesatuan operasionalnya. Oleh karena itu, pengembangan SOP menjadi penting sebagai upaya untuk menanggapi tekanan eksternal dan memastikan bahwa organisasi dapat tetap efisien, terorganisir, dan sesuai dengan kebijakan yang berlaku. Dengan menerapkan SOP, organisasi dapat mencapai standar kinerja yang konsisten dan memitigasi dampak fragmentasi yang mungkin muncul dari tekanan-tekanan eksternal tersebut.

2.5 Rasional Sistem Keputusan Pelaksanaan Pemantauan Ruang Digital Di Indonesia

Meningkatnya kegiatan masyarakat di Internet memberikan tantangan tersendiri bagi pemerintah untuk terus memantau dalam index (objek) besar maupun kecil dari system yang terus terlaksana oleh kebijakan yang berlaku dan terus melakukan perubahan kebijakan untuk menjawab perubahan yang begitu cepat di dunia maya, menjaga keamanan di tengah masyarakat dalam melakukan kegiatan di Internet harus terus dilakukan, meningat meningkatnya kejahatan dunia maya/*cyber crime.*

Rasional yang tinggi di tengah masyarakat membuat pemerintah terus memantau ruang digital untuk memberikan rasa aman dalam berselancar, model rasional ini harus di kembangkan melalui sebuah evaluasi kebijakan yang baik, mengingat pemerintah terus melakukan berbaikan pelayanan *E-Digital* yang terus

di kembangkan dengan cepat harus dilakukan perbaikan secara terus menerus agar tidak terjadi pencurian data yang dapat menimbulkan kerugian di tengah masyarakat.

Menurut Ernet R. House dalam Joko Pramono, kebijakan publik melalui beberapa model, yaitu: (1) model sistem dengan indikator utama efisiensi, (2) model perilaku dengan indikator utama produktivitas dan akuntabilitas, (3) model formulasi keputusan dengan indikator utama efektivitas dan kualitas terjaga, dan (4) model tujuan bebas (goal free) dengan indikator utama pilihan pengguna dan manfaat sosial (2020:49).

Dari model tersebut pentingnya melakukan evaluasi terhadap apa yang menjadi kepentingan hak banyak Orang harus dilakukan evaluasi untuk dilakukan perubahan terhadap kebijakan yang akan dilaksanakan, ke efesiensian Undang-Undang Informasi dan Transaksi Elektronik dapat di ukur dengan berkurangnya kejahatan di ruang *Digital,* pelaksanaan kebijakan dapat dinilai dengan indikator keberhasilan pemerintah dalam menegur prilaku menyimpang ataupun memberikan pemberitahuan secara cepat agar tidak ada korban. Pelaksanaan Implementasi sebuah kebijakan harus dengan formulasi keputusan dengan indikator keberhasilan pemerintah dalam menjaga kerahasian data pribadi maupun kelompok dari kejahatan *cyber crime,* maka dengan ini pemerintah harus mementingkan dampak social yang akan terjadi terhadap *cyber crime.*

> "Id-SIRTII melakukan pemantauan kondisi keamanan Internet Indonesia dengan menggunakan beberapa jalur pemantauan yaitu pemantauan jaringan infrastrutkur Internet Indonesia dengan menggunakan Mata Garuda, pemantauan menggunakan jaringan honeynet id-SIRTII, pemantauan dari Jaringan CERT global, pemantauan dari laporan publik dan pemantauan lewat R&D Id-SIRTII" (BSSN 2018:14). "Berdasarkan hasil pemantauan lalu lintas (trafik) anomali Internet nasional dari bulan Januari sampai bulan Desember 2018, didapatkan sebanyak 232,447,974 serangan siber ke jaringan Indonesia. Port yang terbanyak menjadi target diserang adalah port 123. Negara yang menjadi sumber serangan terbanyak berasal dari Indonesia,

> dan yang menjadi target serangan siber terbanyak adalah Indonesia. Hasil pemantauan jaringan web menemukan 16,939 kasus insiden website (defacement) dengan domain terbanyak menjadi target adalah domain go.id. Ancaman terbesar ke Indonesia tahun ini adalah ancaman malware yang aktivitasnya tercatat sebesar 122 juta dalam tahun ini" (BSSN 2018:15).

Pelaksaan pemantauan ruang *Digital* tidak hanya di lakukan penegak Hukum (Kepolisian dan/atau Kejaksaan) maupun Kementerian Informasi dan Informatika, pemerintah melalui BSSN (Badan Siber dan Sandi Negara) memberikan amanah untuk memantau ruang *Digital*/*Cyber security* sesuai dengan Undang-Undang Keterbukan Informasi Nomor 14 Tahun 2008. Menurut data Badan Siber dan Sandi Negara dari tahun 2018 sampai dengan 2021 mengalami peningkatan mobilitas jaringan Internet di Indonesia ada pun data yang di maksud adalah sebagai berikut ini :

> "Berbeda dengan tahun-tahun lalu, sistem monitoring mata garuda mendeteksi serangan terbesar pada tahun ini adalah serangan percobaan pembocoran data (*attempted information leak*). Serangan ini tidak langsung membuktikan bahwa pengumpulan data informasi berhasil dilakukan sehingga terjadi kebocoran data, akan tetapi merupakan sinyal dan indikasi bahwa percobaan kearah sana sudah dilakukan yang jika kondisinya ternyata sesuai dengan harapan hacker, memungkinkan terjadinya ekskalasi ke arah pengambil alihan sistem dan kebocoran data penting. Serangan malware merupakan serangan kedua terbesar tahun ini, akan tetapi meskipun yang kedua dalam sembilan bulan dari dua belas bulan tahun ini, serangan malware selalu merupakan metoda serangan yang paling sering digunakan dan berada pada peringkat pertama" (BSSN 2019:14).

BAB III

METODE PENELITIAN

3.1 Tempat Penelitian

Lokasi penelitian ini dilakukan pada Kantor Kepolisian Daerah Sumatera Utara di Jalan. Sisingamangraja Km (Kilometer) 10,5, Kota Medan, dimana pemilihan lokasi ini dilakukan secara sengaja dengan pertimbangan lokasi penelitian adalah tempat dilakukannya pengawsan dan pengendalian kejahatan siber di wilayah Hukum Sumateras Utara.

3.2 Metode Penelitian

Riset ini menggunakan pendekatan kualitatif, riset dicoba secara *Transformative*, dengan melaksanakan riset secara bertepatan. Tata cara yang digunakan dalam riset ini merupakan *method design*, Menurut Samsu "Penelitian yang menghasilkan kesimpulan berdasarkan temuan di lapangan hanya akan menjadi suatu konstruksi sosial penelitian pada lapangan tertentu, apabila didekati secara kualitatif semata ....." (2017:170).

Penelitian ini melibatkan pengembangan teori pemahaman realitas dan analisis kompleksitas sosial menggunakan metode kualitatif di DISKRIMSUS POLDASU/ SUBDIT V Cyber Crime. Pendekatan ini dilakukan secara bersamaan dalam satu penelitian. Penelitian ini mengintegrasikan pengembangan teori dan observasi empiris langsung di lapangan, dan analisis kompleksitas sosial untuk menyelaraskan pemahaman mendalam tentang kejahatan *cyber crime* dan penanganannya, pendekatan ini memungkinkan literasi antara pengembangan teori dan pengumpulan data empiris, memastikan relevansi dan kontribusi yang maksimal.

3.3 Informan Utama

Penelitian akan dilakukan secara mendalam dengan memilih dan memanfaatkan informan sebagai hasil penelitian yang akan dilakukan, menurut Prof. Dr. Lexy J. Moleong, M.A. Informan adalah Orang yang dimanfaatkan untuk memberikan Informasi tentang situasi dan kondisi latar penelitian (2014:132), permasalahan yang akan di teliti dapat di proleh secara jelas maupun akurat agar penelitian tepat pada fokus penelitian, Informan utama penelitian ini adalah PANIT (Pembantu Unit) III (Tiga) Siberdit Reskrimsus Polda Sumatera Utara.

3.4 Teknik Pengumpulan Data

Menurut Sugiyono (2012:63) menyatakan bahwa secara umum terdapat 4 (empat) macam teknik pengumpulan data, yaitu observasi, wawancara, dokumentasi dan gabungan/triangulasi. Teknik yang dilakukan penelitian menggunakan pengumpulan data Kualitatif yang merupakan data tidak berbentuk angka, data kualitatif dinyatakan dalam bentuk kata maupun kalimat. Adapun data kualitatif yang penulis butuhkan adalah data tentang gambaran umum objek penelitian pelaksanaan **Analisis Implementasi Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 Yang Telah Diperbaharui Pada Undang-Undang Nomor 19 Tahun 2016 Di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara.** Peneliti menggunakan data penelitian Kualitatif.

1. Wawancara

Menurut Lexy J. Moleong, “wawancara adalah percakapan dengan maksud tertentu. Percakapan itu dilakukan oleh dua pihak, yaitu pewawancara yang mengajukan pertanyaan dan there wawancara yang memberikan jawaban atas

pertanyaan itu" (2014:186). Wawancara yang akan dilakukan adalah wawancara secara informal kepada pelaksana Kepala Subdirektorat V dan Kanit II dan III Siberdit Reskrimsus Polisi daerah Sumatera Utara.

2. Dokumentasi

Dokumentasi dalam penelitian ini diperlukan hal hal yang bersifat variable berupa buku, surat kabar, majalah internet, serta penulis memerlukan dokumen-dokumen yang sudah tersedia di Subditrektorat V Kepolisian Daerah Sumatera Utara.

3. *Field Research* (Penelitian Lapangan)

Penelitian lapangan dilakukan dalam riset penelitian yang akan mencari data primer dengan lansung terjun kelapangan dan mewawancarai pihak yang terlibat dalam penelitian ini.

4. Observasi

Pentingnya pengamatan dan/atau ingatan dalam melakukan perumusan masalah yang berkembang dimasyarakat peneliti melakukan Observasi lapangan pada tanggal 7 Juni 2021 sesuai dengan izin kampus Universitas Pascasarjana Universitas Medan Area nomor: 503/PPS-UMA/WDI/01/VI/2021. Dalam observasi ini terlibat secara langsung dengan kegiatan sehari-hari yang sedang diamati pada Pasal 27, 28, 29, dan 31.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai analis Implementasi Undang-Undang Informasi dan Transaksi Elketronik nomor 11 Tahun 2008 yang telah diperbaharui pada Undang-Undang nomor 19 Tahun 2016 di Kepolisian Negara Republik Indonesia Daerah Sumatera Utara dapat ditarik kesimpulan ialah sebagai berikut :

1. Implementasi UU ITE nomor 11 Tahun 2008 yang diperbaharui pada Undang-Undang nomor 19 Tahun 2016 pada pasal 27 berjalan sesuai dengan UU yang berlaku, SOP *cyber crime* (dapat di lihat pada lampiran IV), dan SKB (dapat di lihat pada lampiran III) yang berlaku.
2. Implementasi UU ITE nomor 11 Tahun 2008 yang diperbaharui pada Undang-Undang nomor 19 Tahun 2016 pada pasal 28 ayat 1 tidak berjalan sesuai dengan UU yang berlaku, dan SKB (dapat di lihat pada lampiran III) yang berlaku hal ini dikarenakan Implementasi SKB pada pasal 28 ayat 1 pada defenisi “konsumen” berkaitan perlindungan konsumen sesuai UU nomor 8 Tahun 1999 tentang pembocoran data nasabah.
3. Implementasi UU ITE nomor 11 Tahun 2008 yang diperbaharui pada Undang-Undang nomor 19 Tahun 2016 pada pasal 29 berjalan sesuai dengan UU yang berlaku, SOP *cyber crime* (dapat di lihat pada lampiran IV), dan SKB (dapat di lihat pada lampiran III) yang berlaku.

4. Implementasi UU ITE nomor 11 Tahun 2008 yang diperbaharui pada Undang-Undang nomor 19 Tahun 2016 pada pasal 31 belum berjalan, dikarenakan pasal tersebut tidak terdapat kasus yang ditemukan di POLDASU.

5.2 Saran

Berdasarkan simpulan di atas maka penulis memberikan saran sebagai berikut di bawah ini :

1. POLDASU seharus melakukan kerja sama berkaitan dengan *cyber crime* dengan Instansi maupun perusahaan *flatform digital* lainnya .
2. Pemerintah seharusnya meninjau ulang berkenaan dengan UU nomor 8 tahun 1999 tentang perlindungan konsumen hal ini agar Subdit V dalam menangani penipuan konsumen yang bersangkutan agar cepat di lakukan pembukaan indentitas pelaku yang berkaitan dengan BANK.
3. Masyarakat seharusnya lebih berhati-hati di dunia maya dalam berbagai hal dan diminta selalu cek keaslian akun, tokoh online, berita, dan transaksi yang dapat menimbulkan kerugian materil.

DAFTAR PUSTAKA

Arikunto, Suharsimi. 2012. Prosedur Penelitian: Suatu Pendekatan Praktik. Cetakan ke-15. Jakarta: Rineka Cipta: Jakarta.

AG. Subarson. 2011. Analisis Kebijakan Publik (konsep, teori dan aplikasi). Yogyakarta: Pustaka Pelajar

Creswell. John. W. 2013. *Research design: qualitative, quantitative, and mixed methods approaches. Los Angeles:* SAGE *Publications.*

McCormick,Keith, dkk. 2017. *SPSS Statistics for Data analysis And Visualization. Wiley: Indianapolis.*

Moleong Lexy J. 2014. Metodologi Penelitian Kualitatif. Bandung: PT. Remaja Rosdakarya.

N. Dunn. William. 2017. Public Policy Analysis: An Integrated Appoach. New York: Routledge.

Pramono. Joko. 2020. Implementasi dan Evaluasi Kebijakan Publik. Solo: Percetakan Kurnia.

Riant Nugroho. 2011. Public Policy: Dinamika Kebijakan- Analisis Kebjikan- Managemen Kebijakan. Jakarta: PT. Elex Media.

Dye R. Thomas. 2017. Understanding Publik Policy. Florida: Fifteenth Edition.

Samsu. 2017. Metode Penelitian (Teori dan Aplikasi Penelitian Kualitatif, Kuantitatif, Mixed Methods, serta Reseach dan Development). Jambi: Pusaka.

Sugiyono, 2012. Metode Penelitian Kuantitatif, Kualitatif Dan R&B. Bandung: Alfabeta.

Tachjan, 2006. Implementasi Kebijakan Publik. Asosiasi Ilmu Politik Indonesia (AIPI): Bandung.

Subarsono, A. G. (2011). Analisis Kebijakan Publik: Konsep, Teori, dan Aplikasi. Yogyakarta: Pustaka Pelajar.

Wahab, S. A. (2008). Analisis Kebijaksanaan: Dari Formulasi ke Implementasi Kebijaksanaan Negara. Jakarta: Bumi Aksara.

jurnal:

Rahardian.Aqsa. 2019. JOM FISIF Vol.6: Edisi 1 Januari – Juni

Permatasari. Iman Amanda, dan Wijaya. Junior Hendri 1 Juni 2019. Vol. 23 No.: 27-41.

Undang - Undang

UU ITE No 11 Tahun 2008

Surat Keputusan Bersama UU ITE

Suber lainya:

https://cloud.bssn.go.id/s/Y9tSycL4Pzci2qW/ Laporan Hasil Monitoring Keamanan Siber 2018.

https://cloud.bssn.go.id/s/nM3mDzCkgycRx4S/Laporan Tahunan 2019 Pusopskamsinas.

https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW#pdfviewer/ Laporan Tahunan Monitoring Keamanan Siber 2020.

https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw/ Laporan Tahunan Monitoring Keamanan Siber 2021.

https://m.kominfo.go.id/content/detail/35229/skb-pedoman-implementasi-uu-ite-ditandatangani-menko-polhukam-berharap-beri-perlindungan-pada-masyarakat/0/berita

https://www.republika.co.id/berita/qs0x08409/ylbhi-pasal-bermasalah-di-uu-ite-bukan-cuma-pasal-27-ayat-1

file:///C:/Users/ediar/Downloads/aptika.kominfo.go.idAhli%20Hukum%20dan%20Akademisi%20Nilai%20Revisi%20UU%20ITE%20Persempit%20Ruang%20Multitafsir.pdf 2023

https://nasional.tempo.co/read/1532466/inilah-deretan-kasus-kriminalisasi-uu-ite-yang-menjerat-jurnalis

https://nasional.kompas.com/read/2022/06/28/18264221/terbukti-melanggar-uu-ite-adam-deni-divonis-4-tahun-penjara

https://tekno.kompas.com/read/2021/02/16/15030007/6-korban-yang-dijerat-pasal-karet-uu-ite

https://www.bbc.com/indonesia/indonesia-48946433

LAMPIRAN I

1. Apakah dalam menjalankan Implementasi Undang-Undang ITE No 11 Tahun 2008 sebagaimana yang telah diubah pada No 19 tahun 2016 Subdirektorat V POLDASU mempunyai penerapan SOP ?

