PELAKSANAAN PENYIDIKAN TINDAK PIDANA PENIPUAN DATA PROGRAM PRAKERJA
(Suatu Penelitian di Kepolisian Resor Bireuen)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Hukum

Oleh :

NAMA : RAFLYAN ALTHAF SUCHEL

NPM : 1801110150

PROGRAM STUDI : ILMU HUKUM

BAGIAN : HUKUM PIDANA

FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH ACEH
BANDA ACEH
2024

Telah Disetujui

Untuk Diajukan Kepada Panitia Ujian Skripsi
Fakultas Hukum Universitas Muhammadiyah Aceh

Judul Skripsi

Pelaksanaan Penyidikan Tindak Pidana Penipuan Data Program Prakerja
(Suatu Penelitian di Kepolisian Resor Bireuen)

Banda Aceh, 31 Juli 2024

Pembimbing,

Nora Mia Azmi, S.H.,M.H

PELAKSANAAN PENYIDIKAN TINDAK PIDANA PENIPUAN DATA PROGRAM PRAKERJA
(Suatu Penelitian di Kepolisian Resor Bireuen)

Oleh

Nama Mahasiswa	: Raflyan Althaf Suchel
No. Mahasiswa	: 1801110150
Program Studi	: Ilmu Hukum
Bagian	: Hukum Pidana

Telah Dipertahankan di Depan Sidang Penguji,
Pada Tanggal 24 Agustus 2024
Dan Dinyatakan Telah Memenuhi Syarat Untuk Diterima

DEWAN PENGUJI

1. Ketua	: **Dr. Mainita, S.H.,M.Hkes**	(.....)
2. Sekretaris	: **Trio Yusandy, S.H., M.Kn**	(.....)
3. Pembimbing/Penguji I	: **Nora Mia Azmi, S.H.,M.H**	(.....)
4. Penguji II	: **Dr. Airi Safrijal, S.H.,M.H`**	(.....)
5. Penguji III	: **Dr. Irfan Iryadi, S.H.,M.Kn**	(.....)

Banda Aceh, 03 September 2024
Universitas Muhammadiyah Aceh
Dekan Fakultas Hukum

Dr. Mainita, S.H.,M.Hkes

ABSTRAK

Raflyan Althaf Suchel, 2024 **PELAKSANAAN PENYIDIKAN TINDAK PIDANA PENIPUAN DATA PROGRAM PRAKERJA (Suatu Penelitian di Kepolisian Resor Bireun) Fakultas Hukum Universitas Muhammadiyah Aceh (iii, 65).,pp.,bibl.,app**

Nora Mia Azmi,.S.H.,M.H

Pasal 378 KUHP tentang tindak pidana penipuan berbunyi, barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum,dengan memakai nama palsu atau martabat palsu,dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidanan penjara paling lama 4 tahun. Dalam penyidikan tindak pidana penipuan data program prakerja di wilayah hukum Kepolisian Resor Bireuen, dilakukan oleh 2 tersangka yang menggunakan NIK korban sehingga mendapatkan sejumlah uang dari hasil pendaftaran program prakerja.

Tujuan penulisan skripsi untuk menjelaskan pelaksanaan penyidikan terhadap tindak pidana penipuan data program prakerja, Hambatan dalam pelaksanaan penyidikan tindak pidana penipuan data program prakerja, Strategi perlindungan data oleh pihak Kepolisian Resor Bireun untuk mencegah terjadinya pembobolan data.

Metode penelitian yang digunakan dalam adalah pendekatan yuridis empiris dengan wilayah penelitian lapangan (*field research*) dan kepustakaan (*library research*). Penelitian lapangan dilakukan guna memperoleh data primer melalui wawancara dengar informan. Penelitian kepustakaan dilakukan untuk memperoleh data sekunder dengan mengetahui bukti-bukti, buku-buku dan perundang-undangan.

Hasil penelitian dikemukakan proses penyidikan dengan mencari informasi data pribadi dalam pelaksanaannya dari tahap penyidikan, Penindakan penyidik melakukan pencarian dan pemeriksaan saksi dan alat bukti yang terkait dengan kejahatan informasi data pribadi, pemeriksaan oleh para ahli dalam kasus *Cybercrime,* penyelesaian berkas perkara hingga penyidik mengirim berkas perkara kepada Jaksa penuntut umum. Hambatan yang ditemukan dalam pelaksanaan penyidikan tindak pidana penipuan data program prakerja antara lain berkaitan dengan perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Srategi perlindungan data pihak Kepolisian Resor Bireuen seperti Upaya Pre-emtif adalah upaya awal yang dilakukan untuk mencegah terjadinya tindak pidana, Upaya Preventif upaya pencegahan dilakukan agar kejahatan tidak terjadi lagi, Upaya Represif adalah upaya tindakan atau penanggulangan yang dilakukan sesudah terjadinya kejahatan (tindak pidana).

Di sarankan kepada penyidik Kepolisian Resor Bireuen dapat melakukan penyempurnaan perangkat hukum, mendidik para penyidik, meningkatkan upaya penyidikan, serta melakukan penanggulangan pencegahan terjadinya tindak pidana manipulasi data dan kepada masyarakat agar lebih menjaga dan peduli terhadap kepentingan berkas-berkas rahasia milik pribadi.

KATA PENGANTAR

Dengan mengucapkan syukur Alhamduillah kehadirat Allah Swt, yang mana telah melimpahkan rahmat dan karunia-Nya sehingga skripsi dengan judul **"Pelaksanaan Penyidikan Tindak Pidana Penipuan Data Program Prakerja (Suatu Penelitian di Kepolisian Resor Bireuen)"**dapat diselesaikan. Shalawat beriring salam disanjung ke pangkuan Nabi Besar Muhammad Saw karena berkat beliau lah yang telah membawa umat manusia dari alam jahiliyah ke alam yang berilmu pengetahuan.

Penulisan skripsi ini dimasudkan guna memenuhi salah satu syarat untuk memperoleh gelar sarjana hukum pada Fakultas Hukum Universitas Muhammadiyah Aceh. Penyusunan skripsi ini tidak mungkin berhasil diselesaikan tanpa kesempatan, bantuan, bimbingan, arahan, serta dorongan semangat dari berbagai pihak. Untuk itu ucapan terimakasih serta penghargaan disampaikan kepada:

1. Ibu Nora Mia Azmi, S.H,.M.H telah memberikan bimbingan, motivasi dan semangat selama penulisan skripsi belakangan ini, sehingga penulisan ini dapat diselesaikan dengan bimbingan ibu yang sangat membantu penulis.
2. Ibu Dr. Mainita, S.H.,M.H.kes selaku Dekan Fakultas Hukum Universitas Muhammadiyah Aceh.
3. Bapak Dr. Airi Safrijal,.S.H,.M.H Selaku dosen wali yang telah memberikan bimbingan akademik dan memberi motivasi kepada penulis.

4. Para dosen dan seluruh tenaga kependidikan di Fakultas Hukum Universitas Muhammadiyah Aceh yang telah membekali ilmu pengetahuan dan bimbingan serta pelayanan akademik yang baik.
5. Semua teman-teman angkatan 2018 Fakultas Hukum Universitas Muhammadiyah Aceh yang telah memberi dorongan semangat dalam menyelesaikan skripsi ini.

Kepada yang terkhusus dan teristimewa Ayahanda Irwan dan Ibunda Vera Andiari tercinta yang senantiasa memberikan kasih sayang nasihat dan motivasi baik secara psikis, dan materi. Serta doa yang tidak henti-hentinya diberikan demi keberhasilan dan kesuksesan untuk menyelesaikan pendidikan dengan baik. Penulisan skripsi ini masih jauh dari kata sempurna, baik dari segi bahasa, maupun dari segi pembahasannya, maka dari itu diharapkan saran dan kritik yang bersifat membangun dan konstruktif untuk perbaikan dimasa yang akan datang. Akhirnya skripsi ini diharapkan bermanfaat bagi para pembaca dan dapat dilanjutkan untuk penulisan selanjutnya. Amin.

Banda Aceh, 02 November 2023

(Raflyan Althaf Suchel**)**

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi menyebabkan dunia menjadi tanpa batas dan menyebakkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejeahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[1]

Kejahatan atau tindak criminal merupakan salah satu bentuk perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat, tidak ada masyarakat yang sepi dari kejahatan. Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan pengguna nya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer.[2]

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga

[1]Ahmad M.Ramli *Cyber Law Dan Haki Dalam Sistem Hukum Indonesia*, Bandung, PT Refika Aditama 2010, hlm 1

[2] Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternative Ancaman Pidana Kerja Social Dan Pidana Pengawasan Bagi Pelaku Cyber Crime,* Yogyakarta Laksabang Mediatama, 2009, hlm 24

perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan). Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime.*

Perbuatan pemalsuan merupakan suatu jenis pelanggaran terhadap kebenaran dan keterpercayaan, dengan tujuan memperoleh keuntungan bagi diri sendiri atau orang lain. Suatu pergaulan hidup yang teratur di dalam masyarakat yang maju teratur tidak dapat berlangsung tanpa adanya jaminan kebenaran atas beberapa bukti surat dan dokumen-dokumen lainnya. Karenanya perbuatan pemalsuan dapat merupakan ancaman bagi kelangsungan hidup dari masyarakat tersebut.[3]

Ketika penyidik memulai tindakan penyidikan kepadanya dibebani kewajiban untuk memberitahukan hal dimulainya penyidikan tersebut kepada penuntut umum. Kebijakan pembatasan kegiatan ini mengakibatkan warga susah untuk berjualan, berdagang atau melaksanakan kegiatan bekerja lainnya sehingga pendapatan warga menjadi berkurang bahkan bisa jadi warga kehilangan mata pencaharian. Kondisi ini diantisipasi oleh pemerintah dengan adanya program prakerja. Ini merupakan program pengembangan kompetensi kerja yang ditujukan untuk pencari kerja,

[3] Adami Chazawi*, Pelajaran Hukum Pidana I*, Raja Grafindo Persada, Jakarta, 2001, Hlm. 3

pekerja/buruh yang terkena pemutusan hubungan kerja, dan/atau pekerja/buruh yang membuthkan peningkatan kompetensi.

Kartu Prakerja merupakan program semi bantuan sosial dimana peserta yang menerima manfaat akan menerima insentif sebesar Rp 3,550.000 juta. Dimana dana tersebut akan dibagi beberapa pos, pos pertama yaitu dana insentif Rp 2.400,000 juta (diberikan selama 4 tahap, disetiap tahap sebesar Rp 600.000), kedua Rp 150.000 (diberikan selama 3 tahap, disetiap tahap sebesar Rp 50.000), dan yang terakhir sebesar 1 juta untuk dana pelatihan (dana ini tidak bisa dicairkan). Untuk pendaftaran program prakerja, para calon dapat mendaftarkan diri kepada staf yang ditetapkan oleh perangkat desa dengan menyerahkan photo KTP dengan NIK yang jelas. Namun dalam pelaksanaannya, kegiatan ini dimanfaatkan oleh orang-orang tertentu untuk mendapatkan keuntungan dengan cara melawan hukum.

