ANALISIS TINDAK PIDANA *CYBER CRIME* TERHADAP PELAKU KEJAHATAN INFORMASI DATA PRIBADI

APRILLIA SADAR

NIM : 4519060126

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Hukum (S.H) pada Program Studi Ilmu Hukum Fakultas Hukum Universitas Bosowa

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM UNIVERSITAS BOSOSWA

2023

LEMBAR PERSETUJUAN PEMBIMBING

Usulan Penelitian dan Penulisan Mahasiswa Hukum :

Nama	: Aprillia Sadar
NIM	: 4519060126
Program Studi	: Ilmu Hukum
Minat	: Pidana
No. Pendaftaran Judul	: 403/Pdn/FH-UBS/VII-Gnj/2022
Tgl. Pendaftaran Judul	: 14 Oktober 2022
Judul Skripsi	: Analisis Tindak Pidana CyberCrime Terhadap Pelaku Kejahatan Informasi Data Pribadi

Telah diperiksa dan diperbaiki untuk dimajukan dalam ujian skripsi mahasiswa program strata satu (S1)

Makassar, 23/8/2023

Disetujui :

Pembimbing I,

Dr. Basri Oner, S.H.,M.H.

Pembimbing II,

Dr. Almusawir, S.H., M.Hum.

Mengetahui :

Dekan Fakultas Hukum

Dr. Yulia A. Hasan S.H., M.H.

PERSETUJUAN UJIAN SKRIPSI

Pimpinan Fakultas Hukum Universitas Bosowa menerangkan bahwa:

Nama	: Aprillia Sadar
NIM	: 4519060126
Program Studi	: Ilmu Hukum
Minat	: Hukum Pidana
No. Pendaftaran Judul	: No.403/Pdn/FH-UBS/VII-Gnj/2022
Tgl. Pendaftaran Judul	: 14 Oktober 2022
Judul Skripsi	: Analisis Tindak Pidana *Cyber Crime* Terhadap Pelaku Kejahatan Informasi Data Pribadi

Telah disetujui skripsinya untuk diajukan dalam ujian skripsi mahasiswa programstrata satu (S1)

Makassar, 30/8/2023

Dr. Yulia A. Hasan, S.H.,M.H

HALAMAN PENGESAHAN

Untuk memenuhi salah satu syarat memperoleh gelar Sarjana Hukum Program Studi Ilmu Hukum pada Fakultas Hukum Universitas Bosowa Makassar, bagian **Hukum Pidana** dan berdasarkan Surat Keputusan Dekan Fakultas Hukum Universitas Bosowa Makassar Nomor A. 308/FH/UNIBOS/VIII/2023 tanggal 29 Agustus 2023 tentang Panitia Ujian Skripsi, Maka pada hari ini Kamis, 7 Agustus 2023 Skripsi ini diterima dan disahkan setelah dipertahankan oleh saudara/i. **APRILLIA SADAR** Pada Nomor Pokok Mahasiswa **4519060126** yang dibimbing oleh **Dr. Basri Oner, S.H., M.H selaku Pembimbing I dan Dr. Almusawir, S.H., M.H. selaku Pembimbing II dihadapan Panitia Ujian Skripsi yang terdiri atas:**

Panitia Ujian

Ketua	Sekretaris,
Dr. Yulia A Hasan, S.H., M.H.	**Dr. Andi Tira, S.H., M.H.**

Tim Penguji

Ketua	**: 1. Dr. Basri Oner,S.H., M.H.**	**(.....)**
	2. Dr. Almusawir, S.H., M.H.	**(.....)**
	3. Prof. Dr. Ruslan Renggong, S.H., M.H.	**(.....)**
	4. Hj. Siti Zubaidah, S.H., M.H.	**(.....)**

HALAMAN PERNYATAN ORISINALITAS

Skripsi dengan Judul "**Analisis Tindak Pidana *Cyber Crime* Terhadap Pelaku Kejahatan Informasi Data Pribadi"** ini adalah hasil karya saya sendiri, dan semua sumber yang di kutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Aprilia Sadar
Nim : 4519060126
Program Studi : Ilmu Hukum

Makassar, 22 September 2023

Aprilia Sadar
4519060126

KATA PENGANTAR

Assalammualaikum Warahmatullahi Wabarakatuh

Alhamdulillah, puji dan Syukur penulis panjatkan ke hadirat Allah SWT yang telah memberikan Rahmat dan Karunia-nya, tak lupa pula shalawat dan salan kita kirimkan kepada Nabi Besar Muhammad SAW beserta para sahabatnya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Analisis Tindak Pidana *Cyber Crime* Terhadap Pelaku Kejahatan Informasi Data Pribadi"**, sebagai syarat untuk menyelesaikan Pendidikan dan memperoleh gelar sebagai Sarjana Hukum di Fakultas Hukum Universitas Bosowa.

Penulis menyadari selama proses penyusunan skripsi ini terdapat kendala yang dihadapi oleh penulis. Namun kendala tersebut menjadi ringan berkat doa, bimbingan serta dukungan dari beberapa pihak. Untuk itu penulis menyampaikan terima kasih kepada pihak yang dimaksud:

1. Bapak dan ibu penulis yang selalu mendoakan dan mendukung penulis selama proses penulisan skripsi;
2. Saudara-saudara yang selalu memberi bantuan kepada penulis;
3. Prof. Dr. Ir. Batara Surya, S.T., M.SI, selaku Rektor Universitas Bosowa Makassar beserta jajarannya;
4. Dr. Yulia A Hasan, S.H.,M.H. selaku Dekan Fakultas Hukum Universita Bosowa;
5. Dr. Basri Oner, S.H.,M.H. selaku pembimbing I yang telah banyak memberikan arahan kepada penulis;

6. Dr. Almusawir, S.H.,M.H, selaku pembimbing II yang telah kritikan dan bimbingan dalam penyususnan skripsi ini.
7. Hj. Siti Zubaidah, S.H.,M.H. selaku penguji I dan Prof. Dr. Ruslan Renggong. S.H.,M.H. selaku penguji II penulis yang telah memberikan saran dan masukan kepada penulis untuk menyempurnakan skripsi ini.
8. Ditreskrimsus Polda Sulsel, Terkhusus kepada Bripka Udiyantop yang telah menjadi narasumber penulis dalam menyelesaikan penelitian ini.
9. Abdillah sas. S.Kom.,M.Pd. selaku Ahli IT Universitas Bosowa yang telah menjadi narasumber penulis dalam menyelesaikan penelitian ini.
10. Para dosen Fakultas Hukum Universitas Bosowa yang telah memberikan ilmu yang sangat bermanfaat kepada penulis.
11. Seluruh pegawai akademik dan administrasi Fakultas Hukum Universitas Bosowa yang dengan sabar membantu memperlancar proses penyusunan skripsi ini.
12. Teman- teman Angkatan 19 Fakultas Hukum Universitas Bosowa.
13. Teman-teman kuliah iren, patrialis, cindy, reyhan, syahril, irghy, vita, ardhia yang membantu dalam penyusunan skripsi ini.
14. Kepada safira, nina, dita dan widy yang selalu ada membantu,membimbing, memberi motivasi serta nasehat yang selalu diberikan kepada penulis dalam menyusun skripsi ini.
15. Kepada Bullung Irma, nilan, baya, sesa, nisa, ira, endah yang selalu memberikan doa, masukan, nasehat dan motivasi untuk penulis dalam menyusun skripsi ini.

Semoga segala amal dan budi baik serta kerja sama dari semua pihak, baik yang tersebut maupun tidak, mendapatkan balasan terbaik dari Allah SWT.

Penulis menyadari bahwa apa yang ada di dalam skripsi ini masih jauh dari Namanya sempurna, untuk itu penulis mengharapkan kritikan dan saran kepada semua pihak demi untuk mendekati yang Namanya sempurna.

Penulis berharap semoga skripsi yang sederhana ini dapat memberikan manfaat yang baik pada bidang hukum dan ilmu bagi semua pihak.

Makassar, 10 Agustus 2023

Penulis

ABSTRAK

APRILLIA SADAR, Analisis Tindak Pidana *Cyber Crime* Terhadap Pelaku Kejahatan Informasi Data Pribadi, Basri Oner selaku pembimbing I dan Almusawir selaku pembimbing II.

Tujuan penelitian ini untuk menganalisis bagaimana proses penyelidikan dan Upaya dalam menyelesaikan proses penyidikan terkait kasus kejahatan *cyber crime* yang dilakukan oleh Kepolisian Daerah Sulawesi Selatan Direktorat Reserse Kriminal Khusus.

Untuk itu penelitian ini menggunakan penelitian normatif empirik. Dengan sumber data primer dan sekunder. Penelitian ini dilakukan di Kepolisian Daerah Sulawesi Selatan dengan melakukan wawancara pada salah satu anggota penyidik pada Ditreskrimsus Kepolisian Daerah Sulawesi Selatan.

Hasil penelitian menunjukkan bahwa dalam proses penyelidikan yang dilakukan masih terdapat beberapa hambatan atau kendala dalam pencarian tersangka, alat bukti, dan saksi adapun Upaya yang dilakukan oleh Kepolisian agar proses penyelidikan berjalan lancar dengan cara : Upaya Aktif dan Upaya Pasif serta dengan mempermudah penyelidikan dapat dilakukan secara tim dengan cara melakukan pelatihan untuk meningkatkan kemampuan tim dan secara tekhnis melakukan komunikasi antar personal *Cyber* Nusantara dan Petugas Interpol yang menangani Kejahatan dunia Maya.

Kata Kunci: Tindak Pidana, Cyber Crime, Informasi Data Pribadi

ABSTRACT

APRILIA SADAR, Analysis of Cyber Crime Crime Against Perpetrators of Personal Data Information Crimes, Basri Oner as supervisor I and Almusawir as supervisor II.

The purpose of this study is to analyze how the investigation process and efforts to complete the investigation process related to cyber crime cases committed by the South Sulawesi Regional Police, Directorate of Special Criminal Investigation.

For this reason, this study uses empirical normative research. With primary and secondary data sources. This research was conducted at the South Sulawesi Regional Police by conducting interviews with one of the investigators at the South Sulawesi Regional Police Criminal Investigation Directorate.

The results of the study indicate that in the investigation process carried out there are still several obstacles or obstacles in the search for suspects, evidence, and witnesses. The efforts made by the Police so that the investigation process runs smoothly by: Active Efforts and Passive Efforts and by facilitating investigations can be carried out effectively. team by conducting training to improve the team's capabilities and technically carry out interpersonal communication between Cyber Nusantara and Interpol Officers who handle Cyber Crime

Keyword : Criminal Act, Cyber Crime, Personal Data Information

DAFTAR ISI

BAB V KESIMPULAN DAN SARAN

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Kejahatan merupakan problematik yang membayangi umat manusia. Tidak dapat dipungkiri bahwa kejahatan pasti terjadi dimana terdapat manusia-manusia yang mempunyai kepentingan berbeda-beda. Kejahatan memang dapat terjadi tanpa mengenal ruang dan waktu, serta dapat dilakukan oleh siapa saja. Kejahatan bukan merupakan peristiwa hereditas (bawaan sejak lahir, warisan), juga bukan merupakan warisan biologis. Tindak kejahatan bisa dilakukan secara sadar yaitu difikirkan, direncanakan dan diarahkan pada maksud tertentu secara sadar benar. Kejahatan merupakan suatu konsepsi yang bersifat abstrak, dimana kejahatan tidak dapat diraba dan dilihat kecuali akibatnya saja.[1]

Kejahatan merupakan suatu fenomena yang kompleks yang dapat dipahami dari berbagai sisi yang berbeda, itu sebabnya dalam keseharian kita dapat menangkap berbagai komentar tentang suatu peristiwa kejahatan yang berbeda satu dengan yang lain. Timbulnya kejahatan salah satunya disebabkan karena kebutuhan yang tidak tercukupi, sehingga kejahatan akan marak di masyarakat. Kejahatan dipandang sebagai bagian dari penyimpangan sosial, artinya bahwa

[1] Wahyu Widodo, *Kriminologi Dan hukum pidana*, (Semarang: UNIVERSITAS PGRI Semarang Press, 2015), hlm 19.