   Baik, terkait pertanyaan itu sudah dalam proses penyelidikan penanganan tindak pidana ITE, kami penyidik dari Subdit V Cyber Subdit Krimsus SOP-nya mengacu kepada Peraturan Kapolri nomor 6 tahun 2019 tentang penyidikan tindak pidana yang kedua adanya Peraturan Kabreskrim (PERKABA) Nomor 1 tahun 2022 tentang SOP pelaksanaan penyidikan tindak bidana, jadi proses penyidikan semuanya mulai dari tahap lidik sampai sidik tetap tidak bisa lepas dari badan Perkap dan Perkaba. Itulah yang menjadi SOP dalam penanganan proses penyidikan tindak Pidana.

2. Kenapa pelaksanaan Undang-Undang ITE diperlukan Surat Keputusan Bersama KOMINFO, KEJAGUNG, dan POLRI dalam melaksanakan Implementasi Kebijakan ini !

   Hal ini dikarenakan di dalam Surat Keputusan Bersama KOMINFO, KEJAGUNG, dan KAPOLRI itu diatur implementasi contohnya dalam hal penerapan pasal 27 ayat 3 undang-undang ITE disitu, dalam khususnya pasal 27 ayat 3 mengenai penghinaan dan penyebaran hal baik itu diatur hal-hal apa yang menjadi acuan dalam hal membuat pengaduan siapa yang dapat melaporkan dan bagaimana pidana ITE itu penghinaan pencemaran nama baik itu juga diatur disitu kan harus merupakan sebuah tuduhan, bukan hanya juga terkait dengan penghinaan pencemaran yang nama baik melalui media online itu tetap mengacu kepada, ekspesialnya ke undang-undang sehingga tidak

semua penghinaan penyertaan yang baik yang melalui ITE dapat kita terapkan ke undang-undang pasal 27 ayat 3 tadi.

3. Adakah kendala dalam melaksanakan Implementasi pada pasal 27, 28, 29, dan 31 ?

   Pasal 27 itu terkait dengan tindak pidana judi, kendalanya ada pada masalah *website* tadi terlalu banyak. Kemudian dalam hal penanganan *website* yang rata-rata webnya itu kan ada di luar negeri, kita disini hanya menindak paling banyak itu player game kemudian terkait pasal 28 ayat 1 penipuan online kendalanya disini, setiap kendala penipuan online itu terkait dengan rekening dari para pelaku rekening Bank yang dipergunakan. kita berbenturan terhadap undang-undang rahasia perbankan dimana rekening penampung rekening yang digunakan oleh tersangka biasanya bukan atas nama tersangka begitu juga dengan nomor *SIM card provident* yang dipergunakan dalam hal registrasi tadi, selalu registrasinya itu atas nama pihak lain begitu juga dengan rekening Bank penampungnya itu yang menjadi kendala dari pihak Bank, kalau kita surati pun kita minta data, selalu tidak pernah memberikan. Itu yang menjadi kendala paling utama dalam proses penipuan online yang kita tangani. Kalau dengan terkait SARA, sudah jelas ada di dalam implementasi SKB tidak ada kendala.

4. Apakah pada Implementasi Pasal 27 Ayat 1 yang berkenaan kesusilaan semuanya berkaitan dengan Pornografi atau ketelanjangan ?

   Dalam hal Pasal 27 Ayat 1 yang berkenaan dengan persusilaan semua berkaitan dengan pornografi.

5. Apakah vidio yang berkaitan dengan Kedokteran yang disebar termaksud konteks kesusilaan ?

   kedokteran sepanjang orangnya tidak keberatan contoh seperti saya, gambar saya gambar seseorang perempuan di posting pada media sosial, biasanya di media sosial yang dipergunakanya mungkin untuk Kepentingan pribadi seorang, mungkin dia akan keberatan Tapi Kalau dia, seperti yang bapak bilang tadi kan tidak mungkin itu ada dipergunakan untuk bidang kedokteran satu lagi yang terkait dengan pornografi dan bermaksud dengan pornografi kan ada undang-undang tersendiri pornografi kasus silaannya beda, pornografinya beda Jadi biasanya yang kita tangani itu rata-rata yang di media sosial.

6. Bagaimana Subdirektorat V Cyber Crime menjalankan tugas pada frasa "muatan melanggar kesusilaan ?

   Hal yang melanggar Kesusilaan perilaku yang diposting pada media sosial sebagaimana penyidik menjalankan tugas pada frasa tersebut Subdit V (Lima) menjalankan tugas sesuai SOP yang di tetapkan tentang kejahatan dunia maya.

7. Pada Pasal 27 Ayat 2, 3 dan 4 Implementasi di titik beratkan pada mendistribusikan dan/atau mentransmisikan yang memiliki muatan perjudian, pencemaran, apakah Subdirektorat V Cyber Crime melakukan penghapusan dan/atau pencegahan serta penegakan Hukum sesuai pedoman SKB sebelum dan/atau sesudah terjadinya korban di dunia maya!

   kalau kita dari cyber, tetap ada edukasi karena kita juga dalam edukasi di media sosial tetap disampaikan edukasi kepada masyarakat itu berarti kan sebelum terjadi pada saat terjadi biasanya kan masyarakat membuat laporan pengaduan Semoga dalam proses penanganan perkaranya Kami tetap mengutamakan mediasi dulu Mediasi itu hanya terkait Pasal 27 ayat 3 Kalau terkait dengan judi online, ayat 2-nya, kalau ditemukan webnya tetap kita lempar ke penipuan supaya dilakukan pemblokiran atau kita takedown terkait dengan ayat keempat-empatnya tetap ada edukasi dari awal dan lebih mengutamakan mediasi Kalau terlalu apapun memang ada kadang-kadang kita

melakukan dari penyidik melakukan takedown dengan cara menyurati. Iya Medianya, sepertinya WhatsApp, perwakilannya kita suratin dan ke balai dikrim juga ada yang intinya, pencegahan tetap dilakukan kalau pendidikan lebih mengutamakan mediasi, restorasi keadilan sesuai dengan perpol nomor

8. Pada Pasal 27 Ayat 3 sering dianggap Masyarakat melanggar HAM, bagaimana Subdirektorat V POLDASU menangani Kebijakan ini ditengah Masyarakat !

Kalau kita dari *Cyber Crime* tetap ada edukasi di media sosial tetap disampaikan edukasi kepada masyarakat itu berarti sebelum terjadi pada saat terjadi Biasanya masyarakat membuat laporan pengaduan perkaranya Kami tetap mengutamakan mediasi dulu Mediasi itu hanya terkait ke 27 ayat 3 Kalau terkait dengan judi online, pasal 2-nya, kalau ditemukan webnya tetap kita lempar ke tim IT supaya dilakukan pemblokiran atau kita takedown terkait dengan pasal ke 4 (Empat) tetap ada edukasi dari awal dan lebih mengutamakan mediasi Kalau terlalu apapun memang ada kadang-kadang kita melakukan dari penyidik melakukan takedown dengan cara menyurati pada profider (jasa layanan internet), benar ya? Iya Media seperti WhatsApp, perwakilannya kita suratin yang intinya pencegahan tetap dilakukan kalau penyidikan lebih mengutamakan mediasi, restorasi keadilan sesuai dengan Peraturan Kepolisian Negara Republik Indonesia Nomor 8 Tahun 2021 tentang Penanganan Tindak Pidana Berdasarkan Keadilan Restoratif, menambah ini jadi kalau terkait dengan perlakuan postingan itu kita mengacu kepada kewenangan kita juga yang namanya postingan itu kan menjadi barang bukti dalam perkara itu ya kan? Dan kita juga nggak bisa langsung tiba-tiba menghapus atau memblokir, seperti itu apabila itu masih dibutuhkan sampai proses peradilan yang bisa kita lakukan itu tentu menyita akunnya dan tidak bisa juga langsung kita hapus sendiri di situ sampai ke persidangan itu akan menjadi barang bukti dan bahkan akun itu pun kita ambil alih apakah akun Facebook, Whatsapp dan postingan masih berada di situ, dan suatu saat bisa saja dibuka di persidangan apabila dibutuhkan nah di persidangan nanti akan memutuskan apakah itu akan dihapus, dihilangkan atau bagaimana, atau dinonaktifkan kalau sampai ke peradilan perkara-perkara yang kita namakan *restoratif justice* itu bisa langsung segera dihapus karena namanya *restoratif justice* itu kan berarti penyelesaiannya itu sudah di luar

jadwal keradilan, itu harus segera dilakukan pemulihan *restoratif justice* itu kan pemulihan keadaan yang paling utama itu kalau itu terkait dengan kehormatan seorang memulihan kehormatan orang itu apabila ada postingan yang menyebarkan pencemaran yang baik terhadap dirinya atau konten-konten asusila terhadap dirinya itu ya segera dihapus dan kemudian ada klarifikasi permohonan maaf juga di media-media ataupun akun-akun yang dipergunakan untuk menyebarluaskan hal-hal itu, segera bisa kita minta untuk dihapus karena perkara itu selesai.

9. Bagaimanakah Subdirektorat V melaksanakan Implementasi Pasal 28 dalam mengindentifikasikan pelanggaran Dunia Maya setiap Ayat yang berlaku pada Kebijakan ini ?

Kalau implementasinya sesuai dengan SKB 3 Menteri yang kemudian kita proses dan biasanya itu kalau dia menyangkut kesalahannya tadi, ayat 2 mengekspos kesalahan, itu langsung kita takedown supaya jangan lebih dikembang mengakibatkan situasi gejolak di masyarakat proses penyidikan tetap kita lakukan tapi sebelum kita take down tetap kita jadikan postingan itu sebagai barang bukti kita angkat akunnya kita sita untuk proses penyidikan dan penuntutannya nantinya, pasal 28 ayat 1 berbeeda dengan ayat 2 mengenai kerugian konsumen yang berkaitan pada berita bohong menyebabkan kerugian konsumen, ini kan delik-delik materil Jelas dulu kerugian orang yang korban baru itu menjadi tindak pidana. Tetapi juga harus dibuktikan terkait dengan penyebaran berita bohong. Jadi dari awal itu juga harus bisa kita buktikan ataupun di dalam rangkaian postingan-postingan yang dilakukannya sehingga orang tergerak dia karena tidak terlepas juga jadi pasal 28 dari unsur-unsur penipuannya. Pada Pasal 28 ayat 2 ini kan yang dirugikan ini sebenarnya masyarakat karena mengacu kepada Sarah, Kentraman Masyarakat Nah untuk kasus-kasus ini kita bisa segera langsung membuat laporan polisi tanpa menunggu ada korban yang melapor contohkan beberapa kali itu polisi melapor ke polisi dan langsung dilakukan penindakan tapi ya apa namanya itu ya postingan-postingannya itu tetap bisa di-take down tetapi sudah dilakukan dulu Provining dan pengambilan bukti-bukti alat bukti elektronik berapa ini kan apa

namanya salinannya atau linknya ataupun capture wire begitu 28 ayat 2 nya jadi kalau masalah penyebarannya tidak semua juga berita bohong itu terkait dengan Sarah sehingga selama ini memang masih bisa dilapisi lagi dengan pasal-pasal seperti 14 terkait dengan penistaan Agama.

karena masalah, tapi kan di dalam SKB itu dijelaskan juga bahwa yang dimaksudkan konsumen itu kan konsumen secara luas ya, secara luas jadi siapa saja yang bertransaksi terkait dengan barang dan jasa yang menyebabkan dia rugi, melalui transaksi elektronik itu dia berhak untuk melaporkan sebagai korban tidak perlu kita buktikan itu dia ada perjanjian apa itu nanti bukan pidana jadi namanya konsumen ini kan publik yang bertransaksi secara elektronik untuk menambahkan apa yang saya ingin bakal ini terkait dengan konsumen itu kan ada undang-undang perlindungan konsumen undang-undang perlindungan konsumen itulah seperti bilang secara umum Siapa yang disebut sebagai konsumen Tetap mengacu ke situ, dan jasa apa atau barang apa yang diberdagangkan, tetap mengacu kepada di dalam undang implementasi SKB tadi, yang disebut dengan konsumen tadi tetap mengacu kepada undang-undang perlindungan konsumen Jadi, kadang-kadang di situ kita nggak bisa lepas dari situ kalau terkait dengan kerjasama ini tidak perlu kita buktikan kita mengacau kepada undang-undang perlindungan konsumen tadi.

10. Apa yang menjadi titik berat dalam melaksanakan Pasal 29 UU ITE, mengingat ini merupakan delik umum bukan delik aduan ?

Kalau pasal 29 yang secara umum di dalam implementasi itu kan disebutkan harus orang yang diadukan pada pasal 29 ini kan pengancaman secara umum karena itu kan bukan secara pribadi, pengancaman itu kan dijelaskan disitu harus ada perubahan ini juga, apakah namanya, walaupun mungkin tidak menimbulkan kerugian materialnya, tapi kan pembuktian kita juga harus ada kerugian inmaterialnya apakah perubahan pilihan berlaku, ada ketakutan masyarakat atau apa namanya itu pengaruh yang membuat masyarakat itu merasa terganggu antar golongan lebih kepada intinya, masalah yang merasa ter dan merasa terancam yang membuat pengaduan kalau dia kan sebuah pengancaman secara pribadi nah makanya titik baratnya. SKB itu tercantum titik beratnya di dalam pasal 29 pada delik umum bukan delik aduan

jadi siapapun bisa melaporkan seperti ada satu tokoh masyarakat bukan pelapor yang melaporkan bukan yang dirugikan yang melaporkan tapi adalah masyarakat, Seperti banyak kasus yang terjadi di Pemilu. Ini banyak berita-berita hoax. Mereka yang tergolong yang melaporkan misalnya calon presiden contohnya. Implementasinya bagaimana melaksanakan apakah ini benar atau tidak, apakah ini merupakan materi antar golongan atau tidak. Karena melihat kalau di postingan, banyak sekali berkaitan dengan pemilu, agama, isu sarah, itu rawan sekali di tengah-tengah masyarakat.

Itu bagaimana cara perlaksanaan implementasi. yang selama ini kita menangani penerapan pasal 29 itu kan tetap mengacu kepada adanya korban ya kan? Kalau itu kan pengancaman secara pribadi kan? Yang itu tadi kita buktikan dulu, pengancamannya itu Ya memang dia bisa saja pengancaman itu dipublikasi, bisa saja dia tertuju melalui pesan SMS, melalui direct messagin dari aplikasi-aplikasi media sosial, bisa saja.

11. Apakah Pasal 31 UU ITE dapat dilakukan Interprensi atau penyadapan secara diam-diam ? lalu bagaimana Subdirektorat V POLDASU melaksanakan Implementasi agar tidak melanggar Ayat 1 dan Ayat 2 !

Selama ini kita belum yang menangani kasus-kasus tentang penyadapan ini belum ada dan kita sendiri pun tidak ada yang melakukan penyadapan kalau sadap-menyadap ini kan ijin dari pengadilan jadi untuk folder saya sendiri terkait dengan katakanlah seperti yang di sadap yang bapak tanya kan tadi itu belum kita tangani, yang kita butuhkan itu adalah karena alat bukti yang kita butuhkan itu biasanya adalah sesuatu yang sudah jadi, yang sudah terposting kita tinggal mengambil dari itu saja, tinggal media-media sosial itu atau akun-akun yang dipergunakan itu dan apabila masyarakat itu merasa WA atau nomor HP-nya di sadap itu bagaimana Pak? karena belum ada kasus sampai saat ini jadi bagaimana menyikapi kasus itu? dalam pelaksanaannya.