Dalam perkembangan internet yang sangat laju tentu sudah dapat diprediksi bahwa akan membawa dampak negatif, dengan memberi kesempatan maupun peluang timbulnya aksi-aksi anti sosial yang tidak pernah terkira bahwa dan dianggap akan terjadi. Ada teori yang menyebutkan *crime is product of society itself* yang dapat diberi arti bahwa masyaratak sendirilah yang menciptakan kejahatan. Lahirnya suatu tindak pidana sebagai dampak negatif dari berkembangnya internet yang begitu laju disebut dengan tindak pidana teknologi informasi atau kejahatan.

Dua Tersangka tindak pidana Informasi dan Transaksi Elektronik (ITE), yang melakukan manipulasi data peserta program prakerja hingga bisa mencairkan bantuan, diringkus Satreskrim Polres Bireuen, Kamis 2 Desember 2021. Kedua tersangka nekad menggunakan ratusan Nomor Induk Kependudukan (NIK) milik orang lain sejak Juli 2021, dan sudah mendapatkan keuntungan hingga Rp 150,000,000 juta dari beberapa kali penarikan insentif yang dilakukan. Keduanya berinisial HE, 36 tahun, pekerjaan wiraswasta, beralamat di Gampong Keude Alue Rheng, Kecamatan Peudada dan RI, 32 tahun, pekerjaan wiraswasta, beralamat Gampong Sangso, Kecamatan Samalanga. Mudahnya akses mendapatkan NIK milik orang lain, kata Kapolres karena salah seorang tersangka berinisial HE, sebelumnya pernah bekerja sebagai penjual jasa (calo) pembuatan Nomor Pokok Wajib Pajak (NPWP) milik orang lain tahun 2018. Kapolres turut merincikan sejumlah barang bukti diamankan yaitu 1 unit CPU rakitan, 1 layar/monitor merek Samsung, 1 keyboard komputer merek gamen, 1 mouse merek gamen,3 HP smartphone/android. Kemudian 1 unit sepeda motor Honda PCX warna merah, 1 sepeda motor Yamaha N-Max warna merah. Juga 1 akta jual beli sebidang tanah, 12 mayam emas, 1 buku tabungan BCA, 1 ATM BCA, uang Rp 7.200.000, dan 300 *simcard* perdana.[4]

[4]Https://Www.Readers.Id/Read/Manipulasi-Data-Program-Prakerja-Dua-Warga-Bireuen-Ditangkap/Index.Html. Diakses Tanggal 5 Maret 2022

Dalam modus operasi yang dilakukan oleh pihak tersangka dalam melakukan tindak pidana manipulasi data program prakerja dengan mendaftarkan NIK masyarakat yang didapatkan dari hasil calo pembuatan nomor pokok wajib pajak (NPWP), NIK yang di berikan oleh korban digunakan untuk mendaftar program bantuan prakerja yang diadakan oleh pemerintah, dengan menggunkan NIK korban para pihak tersangka mendapatkan sejumlah uang yang digunakan untuk keperluan pribadi tersangka.

Tahap penyidikan merupakan salah satu bagian penting dalam rangkaian tahap-tahap yang harus dilalui suatu kasus menuju pengungkapan terbukti atau tidaknya dugaan telah terjadinya suatu tindak pidana. Oleh sebab itu keberadaan tahap penyidikan tidak bisa dilepaskan dari adanya ketentuan perundangan yang mengatur mengenai tindak pidananya.[5]

Di dalam kasus ini penyelidik sebagaimana dimaksud dalam Pasal 5 KUHAP bertugas untuk menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana dan mancari ketenangan dan barang bukti, menyuruh berhenti seorang yang dicurigai dan menanyakan serta memeriksa tanda pengenalan diri, mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Pasal 1 angka (2) KUHAP, Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini

[5]Sahuri Lasmadi, *Tumpang Tindih Kewenangan Penyidikan Pada Tindak Pidana Korupsi Pada Perspektif Sistem Peradilan Pidana*, Jurnal Ilmu Hukum, Volume 2, Nomor 3, Universitas Jenderal Soedirman Fakultas Hukum, Purwokerto, Juli, 2010, Hlm. 10.

untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Pasal 7 Angka (1) KUHAP, (1) Penyidik sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf a karena kewajibannya mempunyai wewenang

a) menerima Iaporan atau pengaduan dari seorang tentang adanya tindak pidana
b) melakukan tindakan pertama pada saat di tempat kejadian
c) menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal diri tersangka
d) melakukan penangkapan, penahanan, penggeledahan dan penyitaan
e) melakukan pemeriksaan dan penyitaan surat
f) mengambil sidik jari dan memotret seorang; g. memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi
g) mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara
h) mengadakan penghentian penyidikan
i) mengadakan tindakan lain menurut hukum yang bertanggung jawab

Pasal 43 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektroni menjelaskan, selain penyidik pejabat Polisi Negara Republik Indonesia, pejabat Pengawai 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.

Kartu Prakerja diterbitkan berdasarkan pada Peratutan Presiden Nomor 36 Tahun 2020 tentang Pengembangan Kompetensi Kerja Melalui Program Kartu Prakerja Perpres Nomor 36 Tahun 2020, dengan aturan pelaksananya adalah Peraturan Menteri Koordinator Bidang Perekonomian Nomor 3 Tahun 2020. Program Prakerja adalah program pengembangan kompetensi kerja yang ditujukan untuk para pencari kerja, pekerja/buruh yang terkena pemutusan hubungan kerja, dan para pekerja yang membutuhkan peningkatan kompetensi. Program Kartu Prakerja merupakan bagian dari Program Pemulihan Ekonomi Nasional (PEN) sektor perlindungan sosial.Namun demikian, perbuatan yang merugikan dan menimbulkan sejumlah masalah karena perbuatan malawan hukum, melampaui wewenang, menggunakan wewenang untuk tujuan lain dari yang menjadi tujuan wewenang tersebut, termasuk kelalaian atau pengabaian kewajiban hukum dalam penyelenggaraan pelayanan publik yang dilakukan oleh Penyelenggara Negara dan pemerintahan yang menimbulkan kerugian bagi pemerintah dan masyarakat. Di Dalam Perpres Nomor 36 Tahun 2020 Mengenai perkembangan kompetensi kerja melalui program prakerja juga memasukkan tentang tuntutan pidana bagi peserta yang melakukan pemalsuan idetitas dan data

diri sebagai landasan hukum untuk mengenaan pidana bagi peserta penerima kartu prakerja yang dibuktikan melakukan pemalsuan indetitas.[6]

Berdasarkan penjelasan diatas, maka penulis tertarik untuk mendalami kasus dengan memilih judul skripsi: **Pelaksanaan Penyidikan Tindak Pidana Penipuan Data Program Prakerja (Suatu Penelitian di Wilayah Hukum Kepolisian Resor Bireuen)**

1. Bagaimana pelaksanaan penyidikan tindak pidana penipuan data program prakerja ?
2. Apa hambatan dalam pelaksanaan penyidikan tindak pidana penipuan data program prakerja ?
3. Bagaimana strategi perlindungan data oleh pihak Kepolisian Resor Bireun untuk mencegah terjadinya pembobolan data ?

B. Ruang Lingkup Dan Tujuan Penelitian

1. Ruang Lingkup Penelitian

Ruang lingkup dalam penelitian ini sesuai dengan judulnya yaitu Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Data Program Prakerja (Suatu Penelitian di Wilayah Hukum Kepolisian Resor Bireuen) Permasalahan tersebut termasuk dalam bidang hukum pidana yang mana data-datanya diperoleh berdasarkan penelitian yuridis empiris atau sering disebut penelitian lapangan yaitu mengkaji ketentuan hukum yang berlaku serta apa yang terjadi dalam kenyataan di masyarakat

[6]Siti Dwi Yana. (2021). Efektivitas Program Kartu Prakerja Dalam Membangun Sumberdaya Manusia. *Jurnal Investasi Islam*, *6*(1), 12-21. Https://Doi.Org/10.32505/Jii.V6i1.2763 Diakses 25 Maret 2022

2. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah dikemukakan sebelumnya, maka yang menjadi tujuan dalam penelitian ini adalah:

1) Untuk menjelaskan pelaksanaan penyidikan terhadap tindak pidana penipuan data program prakerja
2) Untuk menjelaskan hambatan dalam pelaksanaan penyidikan tindak pidana penipuan data program prakerja
3) Untuk menjelaskan strategi perlindungan data oleh pihak Kepolisian Resor Bireun untuk mencegah terjadinya pembobolan data

C. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah Yuridis Empiris atau sering disebut penelitian lapangan, mengkaji ketentuan hukum yang berlaku serta apa yang terjadi dalam kenyataan di masyarakat. Penelitian ini untuk memperoleh informasi serta penjelasan mengenai segala sesuatu diperlakukan pedoman penelitian atau metode penelitian, hal ini dikarenakan dengan menggunakan metode penelitian yang benar diperoleh validitas data serta dapat mempermudah dalam melakukan analisis masalah.[7]

1. Definisi Operasional Variabel Penelitian

[7] Bambang Waluyo,*Penelitian Hukum Dalam Praktek,Sinar Grafika*, Jakarta 2002:Hlm 15

a) Penyidikan adalah suatu tindak lanjut dari kegiatan penyelidikan dengan adanya persyaratan dan pembatasan yang ketat dalam penggunaan upaya paksa setelah pengumpulan bukti permulaan yang cukup guna membuat terang suatu peristiwa yang patut diduga merupakan tindak pidana.
b) Tindak Pidana merupakan terjemahan dari istilah Belanda yaitu *strafbaar feit*. Disamping istilah tindak pidana sebagai terjemahan strafbaar feit itu, dalam bahasa Indonesia terdapat juga istilah lain yang dapat ditemukan dalam beberapa buku hukum pidana dan perundang-undangan hukum pidana, yaitu peristiwa pidana, perbuatan pidana, perbuatan yang boleh dihukum, perbuatan yang dapat dihukum, dan pelanggaran pidana.
c) Manipulasi adalah sebuah proses rekayasa yang secara disengaja dengan melakukan penambahan, penyembunyian, penghilangan atau pengkaburan terhadap bagian atau keseluruhan sebuah sumber informasi, subtansi, realitas, kenyataan, fakta-fakta, data ataupun sejarah yang dibuat berdasarkan sistem perancangan yang bisa dilakukan secara individu, kelompok atau sebuah tata sistem nilai, manipulasi adalah bagian penting dari suatu tujuan tertentu dalam hal tindakan penanaman gagasan, dogma, doktrinisme, sikap, sistem berpikir, perilaku dan kepercayaan tertentu.
d) Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau

dikombinasi dengan informasi lainnya baik secara langsung maupuntidak langsung melalui sistem elektronik dan/atau nonelektronik.

e) Program Prakerja adalah program pengembangan kompetensi kerja yang ditujukan untuk para pencari kerja, pekerja/buruh yang terkena pemutusan hubungan kerja, dan para pekerja yang membutuhkan peningkatan kompetensi. Program Kartu Prakerja merupakan bagian dari Program Pemulihan Ekonomi Nasional (PEN) sektor perlindungan sosial.