Tindakan tersebut berbeda dengan tindakan-tindakan yang dipandang sebagai hal yang normal/biasa di masyarakat.[2]

Berbicara mengenai kejahatan, maka secara empiris definisi kejahatan dapat dilihat dari dua perspektif, pertama adalah kejahatan dalam perspektif yuridis, kejahatan yang dirumuskan sebagai perbuatan yang oleh negara diberi pidana. Pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu. Perbuatan atau kejahatan yang dalam ilmu hukum pidana biasa disebut dengan tindak pidana (*strafbaarfeit*). Kedua, kejahatan dalam arti sosiologis (*kriminologis*) merupakan suatu perbuatan yang dari sisi sosiologis merupakan kejahatan sedangkan dari segi yuridis (*hukum positif*) bukan merupakan suatu kejahatan. Artinya, perbuatan tersebut oleh negara tidak dijatuhi pidana.[3]

Menurut G.W. Bawengan Kejahatan merupakan delik hukum, yakni peristiwa-peristiwa yang berlawanan atau bertentangan dengan asas-asas hukum yang hidup di dalam keyakinan hidup manusia dan terlepas dari undang-undang. Kemudian, Departemen Pendidikan Nasional memberikan batasan pengertian kejahatan sebagai perbuatan yang jahat yang melanggar hukum, perilaku yang bertentangan dengan nilai dan norma yang telah disahkan oleh hukum tertulis. Suara yang lain, J.E. Sahetapy dan B. Marjono Reksodiputro dalam bukunya Paradoks Dalam Kriminologi menyatakan bahwa, kejahatan mengandung konotasi tertentu, yang

[2] Nandang Sambas, Dian Andriasari, *Kriminologi Perspektif Hukum Pidana*, (Jakarta: Sinar Grafika, 2019), hlm 42.
[3] Abdul Wahid, Mohammad Labib, *Kejahatan Mayantara (cyber crime),* (Bandung: Refika Aditama, 2005), hlm 37-38.

merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta berkaitan dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagian mayoritas atau minoritas masyarakat sebagai suatu perbuatan anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu.

Adapun menurut A.S. Alam menjelaskan definisi kejahatan dari dua sudut pandang, yaitu:

1. Dari sudut pandang hukum (*a crime from the legal point of view*). Batasan kejahatan dari sudut pandang ini adalah setiap tingkah laku yang melanggar hukum pidana.
2. Dari sudut pandang masyarakat (*a crime from the sociological point of view*). Batasan kejahatan dari sudut pandang ini adalah setiap perbuatan yang melanggar norma-norma yang masih hidup di dalam masyarakat.[4]

Kejahatan bukan saja normal, dalam arti tidak ada masyarakat tanpa kejahatan. Kejahatan merupakan sesuatu yang diperlukan, sebab ciri masyarakat adalah dinamis dan perbuatan yang telah menggerakkan masyarakat tersebut pada mulanya seringkali disebut sebagai kejahatan.

Saat ini kejahatan telah begitu berkembang pesat. Perubahan, pergeseran tersebut terlihat dari bermunculannya kejahatan-kejahatan baru yang tidak pernah terjadi sebelumnya. Perubahan sosial baik itu teknologi dan ilmu

[4] A. S. Alam, Amir Iilyas, *Pengantar Kriminologi*, (Makassar: Pustaka Refleksi Books, 2010), hlm 16-17.

pengetahuan mendorong pembaharuan hukum pidana dan undang-undang di luar hukum pidana. Pada era globalisasi modernisasi saat ini, pemikiran manusia berkembang semakin kompleks, sehingga lahirlah taraf kebudayaan yang lebih tinggi dan lahirlah karya-karya manusia yang memudahkan mereka dalam menjalani kehidupan yaitu Teknologi.

Teknologi informasi yaitu ilmu yang mencakup teknologi komunikasi untuk memproses, menyimpan data dan mengirim informasi melalui jalur komunikasi yang cepat. Menurut Haag dan Keen (1996) teknologi informasi adalah seperangkat alat yang membantu anda bekerja dengan informasi dan melakukan tugas-tugas yang berhubungan dengan pemrosesan informasi. Adapun menurut Martin (1999) teknologi informasi adalah teknologi yang tidak hanya pada teknologi computer (perangkat keras dan perangkat lunak) yang akan digunakan untuk memproses dan menyimpan informasi, melainkan mencakup teknologi komunikasi untuk mengirim atau menyebarluaskan informasi.[5]

Penggabungan antara teknologi informasi dan telekomunikasi telah menghasilakan suatu revolusi di bidang system informasi. Data atau informasi yang pada jaman dahulu harus memakan waktu berhari-hari untuk diolah sebelum dikirimkan ke sisi lain di dunia, saat ini dapat dilakukan dalam hitungan detik.

[5]TriRachmadi,https://books.google.co.id/book?id=Nor6DwAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false, 20 Maret 2023.

Pada era inilah komputer memasuki babak barunya, yaitu sebagai suatu fasilitas yang dapat memberikan keuntungan bagi masyarakat, sekaligus menjadi sarana efektif sebagai perbuatan melawan hukum, dengan terjadinya perbuatan-perbuatan melawan hukum tersebut, maka ruang lingkup hukum harus diperluas untuk menjangkau perbuatan-perbuatan tersebut.

Dimana di sisi lain pertumbuhan teknologi ini juga dapat memberikan jalan atau cara lain bagi pelaku kejahatan untuk melakukan kejahatan yang baru disebut *Cyber Crime* atau kejahatan dunia maya dengan menggunakan komputer sebagai modus operandi. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan system computer dan system komunikasi baik dalam lingkup lokal maupun global (*internet*) dengan memanfaatkan teknologi informasi berbasis system computer yang merupakan system elektronik yang dapat dilihat secata virtual.[6] Namun adanya kemunculan teknologi online tersebut justru membawa kita harus lebih waspada dan berhati-hati karena semakin tinggi pula resiko yang akan dihadapi terutama ancaman *cyber.*

Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan baru di bidang itu juga muncul, misalnya kejahatan memanipulasi data, *spionase*, sabotase, provokasi, *money laundering*, *hacking*, pencurian software maupun perusakan hardware dan berbagai macam lainnya. Perbuatan

[6] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (CYBER CRIME) Urgensi Pengaturan Dan Celah Hukumnya*, (Jakarta: PT RajaGrafindo Persada, 2013), hlm 3.

melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional.[7]

Munculnya beberapa kasus *cyber crime* atau kejahatan dunia maya di indonesia, seperti pencurian data kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program Komputer contoh beberapa kasus yang bisa kita lihat yang terjadi pada tahun 2022 yaitu kebocoran data pelanggan indihome, 1,3 miliar data registrasi SIM CARD, penyebaran data pribadi para pejabat dan tokoh public, kebocoran data KPU, daftar surat ke Presiden Indonesia.[8]

Sulawesi Selatan sendiri sudah banyak kasus yang terkait dengan kejahatan informasi data pribadi seperti kejahatan Ilegak Akses di Manggala, peretasan kartu debit dan Mastercard nasabah, pelajar SMK Retas dan Perjualbelikan Akun facebook dari Makassar dan Jawa, Pembobolan data nasabah bank BNI di Makassar oleh 2 WNA Rumania dan Scam Aplikasi modus Undangan pernikahan.

B. RUMUSAN MASALAH

Berdasarkan permasalahan kepada pelaku kejahatan infromasi data pribadi yang telah disebutkan di atas maka penulis merumuskan permasalahan yang akan dibahas yaitu :

---

[7] Ahmad Ramli, *Cyber Law Dan HAKI-Dalam System Hukum Indonesia,* (Bandung: Rafika Aditama, 2004), hlm 5.

[8] Febyola Indah, *dkk*, *Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka),* Jurnal Bidang Penelitian Informatika, Vol. 1 No. 1, 2022, hlm 5.

1. Bagaimanakah pelaksanaan proses penyidikan terhadap pelaku kejahatan informasi data pribadi di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan?
2. Apakah hambatan yang terjadi selama pelaksanaan proses penyidikan terhadap pelaku kejahatan informasi data pribadi ?

C. TUJUAN PENELITIAN

Berdasarkan permasalahan yang telah disebutkan Adapun tujuan penelitian yang ingin dicapai yaitu :

1. Untuk mengetahui bagaimana pelaksanaan proses penyidikan terhadap pelaku kejahatan informasi data pribadi di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan.
2. Untuk mengetahui cara mengatasi hambatan yang dialami selama pelaksanaan proses penyidikan terhadap pelaku kejahatan informasi data pribadi.

D. KEGUNAAN PENELITIAN

Kegunaan penelitian ini mencakup dua aspek yaitu :

1. Diharapkan penelitian ini dapat membantu masyarakat saat mengalami kejahatan informasi data pribadi.
2. Diharapkan dapat membantu aparat penegak hukum dalam mengatasi kendala yang dialami dalam pelaksanaan proses penyidikan dalam kasus kejahatan informasi data pribadi.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Cyber Crime

1. Istilah dan Pengertian Cyber Crime

Pada beberapa literature disebutkan bahwa apa yang disebut dengan kejahatan telematika itu pula yang disebut dengan kejahatan *cyber*. Hal ini didasari pada argumentasi bahwa *cyber crime* merupakan kegiatan yang memanfaatkan computer sebagai media yang didukung oleh sistem telekomunikasi sebagaimana baik itu *dial up system*, menggunakan jalur telepon, ataukah *wireless system* yang menggunakan antena khusus yang nirkabel. Konvergensi antara komputer dan sistem telekomunikasi sebagaimana di ataslah yang disebut dengan telematika. Sehingga jika menyebutkan kejahatan telematika, maka yang dimaksud juga adalah *cyber crime*. Akan tetapi disisi lain, beberapa pakar tetap berpendapat baik kejahatan computer, kejahatan *cyber*, maupun kejahatan telematika adalah kejahatan yang sama dengan penamaan yang berbeda.[9]

Tindak Pidana *cyber crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer sebagai alat, sasaran atau tempat terjadinya kejahatan dan jaringan komputer (jaringan internet sebagai medianya). Dalam arti luas, pengertian *cyber crime* adalah semua tindakan ilegal yang dilakukan melalui jaringan komputer dan internet untuk mendapatkan keuntungan dengan merugikan pihak lain. Dalam arti sempit, pengertian *cyber crime* adalah semua tindakan

[9] Maskun, *Kejahatan Siber (Cyber Crime),* (Jakarta : Kencana, 2013), hlm 45.

ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh suatu sistem komputer.

Pengertian Cyber Crime Menurut Para Ahli :

- Menurut Parker (Hamzah 1993:18), *cyber crime* adalah suatu tindakan atau kejadian yang berkaitan dengan teknologi komputer. Dimana seseorang mendapatkan keuntungan dengan merugikan pihak lain.
- Menurut Wahid dan Labib (2010:40), pengertian *cyber crime* adalah semua jenis pemakaian jaringan komputer untuk tujuan kriminal dengan penyalahgunaan kemudahan teknologi digital.
- Menurut Widodo (2011:7), pengertian *cyber crime* adalah semua kegiatan individu atau kelompok yang memakai jaringan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan.
- Menurut *Organization of European Community Development* OECD, kejahatan dunia maya atau *cyber crime* adalah semua akses ilegal terhadap suatu transmisi data. Artinya, semua kegiatan yang tidak sah dalam suatu sistem komputer termasuk suatu tindak kejahatan (Karnasudiraja, 1993:3).[10]

Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi kejahatan computer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam Bahasa inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah *"computer*

[10]Syafnidawaty,https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/,18Februari 2023.

misue", "computer abuse", "computer fraud", "computer-related crime", "computer-asside crime", atau *"computer crime".*[11]

System teknologi informasi berupa internet telah dapat menggeser paradigma para ahli hukum terhadap definisi kejahatan komputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cyber crime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber/maya* melalui system informasi yang digunakan. Jadi tidak sekedar pada komponen hardwarenya saja kejahatan tersebut dimaknai sebagai *cyber crime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh system teknologi informasi yang bersangkutan.[12]

Oleh karena itu, pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan system informasi *(information system)* itu sendiri, serta system komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya (*transmitter/originator to reciptient*).[13] Dengan demikian, kejahatan komputer dapat memiliki pelanggaran formal dan substantif. Kejahatan resmi adalah tindakan seseorang memasuki komputer orang lain tanpa izin, sedangkan kejahatan substantif adalah merugikan orang lain (dokumen keamanan aplikasi komputer dalam sistem perbankan dan aspek penyidikan dan

[11] Puslitbang Hukum dan Peradilan Mahkamah Agung RI, Naskah Akademik *Kejahatan Internet (Cyber crimes),* 2004, hlm 4.
[12] Budi Suhariyanto, *op.cit.,* hlm 10-11.
[13] Didik M. Arief Mansur dan Elisataris Ghultom, *Cyber Law-Aspek Hukum Teknologi Informasi,* (Bandung: Refika Aditama, 2005), hlm 10.

kejahatan). Kejahatan di dunia maya dapat dilakukan dimana saja dan kapan saja dengan syarat adanya jaringan yang memadai.