Nah masyarakat itu sebagai pengguna mereka itu juga membaca apa yang menjadi *term of condition* dari setiap akun-akun atau aplikasi yang mereka pergunakan seperti whatsapp itu ada batas waktu apabila kita ambil alih oleh orang ada batas waktu supaya bisa kita ambil alih lagi dan syaratnya kan

cuma satu nomor yang kita gunakan untuk mendaftarkan whatsapp itu harus benar-benar nomor yang kita pakai dan aktif. Nah pada saat kita menggunakan whatsapp nomornya kita tidak tahu di mana lagi atau nomor SIM-nya.

Hanya kita pergunakan itu sebenarnya tidak kita gunakan. Nomor itu tidak aktif lagi dari *provider* tetapi di *WhatsApp* dia masih bisa dipergunakan. Gak ada caranya lagi kita mau mengambil gambar ini kembali Nah karena itu ya kalau kita mau menggunakan whatsapp, benar-benar whatsapp pribadi ya pergunakanlah nomor yang benar-benar milik kita yang kita pergunakan Nah itu, kalau terkait dengan akun-akun yang lain juga ada juga pengambilan ya, pengambilan lihat akun-akun seperti itu, seperti Facebook maupun Instagram itu juga kendala kita adalah karena ini kan perusahaan-perusahaan yang berada di luar negeri dan mereka juga punya kebijakan-kebijakan tersendiri, karena di Pasal 31 Ayat 1 dan 2 itu ada beberapa aspek pasal, kepolisian berhak di ayat 2, Kepolisian berhak menyadap apabila terjadi pengancaman. Yang mendapat melakukan penyelidikan itu kan hanya perhatian dari penegak hukum kalau terkait yang bapak bilang tadi kadang-kadang penyelidikan dari polisi kan ada masukannya, penyamaran dalam langkah itu sepanjang itu memiliki izin perbuatan yang dilakukan oleh apapun yang ada masalah tidak terpisahkan melanggar itu tapi kadang-kadang ada yang untuk kepentingan pribadi tidak mendapatkan izin.

Ada yang membuat laporan polisi katanya punya saya dihack, punya saya diambil alih ..., setelah kita lihat udah ternyata bukan dihack, kenapa? Udah, dia itu memberikan kode OTP-nya kepada orang lain, kemudian orang ini mengambil, menggunakan mudah, kalau kita masuk ke pasar 31 bisa ke pasar 35 pun bisa manipulasi data jadi contohnya yang biasa kita datang dan sering yang terjadi kita tangani di sini adalah si A menyatakan akun saya, facebook saya dihack oleh orang tapi dia masih bisa mengakses di perangkat HP-nya karena Facebook contohnya bisa di PC bisa, di laptop bisa, di handphone bisa, sekali buka atau malah buka dia masih bisa mengakses disini tapi dia bilang sudah di orang-orang jadi waktu dia buat LP kita dalamin ternyata ada pihak lain yang membuat akun Facebook seolah-olah milik dia makanya pasalnya itu bisa ke 35 bukan ke 31 kalau dia ke 31 itu memang betul-

betul sama sekali tidak bisa diakses Nah kayak Bapak bilang tadi, aku nutup Menurut dia, itu di-hack Tapi setelah kita tanyakan kembali kita sedikit lebih dalam dia masih bisa mengakses dengan perangkat yang lain, terkadang masyarakat sendiri lalai dia memberikan nomor HP-nya, contohnya tadi *provider* SIM *card* tadi pergunakanlah yang memang registrasinya atas nama kita sehingga kalau kita buka youtube nya pakai itu, emailnya apa segala macam kemudian email masuk ke nomor SIM card tadi nah ini udah SIM cardnya bukan atas nama dia terjadi hal yang tidak diinginkan dia lalu mengaku kemari saya punya saya dihack pak ternyata begitu kita tanya registrasi ini pakai apa? OTP-nya ke HP nomor berapa? Nggak, registrasinya dulu atas nama siapa? Udah ternyata atas nama pihak lain tapi dia mengaku di-hack karena kelalaian dia berarti intinya kesadaran masyarakat masih kurang bahkan banyak kita temukan itu mungkin Bapak sendiri registrasinya atas nama siapa?, nama Bapak sendiri kan Paket handphone Bapak yang biasanya kan pakai apa?.

Kalau bapak beli kartu paket data yang sudah terregistrasi pak tau itu salah, tapi bapak beli tapi kalau bapak sadar itu tidak benar pasti gak mau bapak beli Contoh saya SIM card saya, telekomsel ini paket telepon, ini paket data semuanya disini, satu nomor gak pernah saya pake beli yang sudah teregistrasi ini apa gak saya berpikir loh, berarti saya mengajari yang salah kembali ke kepadanya masyarakatnya sendiri nanti ini dibilang punya saya dihack pak tapi pada saat dia buka akun youtube nya tadi atas nama dia email dia tapi ga sadar dia udah kalo kode otp nya verifikasinya masuk ke nombor handphone yang tidak terregistrasi atas nama dia jadi pak, mayoritas seperti itu rata-rata. Masih kurangya kesadarn masyarakat.

12. Apakah Pasal 27, 28, 29, dan 31 UU ITE dapat memberikan defenisi replik atas kejahatan Dunia Maya ?

Kalau kejahatan ITE, setiap tahun, kalau kita lihat dari jumlah laporan pengaduan masyarakat setiap tahun pasti meningkat tidak pernah menurun namanya kejahatan, tetap meningkat jadi tinggal kembali kepada masyarakatnya kadang-kadang lebih banyak ketidak mengertian masyarakat dalam hal menggunakan media elektronik dan sangat banyak karena kejahatan di media sosial pasal 27 ayat 3 ini kan setiap orang yang merasa tercemar nama

baiknya itu langsung melapor padahal ya itu memang pribadinya secara subjektif dia sebagai korban tapi kan penyelidik juga harus membuktikan secara subjektif. pasal 28 ayat 1 ini melihat apa modusnya dulu mungkin, baru hanya postingan-postingan produk-produk mengenai *marketplace* mungkin baru seperti itu tapi berkembang dia berkembang, menjual barang murah, Ada lagi Online Love Scam lyang berpura-pura sebagai pacar Jalanan keadaan Jadi makin berkembang sehingga aplikasi-aplikasi yang di *download* bisa mengambil data maupun *Malware* Jadi kalau berkurang sih tidak. Semakin lama semakin meningkat kemudian kalau kita lihat juga sebenarnya itu penipuan lainnya sebenarnya bisa kita sampaikan itu seperti gunung es yang melapor ke kita itu sebenarnya di pucuknya saja yang terlihat beberapa orang, tapi korban yang sebenarnya itu sangat banyak.

13. Dalam Kebijakan Publik perlu dilakukan evaluasi kembali, apakah menurut Bapak diperlukan Revisi keseluruhan UU ITE untuk menjawab tantangan kedepan ?

    Jika hal ini perlu untuk di evaluasi maka lebih baik UU ITE ditinjau kembali.

LAMPIRAN II

Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (kominfo.go.id).

No	Pasal	Ayat	Penambahan/Perubahan
1.	1	Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.	Di antara angka 6 dan angka 7 Pasal 1 disisipkan 1 (satu) angka, yakni angka 6a Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola dan/ atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.
2.	5	Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya tersebut merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik tidak berlaku untuk:	Ketentuan Pasal 5 tetap dengan perubahan penjelasan ayat (1) dan ayat (2) sehingga penjelasan Pasal 5 menjadi sebagaimana ditetapkan dalam penjelasan pasal demi pasal Undang-Undang ini.

		Surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis. Surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.	
3.	26	Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang harus mendapat persetujuan dari yang bersangkutan. (2) Setiap Orang yang haknya dilanggar sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini..	Ketentuan Pasal 26 ditambah 3 (tiga) ayat, yakni ayat (3), ayat (4), dan ayat (5) sehingga Pasal 26. Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan. Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/ atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan. Ketentuan mengenai tata. cara penghapusan Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (41 diatur dalam peraturan pemerintah.
4.	27	Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik	Ketentuan Pasal 27 tetap dengan perubahan penjelasan ayat (1), ayat (3), dan ayat (4).

		dan/atau Dokumen Elektronik yang memiliki muatan perjudian. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.	
5.	31	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. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan,	Ketentuan ayat (3) dan ayat (4) Pasal 31 diubah; "Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan institusi kewenangannya ditetapkan berdasarkan Undang-Undang.

		dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. 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. Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.	
6.	40	Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan. Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan. Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi. Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya	Di antara ayat (2) dan ayat (3) Pasal 40 disisipkan 2 (dua) ayat, yakni ayat (2a) dan ayat (2b); ketentuan ayat (6) Pasal 40 diubah; serta penjelasan ayat (1) Pasal 40 diubah. Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturang perunga-undangan. Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik yang memiliki mutan yang melanggar hukum.

		serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data. Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya. Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.	
7.	43	Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik. Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan	Ketentuan ayat (2), ayat (3), ayat (5), ayat (6), ayat (7), dan ayat (8) Pasal 43 diubah; diantara ayat (7) dan ayat (8) Pasal 43 disisipkan 1 (satu) ayat, yakni ayat (7a); serta penjelasan ayat (1) Pasal 43 diubah. Penyidikan dibidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan. Penggeledahan dan/ atau penyitaan terhadap system elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana. Penyidik pegawai negeri sipil sebagaimana dimaksud pada ayat (1) berwenang; Menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Memanggil setiap orang atau pihak lainnya untuk didengar dan diperiksa

		ketentuan Peraturan Perundang-undangan. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat. Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum. Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang: menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini; memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini; melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini; melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini; melakukan pemeriksaan terhadap alat dan/atau sarana	sebagai tersangka atau saksi sehubungan dengan adanya dugaan dinda pidana di bidang Teknologi Informasi dan transaksi elektronik: Melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Melakukan pemeriksaan terhadap orang dan/ atau badan usaha yang patut diduga melakukan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Melakukan pemeriksaan terhadap alat dan/ atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga untuk melakukan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Melakukan penyegelan dan penyitaan terhadap alat/ atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundang-undangan; Membuat suatu data dan/ atau system elektronik yang terkait tindak pidana di bidang Teknologi Informasi dan transaksi elektronik agar tidak dapat diakses; Meminta informasi yang terdapat di dalam system elektronik atau informasi yang dihasilkan oleh system elektronik kepada penyelenggara system elektronik yang terkait dengan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik; Meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi dan transaksi elektronik; dan/ tahu.

		yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini; melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang- Undang ini; melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan; meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku. Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam. Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan	Mengadakan penghentian penyidikan tindak pidana di bidang Teknologi Informasi dan transaksi elektronik sesuai dengan ketentuan hukum acara pidana. Penangkapan dan penahanan terhadap pelaku tindak pidana di bidang Teknologi Informasi dan transaksi elektronik dilakukan sesuai dengan ketentuan hukum acara pidana. Penyidik pejabat pegawai negeri sipil sebagaimana dimaksud pada ayat (1) melaksanakan tugasnya memberitahukan dimulainya penyidikan kepada penuntut umum melalui penyidik pejabat polisi negara republic Indonesia. Dalam hal Pendidikan sudah selesai, penyidik pejabat negeri sipil sebagaimana dimaksud pada ayat satu menyampaikan hasil penyidikan kepada penuntut umum melalui penyidik pejabat polisi negara republic Indonesia. Dalam rangka mengungkap tindak pidana informasi elektronik dan transaksi elektronik, penyidik dapat bekerjasama dengan penyidik negara lain untuk berbagi informasi dan alat bukti sesuai dengan ketentuan peraturan perundang-undangan.

		menyampaikan hasilnya kepada penuntut umum. Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.	
8.	45	Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 2.000.000.000,00 (Dua miliyar Rupiah).	Ketentuan pasal 45 diubah serta diantara pasal empat lima dan pasal 46 disisipkan 2 (dua) pasal, yakni pasal 45A dan pasal 45B.

LAMPIRAN III

Pedoman Implementasi Atas Pasal Tertentu Dalam Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomo 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Surat Keputusan Bersama (SKB) (kominfo.go.id).

NO	UU ITE	PEDOMAN IMPLEMENTASI
1.	Pasal 27 ayat (1) Setiap Orang dengan sengaja dan tanpak hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Eleketronik dan/atua Dokumen Elektronik yang memiliki muatan yang melangga kesusilaan.	Pasal 27 ayat (1) Makna frasa "muatan melanggar kesusilaan" dalam arti sempit dimaknai sebagai muatan (konten) pornografi yang diatur dalam Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan/atau delik yang berkaitan dengan kesusilaan sebagaimana diatur dalam Pasal 281 dan 282 KUHP. "Muatan melanggar kesusilaan" dalam arti luas dapat diartikan sebagai muatan (konten) yang berisi sesuatu hal yang oleh masyarakat dianggap melanggar aturan social yang disepakati dalam sebuah masyarakat, dimana aturan tersebut dapat tertulis dan telah disepakati sejak lama. Tidak semua pornografi atau ketelanjangan itu melanggar kesusilaan. Harus dilihat konteks social budaya dan tujuan muatan itu. Contoh: dalam Pendidikan kedokteran tentang anatomi, gambar ketelanjangan yang dikirimkan seorang pengajarkepada anak didik dalam konteks keperluan kuliah, bukanlah melanggar kesusilaan. Jadi harus dilihat dari tujuan dan konteksnya. Konten melanggar kesusilaan yang ditransmisikan dan/atau didistribusikan atau disebarkan dapat dilakukan dengan cara mengirim tunggal ke Orang perseorangan maupun kepada

		banyak Orang (dibagikan, disiarkan, diunggah, atau diposting). Fokus pernuatan yang dilarang pada pasal ini adalah pada perbuatan mentransmisikan, mendistribusikan dan/atau membuat dapat diaksesnya Informasi Eletronik dan/atau Dokumen Elektronik bermatan melanggar kesusilaan, dan bukan pada perbuatan kesusilaannya itu sendiri. Disebut melakukan pernuatan "membuat dapat diaksesnya", jika pelaku sengaja membuat publik bisa melihat, menyimpan ataupun mengirimkan Kembali konten melanggar kesusilaan tersebut. Contoh pernuatan membuat dapat diaksesnya ini adalah mengunggah konten dalam status media social, *tweet, retweet,* membalas komentar, termasuk perbuatan membuka ulang akses *link* atau konten bermuatan kesusilaan yang telah diputus aksesnya berdasarkan peraturan perundnag-undangan, tetapi dibuka Kembali oleh pelaku sehingga menjadi dapat diakses oleh orang banyak. Jadi perbuatan "membuat dapat diaksesnya" adalah perbuatan aktif yang sengaja dilakukan oleh pelaku.
2.	Pasal 27 ayat (2) "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian."	Pasal 27 ayat (2) Titik berat penerapan Pasal 27 ayat (2) UU ITE adalah pada perbuatan seseorang "mentransmisikan, "mendistribusikan", dan "mebuat dapat diaksesnya" secara Elektronik konten (muatan) perjudian yang dilarang atau tidak memiliki izin berdasarkan peraturan perundang-undangan. Jenis konten (Informasi Elektronik/Dokumen Elektronik) perjudian dapat berupa aplikasi, akun, iklan, situs, dan/atau system *billing* operator bandar. Betuk Informasi Elektronik yang memiliki muatan perjudian yang didistribusikan, ditransmisikan

		dan/atua dapat diakses bisa berupa Gambar, Video, suara, dan/atau tulisan. Penyebaran konten perjudian dapat berbentuk transnisi dari suatu perangkat ke perangkat lain, diistribusi atau menyebarkan dari suatu perangkat/pengguna ke banyak perangkat/pengguna.
3	Pasal 27 ayat (3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.	Pasal 27 ayat (3) Sesuai dasar pertimbangan dalam putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008 Tahun 2008, dan Penjelasan Pasal 27 ayat (3) UU ITE, pengertian muatan penghinaan dan/atau pencemaran nama baik merujuk dan tidak bisa dilepaskan dari ketentuan Pasal 310 dan Pasal 311 KUHP. Pasal 310 KUHP merupakan delik menyerang kehormatan seseorang dengan menuduhkan sesuatu hal agar diketahui umum. Sedangkan Pasal 311 KUHP berkaitan dengan perbuatan menuduh seseorang yang tuduhannya diketahui tidak benar oleh pelaku. Dengan pertimbangan Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008 Tahun 2008 tersebut maka dapat disimpulkan, bukan sebuah delik pidana yang melanggar Pasal 27 ayat (3) UU ITE, jika muatan atua konten yang ditransmisikan, didistribusikan, dan/atau dibuat dapat diaksesnya tersebut adalah berupa penghinaan yang katagorinya cacian, ejekan, dan/atau kata-kata tidak pantas. Untuk perbuatan yang demikian dapat menggunakan kualifikasi delik penghinaan ringan sebagaimana dimaksud Pasal 315 KUHP yang murut penjelasan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 dan Putusan Makahmah Konstitusi, tidak termaksuk acuan dalam Pasal 27 ayat (3) UU ITE. Bukan delik yang berkaitan dengan muatan penghinaan dan/atau

		pencemaran nama baik dalam 27 ayat (3) UU ITE, jika muatan atau konten yang ditransmisikan, didistribusikan, dan/atau dibuat dapat diaksesnya tersebut adalah berupa penilain, pendapatan, hasil evaluasi atau sebuah kenyataan. Dalam hal fakta yang dituduhkan merupakan perbuatan yang sedang dalam proses Hukum maka fakta tersebut harus dibuktikan terlebih dahulu kebenarannya sebelum Aparat Penegak Hukum memproses pengaduan atas delik penghinaan dan/atau pencemaran nama baik UU ITE. Delik pidana Pasal 27 ayat (3) UU ITE adalah delik aduan absolut sebagaimana dimaksud dalam ketentuan Pasal 45 ayat (5) UU ITE. Sebagai delik aduan absolut, maka harus korban sendiri yang mengadukan kepada Aparat Penegak Hukum, kecuali dalam hal korban masih di bawah umur atau dalam perwalian. Korban sebagai pelapor harus Orang perseorangan dengan indentitas spesifik, dan bukan institusi, korporasi, profesi atau jabatan. Fokus pemidanaan Pasal 27 ayat (3) UU ITE bukan dititikberatkan pada perasaan korban, melainkan pada perbuatan pelaku yang dilakukan secara sengaja (*dolus*) dengan maksud mendistribusikan/membuat dapat diaksesnya informasi yang muatannya meyerang kehormatan seseorang dengan menuduhkan sesuatu hal supaya diketahui umum (Pasal 310 KUHP). Unsur "supaya diketahui umum" (dalam konteks transmisi, distribusi, dan/atau membuat dapat diakses) sebagimana harus dipenuhi dalam unsur pokok (*klacht delict*) Pasal 310 dan Pasal 311 KUHP yang menjadi rujukan Pasal 27 ayat (3) UU ITE yang harus terpenuhi.