2. Lokasi Dan Populasi Penelitian

Dalam penelitian ini pendekatan yang dilakukan adalah kualitatif, Bodgan dan Taylor mendefinisikan penelitian kualitatif sebagai penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati.[8]

Adapun dalam memperoleh data peneliti menggunakan metode Kualitatif bersifat Deskriptif yang merupakan suatu metode yang bertujuan untuk mendeskripsikan dan menganalisis fenomena, peristiwa, aktivitas sosial, sikap kepercayaan, persepsi, pemikiran orang secara individu maupun kelompok.[9] Data yang didapatkan kemudian dianalisis untuk memperoleh jawaban terhadap suatu permasalahan yang timbul dan hasilnya akan dipaparkan dalam bentuk laporan penelitian.

---

[8] Moleong, Lexy. *"Metode Penelitian Kuantitatif"*, Remaja Rosdakarya, Bandung 2002 hlm. 29.

[9] Nana Syaodih Sukmadinata. "*Metode Penelitian Pendidikan",* PT. Remaja Rosdakarya, Bandung 2007.Hlm. 60

a. Lokasi Penelitia

Untuk mendapatkan data dan informasi yang diperlukan berkaitan dengan permasalahan dan pembahasan penulisan penelitian ini, maka akan dilakukan penelitian dengan memilih lokasi penelitian di Wilayah Hukum Kepolisian Resor Bireuen.

b. Populasi penelitian

Populasi adalah seluruh objek atau seluruh individu,gejala atau seluruh kejadia ataupun seluruh unit yang ingin diteliti. Adapun yang menjadi populasi dalam penelitian ini adalah penyidik Kepolisian Resor Bireuen, Petugas Dinas Ketenagakerjaan dan Korban .

3. Teknik Pengambilan Sempel Data

Metode pengambilan sampel adalah suatu teknik dalam penarikan atau pengambilan sampel penelitian. Metode pengambilan sampel dalam penelitian ini adalah *purposive sampling* teknik ini biasa diartikan sebagai suatu proses pengambilan sampel dengan menentukan terlebih dahulu jumlah sampel yang akan hendak diambil, kemudian pemilih sampel dilakukan dengan berdasarkan tujuan-tujuan tertentu, asalkan tidak menyimpang dari ciri-ciri sampel yang di tentukan.

a. Responden

Responden adalah seseorang atau individu yang akan memberikan data/informasi terhadap pertanyaan yang diajukan oleh peneliti. Adapun yang menjadi responden adalah:

1) Penyidik Kepolisian Resor Bireuen (1 orang)
2) Korban (2 orang)

b. Informan

Informan adalah seseorang yang benar-benar mengetahui suatu persoalan atau permasalahan tertentu yang darinya dapat diperolehin forman yang jelas, akurat, dan terpercaya baik berupa pernyataan, keterangan, atau data-data yang dapat membantu dalam memahami persoalan atau permasalahan tersebut:

1) Akademisi 1 Orang

4. Teknik Pengumpulan Data

Dalam rangka pengumpulan data primer dan data sekunder, maka penulis menggunakan satu jenis pengumpulan data sebagai berikut :

a. Penelitian Kepustakaan.

Mempelajari dan menganalisis buku-buku,makalah ilmiah,perturan perundang-undangan dan bahan-bahan yang berhubungan dengan materi yang dibahas dalam skripsi ini.

b. Penelitian Lapangan.

Dalam penelitian lapangan peneliti menggunakan teknik Wawancara, yakni penulis mengadakan tanya jawab dengan pihak-pihak yang terkait langsung dengan masalah yang dibahas menangani

masalah apa saja yang sering dialami oleh pemilik merek tersebut. Dalam pengumpulan data diperlukan pedoman wawancara yang disusun secara sistematik dan sesuaikan dengan data yang diperlukan.

c. Observasi

Metode observasi merupakan suatu teknik yang dilakukan dengan cara pengamatan secara sengaja, sistematis ke lokasi penelitian untuk dapat melihat objek yang akan diteliti dan memperoleh data yang lebih akurat yang dibutuhkan sebagai pelengkap dalam penelitian. Pengumpulan data dengan observasi langsung atau dengan pengamatan langsung adalah cara pengambilan data dengan menggunakan alat indera yang dalam hal ini lebih difokuskan pada mata.[10]

Dalam observasi ini, peneliti terlibat dengan kegiatan sehari-hari orang yang sedang diamati atau yang digunakan sebagai sumber data penelitian. Sambil melakukan pengamatan, peneliti ikut melakukan apa yang dikerjakan oleh sumber data, dan ikut merasakan suka dukanya. Dengan observasi ini, maka data yang diperoleh akan lebih lengkap, tajam, dan sampai mengetahui pada tingkat makna dari setiap perilaku yang nampak.

Dengan demikian observasi digunakan untuk mengamati secara langsung tentang kondisi objek penelitian atau peristiwa yang sedang terjadi saat itu. Dan peneliti sekaligus harus mencatat dan ikut berpartisipasi dalam kegiatan saat dilapangan. Melalui metode

[10] Zainuddin Ali, *Metode Penelitian Hukum*, Sinar Grafika, Jakarta .2010 hlm 23

observasi tersebut peneliti akan mengamati beberapa hal yang berkaitan dengan penelitian yang dilakukan yaitu mengenai Pelaksanaan Penyidikan Terhadap Tindak Pidana Manipulasi Data Program Prakerja

5. Teknik Menganalisis Data

Pengambilan analisa data dari hasil penelitian dilakukan dengan menggunakan analisa deskriptif, yaitu berusaha menganalisa dengan menjelaskan secara rinci dan apa adanya mengenai objek yang diteliti data yang diperoleh dari hasil penelitian wawancara maupun dari hasil buku-buku yang di berikan diolah untuk kemudian dianalisis dengan menggunakan pendekatan kualitatif. terhadap data yang diperoleh dari responden dan informan, baik secara lisan maupun tulisan yang kemudian dipelajari serta diteliti sebagai suatu kesatuan yang utuh. Dengan demikian penelitian ini diharapkan dapat menghasilkan analisis yang mampu menjawab permasalahan yang telah dirumuskan.

D. Sistematis Penulisan

Untuk memudahkan penyusunan skripsi ini maka disusunlah sistematikanya yang dibagi dalam empat Bab antara lain sebagai berikut:

Bab I, Pendahuluan Merupakan Bab Pendahuluan Yang Terdiri Dari 4 (Empat) Sub Bab Yang Memuat Latar Belakang Masalah,Ruang Lingkup Dan Tujuan Peelitian, Metode Penelitian, Dan Sistematika Penulisan

Bab II, Merupakan Bab Teoritis Dengan Judul Tinjauan Umum Tentang Penyidikan, Bentuk-Bentuk Kejahatan Teknologi Informasi,

Kebijakan Hukum Dalam Penanggulangan Tindak Pidana Teknologi Informasi, Pengertian Penyidikan, Pengertian Manipulasi Data

Bab III, Merupakan Bab Dari Hasil Penelitian Yang Berjudul Pelaksanaan Penyidik Terhadap Tindak Pidana Penipuan Program Prakerja**,** Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Data Program Prakerja, Kendala Penyidik Terhadap Tindak Pidana Penipuan Data Program Prakerja, Strategi Perlindungan Data Oleh Pihak Kepolisian Resor Bireun Untuk Mencegah Terjadinya Pembobolan Data

Bab IV, Penutup Merupakan Bab Penutup Dari Penulisan Skripsi Yang Berisikan Kesimpulan Dari Bab-Bab Yang Telah Di Bahas Sebelumnya Dan Saran Yang Berkaitan Dengan Masalah Yang Di Bahas Dalam Penulisan Skripsi Ini.

BAB II
TINJAUAN UMUM

A. Bentuk-Bentuk Kejahatan Teknologi

Teknologi informasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.[1]

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime*.

Ringkasnya, sesuai dengan ungkapan "kejahatan merupakan produk dari masyarakat sendiri" (crime is a product of society its self), "habitat" baru

[1] Abdul Wahid dan Mohammad Labib, *Kejahtan Mayaantara (Cybercrime*), Bandung, PT Refika Aditama, 2005 hlm. 23.

ini, dengan segala bentuk pola interaksi yang ada didalamya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan lain yang sebelumnya telah dikenal. Kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah *cybercrime*.[2]

Pada masa awalnya, *cybercrime* didefinisikan sebagai kejahatan komputer. Mengenai definisi kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan *istilah computer misuse, computer abuse, computer fraud, computer related crime, computer assistend crime, atau computer crime.* Namun para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian istilah computer crime oleh karena dianggap lebih luas dan bias dipergunakan dalam hubungan internasional.

Adapun bentuk-bentuk kejahatan teknologi informasi dalam empat klarifikasi berikut:

1. Komputer Sebagai Objek

   Dalam kategori ini, bentuk-bentuk *cybercrime* termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat di dalamnya atau perusakan terhadap sarana-sarana komputer seperti Air Condutouring (AC) dan peralatan yang menunjang pengoprasian komputer.

[2] J. E Sahetapy dalam Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum Unisma, Malang,2005.

2. Komputer Sebagai Subjek

   Komputer dapat pula menimbulkan tempat atau lingkungan untuk melakukan kejahatan, misalnya pencurian, penipuan, dan pemalsuan yang menyangkut harta benda dalam bentuk baru yang tidak dapat disentuh (intangible), misalnya pulsa elektronis dan guratan-guratan magnetis.

3. Komputer Sebagai Alat

   Komputer digunakan sebagai alat melakukan kejahatan sehingga sifat peristiwa kejahatan tersebut adalah sangat kompleks dan sulit diketahui. Salah satu contoh adalah seseorang pelaku kejahtan yang mengambil warkat-warkat setoran darai suatu bank dan menulis nomor rekening pelaku dengan tinta magnetis pada warkat-warkat tersebut kemudian melaetakkan kembali ke tempat semula. Nasabah yang akan 46 memasukkan uang akan mengambil dan mengisi warkat yang sudah dibubuhi nomor rekening pelaku kejahatan memroseswarkat-warkat nasabah, komputer secara otomatis akan mengredit sejumlah uang pada rekening pelaku kejahtan. Salah iyu, pelaku kejahtan menarik uang dengan cek dari rekeningnya sebelum peram nasabah yang menyetor mengajukan komplain ke bank.