2. Ruang Lingkup dan Karakteristik Cyber Crime

Membahas ruang lingkup kejahatan telematika adalah hal yang sangat penting dalam rangka memberi batasan cakupan kejahatan telematika. Disadari bahwa perkembangan telematika (internet) yang begitu cepat berbanding lurus dengan modus kejahatan yang muncul. Maka dapat dikatan bahwa ruang lingkup kejahatan siber yaitu: (a) pembajakan, (b) penipuan, (c) pencurian, (d) pornografi, (e) pelecehan, (f) pemfitnahan, dan (g) pemalsuan.

Era globalisasi juga menyebabkan makin canggihnya teknologi informasi sehingga telah membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya modern yang berdampak lebih besar daripada kejahatan konvensional. Berbeda dengan kejahatan konvensional, yang bercirikan setidaknya terdiri dari beberapa hal, di antaranya penjahatnya bisa siapa saja (orang umum berpendidikan maupun orang awam berpendidikan) dan alat yang digunakan sederhana serta kejahatannya tidak perlu menggunakan suatu keahlian.

Kejahatan di bidang teknologi informasi dapat digolongkan sebagai *white colour crime* karena pelaku *cyber crime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli di bidangnya. Selain itu, perbuatan tersebut sering kali dilakukan secara transnasional atau melintasi batas negara sehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan *cyber* ini, yaitu *white colour crime* dan transnational *crime*. Modern di sini diartikan

sebagai kecanggihan dari kejahatan tersebut sehingga pengungkapannya pun melalui sarana yang canggih pula.[14]

Berdasarkan beberapa literatur serta praktiknya, *cyber crime* memiliki beberapa karakteristik, yaitu :[15]

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah *siber*/*cyber* (*cyberspace*), sehingga tidak dapat dipastikan yurisdikasi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apa pun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materil mapun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan secara transnasional melintasi batas negara.

3. Bentuk-bentuk Cyber Crime

Secara umum terdapat beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi, antara lain :

---

[14] Merry Magdalena dan Maswigrantoro Roes Setyadi, *Cyberlaw Tidak Perlu Takut,* (Yogyakarta: Andi, 2007), hlm 82.
[15] Abdul Wahid dan M. Labib, op.cit., hlm 76.

1. *Unauthorized acces to computer system and service*

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu system jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemiliki system jaringan yang dimasukinya,

2. *Illegal Contents*

   Merupakan kejahatan dengan memasukkan data informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban hukum,

3. Data *forgery*

   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet,

4. *Cyber espionage*

   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki system jaringan komputer (*computer network system*) pihak sasaran,

5. *Cyber sabotage and extortion*

   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau system jaringan komputer yang terhubung dengan internet,

6. *Offense against intellectual property*

   Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet,

7. *Infrengments of privacy*

   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data ptibadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materil maupun immaterial seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.[16]

B. Tinjauan Umum Data Pribadi

1. Pengertian dan Jenis Data Pribadi

Setiap negara menggunakan istilah yang berbeda mengenai informasi pribadi dan data pribadi. Akan tetapi, secara substantif kedua istilah tersebut memiliki pengertian yang hampir sama sehingga keduanya sering digunakan bergantian. Amerika Serikat, Kanada dan Australia menggunakan istilah informasi pribadi, sedangkan negara-negara Uni Eropa, Hong Kong, Malaysia dan juga Indonesia menggunakan istilah data pribadi.[17]

Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Dalam Pasal 1 butir 1 peraturan ini, diberikan definisi tentang "Data Pribadi" sebagai bagian dari "Data Perseorangan Tertentu".

"Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi

[16] Budi Suhariyanto, Op. Cit., hlm 15-16.
[17] Sinta Dewi, 2009, *Cyber Law: Perlindungan Privasi Atas Informasi Pribadi dalam E-commerce Menurut Hukum Internasional*, Widya Pajajaran, Bandung, hlm. 71

lainnya baik secara langsung maupun tidak langsung melalui system elektronik atau nonelektronik."

Berdasarkan Pasal 1 angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik atau Permenkominfo 20/2016 mengatur bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Data pribadi juga merupakan salah satu bagian dari hak asasi yakni hak pribadi. Selanjutnya, diuraikan bahwa data pribadi merupakan salah satu bagian dari hak pribadi (*Privacy Rights*) yang memiliki pengertian sebagai berikut:[18]

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Hal ini berarti, penggunaan setiap informasi dan data pribadi melalui media elektronik yang dilakukan tanpa persetujuan pemilik data disebut sebagai sebuah pelanggaran hak privasi.

[18] Tacino, Muhammad Jefri Maruli. *"Perlindungan Hukum Terhadap Hak Pribadi Seseorang Di Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik."* Dinamika: Jurnal Ilmiah Ilmu Hukum, 2020, hlm. 179

Jenis-jenis data pribadi sendiri telah diatur di dalam Pasal 4 Undang-Undang Perlindungan Data Pribadi, yaitu:

1) Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1) huruf a meliputi:
    a. Data dan informasi Kesehatan;
    b. Data biometric;
    c. Data genetika;
    d. Catatan kejahatan;
    e. Data anak;
    f. Data keuangan pribadi;dan/atau
    g. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
2) Data pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1) huruf b meliputi:
    a. Nama lengkap;
    b. Jenis kelamin;
    c. Kewarganegaraan;
    d. Agama;
    e. Status perkawinan;dan/atau
    f. Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Europen Union General Data Protection Regulation (GDPR) mengatur bahwa:[19]

a) *"The following personal data is considered 'sensitive' and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;*
b) *trade-union membership;*
c) *genetic data, biometric data processed solely to identify a human being;*
d) *health-related data; e) data concerning a person's sex life or sexual orientation.*

(Data pribadi berikut dianggap 'sensitif' dan tunduk pada kondisi pemrosesan tertentu:

a) data pribadi yang mengungkapkan asal ras atau etnis, pendapat politik, agama atau kepercayaan;
b) keanggotaan serikat dagng;
c) data genetik, data biometric yang diproses semata-mata untuk mengidentifikasi manusia;
d) data terkait kesehatan;
e) data mengenai kehidupan seks seseorang atau orientasi seksual.)

Selanjutnya, salah satu bentuk data yang dilindungi adalah yang berbentuk informasi elektronik sebagai sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy

[19] Oktaviani Sugiarto, 2019, *Tinjauan Hukum Internasional Terkait Perlindungan Data Pribadi*, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar, hlm. 28

atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi. Informasi elektronik ini dapat terdapat dalam sistem elektronik atau berupa sebuah dokumen elektronik.[20]

2. Asas-asas Perlindungan Data Pribadi

Dasar hokum perlindungan data pribadi ini menerangkan sejumlah asas yang menjadi dasar perlindungan data pribadi. Berdasarkan ketentuan Pasal 3 UU PDP, ada delapan asas yang menjadi landasannya, yakni :

a. Asas perlindungan,
b. Kepastian hukum,
c. Kepentingan umum,
d. Kemanfaatan,
e. Kehati-hatian,
f. Keseimbangan,
g. Pertanggungjawaban, dan
h. Kerahasiaan.

C. Proses penyidikan terhadap pelaku tindak pidana cyber crime dalam bentuk kejahatan informasi data pribadi

1. Pengaturan Tindak Pidana Cyber Crime di Indonesia

Pada umumnya proses peradilan suatu tindak pidana didasarkan pada KUHAP sebagai hukum acara yang berisi tata tertib proses penyelesaian atau penanganan perkara pidana yang dimuat dalam KUHP. KUHAP dan KUHP

[20] Pasal 1 ayat 8 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

sendiri merupakan *leg generalis* dalam hukum pidana. Artinya apabila terdapat undang-undang lain diluar KUHAP dan KUHP yang dimiliki hukum acara khusus dan sanksi pidana yang spesifik, maka ketentuan tersebut berlaku secara *lex specialis.* Berpedoman pada asas *lex specialis,* hukum acara yang berlaku dalam proses peradilan pidana terkait kasus *cyber crime* dalam bentuk kejahatan terhadap informasi data pribadi tetap merujuk pada ketentuan dalam KUHAP.

Selain mengatur tindak pidana siber materil, UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE . Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain:

a. Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika
b. Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data;
c. Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana;
d. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.[21]

[21] Josua Sitompul, https://www.hukumonline.com/klinik/a/landasan-hukum-penanganan-icybercrime-i-di-indonesia-cl5960, 20 Februari 2023.

Seperti yang disebutkan juga dalam Pasal 64 ayat (2) Undang-undang Perlindungan Data Pribadi bahwa "Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses peradilan Perlindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan". Bedanya hanya dari segi penangkapan tersangka dan dibutuhkan Kerjasama dengan beberapa unit khusus, selain itu penanganan penyidikan *cyber crime* juga lebih rumit karena memerlukan kordinasi yang bersifat komprehensif dengan instansi-instansi lain yang berkaitan dengan tindak pidana tersebut.

2. Proses Penyidikan

Adapun rangkaian-rangkaian kegiatannya yaitu :

1. Penyelidikan

Dalam tahap ini petugas menerima informasi atau laporan dari masyarakat tentang adanya suatu peristiwa yang diduga terdapat pidananya sehingga dapat dibuatkan laporan polisi. Kemudian penyidik melakukan pengumpulan barang bukti dan saksi-saksi yang terkait dalam kasus *cyber crime* tersebut, hal ini penyidik mengalami kesulitan dalam hal pembuktian. Banyak saksi maupun tersangka yang susah untuk di identifikasi keberadaannya, sehingga untuk melakukan pemeriksaan maupun penindakan sangat sulit, belum lagi kendala masalah bukti yang amat rumit dikarenakan terkait dengan teknologi informasi ataupun kode-kode digital yang membutuhkan SDM serta peralatan computer forensic yang baik dan cukup canggih.

Dalam kasus kejahatan terhadap informasi data pribadi adapun alat bukti yang telah di sebutkan dalam Undang-undang Perlindungan Data Pribadi dalam Pasal 64 ayat (3) meliputi :

a. Alat bukti sebagaimana dimaksud dalam hukum acara;dan
b. Alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Seperti yang disebutkan diatas bahwa alat bukti yang sah dalam UU PDP yang disebutkan dalam KUHAP dan dalam UU ITE yaitu :

Alat bukti pada KUHAP diatur dalam Pasal 184 ayat (1) :

(1) Alat bukti yang sah ialah :

a. Keterangan saksi
b. Keterangan ahli
c. Surat
d. Petunjuk
e. Keterangan Terdakwa.