		Kriteria "supaya diketahui umum" dapat dipersamakan dengan "agar diketahui publik". Umum atau Publik sendiri dimakanai sebagai kumpulan Orang banyak yang sebagaian besar tidak saling mengenal. Kriteria "diketahui umum" bisa berupa unggahan pada akun sosial media dengan pengaturan bisa diakses publik, unggahan konten atau mensyiarkan sesuatu pada aplikasi grup terbuka dimana siapapun bisa bergabung dalam grup percakapan, serta lalu lintas isi atau informasi tidak ada yang mengendalikan, siapapun bisa *upload* dan berbagi (*share*) keluar, atau dengan kata lain tanpa adanya moderasi tertentu (*open group*). Bukan merupakan delik penghinaan dan/atau pencemaran nama baik dalam hal konten disebarkan melalui sarana grup percakapan yang bersifat tertutup atau terbatas, seperti grup prcakapan keluarga, kelompok akrab, grup kelompok profesi, grup Kantor, grup kampus atau instansi Pendidikan. Untuk memberitakan di Internet yang dilakukan institusi pers, yang merupakan kerja jurnalistik yang sesuai dengan ketentuan Undang-Undang Nomo 40 Tahun 1999 tentang Pres sebagai *lex specialis,* bukan Pasal 27 ayat (3). Untuk kasus terkait Pres perlu melibatkan Dewan Pres. Tetapi jika wartawan secara pribadi mengunggah di media sosial atau Internet, maka tetap berlaku UU ITE termasuk Pasal 27 ayat (3).
4.	Pasal 27 ayat (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan atau pengecaman.	Pasal 27 ayat (4) Titik berat penerapan 27 ayat (4) UU ITE adalah pada perbuatan "mentransmisikan, "mendistribusikan, dan "membuat dapat diaksesnya", secara elektronik konten (muatan) pemerasan dan/ atau pengecaman yang dilakukan oleh seseorang ataupun organisasi atau badan hukum.

		Perbuatan pemerasan sebagaimana dimaksud pasal 27 ayat (4) UU ITE berupa pemaksaan dengan tujuan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Isinya memaksa seseorang, keluarga dan/ atau kelompok orang, dengan kekerasan atau ancaman kekerasan untuk memberikan sesuatu barang, supaya membuat utang atau menghapuskan piutang, yang seluruhnya atau Sebagian adalah kepunyaan orang tersebut. Termasuk dalam perbuatan pidana pasal 27 ayat (4) UU ITE perbuatan mengancam akan membuka rahasia, mengancam menyebarkan data pribadi, foto pribadi, dan/atau video pribadi. Pengecaman dan/atau pemerasan dapat disampaikan secara terbuka maupun tertutup. Dalam melakukan perbuatan pemerasan dan/atau pengecaman, harus dibuktikan adanya motif keuntungan ekonomis yang dilakukan oleh pelaku. Norma pidana pasal 27 ayat (4) UU ITE mengacu pada norma pidana pasal 368 KUHP.
5	Pasal 28 ayat (1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.	Pasal 28 ayat (1) Pidana dalam pasal 28 ayat (1) UU ITE Ini bukan merupakan delik pemi dan Naan terhadap perbuatan menyebarkan berita bohong (*Hoaks*) secara umum, melainkan perbuatan menyebarkan berita bohong dalam konteks transaksi elektronik seperti transaksi perdagangan Daring. Berita atau informasi bohong dikirimkan atau diunggah melalui layanan aplikasi pesan, penyiaran Daring, situs/media social, Loka pasar (*market place*), iklan, dan/atau layanan transaksi lainnya melalui system elektronik. Bentuk transaksi elektronik bisa berupa perikatan antara pelaku usaha/penjual dengan konsumen atau pembeli.

		Pasal 28 ayat (1) UU ITE tidak dapat dikenakan kepada pihak yang melakukan Wanprestasi dan atau mengalami *force majeur*. Pasal 28 ayat (1) UU ITE merupakan delik materil, sehingga kerugian konsumen sebagai akibat berita bohong harus dhitung dan ditentukan nilainya. Definisi "konsumen" pada Pasal 28 ayat (1) UU ITE tujuh pada Undang-Undang Nomor 8 Tahun 1999 tentang perlindungan konsumen.
6.	Pasal 28 ayat (2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).	Pasal 28 ayat (2) Delik utama Pasal 28 ayat (2) UU ITE adalah perbuatan menyebarkan informasi yang menimbulkan rasa kebencian atau permusuhan terhadap individua tau kelompok masyarakat berdasar suku, agama, ras, dan antargolongan (SARA). Bentuk informasi yang disebarkan bisa berupa gambar, video, suara, atau tulisan yang bermakna mengajak, atau mensyiarkan pada orang lain agar ikut rasa kebencian dan/atau permusuhan terhadap individu atau kelompok masyarakat berdasarkan isu sentimen atas SARA. Kriteria "menyebarkan" dapat dipersamakan dengan agar "diketahui umum" bisa berupa Unggahan pada akun media social dengan pengaturan bisa diakses publik, atau mensyiarkan sesuatu pada aplikasi grup percakapan dengan sifat terbuka di mana siapa pun bisa bergabung dalam grup percakapan, lalu lintas isi atau informasi tidak ada yang mengendalikan, siapapun bisa *upload* dan berbagi (*share*) keluar, atau dengan kata lain tanpa adanya moderasi tertentu (open *group*). Perbuatan yang dilarang dalam pasal ini motifnya membangkitkan rasa kebencian dan/atau permusuhan atas dasar SARA. Aparat penegak hukum harus membuktikan motif membangkitkan yang ditandai dengan

		adanya konten mengajak, mempengaruhi, menggerakkan masyarakat, menghasut/mengadu domba dengan tujuan menimbulkan kebencian, dan/atau permusuhan. Frasa "antargolongan" adalah entitas golongan rakyat di luar suku, agama dan ras sebagaimana pengertian antar golongan mengacu putusan mahkamah konstitusi Nomor 76/PUU-XV/2017. Penyampaian pendapat, pernyataan tidak setuju atau tidak suka pada individual tau kelompok masyarakat tidak ter maksud perbuatan yang dilarang, kecuali yang disebarkan itu dapat dibuktikan ada upaya melakukan ajakan, mempengaruhi, dan/atau menggerakkan masyarakat, menghasut/mengadu domba untuk menimbulkan rasa kebencian atau permusuhan berdasarkan isu sentiment perbedaan SARA.
8.	Pasal 36 Setiap orang dengan sengaja dan tanpa haka tau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain.	Pasal 36 Pasal 36 UU ITE Dapat digunakan dalam hal korban kejahatan yang melanggar pasal 27 samapai dengan Pasal 34 UU ITE mengalami kerugian materil yang nyata. Kerugian tersebut hanya untuk kerugian langsung atas perbuatan yang dilakukan, bukan kerugian tidak langsung, bukan berupa potensi kerugian, dan bukan pula kerugian yang bersifat nonmaterial. Kerugian materil tersebut terjadi pada korban, baik korban orang perseorangan ataupun badan hukum. Sebagai delik materil maka kerugian tersebut harus dihitung.ditentukan di lainnya. Nilai kerugian materil merujuk pada peraturan mahkamah Agung Nomor 2 Tahun 2012 tentang penyesuaian Batasan tindak pidana ringan dan jumlah denda dalam KUHP lebih dari Rp2.500.000.- (dua juta lima ratus ribu rupiah).

7.	Pasal 29 Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau Dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditunjukkan secara pribadi.	Pasal 29 Pasal 29 UU ITE dititikberatkan pada perbuatan pengiriman informasi berisi ancaman kekerasan atau menakut-nakuti melalui sarana elektronik yang ditujukan secara pribadi. Pengancaman dapat berbentuk pesan, surat elektronik, gambar, suara, video, tulisan, dan/atau bentuk informasi elektronik dan/atau dokumen elektronik lainnya. Bentuk informasi elektronik dan atau dokumen elektronik yang dikirim berupa ancaman kekerasan, yaitu menyatakan atau menunjukkan niat untuk mencelakakan korban dengan melakukan kekerasan secara fisik maupun psikis. Ancaman tersebut berpotensi untuk diwujudkan, meskipun hanya dikirimkan 1 (satu) kali. Sasaran atau korbannya harus spesifik, ditujukan kepada pribadi atau mengancam jiwa manusia, bukan mengancam akan merusak bangunan atau harta benda. Ketakutan dapat terjadi kepada pribadi, kelompok, keluarga maupun golongan. Dampak ketakutan harus dibuktikan secara nyata antara lain adanya perbuatan perilaku. Harus ada saksi untuk menunjukkan adanya fakta bahwa korban mengalami ketakutan atau tekanan psikis. Pasal 29 UU ITE merupakan delik umum, dan bukan delik aduan. Bukan harus korban sendiri yang melapor.

LAMPIRAN IV

TANDAR OPERASIONAL PROSEDUR (SOP) TENTANG PENANGANAN KEJAHATAN DUNIA MAYA ATAU "CYBER CRIME

BAB I
PENDAHULUAN

A. Umum

1. Undang-undang Kepolisian Negara Republik Indonesia Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia mengamanatkan bahwa tugas pokok Polri yaitu memelihara kamtibmas, melayani, mengayomi dan melindungi masyarakat, serta melakukan penegakan hukum secara demokratis dan menjunjung tinggi prinsip hak asasi manusia;
2. Dimensi tugas kepolisian tidak terlepas dari pengaruh kemajuan atau perkembangan ilmu pengetahuan dan teknologi. Di satu sisi, kemajuan iptek telah membawa hal yang positif bagi kehidupan masyarakat, di sisi lain telah membawa dampak negatif berupa munculnya gangguan Kamtibmas yang berpengaruh pada bentuk dan modus operandi kejahatan yang semakin kompleks;
3. Salah satu kejahatan itu adalah kejahatan di dunia maya yang disebut *"cybercrime"* yang sangat kompleks, ditandai dengan kompleksitas waktu dan tempat pergerakan, tanpa perbatasan *(borderless),* mobilitas tinggi, tidak kenal batas wilayah / negara, pelaku lebih dari satu orang, dan bekerja secara terorganisir;
4. Untuk menjamin terselenggaranya proses penegakan hukum dan pemberantasan kejahatan di dunia maya / *cyber crime* dengan berpedoman pada asas legalitas, asas proporsionalitas, asas akuntabilitas, asas transparansi, serta efektivitas dan efisiensi waktu penyidikan, perlu menetapkan standar operasional prosedur (SOP);
5. Sesuai dengan tuntutan perkembangan masyarakat dan aturan hukum, standar operasional prosedur (SOP) penegakan hukum dan pemberantasan kejahatan di dunia maya/ *cyber crime* ini tidak tertutup untuk terus disempurnakan menurut cara yang berlaku di lingkungan Direktorat Reserse Kriminal Khusus Polda Sumut.

B. Dasar

1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
2. Undang-undang Nomor 23 Tahun 2002 tentang Perlindungan Anak;
3. Undang-undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik perkara Tindak Pidana (Mutual Legal Assistance- MLA);
4. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
5. Undang-undang Nomor 44 Tahun 2008 tentang Pornografi;
6. Undang-undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165, Tambahan Lembaran Negara Republik Indonesia Nomor 3886);
7. Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 4168);
8. Peraturan Pemerintah Nomor 27 Tahun 1983 tentang Pelaksanaan Kitab Undang-Undang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1983 Nomor 36, tambahan Lembaran Negara Nomor 3258);
9. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 12 Tahun 2009 tentang Pengawasan dan Pengendalian Penanganan Perkara Pidana di Lingkungan Kepolisian Negara Republik Indonesia;
10. Peraturan Kapolri No 10 Tahun 2009 tentang Tata Cara dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara dan Laboratoris Kriminalistik Barang Bukti kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia.

C. Maksud dan Tujuan

1. Maksud

   Standar Operasional Prosedur (SOP) ini disusun sebagai pedoman dan acuan bagi para penyidik dalam rangka penanganan dan pemberantasan kejahatan di dunia maya / *cyber crime* di lingkungan Ditreskrimsus Polda Sumut.

2. Tujuan

   Penyusunan Standard Operasional Prosedur (SOP) ini bertujuan untuk menyamakan persepsi dan tindakan dalam rangka penanganan dan pemberantasan kejahatan di dunia maya / *cyber crime* di lingkungan Ditreskrimsus Polda Sumut.

D. Pengertian-pengertian

1. **Informasi elektronik** adalah satu atau sekumpulan data elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu

memahaminya;

2. **Transaksi elektronik** adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan / atau media elektronik lain;
3. **Teknologi informasi** adalah suatu teknologi untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan / atau menyebarkan informasi;
4. **Dokumen elektronik** adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan / atau didengar melalui komputer atau sistem elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, symbol atau perforasi yang memilki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;
5. **Sistem elektronik** adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan / atau menyebarkan informasi elektronik;
6. **Penyelenggaraan sistem elektronik** adalah pemanfaatan sistem elektronik oleh penyelenggara Negara, orang, badan usaha, dan / atau masyarakat;
7. **Jaringan sistem elektronik** adalah terhubungnya dua sistem elektronik atau lebih, yang bersifat tertutup ataupun terbuka;
8. **Komputer** adalah alat untuk memproses data elektronik, magnetic, optic, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan;
9. **Akses** adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan;
7. **Kode akses** adalah angka, huruf, simbol, karakter lain atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses komputer dan / atau sistem elektronik lain;
8. **Kontrak elektronik** adalah perjanjian para pihak yang dibuat melalui sistem elektronik;
9. **Pengirim** adalah subjek hukum yang mengirimkan informasi elektronik dan / atau dokumen elektronik;
10. **Penerima** adalah adalah subjek hukum yang menerima informasi elektronik dan / atau dokumen elektronik;
11. **Nama domain** adalah alamat Internet penyelenggara, negara, orang, badan usaha, dan / atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet;
12. ***Gambling*/perjudian** adalah setiap permainan yang pada umumnya menggantungkan harapan untuk menang pada peruntungan belaka, demikian juga jika harapan itu bertambah karena si pemain lebih terlatih atau lebih terampil.