4. Komputer Sebagai Simbol

   Suatu komputer dapat digunakan sebagai simbol untuk melakukan penipuan atau ancaman, dalam kategori ini termasuk penipuan “Biro Jodoh” yang menyatakan bahwa biro jodoh tersebut memakai komputer

untuk membantu si koraban mencari jodoh, akan tetapi ternyata biro jodoh tersebut sama sekali tidak memakai komputer untuk keperluan tersebut.[3]

B. Pengertian Penipuan Biasa Dan Penipuan *Online*

a. Pengertian Penipuan Biasa

Penipuan berasal dari kata tipu yang berarti perbuatan atau perkataan yang tidak jujur, bohong atau palsu dan sebagainya dengan maksud untuk menyesatkan, atau mencari keuntungan.[4] Tindakan penipuan merupakan suatu tindakan yang merugikan orang lain sehingga termasuk ke dalam tindakan yang dapat dikenakan hukum pidana.

Penipuan dalam Kamus Besar Bahasa Indonesia (KBBI) disebutkan bahwa tipu berarti kecoh, daya cara, perbuatan atau perkataan yang tidak jujur (bohong, palsu, dan sebagainya), dengan maksud untuk menyesatkan, mengakali, mencari untung. Penipuan berarti proses perbuatan, cara menipu, perkara menipu (mengeco). Dengan demikian maka berarti bahwa yang terlibat dalam penipuan adalah dua pihak yaitu orang menipu disebut dengan penipu oleh orang yang tertipu.

Tindak Pidana penipuan yang termuat dalam bab XXV buku II KUHP dari pasal 378-395, titel asli bab ini adalah bedroog, yang oleh banyak ahli diterjemahkan sebagai penipuan atau perbuatan curang. Penipuan memiliki dua pengertian yaitu :

---

[3] Agus Rahardjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*.PT Citra Aditiya Bakti, Bandung 2002 hlm 32

[4] http;/bacaonline.blospot.com/2011/05/hukum-penipuan-melalui.html.diakses pada tanggal 11 Juni 2024 jam 19.00

a) Penipuan dalam arti luas, yaitu semua kejahatan yang dirumuskan dalam bab XXV KUHP.
b) Penipuan dalam arti sempit ialah bentuk penipuan yang dirumuskan dalam pasal 378 (bentuk pokoknya) dan 379 (bentuk khususnya) atau yang biasa disebut dengan oplichting.

Dalam KUHP sendiri merumuskan mengenai pengertian penipuan (Oplichting) pasal 378 yang berbunyi : "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (Hoedaniqheid) palsu, dengan tipu muslihat ataupun rangkaian kebohongan, menggerakkan orang lain untuk mengerahkan barang sesuatu kepadanya atau supaya memberi utang maupun, menghapuskan piutang diancam karena penipuan, dengan pidana penjara paling lama 4 tahun".

b. Pengertian Penipuan *Online*

Penipuan yang dilakukan secara online atau elektronik jelas merupakan hal yang dapat mengakibatkan kerugian bagi orang lain, dan dilarang dalam Undang-undang. Peran serta masyarakat sangat penting dalam upaya mengungkap kejahatan penipuan online.

Sedangkan dalam UU ITE, pasal yang mengatur terkait dengan tindak pidana penipuan khususnya di internet, diatur dalam Pasal 28 ayat (1), yang berbunyi sebagai berikut : Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Ancaman pidana yang dapat dikenakan terhadap pelaku adalah pidana penjaran paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1 miliar sebagaimana disebutkan dalam Pasal 45 ayat (2) UU ITE, perihal ketentuan pidana dari pasal 28 ayat (1) UU ITE. Perlu diketahui sebelumnya, walaupun isi dari Pasal 28 ayat (1) tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan adanya unsur sebagaimana disebutkan dalam pasal tersebut yaitu "kerugian konsumen dalam transaksi elektronik", maka pasal tersebut dapat digunakan terhadap pelaku yang melakukan tindak pidana penipuan di internet.

Terkait adanya 2 (dua) aturan mengenai tindak pidana penipuan di internet atau penipuan secara online yakni Pasal 378 KUHP dan Pasal 27 ayat (1) UU ITE, mengenai kebijakan yang dapat diterapkan kepada pelaku sepenuhnya di kembalikan kepada penyidik untuk menentukan pasal mana yang akan dikenakan terhadap pelaku, disini dibutuhkan kejelian dari pihak penyidik yang menanganiya. Namun tidak menutup kemungkinan juga pihak penyidik dapat menggunakan kedua pasal tersebut secara bersamaan atau istilah yang biasa disebut pasal berlapis, apabila memang unsur-unsur dari kedua pasal tersebut terpenuhi.[5]

C. Pengertian Penyidikan Tindak Pidana *Cybercrime*

Penyidikan menurut Kitab Undang-Undang Hukum Acara Pidana yang tercantung dalan Pasal 1 angka (2) KUHAP diartikan "Serangkaian tindakan

[5] Sudarto. Kapita Selekta Hukum Pidana. Alumni. Bandung, 2006 Hal 11.

penyidik dalam hal dan menurut cara yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terangnya suatu tindak pidana yang terjadi dan guna menemukan tersangkanya."

Penyidikan adalah suatu tindak lanjut dari kegiatan penyelidikan dengan adanya persyaratan dan pembatasan yang ketat dalam penggunaan upaya paksa setelah pengumpulan bukti permulaan yang cukup guna membuat terang suatu peristiwa yang patut diduga merupakan tindak pidana.[6]

Penyidikan merupakan tahapan penyelesaian perkara pidana setelah penyelidikan yang merupakan tahapan permulaan mencari ada atau tidaknya tindak pidana dalam suatu peristiwa. Ketika diketahui ada tindak pidana terjadi, maka saat itulah penyidikan dapat dilakukan berdasarkan hasil penyelidikan. Pada tindakan penyelidikan, penekanannya diletakkan pada tindakan "mencari dan menemukan" suatu "peristiwa" yang dianggap atau diduga sebagai tindakan pidana. Sedangkan pada penyidikan titik berat penekanannya diletakkan pada tindakan "mencari serta mengumpulkan bukti". Penyidikan bertujuan membuat terang tindak pidana yang ditemukan dan juga menentukan pelakunya.

Penyidikan itu dilakukan untuk mencari serta mengumpulkan bukti-bukti yang pada tahap pertama harus dapat memberikan keyakinan walau sifatnya masih sementara, kepada penuntut umum tentang apa yang sebenarnya terjadi atau tentang tindak pidana apa yang telah dilakukan serta

[6]M.Yahya harahap,*Pembahasan permasalahan dan penerapan kuhap*,Sinar Grafika, Jakarta, 2002,Hlm.99

siapa tersangkanya. Penyidikan dilakukan untuk kepentingan peradilan, khususnya untuk kepentingan penuntutan, yaitu dapat atau tidaknya suatu tindakan atau perbuatan itu dilakukan penuntutan.[7]

Tahap penyidikan merupakan salah satu bagian penting dalam rangkaian tahap-tahap yang harus dilalui suatu kasus menuju pengungkapan terbukti atau tidaknya dugaan telah terjadinya suatu tindak pidana. Oleh sebab itu keberadaan tahap penyidikan tidak bisa dilepaskan dari adanya ketentuan perundangan yang mengatur mengenai tindak pidannanya.[8]

Penyidikan sendiri ada yang disebut penyidik yaitu orang yang melakukan penyidikan yang terdiri dari pejabat yang dijelaskan pada Pasal 1 butir (1) Kitab Undang-Undang Hukum Pidana. Pejabat penyidik sendiri terdiri dari Penyidik Polri dan Penyidik Pegawai Negeri Sipil.[9] Penyidikan dalam acara pidana hanya dapat dilakukan berdasarkan undang-undang, hal ini dapat disimpulkan dari kata-kata "menurut cara yang diatur dalam undang-undang ini.[10]

D. Pengertian Perlindungan Data Pribadi

Menurut Pasal 1 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan data pribadi memberikan definisi tentang data pribadi yaitu "Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau

---

[7]Zulkarenaenkoto, *Terobosanhukumdalampenyederhanaanprosesperadilan Pidana,* Jurnal Studi Kepolisian, STIKI, Jakarta, 2011,Hlm.150.

[8]Hib nu Nugroho, *Integralisasi Penyidikan Tindak Pidana Korupsi Di Indonesia*, Media Aksara Prima, Jakarta, 2012, Hlm. 67

[9]M. Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHAP,* Sinar Grafika, Jakarta, 2000, Hlm. 112

[10]Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2000, Hlm. 119

dikombinasi dengan informasi lainnya baik secara langsung maupuntidak langsung melalui sistem elektronik dan/atau nonelektronik".

Undang-Undang ITE tidak memberikan definisi hukum yang jelas tentang data pribadi. Akan tetapi, dilihat dari prespektif penafsiran resmi tentang hak pribadi *(pivacy right)* dalam Pasal 26 ayat (1), maka data pribadi meliputi urusan kehidupan pribadi termasuk (riwayat) komunikasi seseorang dan data tentang seseorang.

Perlindungan hukum itu sendiri adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban, perlindungan hukum korban kejahatan sebagai bagian dari perlindungan masyarakat, dapat diwujudkan dalam berbagai bentuk, seperti melalui pemberian restitusi, kompensasi, pelayanan medis, dan bantuan hukum.[11]

E. Kebijakan Hukum Dalam Penanggulangan Tindak Pidana Teknologi Informasi

a. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *cybercrime*. Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *cybercrime*. Namun undangundang ini hanya mengatur beberapa

[11]Soerjono Soekanto, *Pengantar Penelitian Hukum,* Ui Press. Jakarta, 1984, Hlm 133

tindak pidana yang termasuk tindak pidana *cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomudir tindak-tindak pidana yang berkaitan dengan komputer.

"Pasal 22 yang berbunyi: "Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

1) Akses ke jaringan telekomunikasi; dan atau
2) Akses ke jasa telekomunikasi; dan atau
3) Akses ke jaringan telekomunikasi khusus."

"Pasal 38 yang berbunyi: "Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi"

"Pasal 40 yang berbunyi: "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun"

Bentuk-bentuk tindak pidana *cybercrime* dalam Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamnanya. Telekomunikasi

merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *cybercrime.*

b. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Tanggal 23 April 2008 telah diundangkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini bukanlah undang-undang tindak pidana khusus, melainkan juga memuat tentang pengaturan mengenai pengelolaan informasi dan transaksi elektronik dengan tujuan pembangunan, namun undang-undang ini juga mengantisipasi pengaruh buruk dari pemanfaatan kemajuan teknologi ITE tersebut, yakni dengan diaturnya hukum pidana khususnya tentang tindak pidana yang menyerang kepentingan hukum orang pribadi, masyarakat, atau kepentingan hukum Negara dengan memanfaatkan kemajuan teknologi ITE, atau sering disebut tindak pidana *cybercrime*. Undang-Undang Informasi dan Transaksi Elektronik telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang Informasi dan Transaksi Elektronik (*cybercrime*) dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu. Tindak Pidana Cybercrime dalam Undang-Undang Informasi dan Transaksi Elektronik diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35.

Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 samapai dengan Pasal 34. Sementara ancaman pidananya ditentukan didalam Pasal 45 sampai Pasal 52. Adapun rumusan pasal-pasal tersebut adalah sebagai berikut:

"Pasal 27 yang berbunyi:

1) 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 yang melanggar kesusilaan.
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.
3) 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.
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 pengancaman

"Pasal 28 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA)."

"Pasal 29 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."

"Pasal 30 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

"Pasal 31 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ 36 atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
3) 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.

4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah."

"Pasal 32 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."

"Pasal 33 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat

terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

"Pasal 34 yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
   a) Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk 37 memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33
   b) Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum."

"Pasal 35 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen

Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik."

"Pasal 36 yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain."

"Pasal 37 yang berbunyi: "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."

BAB III
PELAKSANAAN PENYIDIK TINDAK PIDANA PENIPUAN PROGRAM PRAKERJA

A. Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Data Program Prakerja

Dalam penyidikan sendiri ada yang disebut penyidik yaitu orang yang melakukan penyidikan yang terdiri dari pejabat yang dijelaskan pada Pasal 1 butir (1) Kitab Undang-Undang Hukum Pidana. Pejabat penyidik sendiri terdiri dari Penyidik Polri dan Penyidik Pegawai Negeri Sipil. Tahap penyidikan terhadap suatu perkara biasanya dilakukan setelah penyidik mengetahui adanya suatu peristiwa yang diduga merupakan suatu tindak pidana. Disamping itu, penyidikan juga akan dimulai apabila penyidik menerima laporan ataupun pengaduan tentang dugaan telah terjadinya suatu tindak pidana.

Penyidikan merupakan suatu proses atau langkah awal yang merupakan suatu proses penyelesaian suatu tindak pidana yang perlu diselidik dan diusut secara tuntas di dalam sistem peradilan pidana, dari pengertian tersebut, maka bagian-bagian dari hukum acara pidana yang menyangkut tentang Penyidikan adalah ketentuan tentang alat- alat bukti, ketentuan tentang terjadinya delik, pemeriksaan di tempat kejadian, pemanggilan tersangka atau terdakwa, penahan sementara, penggeledahan, pemeriksaan dan introgasi, berita acara, penyitaan, penyampingan perkara, pelimpahan perkara kepada penuntut umum dan pengembalian kepada penyidik untuk disempurnakan. Bedasarkan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik perbuatan

dapat dikatakan pidana apabila setiap orang dengan sengaja dan tanpa hak melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan dokumen elektronik tersebut dianggap seolah-olah data yang otentik.[1]

Pada proses penyidikan penegakan hukum terhadap tindak pidana penipuan data menghadapi hambatan teknis, khususnya pada tahap pemeriksaan saksi dan korban pada tahap penyidikan oleh *reserse* khususnya satuan *cybercrime*. Hal ini dikarenakan seorang saksi yang seharusnya melihat, mendengar atau mengetahui secara nyata suatu tindak pidana tetapi karena sifat tindak pidana manipulasi data dan atau dokumen elektronik adalah dilakukan secara elektronik maka saksi hanya mengetahui setelah tindak pidana tersebut terjadi. Selain itu data serangan di *log server* terkadang sudah dihapus biasanya terjadi pada kasus *deface*, hal ini menyebabkan Penyidik menemui hambatan teknis dalam menemukan faktanya. Agar proses penyidikan tindak pidana manipulasi data dan/atau dokumen elektronik tidak menghadapi hambatan teknis lagi yaitu dengan kerjasama antara penyidik Polri dengan penyidik dan pihak lain untuk saling bertukar informasi dan barang bukti, sehingga barang bukti tersebut dapat digunakan sebagai alat masalah-masalah hukum, bukti untuk membangun keyakinan hakim akan kebenaran tindak pidana yang dilakukan oleh terdakwa. Selanjutnya,

[1] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

informasi atau pendapat dari profesional TI yang ahli di bidangnya harus digunakan, dan informasi yang diperoleh dapat diperhitungkan ketika hakim memutuskan kasus berdasarkan bukti yang tersedia.[2]

Unsur tindak pidana sangat penting untuk diketahui oleh setiap penegak hukum, khususnya penyidik tindak pidana. Unsur tindak pidana penting karena dari unsur-unsurnyalah suatu tindak pidana bisa diidentifikasi dan bisa dibuktikan. Sehingga dalam penegakan hukum pidana adalah hal yang penting untuk mengetahui dan menguraikan unsur tindak pidana. Pada konteks penelitian ini tindak pidana yang dibahas adalah tindak pidana manipulasi informasi elektronik dan/atau dokumen elektronik merupakan perbuatan yang sangat tercela dan dapat merugikan banyak masyarakat. Tindak pidana manipulasi Informasi Elektronik dan/atau Dokumen Elektronik dilakukan melalui media elektronik, sehingga hal-hal yang menyangkut pembuktiannya akan sedikit banyak berbeda dengan tindak pidana biasa.

Tindak Pidana manipulasi informasi elektronik dan/atau dokumen elektronik diatur pada Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik dan ancaman pidananya terdapat pada Pasal 51 dan 45 undang-undang tersebut. Adapun unsur-unsur yang diterapkan oleh penyidik adalah yang pertama unsur subjektif yaitu “Setiap Orang dengan

[2] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

sengaja dan tanpa hak atau melawan hukum". Unsur yang dimaksud "yang dengan sengaja" adalah adanya bukti suatu kehendak untuk mewujudkan unsur di dalam suatu delik menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah pelaku aktif atau yang terbukti melakukan tindakan yang dapat dimaknai sebagai suatu perbuatan hukum termasuk perbuatan secara teknis dalam penggunaan teknologi, namun dengan tanpa mempertimbangan motif dan alasannya sebagaimana yang telah dirumuskan oleh UndangUndang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan pelaku telah mengetahui atau menyadari atau menghendaki akibat dari perbuatan tersebut. Bukti kesengajaan antara lain dapat ditunjukkan dengan perbuatan Pelaku yang terekam ke dalam sistem elektronik, dari catatan aktivitas akun miliknya atau yang sedang dikuasainya atau yang sedang digunakannya dan/atau yang dilaksanakan berulang kali sehingga diketahui oleh Saksi.

Pasal 35 Undang Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini diatur secara alternatif, maksudnya cukup dibuktikan bahwa pelaku dengan sengaja melakukan salah satu atau beberapa dari perbuatan yang dimaksud. Melalui perbuatan-perbuatan ini maka muncul hak yang tidak sah bagi dirinya atau orang lain. Dimana penggunaan hak yang dimaksud adalah tanpa alas hukum atau kewenangan sehingga menjadi tidak sah atau melanggar hak orang lain. Pada perkara ini perbuatan yang dilakukan adalah manipulasi data.

Perbuatan penipuan, yaitu proses rekayasa melalui penambahan atau pengurangan atau penghilangan atau mengkaburkan atau menyembunyikan sebagian atau keseluruhan suatu realitas, kenyataan, fakta-fakta ataupun sejarah dan/atau material (benda) yang dilakukan dengan menggunakan alat sistem perancangan atau sebuah tata sistem nilai, tanpa disadari oleh pihak penerima informasi dan/atau dokumen elektronik sehingga sesuatu itu akan seolah-olah menjadi memiliki makna, substansi/kandungan, yang berbeda dari aslinya (tidak otentik) atau diarahkan pada pengertian lain yang diinginkan oleh pengirim.

Mengenai subjek tindak pidana dalam Undang-Undang Informasi dan Transaksi Elektronik telah ditentukan bahwa subjek yang kepadanya bisa dimintakan pertanggung jawaban terhadap tindak pidana yang berkaitan dengan kejahatan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik adalah orang perorangan dan atau korporasi. Selanjutnya yang dimaksud orang perorangan adalah setiap orang yang sudah dewasa atau sudah menikah menurut undang-undang yang berlaku di Indonesia. Sedangkan yang dimaksud korporasi adalah setiap badan usaha yang berbentuk badan hukum dan yang bukan badan hukum. Selanjutnya di dalam ketentuan lain yang mengatur tentang subjek hukum orang perorangan ditentukan bahwa orang perorangan adalah setiap warga negara Indonesia, warga negara luar negeri, maupun badan hukum. Secara eksplisit Undang-Undang Informasi dan Transaksi Elektronik telah mengatur bahwa pertanggungjawaban hukum korporasi terkait tindak pidana yang diatur

dalam Undang-Undang Informasi dan Transaksi Elektronik menganut sistem perumusan yang alternatif komulatif artinya bisa dipisah dan bisa disatukan unsur tindak pidananya. Sebagaimana diatur dalam Pasal 52 ayat (4) Undang-Undang Informasi dan Transaksi Elektronik. Hal yang menjadi penegasan terhadap pasal tersebut bahwa sifatnya mengandung pemberatan pidana. Mengenai jenis sanksi yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik bahwa terhadap tindak pidana yang berkaiatan dengan kejahatan yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik ditentukan 2 (dua) jenis sanksi yaitu sanksi pidana penjara bagi individu orang perorangan dan atau individu penanggungjawab dalam suatu korporasi serta pidana denda bagi orang perorangan dan atau korporasi.[3]

Tindak pidana yang dilakukan secara elektronik khususnya tindak pidana penipuan elektronik dan atau dokumen elektronik, sering dilakukan dengan menggunakan paksaan atau tipu muslihat terhadap korban. Berbagai tindakan yang sering dilakukan adalah dengan modus yang hampir serupa yaitu seperti memanfaatkan secara melawan hukum perkembangan informasi elektronik. Tindakan pidana yang berupa penipuan informasi dan dokumen elektronik tersebut ditujukan untuk mencuri atau membobol data dengan cara menipu korban. Seperti yang di teliti oleh penulis dalam kasus manipulasi data program prakerja tindakan manipulasi data atau dokumen elektronik yang dialami akan menimbulkan kerugian materil dan kerugian imateril. Tindakan-tindakan manipulasi data atau dokumen elektronik tersebut antara

[3] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

lain seperti: kejahatan kartu kredit antara lain yaitu *Phising, Carding, Hacking, Skimming* dan Ekstrapolasi, tindakan-tindakan jahat tersebut yang sering terjadi di masyarakat Indonesia.

Kejahatan penipuan online bukan hanya menggunakan komputer saja, akan tetapi juga melibatkan teknologi komunikasi di dalam pengoprasianya. Untuk pengaturan hukum *cybercrime* sendiri diatur oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Berdasarkan asas *lex specialis derogat legi generali* ,berarti aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturan-aturan hukum yang umum. Sehingga *cybercrime* termasuk kejahatan khusus dan memiliki aturan sendiri dalam penanganannya.