Alat bukti dalam UU ITE diatur dalam Pasal 5 ayat (1) dan ayat (2) UU ITE, yang menyebutkan:

1. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari

alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

2. Penindakan

Dalam tahap ini penyidik sering mengalami hambatan dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sendiri sulit untuk dipastikan dikarenakan bisa saja tersangka menggunakan komputer atau ponsel yang bukan miliknya bahkan semakin sulit apabila tersangka menggunakan komputer yang ada di warnet seperti kita ketahui bahwa komputer yang ada di warnet sendiri digunakan oleh orang banyak belum lagi apabila tersangka menggunakan identitas palsu untuk memasuki situs tempat menyimpan data milik korban, sehingga diperlukan pelacakan lebih jauh untuk mendapatkan IP Address dari pelaku maupun komputer yang digunakan.

3. Pemeriksaan

Dalam tahap ini melakukan digital forensic pada barang bukti yang telah dikumpulkan oleh penyidik. Pemeriksaan ini dilakukan oleh ahli-ahli dalam kasus *cyber crime* yang terkait dengan ahli infomasi dan transaksi elektronik dan ahli digital forensik. Digital forensic merupakan bagian dari ilmu forensic yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital seperti komputer, handphone, tablet, PDA, *networking devices,* dan sejenisnya.[22]

[22] Mulqadrin Adam,*dkk*., *Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan*, Vol 2 Nomor 3, Journal of Lex Generalis (JLG), 2021, hlm 1108.

Adapun 3 (tiga) kelompok sebagai pelaku digital forensic, yaitu :

a. *Collection Specialist*, yang bertugas sebagai pengumpul barang bukti yang berupa digital evidence,
b. *Examiner*, yang memiliki kemampuan sebagai penguji terhadap media dan untuk mengekstrak data,
c. *Investigator*, yang memiliki keahlian sebagai penyidik.

Dalam tahap ini juga penerapan pasal-pasal yang dapat dikenakan dalam kasus *cyber crime* terutama dalam kasus *cyber crime* yang berkaitan dengan data pribadi dimana telah ada aturan atau undang-undang yang telah dibuat yaitu undang-undang perlindungan data pribadi yang dapat dijadikan sebagai landasan dalam menerapkan sanksi pidana kepada tersangka tetapi tidak hanya itu penerapan undang-undang informasi dan teknologi elektronik juga bisa diterapkan apabila melanggar aturan yang ada didalamnya.

Untuk alat bukti sendiri yaitu saksi sulit untuk ditemukan dikarenakan pada saat kejahatan terjadi atau berlangsung tidak ada satupun saksi yang melihat. Mereka hanya mengetahui selang waktu yang cukup lama setelah kejadian terjadi atau berlangsung dikarenakan tampilan data yang tidak berubah maupun tidak berfungsi.

4. Penyelesaian berkas perkara

Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena belum samanya persepsi diantara aparat penegak hukum. Barang bukti digital adalah

barang bukti dalam kasus *cyber crime* yang belum memiliki rumusan yang jelas dalam penentuannya sebab digital evidence tidak selalu dalam bentuk fisik yang nyata.

Karena dalam kasus *cyber crime* barang bukti utamanya adalah computer tetapi computer hanya merupakan fisiknya sedangkan yang dibutuhkan atau yang utamanya adalah data di dalamnya yang berbentuk file, yang apabila dibuat nyata dengan print membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut bentuk *compact disck* saja, hingga saat ini belum ada Undang-undang yang mengatur mengenai bentuk dari pada barang bukti digital (*digital evidence*) apabila dihadirkan sebagai barang bukti di persidangan.[23]

Dari tahap-tahap yang telah disebutkan diatas masih banyak halangan atau hambatan yang dihadapi oleh pihak penyidik terutama dalah tahap penyelidikan dan penindakan dimana proses tersebut membutuhkan waktu yang lama untuk mendeteksi keberadaan pelaku dan pengadaan saksi.

Dari pembahasan yang telah dijelaskan meskipun dasar dalam pemberian sanksi pidananya menggunakan system Undang-undang Perlindungan Data Pribadi, namun pelaksanaannya tidak terlepas dari KUHAP sebagai salah satu payung hukum yang menjadi acuan dalam penyelesaian perkara pidana khususnya dalam kasus *cyber crime* atau kejahatan di dunia maya.

[23] Sartika Renni, *dkk*., *Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime,* Vol 5, Jurnal Aktual Justice, 2020, hlm 46.

D. Kendala yang dialami penyidik dalam melakukan penyidikan terhadap pelaku tindak pidana Cyber crime dalam bentuk kejahatan informasi data pribadi

Efektivitas berlakunya aspek pidana dalam Undang-undang Perlindungan Data Pribadi dan Undang-undang informasi dan teknologi elektronik dapat dilihat dari aspek substansi dan struktur hukumnya yang meliputi penegak hukum, sumber aparatur penegak hukum serta peran masyarakat dalam konteks penegakan hukum dan juga harus didukung sarana dan prasarana yang memadai agar penegak hukum dengan teknologi informasi pemerintah terwujud.

Dalam upaya penanggulangan *cyber crime* atau kejahatan di dunia maya oleh aparat penegak hukum terkadang masih mengalami hambatan seperti :

a. Dalam tahap penyidikan banyak kendala ataupun hambatan yang dialami oleh tim penyidik terutama dalam tahap penangkapan tersangka dimana hasil pelacakan paling jauh hanya dapat menentukan IP Address dari pelaku dan komputer yang digunakan tetapi belum menemukan tersangkanya belum lagi hal ini semakin sulit apabila menggunakan komputer di warnet dan tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Tidak hanya itu terkadang data yang disimpan secara komputerisasi tersebut tidak diubah oleh tersangka yang dimana akan susah untuk menentukan apakah data tersebut telah dicuri atau tidak.

b. Penyitaan Alat bukti dalam kasus *cyber crime* berbeda dengan alat bukti kejahatan lainnya dimana sasaran atau media *cyber crime* merupakan data-data atau system komputer/internet,[24] sehingga apabila pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat jejak pelaku sulit ditemukan dikarenakan adanya program yang telah dibuat oleh tersangka yang digunakan untuk menghapus system yang digunakan tersangka setelah melakukan *hacking*.
c. Faktor lainnya yaitu faktor teknologi juga menjadi hambatan dikarenakan kemajuan teknologi informasi dimana sarana dan prasana serta fasilitas peralatan canggih dan maju yang dibutuhkan ada saat ini khusunya mengenai data elektronik dari suatu pembuktian tindak pidana *cyber crime* dalam bentuk kejahatan terhadap data pribadi.
d. Sulit memperoleh saksi, dimana dalam kasus *cyber crime* berperan sangat penting dimana jarang sekali terdapat saksi dalam kasus *cyber crime* dikarenakan saksi korban yang tidak menyadari adanya kejahatan yang terjadi pada saat itu yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan.
e. Kurangnya kemampuan penyidik khususnya pada aparat kepolisian dalam menguasai teknologi komputer.

Seperti yang kita ketahui saat ini sangat banyak orang atau masyarakat yang sering mendaftar pada suatu aplikasi atau website yang bahkan tidak ketahui apakah aplikasi atau website tersebut aman dan juga banyaknya orang atau

[24] Mulqadrin Adam,*dkk*., op.cit., hlm 1113.

masyarakat yang tiba-tiba mendapatkan sebuah notifikasi bahwa mereka telah terdaftar pada suatu aplikasi atau website yang mereka sendiri tidak pernah daftar.

Karena ketidaktahuan masyarakatlah yang mengakibatkan semakin tinggi kasus *cyber crime* terutama dalam bentuk kejahatan terhadap data pribadi. Sehingga diharapkan kepada pemerintah maupun non pemerintah, aparat penegak hukum dapat membantu masyarakat atau memberikan arahan kepada masyarakat apabila hal tersebut terjadi.

BAB III

METODE PENELITIAN

A. Lokasi Penelitian

Lokasi penelitian ini dilakukan di Kepolisian Daerah Sulawesi Selatan dan Fakultas Teknik Informasi Universitas Bosowa. Untuk pemilihan lokasi ini didasarkan atas beberapa pertimbangan yaitu telah terjadi kasus tindak pidana *Cyber crime*, termasuk pada pengumpulan data yang dibutuhkan oleh peneliti.

B. Tipe Penelitian

Penelitian ini menggunakan penelitian hukum normatif empiris ini pada dasarnya merupakan penggabungan antara pendekatan hukum normatif dengan adanya penambahan berbagai unsur empiris. Metode penelitian normatif-empiris mengenai implementasi ketentuan hukum normatif (undang-undang) dalam aksinya pada setiap peristiwa hukum tertentu yang terjadi dalam suatu masyarakat.

C. Jenis dan Sumber Data

Penelitian ini didasarkan kepada bahan hukum primer dan sekunder, yaitu penelitian yang mengacu kepada norma-norma yang terdapat dalam peraturan perundang-undangan. Dalam penelitian ini tulisan yang menggunakan pendekatan normative empiris, maka bahan hukum yang digunakan diperoleh melalui penelusuran bahan hukum atau studi pustaka terhadap bahan hukum primer dan sekunder.

a) Bahan hukum primer yang digunakan yaitu:

- Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,
- Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi,
- Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

b) Bahan sekunder berupa jurnal ilmiah, buku-buku, artikel penelitian dan hasil penelitian maupun makalah dengan pembahasan yang berhubungan *cyber crime* dalam bentuk kejahatan terhadap data pribadi.

D. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan yaitu:

a) studi keperpustakaan dengan fokus pada peraturan perundang-undangan, hasil penelitian, jurnal ilmiah dan artikel ilmiah serta kasus-kasus hukum yang digunakan.

b) Wawancara (Interview) yaitu dengan mengadakan komunikasi langsung kepada informan untuk mengumpulkan data untuk memenuhi tujuan

penelitian. Dalam penelitian ini peneliti akan mewawancarai salah satu anggota dari Tim Penyidik Cyber Polda Sulsel dan Ahli IT.

E. Teknik analisis data

Teknik analisis yang digunakan adalah Analisis deskriptif adalah jenis analisis data yang digunakan untuk menggambarkan, menampilkan, dan meringkas sekumpulan data. Pada data kualitatif, teknik analisis ini berupa proses mendeskripsikan, menggambarkan, menganalisis serta meringkas kejadian atau fenomena yang diteliti. Teknik pengumpulan datanya pun dilakukan dengan proses wawancara. Teknik analisis deskriptif ini bertujuan untuk menggambarkan secara untuk dan mendalam terkait fenomena yang diteliti.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Pelaksanaan Proses Penyidikan Terhadap Pelaku Kejahatan Informasi Data Pribadi Di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan

Berdasarkan data yang diperoleh hasil penyelidikan mengenai Kasus Kejahatan Informasi Data Pribadi di Wilayah Hukum Kepolisian Daerah Sulawesi selatan tahun 2021 s.d. 2023 oleh Ditreskrimsus pada table berikut:

Tabel 1

Jumlah Kasus Tindak Pidana Kejahatan Informasi Data Pribadi di Kota Makassar Tahun 2021-2023

Tahun	Kasus Tindak Pidana Informasi Data Pribadi	%
2021	9 Kasus	28%
2022	13 Kasus	40%
2023	10 Kasus	32%
Jumlah Total	**32 Kasus**	**100%**

Sumber : Ditreskrimsus Polda Sulsel Tahun 2021 s.d. 2023

Pada tahun 2021 jumlah penyidikan yang dilaksanakan oleh tim pidana khusus *cyber crime* oleh satuan kerja Ditreskrimsus Polda Sulsel berjumlah 9 kasus dengan presentase 28% di tahun berikutnya yaitu tahun 2022 menjadi naik sebanyak 13 kasus dengan presentase 40% dimana pada tahun tersebut semakin banyak kasus yang terjadi mengenai informasi data pribadi yang tersebar bahkan

dijual dan pada tahun 2023 dimulai pada bulan januari sampai dengan bulan juli sebanyak 10 kasus dengan presentase 32% .