Termasuk juga dalam pengertian itu semua pertaruhan mengenai hasil perlombaan atau permainan lain yang tidak dilakukan oleh petaruh, dan segala pertaruhan lain;

13. **Dokumen** adalah data, rekaman, atau informasi yang dapat dilihat, dibaca dan / atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di kertas, benda fisik apa pun selain kertas atau yang terekam secara elektronik, tetapi tidak terbatas pada:
    a. tulisan, suara, atau gambar;
    b. peta, rancangan, foto, atau sejenisnya;
    c. huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.
17. **Pengawasan** adalah rangkaian kegiatan dan tindakan pengawas berupa pemantauan proses penyidikan, berikut tindakan koreksi terhadap penyimpangan yang ditemukan dalam rangka penyelesaian proses penyidikan sesuai dengan undang-undang dan peraturan yang berlaku serta menjamin proses pelaksanaan kegiatan penyidikan perkara yang dilakukan secara profesional, proposional dan transparan;
18. **Pengendalian penyidikan** adalah kegiatan pemantauan, pengarahan, bimbingan, dan petunjuk kepada penyidik agar proses penyidikan dapat berjalan lebih lancar dan sesuai dengan target yang ditetapkan serta dilakukan oleh pengawas penyidik;
19. **Pusat Pelaporan dan Analisis Transaksi Keuangan** yang selanjutnya disebut **PPATK** adalah lembaga independen yang, dalam melaksanakan tugas dan kewenanganannya, bertanggung jawab kepada Presiden, berkedudukan di ibu kota negara RI, dan, apabila diperlukan, dapat dibuka perwakilan PPATK di daerah. PPATK dibentuk dalam rangka mencegah dan memberantas tindak pidana pencucian uang;
20. **Surat Perintah Penyelidikan** adalah dokumen sah berdasarkan hukum dan peraturan perundang-undangan yang berlaku, yang diterbitkan oleh suatu instansi resmi dan ditandatangani oleh pejabat yang berwenang memberi perintah dalam rangka melaksanakan atau tidak melaksanakan suatu kegiatan yang dapat dipertanggungjawabkan;
21. **Transaksi keuangan** adalah seluruh kegiatan yang menimbulkan hak atau kewajiban atau menyebabkan timbulnya hubungan hukum antara dua pihak atau lebih, termasuk kegiatan transfer dan / atau pemindahbukuan dana yang dilakukan oleh penyedia jasa keuangan.

E. Ruang lingkup

SOP Penanganan Tindak Pidana *Cyber Crime* meliputi penyelidikan dan penyidikan yang terstruktur dan sistematis untuk menjadi standar pelaksanaan penanganan tindak pidana (TP) kejahatan di dunia maya. Kejahatan di dunia maya atau *cyber crime,* terdiri dari *cyber pornography* atau pornografi *on-line*, *cyber gambling* atau perjudian *on-line, pencemaran nama baik/fitnah melalui media elektronik on-line, hacking/cracking*, pada tingkat Ditreskrimsus Polda Sumut.

F. Tata Urut

BAB I PENDAHULUAN
BAB II TATA CARA PENANGANAN TP DI BIDANG *CYBER CRIME*
BAB III PENGAWASAN DAN PENGENDALIAN
BAB IV KETENTUAN LAIN
BAB V PENUTUP

BAB II

TATA CARA PENANGANAN TP DI BIDANG *CYBER CRIME*

A. Jenis TP *Cyber Pornography* (*Pornografi On-Line*)

1. Memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit memuat:

a. persenggamaan, termasuk persenggamaan yang menyimpang;
b. kekerasan seksual;
c. masturbasi atau onani;
d. ketelanjangan atau tampilan yang mengesankan ketelanjangan;
e. alat kelamin; atau
f. pornografi anak.

2. Menyediakan jasa pornografi yang:
   a. Menyajikan secara eksplisit ketelanjangan atau tampilan yang mengesankan ketelanjangan;
   b. menyajikan secara eksplisit alat kelamin;
   c. mengeksploitasi atau memamerkan aktivitas seksual; atau
   d. menawarkan atau mengiklankan, baik langsung maupun tidak langsung, layanan seksual.
3. Meminjamkan atau mengunduh pornografi;
4. Memperdengarkan, mempertontonkan, memanfaatkan, memiliki, atau menyimpan produk pornografi;
5. Dengan sengaja atau atas persetujuan dirinya menjadi objek atau model yang mengandung muatan pornografi;
6. Menjadikan orang lain sebagai objek atau model yang mengandung muatan pornografi;
7. mempertontonkan diri atau orang lain dalam pertunjukan atau di muka umum yang menggambarkan ketelanjangan, eksploitasi seksual, persenggamaan, atau yang bermuatan pornografi lain;
8. Melibatkan anak dalam kegiatan dan / atau sebagai objek;
9. mengajak, membujuk, memanfaatkan, membiarkan, menyalahgunakan kekuasaan atau memaksa anak dalam menggunakan produk atau jasa pornografi.

B. Modus Operandi dalam TP *Cyber Pornography*

1. Penawaran dan Penjualan CD /DVD porno secara *on-line* :

a. *Website* menggunakan *hosting server* dan IP *Address* diluar negeri agar sulit dilacak;
b. Pemesanan *on-line* melalui *chat* dan alamat surel yahoo, gmail, dan provider telepon seluler M2;
c. Pembayaran pembelian CD/DVD *child porn* melalui transfer bank, ataupun melalui ATM;
d. Pelaku menggunakan identitas KTP palsu untuk pembelian *simcard* seluler dan pembukaan rekening bank;
e. Pengiriman CD/DVD porno dilakukan dengan menggunakan jasa kurir seperti TIKI dengan cara berpindah lokasi perusahaan jasa kurir.

2. Organisasi on-line, perusahaan on-line atau individual yang mengeksploitasi dewasa dan anak secara seksual untuk berbagi file :

a. Menggunakan layanan jejaring sosial yang tersedia di Internet dan memiliki akun seperti facebook, myspace, yahoo messenger, blog, pear to pear Lime Wire, you tube;
b. Login dengan user ID alamat surel register ke yahoo.com, gmail.com dan memasukkan identitas fiktif;
c. Menggunakan IP Proxy;
d. Mengoleksi gambar & film porno baik di *file hardisk, flash disk*, dan *hardisk* Internal, telepon seluler ataupun dalam CD atau DVD;
e. Bekerja di Indonesia secara resmi.

C. Tata cara penyidikan TP *Cyber Pornography*

Penanganan TP ini diawali dengan kegiatan penyelidikan yang dapat dilakukan oleh penyidik dengan memperoleh dari hasil *browsing* penyelidikan *online.* sumber; NCB Interpol, penegak hukum ataupun laporan dari masyarakat. Kemudian, berdasarkan informasi itu, dilakukan penyelidikan *on-line* lebih mendalam untuk mendapatkan bukti permulaan cukup dan dapat ditindaklanjuti untuk membuat laporan polisi sebagaimana prosedur dan mekanisme baik di tingkat pusat (Bareskrim) maupun di tingkat kewilayahan. Cara menemukan tindak pidana *cyber pornography* dapat dibedakan sebagai berikut:

1. TP yang ditemukan berdasarkan laporan

Setelah menerima laporan dari masyarakat yang mengadukan TP *Cyber Pornography*, penyidik:

a. membuat laporan polisi model B;
b. memeriksa bukti yang diajukan oleh pelapor;
c. membuat surat perintah penyelidikan; dan
d. melakukan serangkaian penyelidikan dari data yang diserahkan oleh pelapor;

e. dengan adanya berbagai modus yang dilakukan oleh pelaku TP *Cyber Pornography*, penyidik dapat melakukan beberapa tahap penyelidikan dengan menyiapkan kelengkapan berikut:

1. Aplikasikan metode lidik klasik (konvensional) ke dunia *on-line* :
    a. *Under cover* (penyamaran) *on-line* – siapkan alamat surel, akun, user ID samaran;
    b. *Under cover buy on-line* (pembelian terselubung) – siapkan rekening bank;
    c. Lakukan komunikasi *on-line* melalui *email chat*, surel untuk mendapatkan *header* pelaku;
    d. *Lacak header* guna mengetahui IP Address pelaku;
    e. Gunakan *tools* yang tersedia di Internet untuk mengetahui ISP yang digunakan;
    f. Kumpulkan data pelaku sebanyak mungkin, gunakan *search engine* google, friendster, facebook, yahoo group, dsb;
    g. Setiap melakukan investigasi on-line harus dilakukan screenshot;
    h. Aplikasikan metode lidik klasik (konvensional).
2. Koordinasi dengan *internet service provider* & *provider telepon seluler* & PPATK.

a. Bekerja sama dengan penyidik negara lain berkaitan dengan permintaan data asal *provider* Internet;

b. Memeriksa para saksi yang berkaitan dengan hasil penyelidikan yang dituangkan dalam berita acara yang memenuhi persyaratan formal dan materil. Adapun hal yang dapat ditanyakan kepada saksi/korban:

1. identitas saksi;
2. kapan, di mana, dan bagaimana mengenal tersangka baik di Internet maupun bertemu secara langsung;
3. kapan, di mana, dan bagaimana proses pengambilan gambar porno dan siapa yang menyuruh;
4. berapa korban dibayar;
5. siapa saja korban lain; dan
6. nama situs di Internet tempat gambar porno korban dipertontonkan;
7. Penggeledahan dan penyitaan alat bukti dalam TP *cyber porno* sebagaimana dimaksud dalam ketentuan perundang-undangan; dan objek yang terkait dalam TP *cyber porno* harus dilakukan atas izin ketua pengadilan setempat, sesuai dengan pasal 43 (3) Undang-undang Nomor 11 Tahun 2008 tentang ITE;
8. Alat bukti lain berupa informasi elektronik dan / atau dokumen elektronik yang diperlukan dalam penyidikan antara lain yang berikut:

1. Barang bukti digital:

a) PDA, *cradle*, dan *charger*;

b) Media Penyimpanan data seperti *hardisk* (PC dan laptop), *floppy disk*, ZipDisk;

c) Pita back-up (berbagai macam pita rekaman);
d) Alat penyimpanan data lain;
e) Berbagai alat lain USB, telepon genggam.
2. Alat lain yang harus disita:
a) CD dan DVD porno;
b) kunci komputer;
c) *cradles*; dan
d) majalah porno & peralatan hubungan seksual.
3. Pemeriksaan barang bukti digital di TKP dapat dilakukan secara forensik oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital. Adapun tindakan penanganan barang bukti elektronik di TKP sebagai berikut:

a. Terhadap barang bukti komputer/laptop:

1. Apabila komputer/laptop dalam kondisi tidak nyala (mati), segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya;
2. Apabila komputer/laptop dalam kondisi nyala (hidup), ambil foto terlebih dahulu semua bagian komputer, termasuk layar komputer/laptop, catat tanggal serta waktu saat komputer/laptop itu hidup, dan catat semua program yang sedang berjalan/sedang beroperasi. Setelah mengambil foto dan mencatat, segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya;
3. Matikan sambungan dari akses *remote* (telepon genggam atau modem), pisahkan komputer dari *movie digital camera* (*web camera*);
4. Jika yang ditemukan di TKP adalah laptop yang masih menyala (hidup), ambil foto secara keseluruhan dan catat tanggal serta waktu saat laptop itu hidup dan catat semua program yang sedang berjalan/sedang beroperasi di laptop itu. Setelah itu, tekan *power* laptop selama 30 detik sampai layar di laptop menjadi hitam (dikenal dengan *hard power down*).

b. CD/DVD dan USB *thumb drive/memory card* :
Amankan barang bukti berupa CD/DVD dan USB thumb drive/memory *card*, bungkus dengan kantong barang bukti yang sudah disiapkan untuk diangkut (diperlakukan sama seperti barang pecah belah).

c. Telepon genggam (hand phone) ;
Jika menemukan telepon genggam yang mungkin terkait dengan TP yang sedang ditangani, segera matikan/nonaktifkan telepon genggam, jangan pernah menyita telepon genggam dalam keadaan terus-menerus hidup karena akan mengubah data komunikasi telepon genggam dengan BTS yang dilaluinya. Jika dalam keadaan mendesak dapat mencabut baterai dari telepon genggam itu dan masukkan ke dalam kantong barang bukti yang sudah disiapkan.

d. Selain pemeriksaan secara laboratoris yang dilakukan oleh Subdit II Cyber Crime Ditreskrimsus Polda Sumut, penyidik dapat memeriksakan kepada Laboratorium

Forensik Mabes Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut dengan memenuhi persyaratan formal:

1. permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
2. laporan polisi;
3. BAP saksi/tersangka atau laporan kemajuan; dan
4. BA pengambilan, penyitaan, dan pembungkusan barang bukti.

2. Pemeriksaan barang bukti perangkat komputer wajib memenuhi persyaratan teknis:

1. penanganan barang bukti komputer, yang berkaitan dengan data yang tersimpan dalam *harddisk* atau penyimpanan adat (*storage*) lain, sejak penanganan pertama harus sesuai dengan tata cara yang berlaku karena barang bukti memiliki sifat yang mudah hilang/berubah (*volatile*), dan bila penyidik tidak memahami tata cara penyitaan barang bukti komputer, dapat meminta bantuan Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut;
2. barang bukti dikirimkan secara lengkap dengan seluruh sistemnya;
3. barang bukti dibungkus, diikat, dilak, disegel, dan diberi label; dan
4. pengiriman barang bukti ke Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut tidak dapat melalui pos paket atau kurir (diantar oleh penyidik yang menangani perkara).
5. Tata cara penyitaan barang bukti komputer yang sedang digunakan untuk melakukan kejahatan adalah:

a. mematikan aktivitas komputer dari *server* untuk komputer yang terhubung dengan *network*;

b. mencabut kabel *input* komputer dari sumber arus listrik sebelum komputer di-*shut down* (dimatikan secara kasar), untuk laptop/notebook dicabut pula baterainya.

1. mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
2. mencatat spesifikasi komputer dan peralatan *input/output* (I/O) yang terpasang pada komputer;
3. mencabut semua kabel yang terpasang pada komputer dan I/Onya, masing-masing diberi tanda yang berbeda agar memudahkan pemasangannya kembali;
4. menyita barang bukti lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, *magnetic tape, memory card, flash disk, external harddisk*, dan buku petunjuk;
5. mencatat tanggal dan waktu penyitaan; dan
6. memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

6. Tata cara penyitaan barang bukti komputer yang sudah dimatikan adalah:

1. mencari informasi kapan komputer digunakan tersangka untuk melakukan kejahatannya;
2. mencari keterangan mengenai pengunaan komputer yang dijadikan barang bukti

sesudah digunakan untuk melakukan kejahatan;

3. mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
4. mencatat spesifikasi komputer dan peralatan *input/output* (I/O) yang terpasang pada komputer;
5. mencabut semua kabel yang terpasang pada komputer dan I/Onya, masing-masing Diberi tanda yang berbeda agar memudahkan pemasangannya kembali;
6. menyita barang bukti lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, *magnetic tape, memory card, flash disk, external harddisk*, dan buku petunjuk;
7. mencatat tanggal dan waktu penyitaan; dan
8. memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan;
7. Setelah memeriksa secara menyeluruh barang bukti, penyidik meminta keterangan kepada ahli yang terdiri dari ahli forensik, Depkominfo, dan akademisi;

Adapun hal yang ditanyakan kepada ahli dari Depkominfo atau akademisi:

1. korelasi antara TP yang terjadi dan UU serta peraturan yang berkaitan dengan pornografi di Internet dan keahliannya;
2. jabatan, tugas, dan tanggung jawabnya;
3. penjelasan tentang masalah yang berkaitan dengan pornografi di Internet dengan aturan pada undang-undang yang berlaku; dan
4. pelanggaran apa pun yang terjadi dikaitkan dengan kasus yang sedang dilakukan penyidikan.
5. Hal yang ditanyakan kepada ahli forensik.

a. Korelasi antara TP yang terjadi dan undang-undang serta peraturan yang berkaitan dengan pornografi di Internet dan keahliannya;
b. Jabatan, tugas, dan tanggung jawabnya;
c. Penjelasan tentang masalah yang berkaitan dengan pornografi di Internet dengan aturan pada undang-undang yang berlaku;
d. Dalam pemeriksaan barang bukti yang dilakukan oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut, ditanyakan tata cara dan prosedur permintaan serta penyerahan barang bukti digital; dan
e. Pemeriksaan Laboratorium Digital Forensik dan hasilnya dicatat.
f. Setelah mempunyai alat bukti yang sah dari pemeriksaan laboratoris terhadap barang bukti digital, penyidik melanjutkan penyidikan dengan melengkapi berkas serta melakukan serangkaian penyidikan lain.