Kejahatan siber yang selanjutnya disebut *cybercrime* merupakan kejahatan yang termasuk baru dibandingkan dengan kejahatan pembunuhan ataupun pencurian, akan tetapi kejahatan siber sama merugikannya bagi manusia. Kejahatan siber memang tidak dapat dirasakan secara fisik namun sama merugikannya seperti pembunuhan, perampokan atau pencurian.

Seperti yang terjadi dalam kasus yang dilakukan oleh dua tersangka tindak pidana Informasi dan Transaksi Elektronik (ITE), yang melakukan manipulasi data peserta program prakerja hingga bisa mencairkan bantuan, diringkus Satreskrim Polres Bireuen, Kamis 2 Desember 2021. Kedua tersangka nekat menggunakan ratusan Nomor Induk Kependudukan (NIK) milik orang lain sejak Juli 2021, dan sudah mendapatkan keuntungan hingga

Rp 150,000,000 juta dari beberapa kali penarikan insentif yang dilakukan. Keduanya berinisial HE, 36 tahun, pekerjaan wiraswasta, beralamat di Gampong Keude Alue Rheng, Kecamatan Peudada dan RI, 32 tahun, pekerjaan wiraswasta, beralamat Gampong Sangso, Kecamatan Samalanga. Mudahnya akses mendapatkan NIK milik orang lain, kata Kapolres karena salah seorang tersangka berinisial HE, sebelumnya pernah bekerja sebagai penjual jasa (calo) pembuatan Nomor Pokok Wajib Pajak (NPWP) milik orang lain tahun 2018.[4]

Pendaftaran Kartu Prakerja di tujukan bagi pencari kerja, pekerja/buruh yang terkena PHK, atau pekerja/buruh yang membutuhkan peningkatan kompetensi kerja, seperti pekerja/buruh yang dirumahkan dan pekerja bukan penerima upah, termasuk pelaku usaha mikro dan kecil. Untuk itu, harus memenuhi persyaratan sebagai warga negara Indonesia berusia paling rendah 18 (delapan belas) tahun dan tidak sedang mengikuti pendidikan formal. Untuk merespon dampak dari pandemi COVID-19, Program Kartu Prakerja untuk sementara waktu akan diprioritaskan bagi pekerja/buruh yang dirumahkan maupun pelaku usaha mikro dan kecil yang terdampak penghidupannya. Difabel juga dianjurkan untuk mendaftar dan mengikuti Program Kartu Prakerja. Dalam 1 (satu) Kartu Keluarga hanya diperbolehkan maksimal 2 (dua) NIK yang menjadi Penerima Kartu Prakerja. Hanya warga negara Indonesia yang berumur minimal 18 tahun dan maksimal 64 tahun yang dapat menjadi Penerima Kartu Prakerja. Solusi yang ditawarkan pada

[4] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

program Kartu Prakerja diantaranya membantu meringankan biaya pelatihan yang ditanggung pekerja dan perusahaan. Mendorong kebekerjaan dengan mengurangi ketidak cocokan, mengurangi biaya untuk mencari informasi mengenai pelatihan, menjadi komplementer dari pendidikan formal, dan membantu daya beli masyarakat yang terdampak mata pencahariannya akibat COVID-19. Akan tetapi yang terjadi dalam kasus yang penulis teliti terjadinya pelanggaran manipulasi data pribadi masyarakat yang merugikan sebagian kalangan masyarakat.

Hal ini dibuktikan dari banyaknya kasus *cybercrime* yang tak dapat dituntaskan oleh sistem peradilan Indonesia. Persoalannya terdapat pada sulitnya mencari pasal-pasal yang dapat dipakai sebagai landasan tuntutan di Pengadilan kepada pelaku penyalahgunaan teknologi (*Cybercrime*) berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai terobosan untuk dapat menjadi landasan dan perluasan asas-asas beserta sanksi pidananya yang saat ini telah mengalami amandemen menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[5]

Pemalsuan identitas data diri menurut Pasal 378 KUHP menyebutkan barang siapa dengan sengaja memasukkan nama atau identitas pribadi, melakukan tipu muslihat, kebohongan untuk mendapatkan keuntungan secara

[5] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

pribadi maka disebut sebagai tindakan penipuan dengan hukuman maksimal 4 tahun penjar

Marak Kartu Tanda Penduduk (KTP) sebagai identitas diri sangat penting bagi pemerintah untuk pengurusan administrasi kependudukan dan pengolahan data penduduk. Pada saat masih sering banyak kasus pemalsuan KTP yang dapat berakibat menjadi suatu tindak kriminal. NIK (Nomor Induk Kependudukan) sebagai Identitas penting dapat berubah-ubah karena setiap daerah berbeda-beda. Proses pembuatan KTP dilakukan secara manual membutuhkan waktu proses yang lama dan terkadang tidak efektif, proses yang seperti ini kadang membuat masyarakat enggan untuk melakukan pengurusan KTP. Identitas yang seharusnya menjadi salah satu tanda pengenal jati diri maupun status yang benar dari seseorang dipalsukan. Kejahatan pemalsuan Identitas mengandung sistem ketidak benaran atau palsu atas suatu hal (objek) yang sesuatunya itu nampak dari luar seolah-olah benar adanya, padahal sesungguhnya bertentangan dengan yang sebenarnya perbuatan pemalsuan Identitas merupakan suatu jenis pelanggaran terhadap 2 norma dasar, yaitu kebenaran dan ketertiban masyarakat.

Adapun bentuk-bentuk dari dokumen kependudukan tersebut, pada intinya meliputi antara lain Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), Kartu Tanda Penduduk Elektronik (KTP-el), Akta/Surat Nikah/Cerai, Akta Kelahiran/Kematian, Akta Pengesahan Anak, Pengangkatan Anak, Perubahan Nama dan Perubahan Status Kewarganegaraan. Sekilas pemalsuan dokumen kependudukan tampak

sederhana, dan sudah lazim terjadi. Namun demikian, meskipun kelihatannya sederhana, pemalsuan dokumen kependudukan dapat menimbulkan dampak yang serius, yakni munculnya berbagai tindak pidana di tengah masyarakat.

Kejahatan tersebut dibedakan menjadi 2 kategori, yakni *cybercrime* dalam pengertian sempit dan dalam pengertian luar. *Cybercrime* dalam pengertian sempit adalah kejahatan terhadap system komputer, sedangkan dalam pengertian luas mencakup kejahatan terhadap sistem jaringan komputer dan kejahatan yang menggunakan sarana komputer.[6]

Penyalahgunaan telah menjadi salah satu agenda dari kejahatan di tingakat global. Kejahatan di tingkat global ini menjadi ujian berat bagi masing-masing negara untuk memeranginya. Alat yang digunakan oleh negara untuk memerangi *cybercrime* ini adalah hukum. Hukum difungsikan salah satunya mencegah terjadinya penyebaran *cybercrime*, serta menindak jika *cybercrime* berbukti telah menyerang atau merugikan masyarakat dan negara.

Kitab Undang-Undang Hukum Pidana (KUHP) telah mengatur hubungan-hubungan hukum tentang kejahatan yang berkaitan dengan dengan komputer (*computer crime*) yang kemudian berkembang menjadi *Cybercrime*. Keterdesakan kebutuhan nasional ini bisa dilihat dari adanya fakta bahwa aturan-aturan yang konvensional tidak dapat diandalkan dalam upaya penanggulangan kejahatan *cybercrime*, baik secara materiil (KUHP) maupun formal (KUHAP). Sebagaimana diketahui bahwa keberadaan KUHP

[6] Widodo, *Sistem Pemidanaan Dalam Cybercrime Altenatif Ancaman Pidana Kerja Social Dan Pidana Pengawasan Bagi Pelaku Cybercrime*, Laksabang Mediatama, Yogyakarta 2009 Hlm.24

dan KUHAP sebagai induk dari aturan hukum pidana dan acara pidana masih belum mampu menanggulangi kejahatan di dunia *cyber* yang berkaitan dengan tindak pidana yang baru (berdimensi dunia maya). Ketentuan yang terdapat dalam KUHP mengenai *cybercrime* masih bersifat global. Jika ditinjau dari perspektif penafsiran hukum tentunya hal yang diatur secara global dalam KUHP dapat dilakukan penyesuaian secara praktis sebelum terakomodasi dalam undang-undang khusus yang mengaturnya secara terperinci.

Adapun tahapan penyidikan yang dilakukan oleh pihak Kepolisian Resor Bireuen dalam kasus tindak pidana manipulasi data program prakerja.[7]

1. Penyidikan

   Dalam tahap ini petugas menerima informasi atau laporan dari masyarakat tentang adanya suatu peristiwa yang diduga terdapat tindak pidana sehingga dapat dibuatkan laporan polisi. Kemudian penyidik melakukan pengumpulan barang bukti dan saksi-saksi yang terkait dalam kasus *cybercrime* 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.

[7] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

Dalam kasus manipulasi data pribadi adapun alat bukti yang telah di sebutkan dalam Undang-undang Perlindungan Data Pribadi dalam Pasal 64 ayat (3) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi meliputi :

a. Alat bukti sebagaimana dimaksud dalam hukum acara
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 Undang-Undang Perlindungan Data Pribadi yang disebutkan dalam KUHAP dan dalam Undang-Undang Informasi dan Transaksi Elektronik yaitu : Alat bukti pada KUHAP diatur dalam Pasal 184 ayat (1) menyebutkan, (1) Alat bukti yang sah

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

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 luar 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 oleh para ahli dalam kasus *Cybercrime*

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 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.

Dalam tahap ini melakukan digital forensic pada barang bukti yang telah dikumpulkan oleh penyidik. Pemeriksaan ini dilakukan oleh ahli-ahli dalam kasus *cybercrime* 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.

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 24 barang bukti dalam kasus *cybercrime* yang belum

memiliki rumusan yang jelas dalam penentuannya sebab digital evidence tidak selalu dalam bentuk fisik yang nyata. Karena dalam kasus *cybercrime* 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. 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.

5. 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

B. Hambatan Penyidik Terhadap Tindak Pidana Penipuan Data Program Prakerja

Kasus tindak pidana manipulasi data adalah suatu kasus yang memiliki kekhususan tersendiri dari kasus-kasus pidana umum lainnya, hal ini berpengaruh terhadap proses penyidikan yang khusus pula terhadap kasus manipulasi. Penyidik yang mempunyai wewenang khusus untuk melakukan

proses penyidikan terhadap kasus *cybercrime* adalah reserse khususnya satuan *cybercrime*, adapun dasar hukum pelaksanaan wewenang tersebut yaitu undang-undang terkait dengan tindak pidana *cybercrime* di Indoensia. Penyidik yang tergabung dalam satuan *cybercrime* bertugas melakukan penyidikan terhadap tindak pidana *cybercrime* yang terjadi di Indonesia.