Menurut keterangan Udiyanto bahwa kasus yang paling sering ditangani adalah kasus penipuan lewat media sosial dan peretasan akun yang kemudian mengambil seluruh data yang dibutuhkan oleh pelaku untuk mendapatkan keuntungan dari korban. Kerugian yang paling banyak dialami oleh korban sejauh ini yaitu kerugian berupa materil maupun immaterial.[25]

Korban tindak pidana *cyber crime* dalam kasus kejahatan informasi data pribadi tidak hanya individu tetapi ada juga kelompok Masyarakat maupun badan usaha. Kebanyakan korban lalai karena tidak mengetahui perbuatannya, seperti tidak menutup akun pribadinya dan mengklik link yang ada sehingga hal tersebut mengakibatkan korban tanpa sadar memberi akses kepada pelaku untuk mejelajahi maupun mengambil alih akun sang korban, hal seperti ini juga bisa terjadi jika ponsel atau laptop korban dicuri dan data yang tersimpan kemudian digunakan untuk melakukan kejahatan atau *carding* yang umum dikenal. Bahkan ada korban dari tindak pidana kejahatan infromasi data pribadi yang tidak melaporkan kasusnya kepada pihak yang berwajib atau memilih menyelesaikannya sendiri.

1. Tahapan Penyidikan Kepolisian Daerah Sulawesi Selatan dalam Kasus Kejahatan Informasi Data Pribadi

Menurut Udiyanto bahwa Pada dasarnya proses peradilan suatu tindak pidana mengikuti KUHAP sebagai hukum acara yang digunakan dalam

[25] Hasil Wawancara dengan Bripka Udiyanto Selaku Banit 1 Subdit 5 Tipidsiber Ditreskrimsus Polda Sulsel Pada Tanggal 18 Juli 2023

penyelesaian suatu kasus tindak pidana, tetapi dalam kasus *cyber crime* terkhusus kejahatan informasi data pribadi sendiri telah dibuatkan suatu undang-undang yang dapat dijadikan dasar dalam proses penyelesaian kasus tindak pidana pencurian data pribadi yaitu Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi, dimana di dalamnya telah disebutkan dalam pasal 64 ayat (2) bahwa "Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses peradilan perlindungan data pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan".

Menurut udiyanto dalam melakukan penyelidikan didasarkan pada Undang-Undang Perlindungan Data Pribadi dan KUHAP dalam proses penyidikan.[26]

1. Adanya laporan dari masyarakat,

   Laporan Masyarakat atau Upaya pasif yang dilakukan kepolisian dengan menerima laporan dari Masyarakat yang menjadi korban atau dirugikan dengan adanya penyalahgunaan data pribadi kemudian melakukan penyelidikan dan penyidikan terhadap pelaku kejahatan data pribadi.

2. Penyidik melakukan pencarian dan pemeriksaan saksi dan alat bukti yang terkait dengan kejahatan informasi data pribadi,

   Dalam tahap ini penyidik sering mengalami beberapa hambatan seperti yang disampaikan oleh Udiyanto bahwa dalam proses pencarian

[26] Hasil Wawancara dengan Bripka Udiyanto Selaku Banit 1 Subdit 5 Tipidsiber Ditreskrimsus Polda Sulsel Pada Tanggal 18 Juli 2023

saksi membutuhkan waktu yang sangat lama dikarenakan dalam proses kejahatannya tidak ada yang melihat selama terjadinya kejahatan secara langsung dan terkait dengan barang bukti yang bukan milik pelaku, dalam hal ini maka yang diperiksa terlebih dahulu adalah pemegang alat tersebut, kemudian diambil keterangannya sebagai keterangan saksi.

Kejahatan yang terjadi saat ini banyak yang dilakukan oleh pelaku melalui *website* atau *link* maka tidak dapat dijadikan barang bukti dan tidak dapat disita karena bersifat maya dan dapat berubah-ubah atau dihapus. Seperti yang disebutkan dalam pasal 5 angka (1) UU ITE bahwa "informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetak merupakan alat bukti hukum yang sah". Sebuah website atau link dapat dijadikan sebagai bukti dapat dilakukan seperti berikut :

a. *Website* atau *link* merupakan Informasi Elektronik dan/atau Dokumen Elektronik yang hanya dapat dibaca menggunakan Sistem Elektronik, namun untuk memudahkan pengumpulan barang bukti dapat disita dengan melakukan tangkapan layar dan/atau mencetak langsung *website* atau *link* yang digunakan pada lembaran kertas, hal tersebut sesuai denga bunyi Pasal 5 angka (1) UU ITE berbunyi "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah".

b. Melakukan pengambil alihan akun dilakukan dengan cara merubah *login* (mengambil alih *website* atau *link*) kemudian dituangkan dalam berita acara.
c. Melakukan *Download* isi *website* atau *link* dan meletakkan kedalam alat penyimpanan data berupa *Flashdisk*, *Harddisk*, dan lain-lain.
d. Melakukan Pengujian Laboratorium Forensik terhadap *device* untuk menetapkan jejak-jejak *website* atau *link* pada *device* yang digunakan.

Untuk pembuktian di persidangan sendiri apabila bukti dalam bentuk flashdisk, harddisk dan lain-lainnya maka untuk membuktikan keotentikannya maka para Ahli IT ataupun Ahli Forensik akan melakukan sumpah.

Ketika berhadapan dengan kejahatan dunia maya aparat penegak hukum harus memperhatikan bukti digital yang digunakan sebagai faktor dalam melakukan perbuatannya. Karena bukti digital memiliki status yang sangat penting untuk proses pembuktian di pengadilan. Tentang alat Bukti digital juga akan menentukan tindakan apa yang diambil terdakwa bersalah atau tidak menurut hukum.

3. Dilakukan gelar perkara,

Gelar perkara dilakukan untuk menentukan tersangka yang dilakukan dengan sangat hati-hati dan teliti serta didukung dengan keterangan para saksi dan barang bukti yang kuat.

Gelar perkara menurtu pasal 1 angka 17 Peraturan Kepala Badan Reserse Kriminal Nomor 4 Tahun 2014 adalah kegiatan penyampaian penejelasan tentang proses atau hasil penyelidikan oleh penyidik kepada peserta gelar perkara dalam bentuk diskudi kelompok untuk mendapatkan tanggapan/masukan/koreksi dalam rangka menghasilkan rekomendasi untuk menentukan tindaklanjut proses penyidikan.

Ada tiga tahapan dalam gelar perkara :

1) Awal proses penyidikan;
2) Pertengahan proses penyidikan; dan
3) Akhir proses penyidikan.

Dari proses gelar perkara tersebut penyidik dapat melakukan penetapan tersangka. Tersangka sendiri memiliki pengertian yang disebutkan dalam Pasal 1 butir 14 KUHAP yaitu Tersangka adalah seorang yang karena perbuatannya atau keadaannya, berdasarkan bukti permulaan patut diduga sebagai pelaku tindak pidana, yakni minimal 2 alat bukti yang disebut dalam pasal 184 KUHAP.

Dalam mencari pelaku atau yang telah ditetapkan sebagai tersangka ada beberapa kendala yang dihadapi tim *cyber* :

- dimana sulitnya melakukan *profiling* terhadap pelaku karena jejak data elektronik yang ditinggalkan. Menurut Abdillah, *Profiling* sama dengan mengumpulkan data mengenai informasi pribadi seseorang, biasanya profiling sendiri di IT dibagian digital marketing dipakai untuk

menampilkan hal-hal yang interestik yang berhubungan dengan seseorang.[27]

- pelaku mudah menghilangkan jejak dengan menghilangkan alat yang digunakan untuk melakukan perbuatannya,
- pelaku bertempat tinggal ditempat yang sulit dijangkau, diluar provinsi, atau bahkan diluar negeri.

4. Penyidik melakukan pemeriksaan terhadap barang bukti digital di Lab. Forensik

   Ditahap ini semua barang bukti digital yang telah disita oleh penyidik diperiksa oleh ahli IT di mini Lab.Siber di *Cyber crime* Ditreskrimsus Polda Sulsel dimana para Ahli IT yang melakukan pemeriksaan barang bukti digital telah bersertifikat dari luar negeri.

   Biasanya dalam pemeriksaan barang bukti digital untuk mencari pelaku diutamakan pada *device* atau alat yang digunakan dengan menganalisis jejak-jejak elektronik hingga menemukan *device* oleh tim. Dimana hanya *provider* telekomunikasi dan polisi karena yang dilacak adalah kode *IMEI* dan *MAC Addrees*.

5. Pemeriksaan oleh para ahli dalam kasus *cyber crime*

   Pada Pasal 120 KUHAP disebutkan apabila dianggap perlu oleh penyidik, ia dapat meminta bantuan pendapat seorang ahli atau orang yang memiliki keahlian khusus untuk membantu proses penyidikan. Menurut Udiyanto bahwa dalam penyidikan terutama dalam kejahatan data pribadi

[27] Hasil Wawancara dengan salah satu Ahli IT universitas Bosowa yaitu Bapak Abdillah Sas. S.Kom.,M.Pd. Pada Tanggal 25 Juli 2023

yang dibutuhkan bukan hanya ahli IT tetapi tetap dibutuhkan ahli lain yang berkompetensi untuk menguji keaslian data seperti Ahli Forensik Cyber, ahli pidana untuk menentukan jenis pidana yang terjadi dan instansi terkait yang dapat menjelaskan data pribadi secara formil.[28]

6. Penyidik mengirim berkas perkara kepada jaksa penuntut umum

   Apabila penyidikan telah dianggap selesai dan telah dituangkan dalam bentuk berkas perkara maka penyidik wajib menyerahkan tersangka dan barang bukti ke jaksa penuntut umum.

2. Penerapan Sanksi Pidana dalam Kasus Kejahatan Informasi Data Pribadi

Salah satu cara untuk memerangi kejahatan masyarakat seperti kejahatan siber adalah dengan menggunakan instrumen hukum pidana, yang berarti memberikan sanksi pidana kepada pelaku tindak pidana yang termasuk dalam kategori kejahatan siber. Tindak pidana siber atau kejahatan siber dalam kasus yang menyangkut data pribadi yang secara khusus sanksi pidananya telah diatur dalam Undang-undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan perundang-undangan lainnya :

a) Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi

   Sebagaimana telah diatur berbagai macam hal di dalamnya terkait dengan larangan dan ketentuan pidana dalam informasi data pribadi :

[28] Hasil Wawancara dengan Bripka Udiyanto Selaku Banit 1 Subdit 5 Tipidsiber Ditreskrimsus Polda Sulsel Pada Tanggal 18 Juli 2023

1) Pasal 67 ayat (1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah), (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah), (3) Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.00O.OOO.000,00 (lima miliar rupiah).

b) Undang-Undang No 11 Tahun 2008 jo Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Prinsipnya, UU ITE mengatur perlindungan data pribadi, tetapi karena bentuknya yang tidak jelas, seringkali dianggap tidak mengatur tentang perlindungan data pribadi. Data pribadi dalam bentuk elektronik yang disimpan, ditransfer, atau ditransmisikan adalah subjek UU ITE, jadi jelas

sangat luas. Karena itu, UU ITE menetapkan beberapa aturan yang secara tidak langsung melindungi data pribadi yaitu :

1) Pasal 46 ayat (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah). (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).
2) Pasal 47 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).
3) Pasal 48 ayat (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun

dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah). (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

4) Pasal 50 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pemberian sanksi pidana dalam hal agar pelaku jera akan kejahatan yang dilakukannya belum tentu dapat mengganti kerugian yang dialami oleh korban. Adapun pertanggungjawaban yang dapat dilakukan oleh pelaku dengan mengganti semua kerugian yang dialami oleh korban dimana sesuai dengan Surat Keputusan Bersama yang ditandatangani oleh Menteri Komunikasi dan informatika, Kapolri, dan Jaksa Agung Tentang Pedoman Kriteria Implementasi UU ITE.[29] Hanya dengan demikian pertanggungjawaban pidana akan dipertimbangkan.[30]

[29] Kurniawan Prasatya Atmanagara, Mustawa Nur, Muhammad Halwan, *Analisis Hukum Pertanggung Jawaban Pidana Terkait Berita Bohong Menurut Undang-Undang Informasi Dan Transaksi Elektronik Di Polda Sulawesi Selatan,* Vol 20 Nomor 3, Clavia: Journal Of Law, 2022, hlm 334.