D. TP yang ditemukan berdasarkan temuan

Apabila menemukan TP, penyidik melakukan serangkaian penyelidikan:

a. Membuat laporan polisi model A;
b. Membuat surat perintah penyelidikan;
c. Penyidik dapat melakukan beberapa tahap penyelidikan dengan menyiapkan yang

berikut:

1) Aplikasikan metode lidik klasik (konvensional) ke dunia *online* :
    a. *Under cover* (penyamaran) *on-line* – siapkan adres surel, akun, user ID samaran;
    b. *Under cover buy on-line* (pembelian terselubung) – siapkan rekening bank;
    c. Lakukan komunikasi *on-line* melalui *chat*, email untuk mendapatkan *header* pelaku;
    d. Lacak *header* guna mengetahui IP Address pelaku;
    e. Gunakan *tools* yang tersedia di Internet untuk mengetahui ISP yang digunakan;
    f. Kumpulkan data pelaku sebanyak mungkin, gunakan *search engine* google, freindster, facebook, yahoo group, dsb;
    g. Setiap melakukan investigasi on-line harus dilakukan screenshot.
2) Aplikasikan metode lidik klasik (konvensional);
3) Koordinasi dengan *Internet Service Provider* & *Provider telepon seluler* & PPATK.

a. Melakukan kerja sama dengan penyidik negara lain berkaitan dengan permintaan data asal provider Internet;
b. Melakukan pemeriksaan para saksi yang berkaitan dengan hasil penyelidikan;
c. Penggeledahan dan penyitaan alat bukti dalam TP *cyber porno* sebagaimana dimaksud dalam ketentuan perundang-undangan; dan terhadap objek yang terkait dalam TP *cyber porno* harus dilakukan atas izin ketua pengadilan setempat, sesuai dengan pasal 43 (3) Undang-Undang Nomor 11 Tahun 2008 tentang ITE;
d. Alat bukti lain berupa informasi elektronik dan / atau dokumen elektronik yang diperlukan dalam penyidikan adalah yang berikut:

4) Barang bukti digital :

a) PDA, *cradle* dan *charger*;
b) Media Penyimpanan data seperti *hardisk* (PCdan laptop), *floppy disk*, *zip disk*;
c) Pita *back-up* (berbagai macam pita rekaman);
d) Alat penyimpanan data lain;
e) Berbagai alat lain USB, telepon genggam.

5) Alat lain yang harus disita

a) CD dan DVD porno.
b) Kunci komputer.
c) Majalah porno dan peralatan hubungan seksual.

6) Pemeriksaan barang bukti digital di TKP dapat dilakukan secara forensik yang dilakukan oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital. adapun tindakan penanganan barang bukti elektronik di TKP sebagai berikut:

1) Terhadap barang bukti komputer/laptop:

a) Apabila komputer/laptop dalam kondisi tidak nyala (mati), segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya;

b) Apabila komputer/laptop dalam kondisi nyala (hidup), ambil foto terlebih dahulu semua bagian komputer, termasuk layar komputer/laptop dan catat tanggal dan waktu saat komputer/laptop itu hidup dan catat semua program yang sedang berjalan/sedang beroperasi dikomputer/laptop itu. Setelah mengambil foto dan mencatat, segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya;

c) Matikan sambungan dari akses remote (telepon genggam atau modem) pisahkan komputer dari *camera movie digital* (*web camera*);

d) Jika yang ditemukan di TKP adalah laptop yang masih menyala (hidup), ambil foto secara keseluruhan, catat tanggal dan waktu saat laptop itu hidup, dan catat semua program yang sedang berjalan/sedang beroperasi di laptop itu. Setelah itu, tekan *power* laptop selama 30 detik sampai layar di laptop menjadi hitam (dikenal dengan *hard power down*).

2) CD/DVD dan USB *thumb drive*/*memory card* :

Amankan barang bukti berupa CD/DVD dan USB *thumb drive*/ *memory card*, bungkus dengan memakai kantong barang bukti yang sudah disiapkan untuk diangkut (diperlakukan sama dengan barang pecah belah).

3) Telepon genggam (Telepon genggam) :

Jika menemukan telepon genggam yang kemungkinan terkait dengan TP yang sedang ditangani segera matikan/nonaktifkan telepon genggam itu, jangan pernah melakukan penyitaan terhadap telepon genggam dalam keadaan terus menerus hidup karena itu akan merubah data komunikasi telepon genggam dengan BTS yang dilaluinya. Jika dalam keadaan mendesak dapat mencabut baterai dari telepon genggam itu dan masukan ke dalam kantong barang bukti yang sudah disiapkan.

4) Selain pemeriksaan secara laboratoris yang dilakukan oleh Subdit II Cyber Crime, penyidik dapat memeriksakan kepada Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut dengan memenuhi persyaratan formal sebagai berikut:

1. Permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
2. laporan polisi;
3. BAP saksi/tersangka atau laporan kemajuan; dan
4. BA pengambilan, penyitaan dan pembungkusan barang bukti.

5) Pemeriksaan barang bukti perangkat komputer wajib memenuhi persyaratan teknis sebagai berikut:

1. Penanganan barang bukti komputer, yang berkaitan dengan data yang tersimpan dalam harddisk atau penyimpanan adat (*storage*) lain, dari sejak penanganan pertama harus sesuai dengan tata cara yang berlaku, karena barang bukti memiliki

sifat yang mudah hilang/berubah (*volatile*), dan bila penyidik tidak memahami tata cara penyitaan barang bukti komputer, dapat meminta bantuan Labfor Polri;
2. Barang bukti dikirimkan secara lengkap dengan seluruh sistemnya;
3. Barang bukti dibungkus, diikat, dilak, disegel dan diberi label; dan
4. Pengiriman barang bukti ke Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut tidak dapat melalui pos paket atau kurir (diantar oleh penyidik yang menangani perkara).

6) Tata cara penyitaan barang bukti komputer yang sedang digunakan untuk melakukan kejahatan adalah sebagai berikut:

1. Mematikan aktivitas komputer dari server untuk komputer yang terhubung dengan network;
2. Mencabut kabel input komputer dari sumber arus listrik sebelum komputer di shut down (mematikan secara kasar), untuk laptop/notebook dicabut pula baterainya;
3. Mematikan saklar pasokan listrik dan segel sakla itu untuk menghindari menghidupkan tanpa sengaja;
4. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
5. Mencabut semua kabel yang terpasang pada komputer dan I/Onya, masing-masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
6. Menyita barang bukti lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external hard disk*, dan buku petunjuk ;
7. Mencatat tanggal dan waktu penyitaan; dan
8. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

7) Tata cara penyitaan barang bukti komputer yang sudah dimatikan adalah:

1. Mencari informasi kapan komputer digunakan tersangka untuk melakukan kejahatannya;
2. Mencari keterangan mengenai pengunaan komputer yang dijadikan sebagai barang bukti sesudah digunakan untuk melakukan kejahatan; dan
3. Mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
4. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
5. Mencabut semua kabel yang terpasang pada komputer dan I/Onya, masing-masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
6. Menyita barang bukri lain yang ada hubungannya dengan komputer, seperti disket, CD/DVD, *magnetic tape, memory card, flash disk, external harddisk*, dan buku petunjuk;
7. Mencatat tanggal dan waktu penyitaan; dan
8. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

9. Setelah melaksanakan rangkaian pemeriksaan terhadap barang bukti, penyidik meminta keterangan kepada ahli yang terdiri atas ahli forensik, Depkominfo, dan akademisi.

8) Adapun hal-hal yang dipertanyakan terhadap ahli dari Depkominfo atau Akademisi:

1. Korelasi antara TP yang terjadi dengan UU serta peraturan berkaitan dengan pornografi di Internet dan keahliannya;
2. Jabatan, tugas dan tanggung jawabnya;
3. Penjelasan tentang masalah yang berkaitan dengan pornografi diInternet dgn aturan pada UU yg ada;
4. Pelanggaran apa yang terjadi dikaitkan dengan kasus yang sedang dilakukan penyidikan.

9) Hal-hal yang dipertanyakan terhadap ahli forensik:

1. Korelasi antara TP yang terjadi dengan UU serta peraturan berkaitan dengan pornografi di Internet dan keahliannya;
2. Jabatan, tugas dan tanggung jawabnya;
3. Penjelasan tentang masalah yang berkaitan dengan pornografi diInternet dgn aturan pada UU yg ada;
4. Terhadap pemeriksaan barang bukti yang dilakukan oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut, ditanyakan tentang tata cara dan prosedur permintaan dan penyerahan barang bukti digital;
5. Pemeriksaan Laboratorium Digital Forensik dan Hasil lab dibuat secara tertulis.

10) Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain.

E. Tata Cara Penanganan TP Perjudian Melalui Media Elektronik (*Cyber Gambling*)

1. Jenis Perjudian secara *on-line*/Cyber Gambling, Perjudian yang dilakukan saat ini bukan hanya yang konvensional/biasa melainkan sudah melalui media internet. Jenis perjudian yang biasa ditawarkan melalui Internet adalah:

a. SEPAK BOLA;
b. SICBO (Dadu);
c. ROLET (Bola Jalan);
d. BACARRAT (Kartu);
e. MICKEY MOUSE;
f. DLL

2. TP Cyber gambling/perjudian melalui media elektronik biasanya dilakukan dengan modus operandi sebagai berikut:

a. Mem-*posting* suatu tulisan dan atau gambar di *blog*/wesbsite/situs yang menawarkan beberapa permainan yang memiliki muatan perjudian yaitu tiap-tiap permainan mengandung unsur pertaruhan dimana pada umumnya kemungkinan

mendapat untung bergantung pada peruntungan belaka;

b. Menyediakan rekening penampung untuk mempermudah bertransaksi antara pemain dengan Bandar atau agen perjudian.

3. Tata cara penyidikan TP *Cyber* gambling/perjudian secara *on-line*

"Dalam menangani perjudian *on-line* di Internet perlu dilakukan penyelidikan terlebih dahulu, baik adanya informasi ataupun penyidik yang melakukan penyelidikan adanya dugaan permainan judi on-line itu".

a. Penyelidikan yang dilakukan perlu diperhatikan dengan tahapan sebagai berikut:

1. Setelah mendapatkan informasi maupun temuan membuat laporan polisi;
2. Membuat surat perintah penyelidikan;
3. Masuk ke dalam *website* yang menjadi sasaran kegiatan perjudian *on-line*, perlu diketahui dan di perhatikan apabila mulai melakukan lidik dan masuk ke *website* tsb, jangan gunakan fasilitas Internet di kantor atau rumah, tetapi fasilitas umum seperti *hotspot* atau warnet karena pelaku dapat melihat atau melacak kembali siapa saja yang masuk ke dalam *website*, sebagaimana kita dapat mengetahui siapa yang mengatur *website* tsb;
4. Memperhatikan aktivitas yang dilakukan di Internet pada *Server Logs* dimana dimana penyidik dapat menemukan barang bukti atau data yang dibutuhkan dalam melakukan penyelidikan seperti IP pemakai, kapan digunakan, apa yang dilihat, apa data yang di cari dengan menggunakan *search engine* dan *browser* apa yang digunakan;
5. Apa yang terdapat didalam *Server Log* menunjukkan koneksi yang terjadi tidak hanya pengguna tetapi juga pemilik web sites yang dikunjungi, koneksi di log juga dapat menunjukkan materi yang terdapat didalam web, kapan web di perbaharui dan kemana hubungan dilakukan;
6. Setelah melakukan penyelidikan diatas, penyidik segera berkoordinasi dengan ISP (internet service provider), provider selluler dan monitoring center (Bareskrim Polri) untuk meminta data-data log file dan Data Detail record dari target yang akan dilakukan penyelidikan lebih dalam;
7. Permintaan data itu dengan permintaan tertulis yang ditujukan kepada provider-provider yang terkait;
8. Apabila telah mendapatkan hasil dari permintan data itu, penyidik mengambil langkah penyidikan yaitu dengan upaya paksa.
9. Setelah melakukan penyelidikan terhadap dugaan perjudian on-line itu,penyidik perlu melakukan serangkaian langkah sebagai berikut:
10. Membuat perencanaan/taktik dalam melakukan upaya paksa berupa penangkapan, penggeledahan, penyitaan dll.
11. Meminta izin kepada ketua pengadilan negeri setempat sebelum melakukan penggeledahan dan penyitaan terhadap barang bukti yang disita.
    1. Barang bukti yang berupa sistem elektronikyang terkait dengan dugaan TP;
    2. Barang bukti yang dapat disita yang ada kaitannya denga TP itu antara lain; komputer, telepon genggam , laptop dan media elektronik lain;

3. Pemeriksaan barang bukti digital di TKP dapat dilakukan secara forensik yang dilakukan oleh petugas dari Unit Cyber Crime Subdit II Perbankan Ditreskrimsus Polda Sumut dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital, adapun tindakan penanganan barang bukti elektronik di TKP sebagai berikut:

a) Terhadap barang bukti Komputer/Laptop:

a. Apabila komputer/laptop dalam kondisi tidak nyala (mati) segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya.
b. Apabila komputer/laptop dalam kondisi nyala (hidup) ambil foto terlebih dahulu seluruh bagian komputer, termasuk layar komputer/laptop dan catat tanggal dan waktu saat komputer/laptop itu hidup dan catat semua program yang sedang berjalan/sedang beroperasi di komputer/laptop itu. Setelah mengambil foto dan mencatat segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya.
c. Matikan sambungan dari akses remote (telpon genggam atau modem) pisahkan komputer dari kamera movie digital (web camera).
d. Jika yang ditemukan di TKP adalah laptop yang masih menyala (hidup) ambil foto secara keseluruhan dan catat tanggal dan waktu saat laptop itu hidup dan catat semua program yang sedang berjalan/sedang beroperasi di laptop itu, setelah itu tekan *power* laptop selama 30 detik sampai layar di laptop menjadi hitam (dikenal dengan *hard power down*).

b) CD/DVD dan USB *thumb drive*/ *memory card.*

Amankan barang bukti berupa CD/DVD dan USB *thumb drive*/ *memory card*, bungkus dengan memakai kantong barang bukti yang sudah disiapkan untuk diangkut (diperlakukan sama dengan barang pecah belah).

c) Telepon genggam.

Jika menemukan telepon genggam yang kemungkinan terkait dengan TP yang sedang ditangani segera matikan /nonaktifkan telepon genggam itu, jangan pernah melakukan penyitaan terhadap telepon genggam dalam keadaan terus menerus hidup karena itu akan merubah data komunikasi telepon genggam dengan BTS yang dilaluinya. Jika dalam keadaan mendesak dapat mencabut baterai dari telepon genggam itu dan masukan ke dalam kantong barang bukti yang sudah disiapkan.

12. Selain pemeriksaan secara laboratoris yang dilakukan oleh Subdit II Cyber Crime Ditreskrimsus Polda Sumut, penyidik dapat memeriksakan kepada Laboratorium Forensik Mabes Polri dengan memenuhi persyaratan formal sebagai berikut :

a. permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
b. laporan polisi;
c. BAP saksi/tersangka atau laporan kemajuan; dan
d. BA pengambilan, penyitaan dan pembungkusan barang bukti.

4. Pemeriksaan barang bukti perangkat komputer wajib memenuhi persyaratan teknis sebagai berikut :

a. Penanganan barang bukti komputer, yang berkaitan dengan data yang tersimpan dalam harddisk atau penyimpanan adat (*storage*) lain, dari sejak penanganan pertama harus sesuai dengan tata cara yang berlaku, karena barang bukti memiliki sifat yang mudah hilang/berubah (*volatile*), dan bila penyidik tidak memahami tata cara penyitaan barang bukti komputer, dapat meminta bantuan Labfor Polri;
b. Barang bukti dikirimkan secara lengkap dengan seluruh sistemnya;
c. Barang bukti dibungkus, diikat, dilak, disegel dan diberi label; dan
d. pengiriman barang bukti ke Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut tidak dapat melalui pos paket atau kurir (diantar oleh penyidik yang menangani perkara).