Wewenang tersebut menjadikan penyidik berwenang untuk mengumpulkan alat bukti terkait dengan kasus *cybercrime* tersebut. Pedoman alat bukti telah diatur dalam ketentuan Pasal 184 KUHAP, yang menentukan bahwa alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Susunan alat bukti tersebut telah menentukan kekuatan pembuktian suatu tindak pidana. Penyidik dalam menyidik tindak pidana *cybercrime* alat bukti bisa berupa informasi elektronik dan dokumen elektronik yang bisa dihadirkan dalam persidangan bisa berupa tangkapan layar atau hasil cetakan file. Informasi dan dokumen elektronik tersebut bisa menjadi alat bukti yang sah dan digunakan sebagai dasar pertimbangan dalam putusan hakim jika diperoleh dari proses penyidikan yang sesuai dengan aturan dalam Undang-Undang ITE. Informasi atau dokumen elektronik yang merupakan hasil penyidikan dan dicetak selanjutnya dihadirkan di muka sidang bisa menjadi alat bukti yang saah secara hukum. Alat bukti tersebut merupakan perluasan makna dari alat bukti yang selama ini diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang berlaku sebagai hukum positif di Indonesia dan dijadikan pedoman dalam menentukan alat bukti suatu tindak pidana. Hasil

cetakan informasi atau dokumen elektronik tersebut yang dijadikan alat bukti berlaku sebagai alat bukti yang sah apabila setidaknya memenuhi persyaratan antara lain yaitu surat yang menurut undang-undang harus berbentuk tertulis, dan persyaratan yang lain yaitu dokumen atau informasi elektronik tersebut harus bersifat otentik karena dibuat oleh pejabat yang berwenang. Ada penjelasan lainnya yang masyaratkan bahwa informasi atau dokumen elektronik tersebut bisa digunakan sebagai alat bukti yang sah menurut hukum apabila bisa diakses secara umum, bisa dijamin kebenarannya serta bisa didukung oleh ahli di bidang digital forensik.

Pada kasus Tindak Pidana Manipulasi Data Program Prakerja secara spesifik tentang tindak pidana manipulasi data dan/atau dokumen elektronik dalam praktik di lapangan ternyata pada tahap penyidikan terhadap kasus tersebut, sering kali penyidik diperhadapkan pada kendala atau hambatan teknis yang sedikit banyak berpengaruh terhadap nilai pembuktian ketika kasus tindak pidana manipulasi data dan/atau dokumen elektronik tersebut dipersidangkan. Kendala teknis tersebut lebih kepada sarana dan prasarana yang mendukung proses penemuan alat bukti untuk membuktikan dan membuat terang suatu tindak pidana manipulasi data dan/atau dokumen elektronik.[8]

Adapun kendala dan hambatan yang dihadapi Penyidik Terhadap Tindak Pidana Penipuan Data Program Prakerja.

[8] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

1. Perangkat hukum yang belum memadai Para penyidik (khususnya Polsek) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat Undang-Undang yang khusus mengatur *cybercrime*.
2. Kemampuan penyidik Secara umum penyidik Polsek masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah
    a. Kurangnya pengetahuan tentang komputer.
    b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *Cybercrime* masih terbatas.
    c. Faktor sistem pembuktian yang menyulitkan para penyidik
3. Alat Bukti Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *Cybercrime* antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *Cybercrime* seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.
4. Fasilitas komputer forensik Untuk membuktikan jejak-jejak para *hacker* dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan

program-program dan data-data komputer, sarana Polsek belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap datadata digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (image, program, dsb). Dalam hal ini Polsek masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness.*

5. 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.

Selain itu kendala atau hambatan teknis yang dihadapi seorang penyidik dalam menangani tindak pidana manipulasi data dan/atau dokumen elektronik

adalah menemukan tersangka, menentukan tempat kejadian, tindak pidananya dan kesulitan dalam menentukan waktu terjadinya tindak pidana manipulasi data dan/atau dokumen elektronik.[9]

Kendala teknis lainnya yaitu banyak teknologi yang dirancang dengan sistem keamanan yang sulit untuk dibaca atau diketahui oleh orang lain dengan menggunakan kata sandi atau password untuk bisa masuk ke dalam sistem elektronik tersebut. Sehingga kesulitan tersebut yang menjadi hambatan teknis penyidik dalam menangani tindak pidana manipulasi data dan/atau dokumen elektronik, dan dibutuhkannya sumber daya manusia yang mumpuni dan peralatan komputer forensik yang baik.

Terkait dengan penentuan tempat kejadian tindak pidana yang dilakukan secara elektronik seperti halnya tindak pidana manipulasi data dan/atau dokumen elektronik terutama mengenai kompetensi kepolisian daerah mana yang berwenang memeriksa tindak pidana manipulasi data dan/atau dokumen elektronik tersebut. Selain itu mengenai penentuan waktu kejadian dalam tindak pidana manipulasi data dan/atau dokumen elektronik menjadi permasalahan sendiri karena tindakan pidana tersebut apabila tidak ditangani secara patut oleh penyidik yang mumpuni maka kesulitan menentukan waktu kejadian dalam tindak pidana manipulasi data dan/atau dokumen elektronik akan terjadi.

[9] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun,Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

Seperti hal lainnya yang terkait dengan penyidikan tindak pidana manipulasi data dan/atau dokumen elektronik dari hasil pencarian terjauh hanya mengembalikan alamat IP pelaku dan komputer yang digunakan. Ada banyak masalah dalam penyitaan bukti karena pengadu biasanya terlalu lambat untuk melapor, menyebabkan data penyerangan dihapus dari *log server*, yang biasanya terjadi pada kasus pelanggaran, sehingga sangat sulit bagi penyelidik untuk menemukan kesulitannya adalah *log statistik* yang terdapat di server, karena server biasanya otomatis. Hapus *log* yang ada untuk mengurangi beban *server*. Oleh karena itu, penyidik mungkin tidak mendapatkan data yang perlu dijadikan bukti, padahal data log statistik merupakan salah satu alat bukti yang paling penting.

Pemeriksaan saksi dan korban menghadapi banyak kendala karena tidak ada saksi yang melihat tindak pidana (*testimonium de auditu*) pada saat tindak pidana itu terjadi atau dilakukan. Mereka baru mengetahuinya setelah kejadian itu terjadi, karena mereka merasakan dampak penyerangan yang telah dilakukan. Saksi ahli berperan sangat penting dalam memberikan keterangan dalam perkara pidana yang berkaitan dengan manipulasi informasi dan/atau dokumen elektronik, karena yang terjadi di dunia maya memerlukan keahlian dan pengetahuan khusus. Dalam tindak pidana manipulasi informasi dan/atau dokumen elektronik, saksi ahli dapat terdiri dari lebih dari satu saksi ahli, tergantung pada permasalahan yang dihadapi, seperti dalam perkara

pembelaan, selain saksi ahli yang mahir dalam desain grafis dan saksi ahli yang mengerti masalah jaringan dan saksi juga membutuhkan ahli program.[10]

Kendala lain bagi penegak hukum untuk menggunakan alat bukti digital melalui forensik komputer adalah lemahnya digital forensik, karena Lab Komputer Kepolisian Resor Bireuen belum tersedia. Seperti disebutkan di atas, pemeriksaan alat bukti digital dilakukan oleh para ahli. Seperti, laboratorium forensik yang digunakan berada di wilayah hukum Polda Aceh. Laboratorium forensik digital tidak dimiliki Polri di semua daerah. Keberadaannya sangat penting untuk mencegah dan menangani kasus-kasus yang berkaitan dengan kejahatan dunia elektronik. Kendala lain adalah kejahatan elektronik luar yurisdiksi hukum Indonesia sehingga menyulitkan penyidik untuk mengambil tindakan dan sangat baik dalam mengejar pelaku kejahatan/operator. Komisi dari semua jenis kejahatan. Hal ini terkait dengan kurangnya sumber daya manusia dalam hal pengetahuan teknologi digital dan kode digital di tingkat Polres, kejaksaan dan hakim, sehingga jelas ada masalah dalam menangani kejahatan dunia maya. Selain itu, undang-undang kejahatan dunia maya masih lemah, faktor yang dapat digunakan penjahat dunia maya untuk menemukan celah hukum untuk menghindari hukum.

Upaya digitalisasi bukti dengan menggunakan komputer forensik melibatkan pertukaran informasi dan kesaksian dari detektif polsek dan penyidik dari negara lain, yang dapat digunakan sebagai bukti untuk

[10] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

meyakinkan juri akan kebenaran kasus tersebut dilakukan oleh terdakwa. Oleh karena itu, penegakan hukum memerlukan kerja sama. Selain itu, hakim dapat meninjau perkara berdasarkan bukti-bukti, dengan menggunakan keterangan, keterangan dan pendapat yang tersedia dari para ahli telematika di bidangnya. Mendeklarasikan dan mengamankan bukti digital untuk analisis jangka panjang sehingga dapat dimintai pertanggungjawaban. Dengan pendekatan teknologi, aparat penegak hukum dan masyarakat dunia tidak dapat menyelesaikan permasalahan melalui pemanfaatan teknologi dalam pemrosesan perkara pidana.

C. Strategi Perlindungan Data Oleh Pihak Kepolisian Resor Bireuen Untuk Mencegah Terjadinya Pembobolan Data

Pasal 26 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjelaskan, perlindungan data pribadi dalam kaitannya pemanfaatan teknologi informasi. Dijelaskan bahwa data pribadi adalah salah satu bagian dari hak pribadi (*privacy rights*) yang mengandung pengertian merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.[11]

Menurut Pasal 1 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindunga Rahasia Pribadi menjelaskan,“Data Pribadi adalah

[11] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupuntidak langsung melalui sistem elektronik dan/atau nonelektronik

Dalam strategi perlindungan data pihak Kepolisian Resor Bireuen diminta lebih lagi dalam memanfaatkan ruang internet dan terus mengikuti perkembangan zaman terlebih dalam hal teknologi informasi dan teknologi komunikasi selain itu pada pihak Kepolisian diminta menjaga keadaan atau etika berbudaya yang baik di dalam internet itu sendiri, mengedepankan upaya preemtive dan preventif dan menjadi mediator serta memfaslitasi pihak yang bersengketa dan diharapkan mengambil keputusan yang kolektif dengan melibatkan pihak-pihak yang berkompeten serta mengedepankan hukum pidana sebagai upaya terakhir atau (*ultimum remidium*) dalam terkhusus dalam hal perkara *cybercrime* dan mengedepankan *restorative justice* serta pengawasan dalam setiap langkah penyidikan dan kordinasi antar lembaga penegak hukum itu sendiri.[12]

Fakta dilapangan menunjukan bahwa pencegahan *cybercrime* di wilayah Kepolisian Resor Bireuen belum berjalan sebagai mana mestinya baik melalui sarana penal maupun non penal. Pencegahan melalui sarana non penal atau preventif seperti patroli siber ataupun melalui sosialisasi tentang bahaya *cybercrime* yang belum memberikan dampak pada kejahatan

[12] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun,Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

cybercrime. Dari sisi penal ternyata dari sekian banyaknya kasus hanya sedikit yang sampai ke proses peradilan, jika melihat apa yang dilakukan oleh pihak Kepolisian Resor Bireuen, pencegahan *cybercrime* belum sepenuhnya terlaksana dengan baik. Kenyataannya pencegahan yang dilakukan oleh Polda Jam Kepolisian Resor Bireuen belum cukup efektif untuk menanggulangi *cybercrime*. Semakin maraknya *cybercrime* di wilayah hukum Kepolisian Resor Bireuen, antara kegiatan yang dilakukan oleh Kepolisian Resor Bireuen terjadi kesenjangan dengan fakta dilapangan atau kenyataan yang ada.