[30] Sahiruddin, Ruslan Renggong, Basri Oner, *Analisis Hukum Tindak Pidana Kelalaian Mengemudikan Kendaraan Bermotor Mnegdampakkan Orang Lain Meninggal Dunia (Studi Kasus Putusan Pengadilan Negeri Maros No.48/Pid.Sus/2020/PN.Mrs),* Vol 10 No.3, Clavia: Journal Of Law, 2022, hlm 399.

Tabel 2

Pedoman Kriteria Implementasi UU ITE

No	UU ITE	PEDOMAN IMPLEMENTASI
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 a. Pasal 36 UU ITE dapat digunakan dalam hal korban kejahatan yang melanggar Pasal 27 sampai dengan Pasal 34 UU ITE mengalami kerugian materiil yang nyata. b. Kerugian tersebut hanya untuk kerugian langsung atas perbuatan yang dilakukan, bukan kerugian tidak langsung, bukan berupa potensi kerugian, dan bukan pula kerugian yang bersifat nonmateriil. c. Kerugian materiil tersebut terjadi pada korban, baik korban orang perseorangan atapun badan hukum. d. Sebagai delik materiil maka kerugian tersebut harus dihitung dan ditentukan nilainnya. e. Nilai kerugian materiil 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).

Sumber : Surat Keputusan Bersama Menteri Komunikasi dan Informatika, Jaksa Agung Republik Indonesia, dan Kepala Kepolisian Negara Republik Indonesia

B. Hambatan Yang Terjadi Selama Proses Penyidikan Terhadap Pelaku Kejahatan Informasi Data Pribadi

Menurut udiyanto dalam proses penyidikan tentu ada beberapa hambatan yang dialami oleh tim penyidik yang tentunya tidak bisa dihindari. Hambatan yang dialami seperti :

1. Sarana dan prasarana

   Sarana dan prasarana yang tidak memadai merupakan salah satu hambatan dalam penyelidikan. Sarana dan prasarana sendiri merupakan hal terpenting dalam pencarian bukti dan pelaku. Dalam pelaksanaan penegkan hukum dalam kasus kejahatan informasi sendiri membutuhkan alat yang lebih canggih dikarenakan perkembangan teknologi yang semakin berkembang dan pengguna yang semakin banyak. Dalam hal pencarian bukti sendiri terkadang masih susah untuk ditemukan dikarenakan titik lokasi alat itu sendiri yang berpindah-pindah apabila pelaku menggunakan alat yang bukan miliknya tidak hanya itu alat bukti yang berupa data atau sistem tentu saja juga sangat mudah untuk dihilangkan dengan cara dihapus, sedangkan dalam pencarian pelaku yang bisa saja menggunakan akun yang bukan miliknya atau akun palsu dimana untuk bisa mengakses suatu akun tentu membutuhkan waktu yang lama sehingga dibutuhkan suatu teknologi yang bisa digunakan untuk mempercepat dalam pencarian pelaku maupun alat bukti. Dalam beberapa kasus, penyelidik mungkin tidak dapat menangani kekurangan alat dan struktur canggih untuk mendukung proses penyelidikan.[31] Dengan pemenuhan alat-alat yang lebih canggih dan lebih baik diharapkan dapat menghilangkan hambatan yang ada.

[31] Nur Rahma Indah, Abd. Haris Hamid & Siti Zubaidah, *Penyidikan Tindak Pidana Skimming Dalam Transaksi Elektronik Oleh Kepolisian Daerah Sulawesi Selatan,* Vol 19 Nomor 3, Clavia: Journal Of Law, 2021, hlm 350.

2. Kemampuan penyidik

   Berbagai cara yang dilakukan penyidik dalam pengungkapan kejahatan informasi data pribadi tetapi masih kurangnya kemampuan dan kualitas penyidik yang dimana tentu saja pemahaman akan kejahatan informasi data pribadi dan teknologi dibutuhkan oleh penyidik yang menangani kasus tersebut. Dalam peningkatan penyidik sendiri dapat dilakukan dengan cara memberikan pelatihan untuk meningkatkan kemampuan dan kualitas penyidik.

3. Masyarakat

   Kurangnya pengetahuan dan pemahaman masyarakat terkait dengan kejahatan yang semakin meningkat dengan modus-modus terbaru yang tentunya menggunakan teknologi canggih terutama kejahatan yang bersangkutan dengan informasi data pribadi dimana sekarang semua aplikasi yang digunakan oleh Masyarakat tentu saja harus melalui pendaftaran yang wajib di isi dengan informasi yang terkait dengan data pribadi dan tentu saja sekarang dibutuhkan verifikasi dengan cara mengkil suatu link atau website yang dikirimkan setelah melakukan pendaftaran. Dengan ketidaktahuan Masyarakat tersebut memberikan peluang atau akses kepada pelaku untuk dapat mengambil maupun mencuri data milik Masyarakat. Sehingga pelaku dalam melakukan kejahatannya sendiri tidak harus bertemu dengan korban tetapi bisa dilakukan dengan jarak antara pelaku dan korban yang sangat jauh.

4. Korban

Banyaknya korban yang masih enggan untuk melaporkan kejahatan yang dialami karena ketidaktahuan korban mengenai kejahatan yang sudah terjadi. Kejahatan *cyber crime* sendiri memang sering terjadi tanpa diketahui oleh korban bahkan saat kejahatanpun terjadi tidak ada yang melihat atau tidak ada saksi. Kebanyakan korban akan menyadari setelah memeriksa atau data informasi yang digunakan korban tidak dapat digunakan dan hilang atau tidak dapat dideteksi.

5. Pelaku

   Pelaku yang sangat mengerti dengan perkembangan teknologi yang menjadi salah satu hambatan bagi penyidik dalam pencarian pelaku dan pelaku yang menggunakan identitas palsu atau identitas orang lain tidak hanya itu tetapi juga pelaku dapat menghilangkan data atau sistem yang digunakan untuk memasuki, mengambil atau mencuri data informasi yang dibutuhkan untuk melakukan kejahatan.[32]

Dari beberapa hambatan yang telah disebutkan di atas dapat membuat proses penyelidikan menjadi lebih lama dalam menyelesaikan kasus dan kegiatan pihak kepolisian dalam menangani kejahatan cyber crime, maka dengan melakukan Pemenuhan atas hambatan yang telah disebutkan agar segera diatasi agar dalam pelaksanaan penegakan hukum dapat dilakukan dengan cepat dan lancar.

[32] Hasil Wawancara dengan Bripka Udiyanto Selaku Banit 1 Subdit 5 Tipidsiber Ditreskrimsus Polda Sulsel Pada Tanggal 18 Juli 2023

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan :

Berdasarkan uraian hasil penelitian, maka penulis dapat menarik kesimpulan sebagai berikut:

1. Bahwa dalam tahap pelaksanaan proses penyidikan mengenai kasus yang terkait dengan informasi data pribadi dalam pelaksanaannya belum sepenuhnya terlaksana.
2. Dalam pelaksanaan proses penyidikan sendiri masih ada hambatan yang dialami oleh tim tim penyidik terutama dalam mengungkap pelaku dimana dalam mengungkap pelaku tim *cyber* POLDA SULSEL melakukan Upaya secara aktif dengan cara melakukan Patroli *Cyber* untuk mencari pelaku kejahatan data pribadi melalui media-media online yang dilakukan oleh Tim Patroli *Cyber*, melakukan pengumpulan informasi, serta penyelidikan dan penyidikan terhadap pelaku kejahatan data pribadi dan pasif dilakukan dengan menerima laporan masyarakat yang menjadi korban atau dirugikan dengan adanya penyalah gunaan data pribadi kemudian melakukan penyelidikan dan penyidikan terhadap pelaku kejahatan data pribadi, barang bukti yang susah ditemukan karena kurangnya sarana dan prasarana yang tersedia, korban yang masih enggan dalam melaporkan kejahatan dikarenakan ketidaktahuan akan kejahatan yang terjadi maupun pelaku yang semakin pintar dalam menggunakan teknologi. Dari hambatan yang ada selama proses

penyelidikan mengakibatkan waktunya semakin lama untuk menyelesaikan kasus.

B. Saran

1. Disarankan kepada penyidik dalam mengatasi hambatan yang ada dengan pembaharuan sarana dan prasarana yang ada dan lebih menguasai serta meningkatkan kemampuan penyidik terkhusus yang berkaitan dengan kejahatan cyber crime.
2. Masyarakat yang dalam menggunakan teknologi agar selalu berhati-hati dalam menyebarkan infromasi pribadi dan lebih sering mengupdate atau mencari tahu kejahatan yang sering terjadi.
3. Melakukan Kerjasama dengan beberapa instansi yang terkait dengan kejahatan yang terjadi.

DAFTAR PUSTAKA

BUKU

Abdul Wahid & Muhammad Labib, 2005, *Kejahatan Mayantara (CyberCrime)*, Refika Aditama, Bandung.

A.S. Alam & Amir Ilyas, 2010, *Pengantar Kriminologi,* Pustaka Refleksi Books, Makassar.

Ahmad Ramli, 2004, *Cyber Law dan HAKI-Dalam System Hukum Indonesia,* Rafika Aditama, Bandung.

Budi Suharriyanto, 2013, *Tindak Pidana Teknologi Informasi (CYBERCRIME) Urgensi Pengaturan dan Celah Hukumnya,* PT RajaGrafindo Persada, Jakarta.

Didik M. Arief Mansur & Elisataris Ghultom, 2005, *Cyber Law Aspek Indonesia Teknologi Informasi,* Rafika Aditama, Bandung.

Maskun, 2013, *Kejahatan Siber (Cyber Crime),* Kencana, Jakarta.

Merry Magdalena & Maswigantoro Roes Seiyadi, 2007, *Cyber Law Tidak Perlu Takut,* Andi, Yogyakarta.

Nandang Sambas & Dian Andriasari, 2019, *Kriminologi Perspektif Hukum Pidana,* Sinar Grafika, Jakarta.

Sinta Dewi, 2009, *Cyber Law: Perlundingan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional,* Widya Pajajaran, Bandung.

Wahyu Widodo, 2015, *Kriminologi & Hukum Pidana,* Universitas PGRI Semarang, Semarang.

WEBSITE

JosuaSitompul,https://www.hukumonline.com/klinik/a/landasan-hukumpenanganan-icybercrime-i-di-indonesia-cl5960, 20 Februari 2023.

Syafnidawaty,https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/,18 Februari 2023.

TriRachmadi,https://books.google.co.id/book?id=Nor6DwAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false,20 Maret 2023.

JURNAL

Kurniawan Prasatya Atmanagara, Mustawa Nur & Muhammad Halwan, 2022, Analisis Hukum Pertanggung Jawaban Pidana Terkait Berita Bohong Menurut Undang-Undang Informasi Dan Transaksi Elektronik Di Polda Sulawesi Selatan, *Jurnal Clavia Of Law,* **Volume 20 No 3,** hlm 334.

Mulqadrin Adam., Kamri Ahmad & Hamza Baharuddin, 2021, Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan, *Jurnal of Lex Generalis (JLG),* **Volume 2,** hlm 1108.

Nur Rahma Indah, Abd. Haris Hamid & Siti Zubaidah, 2021, Penyidikan Tindak Pidana Skimming Dalam Transaksi Elektronik Oleh Kepolisian Daerah Sulawesi Selatan, *Jurnal Clavia Of Law,* **Vol 19 Nomor 3**, hlm 350.

Febyola Indah, dkk., 2022, Peran Cyber Security terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka), *Jurnal Bidang Penelitian Informasi,* **Volume 2**, hlm 5.

Renni Sartika., Sepuh, A.I.S., Ni Putu, R.K.S., 2020, Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime, *Jurnal Aktual Justice,* **Volume 5**, hlm 46.