5. Tata cara penyitaan barang bukti komputer yang sedang digunakan untuk melakukan kejahatan adalah sebagai berikut :
   a. Mematikan aktivitas komputer dari server untuk komputer yang terhubung dengan network;

a. Mencabut kabel input komputer dari sumber arus listrik sebelum komputer di shut down (mematikan secara kasar), untuk laptop/notebook dicabut pula baterainya;
b. Mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
c. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
d. Mencabut semua kabel yang terpasang pada komputer dan I/O-nya, masing- masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
e. Menyita barang bukti lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external harddisk*, dan buku petunjuk;
f. Mencatat tanggal dan waktu penyitaan; dan
g. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

6. Tata cara penyitaan barang bukti komputer yang sudah dimatikan adalah sebagai berikut:

a. Mencari informasi kapan komputer digunakan tersangka untuk melakukan kejahatannya;
b. Mencari keterangan mengenai pengunaan komputer yang dijadikan sebagai barang bukti sesudah digunakan untuk melakukan kejahatan; dan
c. Mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
d. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
e. Mencabut semua kabel yang terpasang pada komputer dan I/O-nya, masing- masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
f. Menyita barang bukri lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external harddisk*, dan

buku petunjuk ;

g. Mencatat tanggal dan waktu penyitaan; dan
h. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

7. Terhadap para tersangka agar dilakukan pemeriksaan dengan beberapa hal yang perlu ditanyakan:
   a. identitas lengkapnya;
   b. riwayat hidupnya;
   c. Kronologi perbuatan tersangka dalam hal melakukan perjudian melalui media elektronik.
   d. kemampuan menjalankan komputer,gadget dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus.
8. Para tersangka yang memenuhi unsur dalam ketentuan ditahan sesuai dengan KUH Acara Pidana.
9. Para saksi yang mungkin sekaligus tersangka diperiksa dan hasilnya dituangkan dalam berita acara yang memenuhi persyaratan formal dan materiel. Hal yang perlu dipertanyakan:
   a. Proses saling mengenal dengan tersangka;
   b. jumlah karyawan perjudian *on-line* dan tugasnya; dan
   c. dan lain-lain sesuai dengan kasus;
10. Setelah melakukan rangkaian pemeriksaan terhadap barang bukti, penyidik meminta keterangan kepada saksi ahli dari Depkominfo:
   a. kepada ahli bidang hukum khusus UU ITE tentang pemenuhan unsur-unsur pasal yang disangkakan;
   b. kepada ahli secara teknis tentang permasalahan yang disangkakan;
11. Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital alat bukti lain, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain.
   1. Prosedur permintaan bantuan pemeriksaan bukti digital kepada Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut:
   a. Penyidik membuat surat yang ditandatangani oleh Kepala Kesatuan Kewilayahan dan ditujukan kepada Dirkrimsus Polda Sumut Up. Kasubdit Cyber Crime, perihal permintaan bantuan pemeriksaan laboratoris kriminalistik barang bukti digital;
   b. tembusan surat kepada Kapolda Sumut dan Team IT & Cyber Crime;
   c. isi surat menjelaskan data yang dibutuhkan oleh penyidik dari barang bukti digital dengan menyebutkan kata kunci/*keyword* tertentu. (contoh: jika yang dicari merupakan dokumen elektronik, penyidik harus memberikan nama dokumen elektronik yang akan dicari secara benar).
   2. Lampiran surat permintaan:
   a. Laporan Polisi;
   b. BA Penyitaan Barang Bukti;
   c. BA Pembungkusan/Penyegelan Barang Bukti;

d. Laporan Kemajuan (Resume);
3. Barang bukti dibungkus dengan plastik antistatik dan diantarkan langsung ke Subdit II Cyber Crime Ditreskrimsus Polda Sumut.

F. Tata Cara Penanganan TP Pencemaran Nama Baik/Fitnah Melalui Media Elektronik

1. Etnis tindak pidana pencemarannama baik/fitnah melalui media elektronik antara lain:
   a. mencemarkan/fitnah melalui *website*;
   b. mencemarkan/fitnah melalui *blog*;
   c. mencemarkan/fitnah melalui e-mail;
   d. mencemarkan/fitnah melalui situs jejaring sosial; dan
   e. mencemarkan/fitnah melalui SMS.
2. TP pencemaran nama baik/fitnah melalui media elektronik dilakukan dengan modus operandi sebagai berikut:
   a. Mem-*posting* sebuah tulisan dan atau gambar di blog/wesbsite/situs jejaring sosial, yang bernada pencemaran atau fitnah terhadap korban dengan menggunakan nama palsu dan / atau julukan;
   b. Mengirimkan SMS dengan nada pencemaran atau fitnah terhadap korban kepada banyak orang sehingga diketahui oleh umum, dengan menggunakan nomor HP yang tidak jelas.
3. Tata cara penyidikan tindak pidana pencemaran nama baik melalui media elektronik. TP pencemaran nama baik melalui media elektronik memerlukan perlakuan khusus, artinya berdasarkan pengaduan dari seseorang yang menjadi korban pencemaran nama baik melalui media elektronik. Penanganan dalam TP ini dilakukan dengan langkah sebagai berikut:
   a. Pencemaran nama baik melalui blog/*website*/situs jejaring sosial
      1. membuat laporan polisi model B;
      2. membuat surat perintah penyelidikan dan penyidikan;
      3. memeriksa saksi korban dengan meminta bukti adanya pencemaran nama baik yang dialami;
   b. sesuai dengan modus yang ada, penyidik melakukan penyelidikan dengan cara:
   1. Aplikasikan metode lidik klasik (konvensional) ke dunia *on-line*:
      a. *Under cover* (penyamaran) *on-line*, siapkan alamat surel, akun, user ID samaran.
      b. Lakukan komunikasi *on-line* melalui chat, email untuk mendapatkan header pelaku.
      c. Lacak header guna mengetahui IP Address pelaku.
      d. Gunakan *tools* yang tersedia di Internet untuk mengetahui ISP yang digunakan.
      e. Kumpulkan data pelaku sebanyak mungkin gunakan *search engine* google, freindster, facebook, yahoo group, dsb.

2. Setelah ditemukan identitas pelaku, penyidik dengan menggunakan aplikasi metode lidik klasik (konvensional) mencari alamat dari asal IP Address pelaku;

a. Melakukan koordinasi dengan *Internet Service Provider,* untuk meminta keterangan dari IP address yang digunakan oleh pelaku penyidik mengirimkan surat permintaan kepada ISP, surat ditandatangani oleh Direktur Tipideksus utk tingkat Bareskrim dan Direktur Reskrim/Sus untuk tingkat Polda.

b. Setelah mengumpulkan keterangan dari para saksi dan ISP, penyidik menyiapkan langkah selanjutnya dengan upaya paksa;

c. Sebelum melakukan penggeledahan dan penyitaan, penyidik meminta izin kepada ketua pengadilan negeri setempat terhadap barang bukti yang ada kaitannya dengan TP itu, seperti komputer, harddisk, laptop, dan media elektronik lain;

d. Setelah melakukan upaya paksa berupa penggeledahan, penyitaan, dan penangkapan terhadap para pelaku, penyidik melakukan olah TKP terhadap barang bukti digital. Pemeriksaan barang bukti digital di TKP dilakukan secara forensik oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital. Adapun tindakan penanganan barang bukti elektronik di TKP sebagai berikut:

a) Terhadap barang bukti Komputer/Laptop:

Apabila komputer/laptop dalam kondisi tidak nyala (mati) segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya".

a. Apabila komputer/laptop dalam kondisi nyala (hidup), ambil foto terlebih dahulu semua bagian komputer, termasuk layar komputer/laptop, catat tanggal serta waktu saat komputer/laptop itu hidup, dan catat semua program yang sedang berjalan/sedang beroperasi. Setelah mengambil foto dan mencatat, segera copot daya listriknya dari semua alat elektronik, cabut kabel listrik dari komputer bukan dari sumbernya.

b. Matikan sambungan dari akses *remote* (telepon genggam atau modem) pisahkan komputer dari *movie digital camera* (*web camera*).

c. Jika yang ditemukan di TKP adalah laptop yang masih menyala (hidup), ambil foto secara keseluruhan dan catat tanggal serta waktu saat laptop itu hidup dan catat semua program yang sedang berjalan/sedang beroperasi di laptop itu. Setelah itu, tekan *power* laptop selama 30 detik sampai layar di laptop menjadi hitam (dikenal dengan *hard power down*)

b) CD/DVD dan USB *thumb drive*/*memory card.*

Amankan barang bukti berupa CD/DVD dan USB *thumb drive/memory card*, bungkus dengan memakai kantong barang bukti yang sudah disiapkan untuk diangkut (dimemperlakukan sama dengan barang pecah belah).

c) Telepon genggam.
Jika menemukan telepon genggam yang kemungkinan terkait dengan TP yang sedang ditangani segera matikan/nonaktifkan telepon genggam itu, jangan pernah melakukan penyitaan terhadap telepon genggam dalam keadaan terus menerus hidup karena itu akan merubah data komunikasi telepon genggam dengan BTS yang dilaluinya. Jika dalam keadaan mendesak dapat mencabut baterai dari telepon genggam itu dan masukan ke dalam kantong barang bukti yang sudah disiapkan.

3. Selain pemeriksaan secara laboratoris yang dilakukan oleh Subdit II Cyber Crime Ditreskrimsus Polda Sumut, penyidik dapat memeriksakan kepada Laboratorium Forensik Mabes Polri dengan memenuhi persyaratan formal:
   a. permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
   b. laporan polisi;
   c. BAP saksi/tersangka atau laporan kemajuan; dan
   d. BA pengambilan, penyitaan dan pembungkusan barang bukti.
   e. Pemeriksaan barang bukti perangkat komputer wajib memenuhi persyaratan teknis:
   1. penanganan barang bukti komputer, yang berkaitan dengan data yang tersimpan dalam harddisk atau penyimpanan adat (*storage*) lain, dari sejak penanganan pertama harus sesuai dengan tata cara yang berlaku, karena barang bukti memiliki sifat yang mudah hilang/berubah (*volatile*), dan bila penyidik tidak memahami tata cara penyitaan barang bukti komputer, dapat meminta bantuan Labfor Polri;
   2. barang bukti dikirimkan secara lengkap dengan seluruh sistemnya;
   3. barang bukti dibungkus, diikat, dilak, disegel dan diberi label; dan
   4. Pengiriman barang bukti ke Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut tidak dapat melalui pos paket atau kurir (diantar oleh penyidik yang menangani perkara).
4. Tata cara penyitaan barang bukti komputer yang sedang digunakan untuk melakukan kejahatan adalah:
   a. mematikan aktivitas komputer dari server untuk komputer yang terhubung dengan network;
   b. mencabut kabel input komputer dari sumber arus listrik sebelum komputer di shut down (mematikan secara kasar), untuk laptop/notebook dicabut pula baterainya;
   c. mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkantanpa sengaja;
   d. mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
   e. mencabut semua kabel yang terpasang pada komputer dan I/O- nya, masing-masing diberi tanda yang berbeda agar memudahkan pemasangannya kembali;

f. menyita barang bukri lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external harddisk*, dan buku petunjuk ;
g. mencatat tanggal dan waktu penyitaan; dan
h. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

5. Tata cara penyitaan barang bukti komputer yang sudah dimatikan adalah: mencari informasi kapan komputer digunakan tersangka untuk melakukan kejahatannya
   a. mencari keterangan mengenai pengunaan komputer yang dijadikan sebagai barang bukti sesudah digunakan untuk melakukan kejahatan;
   b. mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
   c. mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
   d. mencabut semua kabel yang terpasang pada komputer dan I/O- nya, masing-masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
   e. menyita barang bukti lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, *magnetic tape, memory card, flash disk, external harddisk*, dan buku petunjuk ;
   f. mencatat tanggal dan waktu penyitaan; dan
   g. memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.
6. Terhadap para tersangka agar dilakukan pemeriksaan dengan pertanyaan mengenai:
   a. identitas lengkapnya;
   b. riwayat hidupnya;
   c. kronologi perbuatan tersangka dalam hal melakukan pencemaran nama baik /fitnah melalui media elektronik;
   d. kemampuan menjalankan komputer, *gadget* dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus;
   e. alat apa saja yang digunakan dalam melakukan perbuatan itu.
7. Para tersangka yang memenuhi unsur dalam ketentuan itu ditahan sesuai dengan KUH Acara Pidana.
8. Para saksi yang mungkin sekaligus tersangka dipemeriksa yang hasilnya dituangkan dalam berita acara yang memenuhi persyaratan formal dan materiil. Hal yang perlu dipertanyakan:
   a. proses saling mengenal dengan tersangka;
   b. apa saja yang membuat saksi menjadi merasa tercemar nama baiknya atau difitnah;
   c. melalui media apa saja perbuatan itu dilakukan; dan

d. lain-lain sesuai dengan kasus.

4. Setelah rangkaian pemeriksaan terhadap barang bukti, penyidik meminta keterangan terhadap saksi ahli dari Depkominfo antara lain tentang :
   a. Ahli bidang hukum khusus UU ITE tentang pemenuhan unsur- unsur pasal yang disangkakan;
   b. Ahli secara teknis tentang permasalahan yang disangkakan.
5. Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital alat bukti lain, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain. Pencemaran nama baik melalui media Short Message Service (SMS):
   1. Membuat laporan polisi model B;
   2. Memeriksa saksi korban;
   3. Membuat surat perintah penyelidikan dan penyidikan;
   4. Meminta barang bukti telepon genggam dari saksi korban dimana terdapat kata-kata atau tulisan yang membuat korban menjadi tercemar;
   5. Setelah melihat SMS dari pelaku ke korban, penyidik mencatat nomor HP yang digunakan oleh pelaku untuk melakukan perbuatan tsb;
   6. Setelah mengetahui nomornya, penyidik membuat surat kepada *provider* yang terkait dengan nomor itu;
   7. Surat yang ditujukan kepada provider seluler berisikan permintaan data *log file*, SMS dan Call Detail Record yang ada pada nomor yang digunakan oleh pelaku ditandatangani oleh Direktur Tipideksus untuk tingkat Bareskrim dan Direktur Reskrim/Sus untuk tingkat Polda;
   8. Setelah mendapatkan data yang dimaksud, penyidik mulai melakukan penyelidikan dengan membaca *log file* yang ada pada nomor yang dimintakan, data yang dicari yang berkaitan dengan nomor terakhir yang dihubungi, lokasi terakhir dari nomor itu, dalam inbox sms dilihat dengan siapa saja berhubungan;
   9. Setelah ditemukan identitas pelaku, penyidik dengan menggunakan aplikasi metode lidik klasik (konvensional) mencari alamat/keberadaan pelaku;
   10. Dalam persiapan melakukan upaya paksa terhadap pelaku yang setelah diketahui identitasnya melalui permintaan kepada provider seluler, penyidik meminta izin ke ketua pengadilan negeri setempat untukmelakukan penggeledahan dan penyitaan;

1. Selain dari pemeriksaan dengan permintaan kepada provider seluler, penyidik mengirimkan perangkat telekomunikasi yang telah disita dari pelaku ke Puslabfor Polri utk dilakukan pemeriksaan secara laboratories;

2. Pemeriksaan barang bukti perangkat telekomunikasi secara laboratoris ke Puslabfor wajib memenuhi:

a) Persyaratan formal:
   (1) permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
   (2) laporan polisi;
   (3) BAP saksi/tersangka atau laporan kemajuan; dan
   (4) BA pengambilan, penyitaan dan pembungkusan barang bukti.

b) Persyaratan teknis:
   (1) barang bukti secara lengkap dikirimkan ke Labfor Polri, beserta seluruh sistemnya;
   (2) apabila barang bukti merupakan perangkat telekomunikasi yang tidak sederhana, pengiriman barang bukti harus dilengkapi dengan:
      a. Spesifikasi teknis, gambar konstruksi, dan pedoman penggunaan (*operating manual*) dari pabrik pembuatnya; dan.
      b. Dokumen riwayat pemakaian dan perawatan dari pengguna *(log book*), terutama berkaitan dengan kejadian kasus .
   (3) Barang bukti dibungkus, diikat, dilak, disegel dan diberi label;
   (4) Apabila terdapat barang bukti yang diduga palsu atau tidak sesuai spesifikasinya, selain dikirimkan barang buktinya, wajib dikirimkan barang pembandingnya yang dilengkapi dengan pernyataan keaslian pembanding dari produsen resmi;
   (5) Pengiriman barang bukti ke Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut tidak dapat melalui pos paket atau kurir (diantar oleh penyidik yang menangani perkara), dan
   (6) Barang bukti yang ukuran dan kondisinya tidak dapat dikirim ke Labfor Polri dapat diperiksa di tempat asalnya (TKP) oleh pemeriksa ahli dari Labfor Polri dengan mempertahankan keaslian (*status quo*) TKP.