Adapun upaya yang dilakukan dalam perlindungan data oleh pihak Kepolisian Resor Bireuen untuk mencegah terjadinya pembobolan data[13]

1. Upaya Pre-emtif adalah upaya awal yang dilakukan oleh pihak Kepolisian Resor Bireuen untuk mencegah terjadinya tindak pidana. Usaha-usaha yang dilakukan dalam penanggulan kejahatan secara pre-emtif menanamkan nilai-nilai dan norma-norma yang baik sehingga norma-norma tersebut terinternalisai dalam diri seseorang. Meskipun ada kesempatan untuk melakukan pelanggaran/kejahatan tapi tidak ada niatnya untuk melakukan hal tersebut maka tidak akan terjadi kejahatan. Jadi dalam usaha pre-emtif faktor niat menjadi hilang meskipun ada kesempatan. Dalam upaya penangulangan pre-emtif ini pihak Kepolisian Resor Bireuen sebagai penegak hukum melakukan kegiatan seperti melakukan penyuluhan kepada

[13] Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun, Wawancara Tanggal 9 Oktober 2023, Pukul 10:22

masyarakat, memberikan penerangan, bimbingan, kegiatan tatap muka langsung, dan melakukan kegiatan sambaing.

2. Upaya Preventif adalah upaya pencegahan yang dilakukan agar kejahatan tidak terjadi. Karena seperti yang kita ketahui bersama kejahatan merupakan suatu fenomena kompleks yang terjadi disekeliling kita dan sangat meresahkan masyarakat. Dibandingkan upaya pre-emtif, upaya preventif jauh lebih baik karena sebelum terjadinya kejahatan, upayaupaya tersebut dipikirkan agar bagaimana kejahatan tersebut tidak terjadi. Banyak cara yang dilakukan untuk bagaimana kejahatan tersebut tidak terjadi, salah satunya melakukan sosialisi tentang suatu peraturan perundang-undangan bahwa apabila seseorang melakukan kejahatan akan diancam dengan sanksi pidana yang dapat membuat mereka dipenjara. Karena landasan tersebut masyarakat merasa takut untuk melakukan kejahatan. Upaya-upaya yang dilakukan pihak kepolisian memberikan, pengawalan, penjagaan, patroli kepada masyarakat mengenai Tindakan-tindakan sosial yang dapat menyebabkan terjadinya kejahatan dalam lingkungan masyarakat. Tindakan preventif pada *cybercrime* yang dilakukan adalah dengan membentuk patroli siber. Patroli juga dilakukan dalam *cyberspace* sebagai bentuk pencegahan dari kejahatan. Patroli yang dilakukan *cyberspace* adalah bentuk lain daripada patroli di dunia nyata, apa yang dilakukan cyberspace disebut patroli siber, patroli ini merupakan kebijakan Kepolisian di bidang *cybercrime* untuk menangulangi kejahatan yang dibentuk oleh Kepolisian Resor Bireuen

3. Upaya Represif adalah upaya tindakan atau penanggulangan yang dilakukan sesudah terjadinya kejahatan (tindak pidana). Tindak represif meliputi penyelidikan, penyidikan, penuntutan, sampai di laksanakannya pidana. Itu Ini semua merupakan kegiatan yang dilakukan oleh badanbadan yang bersangkutan dalam menanggulangi kejahatan dan merupakan komponen penting dalam politik kriminil. Tujuan dari adanya upaya represif yaitu agar seseorang yang telah melakukan tindak kejahatan tidak terulang lagi hal yang sama dan memikirkan untuk menyembuhkan terhadap pelaku kejahatan, dengan cara secara tidak langsung akan di penjara atau dimasukkan ke dalam rumah tahanan. Dengan harapan agar didalam rumah tahanan tersebut mereka mendapatkan bimbingan dan binaan sebaik mungkin agar mereka tidak melakukan kejahatan setelah melakukan perbuatan tersebut

BAB IV
PENUTUP

Bedasarkan dari berbagai uraian yang telah dikemukakan dalam bab-bab di atas,maka dalam bab ini terakhir ini akan ditarik kesimpulan dan saran sebagai berikut :

A. Kesimpulan

Kesimpulan dalam penelitian ini berdasarkan dari hasil pembahasan di antara lain :

1. Pelaksanaan proses penyidikan kasus tindak pidana penipuan data program prakerja yang terkait dengan informasi data pribadi dalam pelaksanaannya dari tahap penyidikn, Penindakan penyidik melakukan pencarian dan pemeriksaan saksi dan alat bukti yang terkait dengan kejahatan informasi data pribadi, Pemeriksaan oleh para ahli dalam kasus *Cybercrime,* Penyelesaian berkas perkara hingga Penyidik mengirim berkas perkara kepada jaksa penuntut umum.
2. Kendala atau hambatan yang ditemukan dalam Pelaksanaan Penyidikan Tindak Pidana penipuan Data Program Prakerja antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik
3. Srategi perlindungan data pihak Kepolisian Resor Bireuen diminta lebih lagi dalam memanfaatkan ruang internet dan terus mengikuti perkembangan zaman terlebih dalam hal teknologi informasi dan teknologi komunikasi, Adapun upaya-upaya strategi perlindungan data Upaya Pre-emtif adalah upaya awal yang dilakukan oleh pihak

Kepolisian Resor Bireuen untuk mencegah terjadinya tindak pidana, Upaya Preventif adalah upaya pencegahan yang dilakukan agar kejahatan tidak terjadi lagi, Upaya Represif adalah upaya tindakan atau penanggulangan yang dilakukan sesudah terjadinya kejahatan (tindak pidana).

A. Saran

1. Disarankan kepada penyidik Kepolisian Resor Bireuen dapat melakukan penyempurnaan perangkat hukum, mendidik para penyidik, serta melakukan upaya penanggulangan pencegahan terjadinya tindak pidana penipuan data
2. Disarankan kepada masyarakat agar lebih menjaga dan peduli terhadap kepentingan berkas-berkas rahasia milik pribadi

DAFTAR PUSTAKA

A. BUKU

Abdul Wahid dan Mohammad Labib, *Kejahtan Mayaantara (Cybercrime*), PT Refika Aditama, Bandung 2005

Adami Chazawi, *Pelajaran Hukum Pidana Bagian 1,* PT. Raja Grafindo Persada Jakarta 2014

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2000

Ahmad M.Ramli *Cyber Law Dan Haki Dalam Sistem Hukum Indonesia*, PT Refika Aditama, Bandung 2010

Bambang Waluyo*,penelitian hukum dalam praktek,sinar Grafika*, Jakarta.2002

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

Budi Suhariyanto, *Tindak Pidana Teknologi Informasi*, Rajagrafindo Persada Jakarta,2015

Hibnu Nugroho, *Integralisasi Penyidikan Tindak Pidana Korupsi di Indonesia*, Media Aksara Prima, Jakarta, 2012

Lamintang, P.A.F., *Dasar-Dasar Hukum Pidana Indonesia,* Cet III, Citra Aditya Bakti, Bandung 2002

Leden Marpaung, *Asas Teori Praktik Hukum Pidana*, PT. Sinar Grafika Jakarta 2005

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

Moeljatno, *Asas-asas Hukum Pidana*, Rineka Cipta Jakarta 2009

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

Sofian Satrawidjaja, *Hukum Pidana I*, Amrico, Bandung, 2002

Soerjono Soekanto, *Pengantar Penelitian Hukum,* Ui Press. Jakarta, 1984

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

B. PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Dasar Negara Republik Indonesia 1945

Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektroni Perubahan Dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektroni

C. JURNAL/MAKALAH

Elviandri dkk, Quo Vadis *Negara Kesejahteraan Meneguhkan Ideologi Welfare State Negara Hukum Kesejahteraan Indonesia*, Jurnal Mimbar Hukum, Edisi No 2 Vol 31, 2019

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,

Sahuri Lasmadi, *Tumpang Tindih Kewenangan Penyidikan Pada Tindak Pidana Korupsi Pada Perspektif Sistem Peradilan Pidana*, Jurnal Ilmu Hukum, Volume 2, Nomor 3, Universitas Jenderal Soedirman Fakultas Hukum, Purwokerto, Juli, 2010

Siti Dwi Yana. (2021). Efektivitas Program Kartu Prakerja dalam Membangun Sumberdaya Manusia. *Jurnal Investasi Islam*, *6*(1), 12-21. https://doi.org/10.32505/jii.v6i1.2763 diakses 25 Maret 2022

Zahrotunnimah, *Langkah Taktis Pemerintah Daerah Dalam Pencegahan Penyebaran Virus Corona Covid-19 di Indonesia*, Jurnal Salam : Jurnal Sosial & Budaya Syar-i, Vol. 7 No. 3 (2020), pp.247-260, DOI: 10.15408/sjsbs.v7i3.15103, Jakarta : FSH UIN Syarif Hidayatullah, 2020ZulkarenaenKoto,

TerobosanHukumDalamPenyederhanaanProsesPeradilan Pidana, Jurnal Studi Kepolisian, STIKI, Jakarta, 2011

https://www.readers.id/read/manipulasi-data-program-prakerja-dua-warga-bireuen-ditangkap/index.html.Diakses tanggal 5 Maret 2022

LAMPIRAN

Bripka Taufiq Banit IV Tipidter Satreskrim Polres Bireun

Lampiran Pertanyaan

1. Bagaimana Pelaksanaan Penyidikan Terhadap Tindak Pidana Penipuan Data Program Prakerja ?
2. Kendala Apasaja Yang Dihadapi Penyidik Terhadap Tindak Pidana Penipuan Data Program Prakerja ?
3. Strategi Perlindungan Data Oleh Pihak Kepolisian Resor Bireuen Untuk Mencegah Terjadinya Pembobolan Data ?
4. Upaya Apa Saja Yang Dilakukan Oleh Pihak Kepolisian Resor Bireun Untuk Menlindungi Masyarakat Agar Tidak Terjadi Tindak Pidana ?
5. Saran Yang Diberikan Oleh Pihak Kepolisian Resor Bireuen Untuk Penelitian Ini ?
6. Adakan Kasus-Kasus ITE Yang Lain Terjadi Di Wilayah Kepolisian Resor Bireuen ?