Sahiruddin, Ruslan Renggong, Basri Oner, 2022, Analisis Hukum Tindak Pidana Kelalaian Mengemudikan Kendaraan Bermotor Mengdampakkan Orang Lain Meninggal Dunia (Studi Kasus Putusan Pengadilan Negeri Maros No.48/Pid.Sus/2020/PN.Mrs), *Jurnal Clavia Of Law,* **Vol 20 Nomor 3**, hlm 399.

SKRIPSI

Oktaviani Sugiarto, 2019, Tinjauan Hukum Internasional Terkait Perlindungan Data Pribadi, Skripsi. Tidak Diterbitkan, Fakultas Hukum, Universitas

Hasanuddin: Makassar.

UNDANG-UNDANG

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang Undang Nomor 10 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektroni

Surat Keputusan Bersama Menteri Komunikasi dan Informatika Republik Indonesia, Jaksa Agung Republik Indonesia, dan Kepala Kepolisian Negara Republik Indonesia Nomor 229 Tahun 2021, Nomor 154 Tahun 2021, Nomor KB/2/VI/2021 tentang 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 Infomasi dan Transaksi Elektronik

L

A

M

P

I

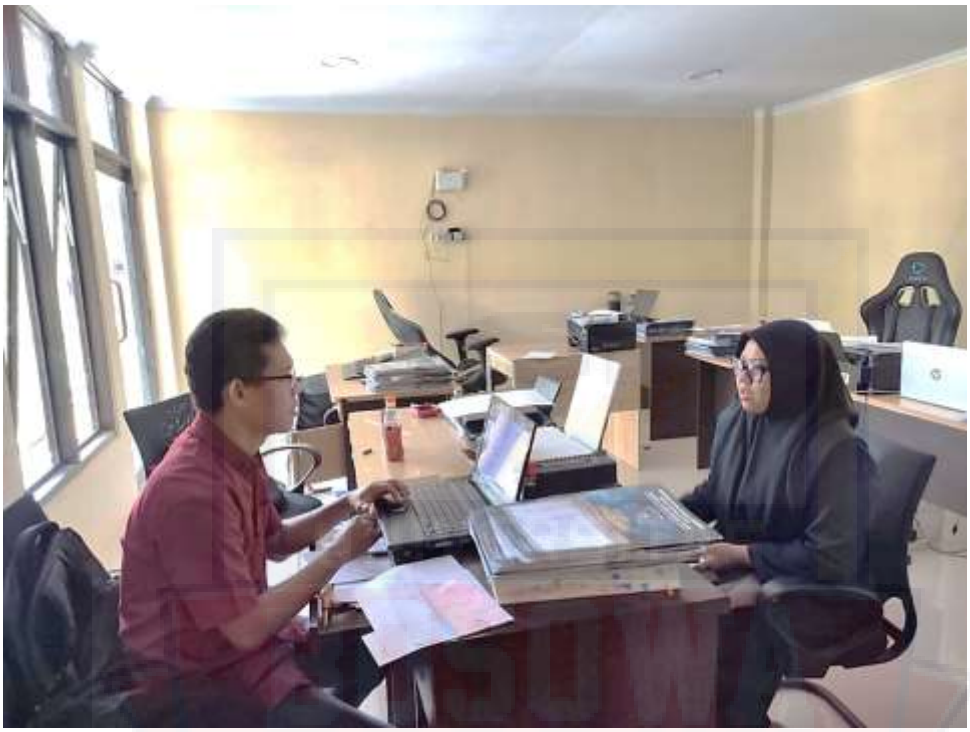
R

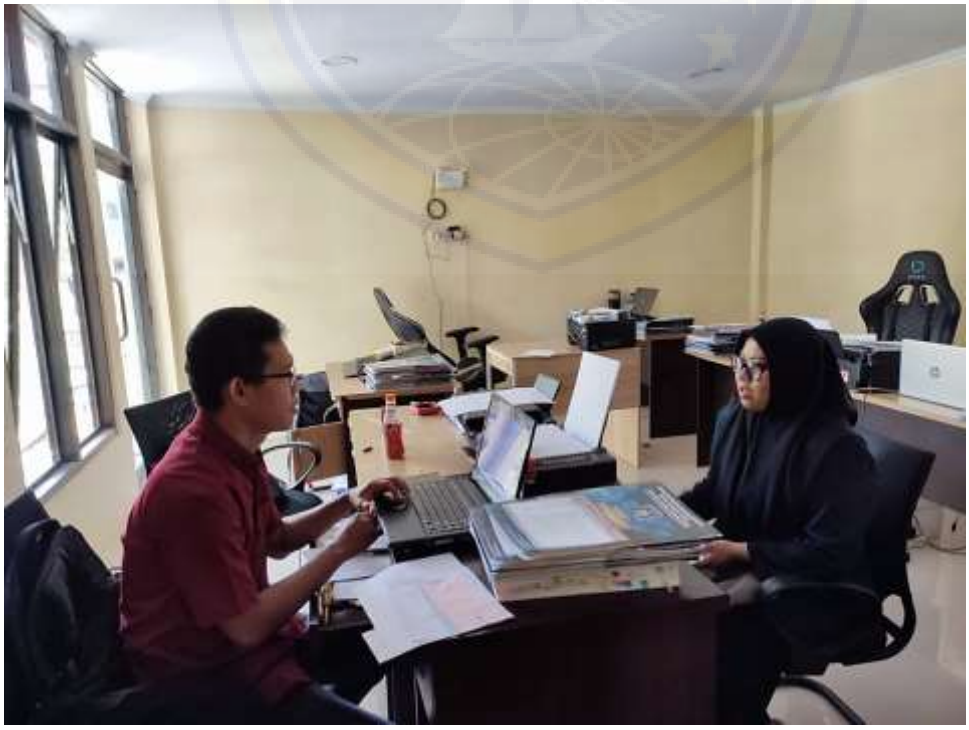
A

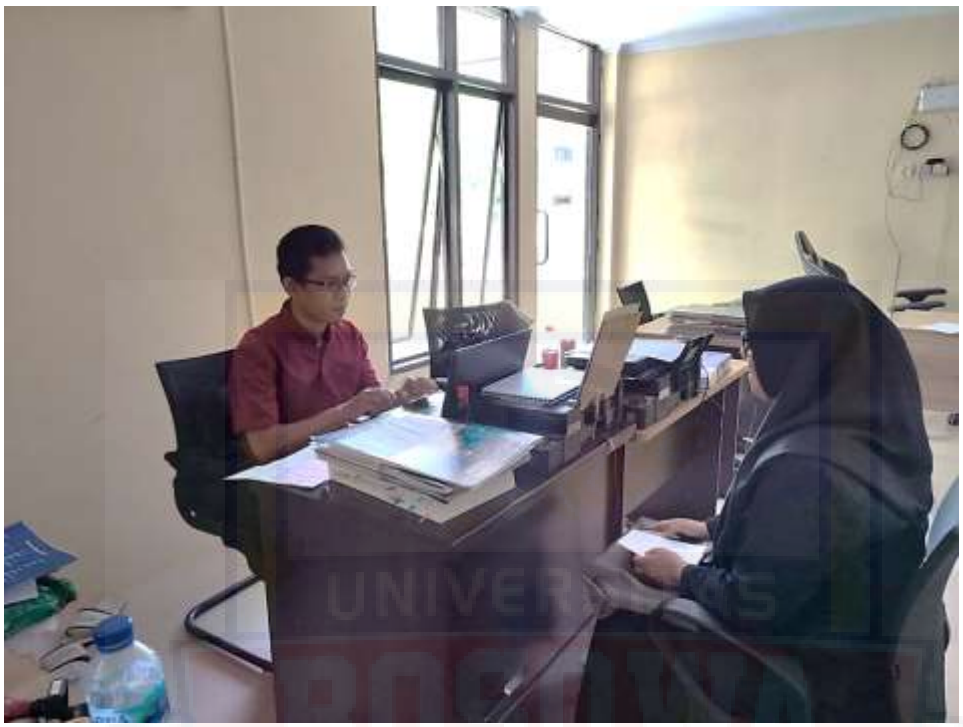
N

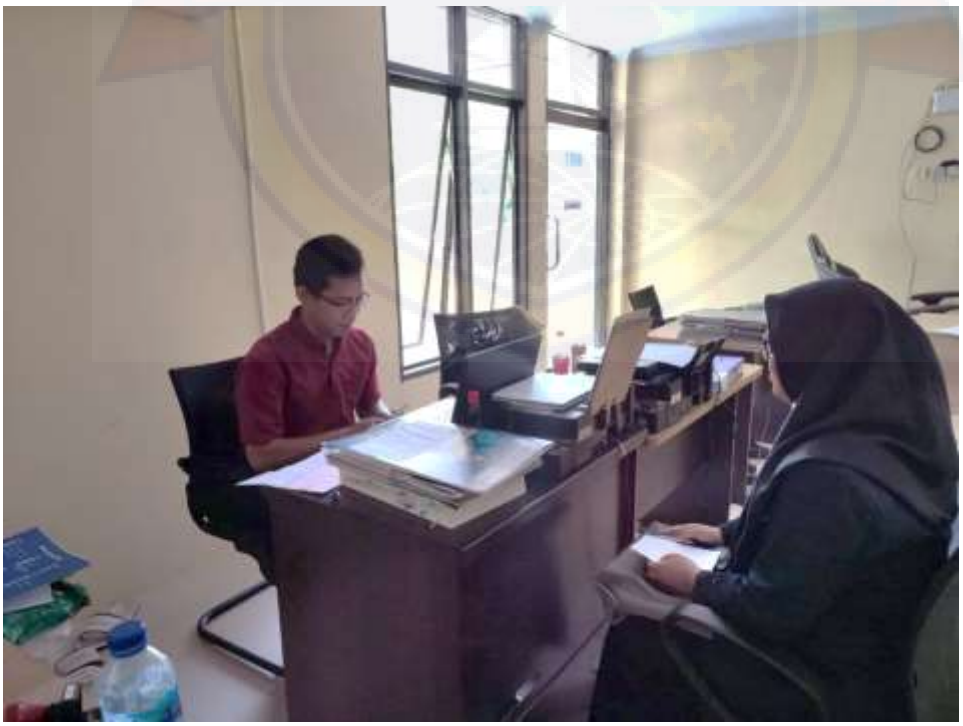
LAMPIRAN 1

Dokumentasi wawancara Ditreskrimsus Polda Sulsel



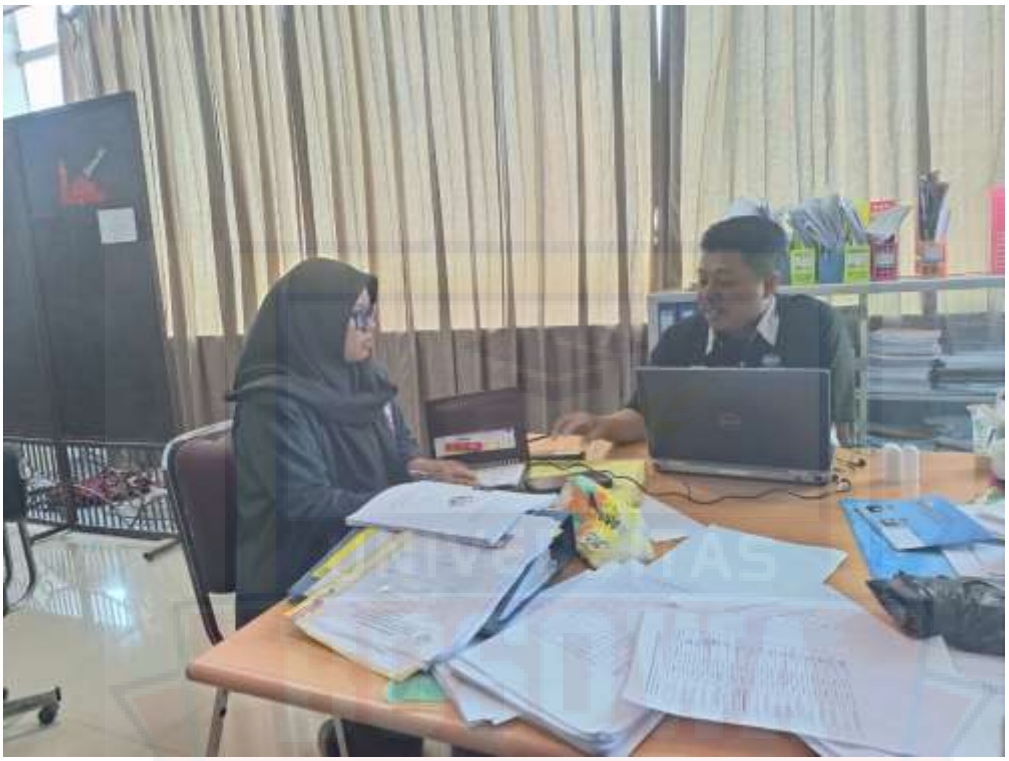


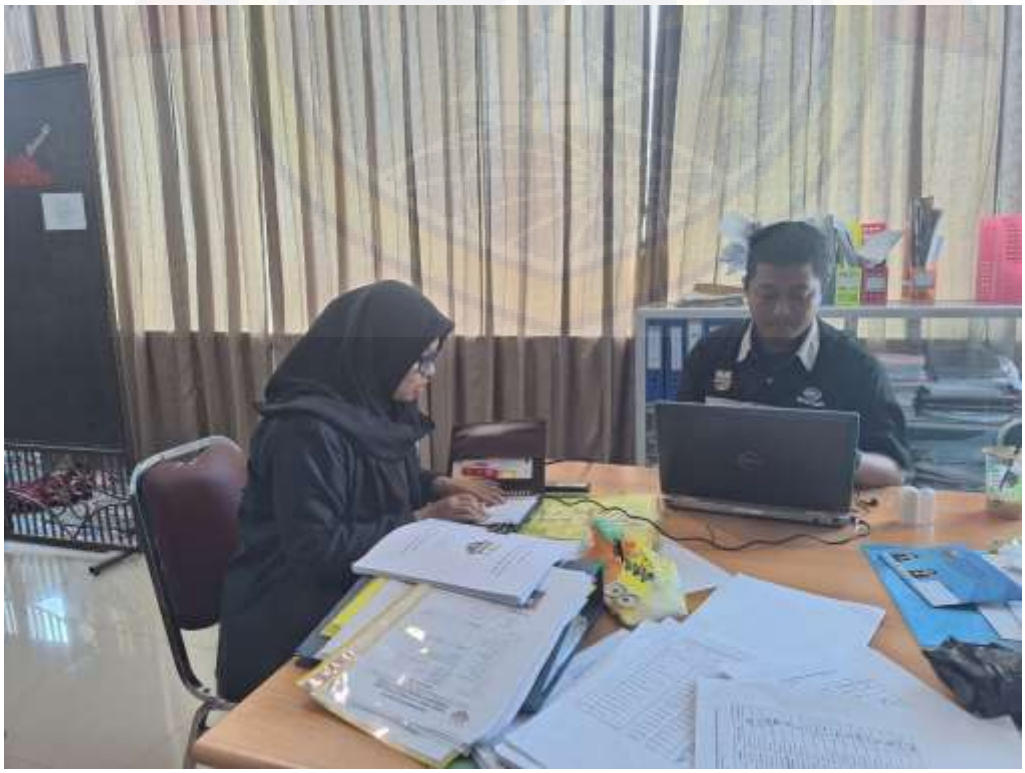


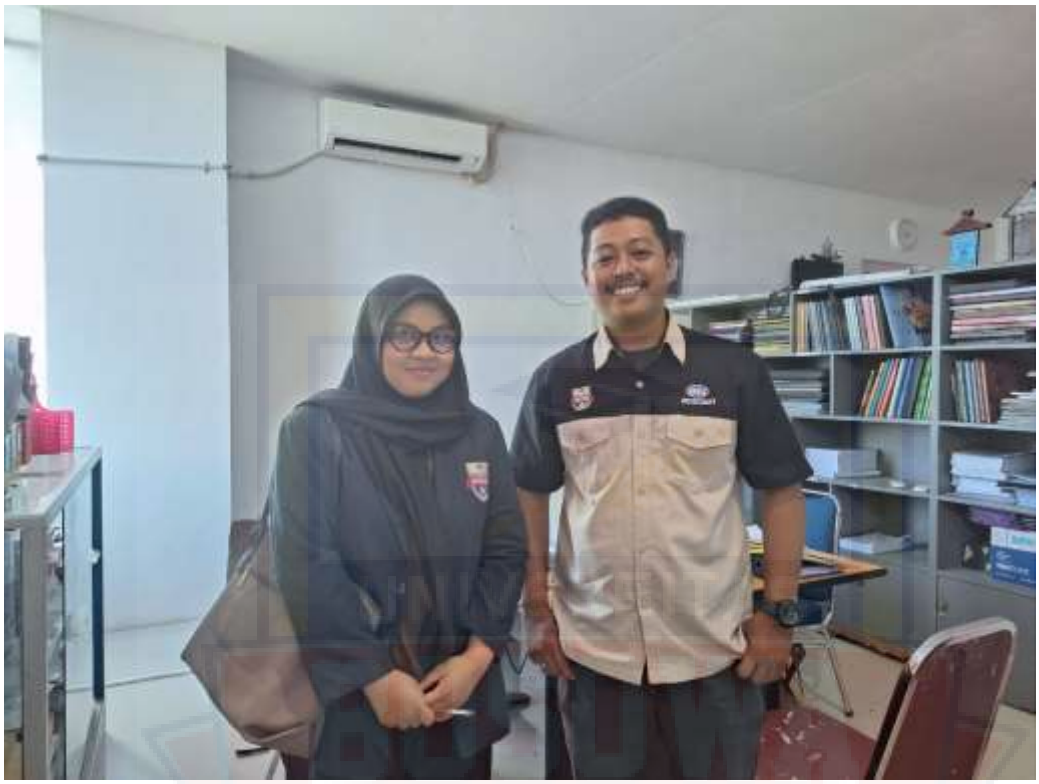


LAMPIRAN 2

Dokumentasi wawancara dengan Ahli IT Universitas Bosowa