1. Setelah mendapatkan alat bukti, penyidik melakukan pemeriksaan terhadap para saksi guna memenuhi unsur TP.
2. Terhadap para tersangka agar dilakukan pemeriksaan dengan menanyakan beberapa hal:
   a) Identitas lengkapnya;
   b) Riwayat hidupnya;
   c) Kronologi perbuatan tersangka dalam hal melakukan pencemaran nama baik /fitnah melalui media elektronik;
   d) Kemampuan menjalankan komputer,gadget dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus;
   e) Alat apa saja yang digunakan dalam melakukan perbuatan itu.

15. Para tersangka yang memenuhi unsur dalam ketentuan ditahan sesuai dengan KUH Acara Pidana.
16. Para saksi yang mungkin sekaligus tersangka diperiksa. Hasilnya dituangkan dalam

berita acara yang memenuhi persyaratan formal dan materiel, hal-hal yang perlu dipertanyakan:

a) Proses saling mengenal dengan tersangka;
b) Apa saja yang membuat saksi menjadi merasa tercemar nama baiknya atau fitnah;
c) Melalui media apa saja perbuatan itu dilakukanl;
d) Dan lain-lain sesuai dengan kasus.

17. Setelah rangkaian pemeriksaan terhadap barang bukti, penyidik meminta keterangan kepada saksi ahli dari Depkominfo:
    a) kepada ahli bidang hukum khusus UU ITE tentang pemenuhan unsur pasal yang disangkakan; dan
    b) kepada ahli teknis tentang permasalahan yang disangkakan.
18. Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital alat bukti lain, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain. Prosedur permintaan bantuan pemeriksaan bukti digital kepada Labfor Polri dan Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut:
    a. Penyidik membuat surat yang ditandatangani oleh Kepala Kesatuan Kewilayahan dan ditujukan kepada Dirkrimsus Polda Sumut Up. Kasubdit II Cyber Crime, perihal permintaan bantuan pemeriksaan laboratoris kriminalistik Barang Bukti Digital;
    b. Tembusan surat kepada Kapolda Sumut dan Team IT & Cyber Crime;
    c. Isi surat menjelaskan data yang dibutuhkan oleh Penyidik dari Bukti Digital dengan menyebutkan kata kunci/keyword tertentu. (contoh: jika yang dicari merupakan dokumen elektronik, penyidik harus memberikan nama dokumen elektronik yang akan dicari secara benar);
19. Surat permintaan dilampiri:
    a. Laporan Polisi;
    b. BA Penyitaan Barang Bukti;
    c. BA Pembungkusan/Penyegelan Barang Bukti;
    d. Laporan Kemajuan (Resume)
20. Barang bukti dibungkus dengan plastic anti-statik dan diantarkan langsung ke Subdit II Cyber Crime Ditreskrimsus Polda Sumut.

F. Tata Cara Penanganan TP Penipuan Melalui Media Elektronik (*Cyber Fraud*)

a. Jenis TP penipuan melalui media elektronik Berbagai cara penipuan yang dilakukan antara lain melalui *Website*, *blog*, e-mail, situs jejaring sosial dan SMS. Pasal yang dilanggar : pasal 28 ayat (1) Undang-undang No.11 Tahun 2008 tentang ITE (Informasi dan Transaksi Elektronik) Jo pasal 378 KUHP.
b. Modus operandi TP penipuan melalui media elektronik dilakukan dengan modus operandi sebagai berikut:

1. Mem-*posting* sebuah tulisan dan / atau gambar di *blog/wesbsite*/situs jejaring sosial, yang menyesatkan dan berita bohong yang mengakibatkan kerugian konsumen

dalam transaksi elektronik;

2. Mengirimkan SMS yang menyesatkan dan berita bohong terhadap korban.

c. Tata cara penyidikan TP penipuan melalui media elektronik Dalam menangani TP penipuan yang dilakukan dengan melalui media elektronik, penyidik memedomani ketentuan yang ada dengan langkah sebagai berikut.

1. Tahapan penyidikan Kegiatan penyelidikan dapat dilakukan oleh penyidik atau menerima informasi dari pihak pelapor, dilanjutkan dengan pembuatan laporan polisi serta surat perintah tugas dan surat perintah penyelidikan, dan

2. Berkoordinasi dengan pihak ISP (internet service provider), Provider Seluler dan Monitoring Center (bareskrim Polri) untuk meminta data *log file* dan *call detail record* dari target yang akan di Lidik.

1. Membuat laporan polisi model B.
2. Membuat surat perintah penyelidikan dan penyidikan.
3. Memeriksa saksi korban dengan meminta bukti adanya penipuan yang dialami.

d. Sesuai dengan modus yang ada , penyidik melakukan penyelidikan dengan cara :

a. Aplikasikan metode lidik klasik (konvensional) ke dunia *on-line*

1. Under cover (penyamaran) *on-line*,siapkan Alamat surel, akun, user ID samaran;
2. Lakukan komunikasi *on line* melalui *chat*, email untuk mendapatkan *header* pelaku;
3. Lacak *header* guna mengetahui *IP Address* pelaku.

1. Gunakan *tools* yang tersedia di Internet untuk mengetahui ISP yang digunakan.
2. Kumpulkan data pelaku sebanyak mungkin, gunakan *search engine* google, freindster, facebook, yahoo group, dsb.

b. Setelah ditemukan identitas pelaku, penyidik dengan menggunakan aplikasi metode lidik klasik (konvensional) mencari alamat dari asal IP Address pelaku;

c. Melakukan koordinasi dengan *Internet Service Provider,* untuk meminta keterangan dari IP address yang digunakan oleh pelaku penyidik mengirimkan surat permintaan kepada ISP, surat ditandatangani oleh Direktur Tipideksus utk tingkat Bareskrim dan Direktur Reskrim/Sus untuk tingkat polda.

1. Setelah penyidik telah mengumpulkan keterangan dari para saksi dan ISP, penyidik menyiapkan langkah selanjutnya dengan upaya paksa.
2. Sebelum melakukan penggeledahan dan penyitaan, penyidik meminta izin kepada ketua pengadilan negeri setempat terhadap barang bukti yang ada kaitannya dengan TP itu seperti komputer, harddisk, laptop dan media elektronik lain.
3. Setelah melakukan upaya paksa berupa penggeledahan, penyitaan dan penangkapan terhadap para pelaku, penyidik melakukan olah TKP terhadap barang bukti digital dengan pemeriksaan barang bukti digital di TKP dilakukan secara laboratorium forensik yang dilakukan oleh petugas dari Subdit II Cyber Crime Ditreskrimsus Polda Sumut dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital.
4. Selain pemeriksaan secara laboratoris yang dilakukan oleh Subdit II Cyber Crime Ditreskrimsus Polda Sumut, penyidik dapat memeriksakan kepada Laboratorium

Forensik Mabes Polri dengan memenuhi persyaratan formal:

a. Permintaan tertulis dari kepala kesatuan kewilayahan atau kepala/pimpinan instansi;
b. laporan polisi;
c. BAP saksi/tersangka atau laporan kemajuan; dan
d. BA pengambilan, penyitaan dan pembungkusan barang bukti

5. Pemeriksaan barang bukti perangkat komputer wajib memenuhi persyaratan teknis:

a. Penanganan barang bukti komputer, yang berkaitan dengan data yang tersimpan dalam *harddisk* atau penyimpanan adat (*storage*) lain, dari sejak penanganan pertama harus sesuai dengan tata cara yang berlaku, karena barang bukti memiliki sifat yang mudah hilang/berubah (*volatile*), dan bila penyidik tidak memahami tata cara penyitaan barang bukti komputer, dapat meminta bantuan Labfor Polri;
b. Barang bukti dikirimkan secara lengkap dengan seluruh sistemnya;
c. Barang bukti dibungkus, diikat, dilak, disegel, dan diberi label; dan
d. Pengiriman barang bukti ke Labfor Polri dapat melalui pos paket atau kurir.

6. Tata cara penyitaan barang bukti komputer yang sedang digunakan untuk melakukan kejahatan adalah:

a. mematikan aktivitas komputer dari server untuk komputer yang terhubung dengan *network*;
b. mencabut kabel input komputer dari sumber arus listrik sebelum komputer di *shut down* (mematikan secara kasar), untuk laptop/notebook dicabut pula baterainya;
c. Mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
d. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
e. Mencabut semua kabel yang terpasang pada komputer dan I/O-nya, masing-masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;
f. Menyita barang bukri lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external harddisk*, dan buku petunjuk ;
   a. Mencatat tanggal dan waktu penyitaan; dan
   b. Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

1. Tata cara penyitaan barang bukti komputer yang sudah dimatikan adalah:

a. Mencari informasi kapan komputer digunakan tersangka untuk melakukan kejahatannya;
b. Mencari keterangan mengenai pengunaan komputer yang dijadikan sebagai barang bukti sesudah digunakan untuk melakukan kejahatan; dan Mematikan saklar pasokan listrik dan segel saklar itu untuk menghindari menghidupkan tanpa sengaja;
c. Mencatat spesifikasi komputer dan peralatan input/output (I/O) yang terpasang pada komputer itu;
d. Mencabut semua kabel yang terpasang pada komputer dan I/O-nya, masing-masing diberi tanda yang berbeda agar memudahkan pada pemasangannya kembali;

e. Menyita barang bukri lain yang ada hubungannya dengan komputer, antara lain disket, CD/DVD, magnetic tape, *memory card*, *flash disk*, *external harddisk*, dan buku petunjuk;

a. Mencatat tanggal dan waktu penyitaan; dan Memperlakukan barang bukti dengan hati-hati seperti barang pecah pada saat pengangkutan.

7. Para tersangka agar diperksa dengan mengajukan pertanyaan tentang:
a. Identitas lengkapnya.
b. Riwayat hidupnya.
c. Kronologi perbuatan tersangka dalam hal melakukan penipuan melalui media elektronik.
d. Kemampuan menjalankan komputer,gadget dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus.
e. Alat apa saja yang digunakan dalam melakukan perbuatan itu.
8. Para tersangka yang memenuhi unsur dalam ketentuan ditahan sesuai dengan KUH Acara Pidana.
9. Para saksi yang kemungkinan sebagai tersangka dilakukan pemeriksaan yang dituangkan dalam berita acara yang memenuhi persyaratan formal dan materiel, hal-hal yang perlu dipertanyakan:
a. proses saling mengenal dengan tersangka;
b. apa saja yang membuat saksi menjadi merasa ditipu;
c. apa saja kerugian yang dialaminya;
d. melalui media apa perbuatan itu dilakukan;
e. dan lain-lain sesuai dengan kasus.
10. Setelah melakukan rangkaian pemeriksaan terhadap barang bukti, penyidik meminta keterangan kepada saksi ahli dari Depkominfo:
a. kepada ahli bidang hukum khusus UU ITE tentang pemenuhan unsur pasal yang disangkakan;
b. kepada ahli secara teknis tentang permasalahan yang disangkakan.
12. Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital alat bukti lain, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain. Prosedur permintaan bantuan pemeriksaan bukti digital kepada Laboratorium Digital Forensik Subdit II Cyber Crime:
1. Penyidik membuat surat yang ditandatangani oleh Kepala Kesatuan Kewilayahan dan ditujukan kepada Dirreskrimsus Polda Sumut Up. Kasubdit II Cyber Crime, perihal permintaan bantuan pemeriksaan laboratoris kriminalistik Barang Bukti Digital;
2. Tembusan surat kepada Kapolda Sumut dan Team IT Cyber Crime.
3. Isi surat menjelaskan data yang dibutuhkan oleh Penyidik dari Bukti Digital dengan menyebutkan kata kunci/*keyword* tertentu. (contoh : jika yang dicari merupakan dokumen elektronik, penyidik harus memberikan nama dokumen elektronik yang akan dicari secara benar).

13. Surat permintaan dilampiri:

a. Laporan Polisi;
b. BA Penyitaan Barang Bukti;
c. BA Pembungkusan/Penyegelan Barang Bukti;
d. Laporan Kemajuan (Resume).
e. Barang bukti dibungkus dengan plastik antistatik dan diantarkan langsung ke Subdit II Cyber Crime.

G. Kegiatan Lain yang diperlukan Guna memperlancar Pelaksanaan Penyelidikan Dan Penyidikan.

Penyelidikan dan penyidikan perkara *cyber crime* memiliki kekhususan, artinya kejahatan yang terjadi merupakan ”maya” atau tidak dapat terlihat oleh kita karena menggunakan media Internet maupun elektronik sehingga diperlukan kerja sama antarpenyidik dengan lembaga lain ataupun dengan komunitas dunia maya seperti Departemen Kementerian Informasi dan Telekomunikasi, akademisi atau universitas, bank atau Lembaga Penyedia Jasa Internet, komunitas Internet, para *blogger*. Kerja sama yang dapat dilakukan antara lain :

1. Berkoordinasi aktif dengan lembaga lain dengan saling menukar informasi tentang adanya kejahatan dunia maya;
2. Berkoordinasi dengan NCB-Interpol kaitan dengan kejahatan lintas negara dan penggunaan server yang ada diluar Indonesia;
3. meningkatkan Kapasitas antar Lembaga dengan mengisi Pendidikan, Pelatihan atau Seminar Anti Cyber Crime;
4. membentuk Forum Kerja sama antar-Lembaga Penanganan Perkara Cyber Crime; dan
5. Saling berbagi info dengan komunitas pengguna Internet atau para *blogger*.

BAB III
PENGAWAAN DAN PENGENDALIAN

A. Pengawasan

Pengawasan penanganan TP di Bidang Cyber Crime dilakukan oleh Direktur dan Wadir Tipideksus.

B. Pengendalian

Pengendalian kegiatan penyelidikan dan penyidikan pengelolaan dan penanganan TP di Bidang Cyber Crime, dilakukan secara berjenjang di lingkungan Polri dan ketentuan lain atau peraturan lain yang mengatur tentang sistem pengendalian kegiatan penyelidikan”.

BAB IV
KETENTUAN LAIN

A. Ketentuan Umum

Dalam tata cara penanganan TP di Bidang Cyber Crime harus selalu memperhatikan dan memedomani prinsip yang berikut.

1. Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan dengan memperhatikan perlindungan bagi privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.
2. Setiap kegiatan penyelidikan, harus berdasarkan Surat Perintah yang sesuai dengan subjeknya.
3. Tetap memedomani peraturan perundang-undangan serta peraturan lain yang berkaitan dengan TP kejahatan dunia maya atau *cyber crime*.

B. Ketentuan Khusus

1. Dalam penanganan bukti elektronik atau bukti digital, kerahasiaan data merupakan tanggung jawab pemeriksa pada Laboratorium Digital Forensik Subdit II Cyber Crime Ditreskrimsus Polda Sumut.
2. Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang- Undang tentang Hukum Acara Pidana untuk melakukan penyidikan TP di bidang Teknologi Informasi dan Transaksi Elektronik.
3. Dalam rangka mengungkap TP Informasi elektronik dan Transaksi elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti

BAB VII
P E N U T U P

A. Standar Operasional Prosedur (SOP) Penanganan kejahatan di dunia maya/*cyber crime* di lingkungan Subdit II Cyber Crime Ditreskrimsus Polda Sumut ini disusun untuk dipedomani dan dilaksanakan sebagaimana mestinya.Hal yang belum diatur dalam Standar Operasional Prosedur (SOP) ini akan ditentukan kemudian.

B. Standar operasional prosedur ini mulai berlaku pada tanggal ditetapkan.

ditetapkan di : Medan
pada taggal : Oktober 2016

DIREKTUR RESERSE KRIMINAL KHUSUS POLDA SUMUT

Drs. TOGA HABINSARAN PANJAITAN KOMISARIS BESAR POLISI NRP 67100294

Sumber : Dokumentasi *Cyber Crime* Ditreskrimsus V Polda Sumut