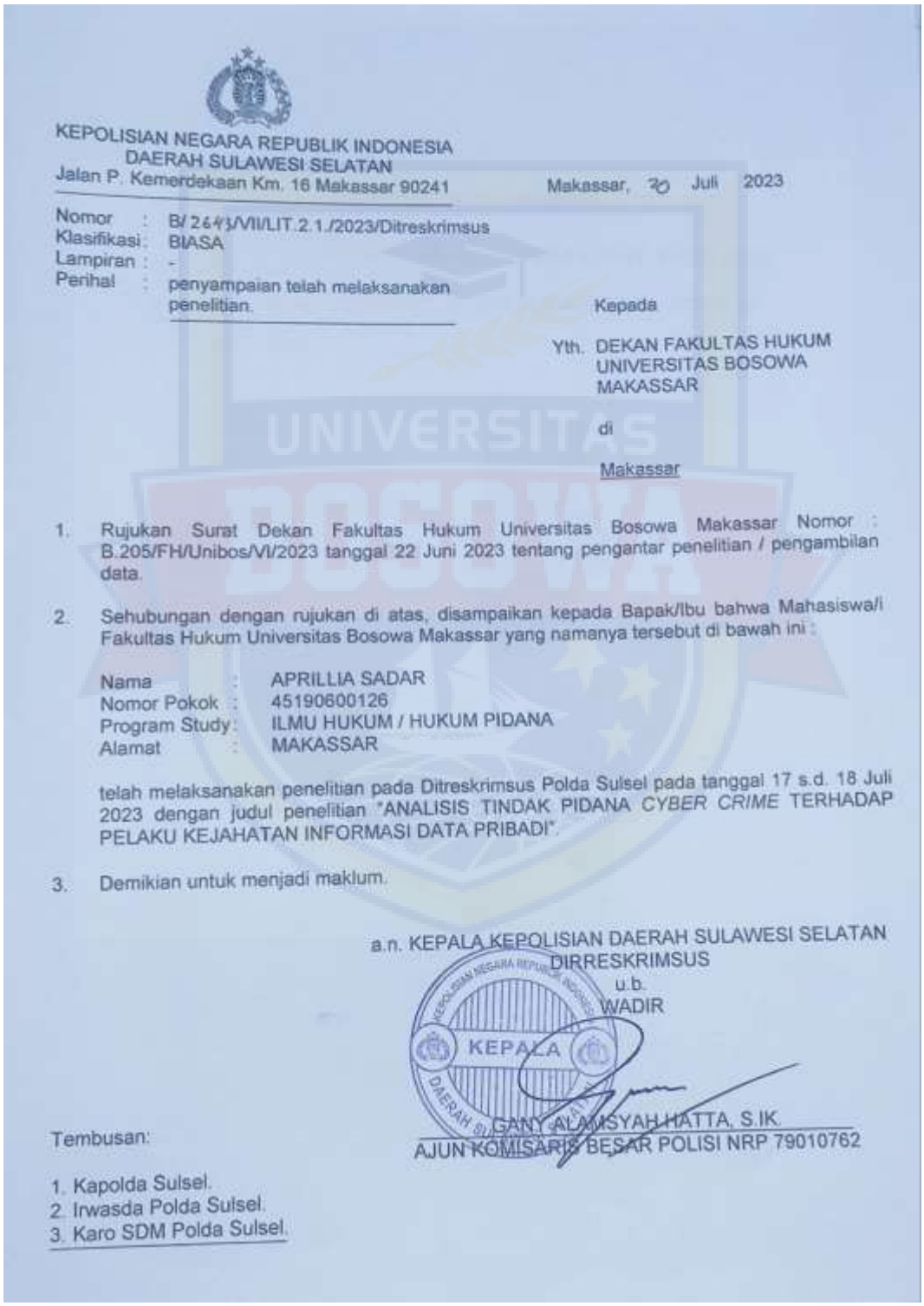






LAMPIRAN 3

Surat Keterangan Telah Melaksanakan Penelitian di Polda Sulsel



KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH SULAWESI SELATAN
Jalan P. Kemerdekaan Km. 16 Makassar 90241

Makassar, 20 Juli 2023

Nomor : B/ 2643/VII/LIT.2.1./2023/Ditreskrimsus
Klasifikasi : BIASA
Lampiran : -
Perihal : penyampaian telah melaksanakan penelitian.

Kepada

Yth. DEKAN FAKULTAS HUKUM
UNIVERSITAS BOSOWA
MAKASSAR

di

Makassar

1. Rujukan Surat Dekan Fakultas Hukum Universitas Bosowa Makassar Nomor : B.205/FH/Unibos/VI/2023 tanggal 22 Juni 2023 tentang pengantar penelitian / pengambilan data.

2. Sehubungan dengan rujukan di atas, disampaikan kepada Bapak/Ibu bahwa Mahasiswa/i Fakultas Hukum Universitas Bosowa Makassar yang namanya tersebut di bawah ini :

   Nama : APRILLIA SADAR
   Nomor Pokok : 45190600126
   Program Study : ILMU HUKUM / HUKUM PIDANA
   Alamat : MAKASSAR

   telah melaksanakan penelitian pada Ditreskrimsus Polda Sulsel pada tanggal 17 s.d. 18 Juli 2023 dengan judul penelitian "ANALISIS TINDAK PIDANA *CYBER CRIME* TERHADAP PELAKU KEJAHATAN INFORMASI DATA PRIBADI".

3. Demikian untuk menjadi maklum.

a.n. KEPALA KEPOLISIAN DAERAH SULAWESI SELATAN
DIRRESKRIMSUS
u.b.
WADIR

KEPALA

GANY ALAMSYAH HATTA, S.IK.
AJUN KOMISARIS BESAR POLISI NRP 79010762

Tembusan:

1. Kapolda Sulsel.
2. Irwasda Polda Sulsel.
3. Karo SDM Polda Sulsel.