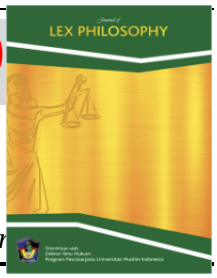
Journal of Lex Philosophy (JLP)
Volume 5, Nomor 1, Juni 2024
P-ISSN: 2722-1237, E-ISSN: 2722-2020
Website: http: pasca-umi.ac.id/index.php/jlp
This work is licensed under a Creative Commons Attribution 4.0 International Licer



Efektivitas Fungsi Kepolisian dalam Penyidikan Penyalahgunaan Informasi Dan Transaksi Elektronik

Muliadi[1], La Ode Husen[2] & A. Istiqlal Assaad[2]

[1]*Fakultas Hukum, Universitas Muslim Indonesia*
[2]*Magister Ilmu Hukum, Universitas Muslim Indonesia*
[*]*Koresponden Penulis, E-mail*: muliadi.muliadi@umi.ac.id

Submitted: 1 Maret 2024; Revised: 10 April 2024; Accepted: 16 April 2024

ABSTRAK
Tujuan penelitian menganalisis efektivitas fungsi kepolisian dalam penyidikan penyalahgunaan informasi dan transaksi elektronik di kota makassar oleh serta 2) untuk mengetahui dan menganalisa faktor-faktor yang mempengaruhi efektivitas fungsi kepolisian dalam penyidikan penyalahgunaan informasi dan transaksi elektronik di kota makassar oleh Tipe penelitian ini adalah empiris, data yang diperoleh penulis dari studi dokumen maupun wawancara dengan pihak yang berkepentingan dalam hal ini penyidik Polda Sulsel. Hasil Penelitian penulis mendapatkan bahwa: 1). Efektivitas penyidikan oleh Kepolisian terhadap penyalahgunaan Informasi dan Transaksi Elektronik (ITE) masih kurang efektif 2) Faktor-faktor yang menjadi kendala yang dihadapi oleh pihak Kepolisian dalam penyidikan tindak pidana penyalahgunaan Informasi dan Transaksi Elektronik (ITE): Aspek Penyidik, kemampuan dan skill penyidik.

Kata Kunci: *Penyidikan; Polisi, Informasi & Transaksi; Elektronik*

ABSTRACT
The research objective is to analyze the effectiveness of the police function in investigating the misuse of information and electronic transactions in the city of Makassar by and 2) to determine and analyze the factors that influence the effectiveness of the police function in investigating the misuse of information and electronic transactions in the city of Makassar by The type of this research is empirical, data obtained by the author from document studies and interviews with interested parties, in this case South Sulawesi Regional Police investigators. The author's research results found that: 1). The effectiveness of investigations by the Police regarding misuse of Information and Electronic Transactions (ITE) is still less effective 2) Factors that become obstacles faced by the Police in investigating criminal acts of misuse of Information and Electronic Transactions (ITE): Investigator aspects, abilities and skills of investigators.

Keywords: *Investigation; Police, Information & Transactions; Electronic*

PENDAHULUAN

Perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru (Sufianto, 2019). Penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan Peraturan Perundang-undangan demi kepentingan nasional. Pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat (Djanggih & Qamar, 2018).

Pemanfaatan Tekhnologi Informasi, media dan komunikasi telah mengubah aktivitas sosial masyarakat, baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan tekhnologi informasi dan komunikasi telah pula menyebabkan hubungan dunia tanpa batas dan menyebabkan perubahan sosial, ekonomi dan budaya secara signifikan berlangsung demikian cepat (Nashihin, Baroroh & Ali,2020).

Seiring dengan perkembangan zaman kejahatan yang masih terus terjadi sampai sekarang adalah kejahatan siber, Kejahatan siber, atau dikenal pula dengan cybercrime, adalah suatu bentuk kejahatan yang terjadi di jagat maya melalui komputer, perangkat seluler, dan jejaring internet (Bahri, 2023). Pelaku kejahatan siber ini umumnya adalah 'orang-orang pintar' yang paham bagaimana algoritma dan pemrograman komputer dijalankan. Melalui algoritma tertentu, pelaku dapat dengan mudah menganalisis, mencari celah, lalu pada akhirnya membobol perangkat kita. Saat pelaku sudah menguasai perangkat, pelaku dapat dengan leluasa mencuri data-data kita dan memanfaatkannya untuk keuntungan pribadi pelaku (Djanggih, 2018).

Terhadap kejahatan tersebut peran serta penegak hukum sangat dibutuhkan untuk memberantas kejahatan yang terjadi didalam Masyarakat, Fungsi polisi terdapat dalam pasal 2 Undang-undang No.2 Tahun 2002 yang berbunyi : "Fungsi kepolisian adalah salah satu fungsi pemerintahan Negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat (Ramadhan, 2021)." Pengertian kepolisian sebagai fungsi tersebut diatas sebagai salah satu fungsi pemerintahan negara dibidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, pelindung, pengayoman dan pelayanan kepada masyarakat (Arif, 2021). Sedangkan pengertian kepolisian sebagai lembaga adalah organ pemerintah yang ditetapkan sebagai suatu lembaga yang diberikan kewenangan menjalankan fungsinya berdasarkan peraturan perundang-undangan.

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat (Ketaren, 2016). Teknologi informasi saat ini menjadi pedang bermata dua karena selain membenkan kontribusi bagi peningkatan kesejahteraan kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Salah satu perkembangan teknologi yang sering

digunakan dan dibutuhkan semua kalangan masyarakat adalah komputer Dengan komputer seseorang dapat dengan mudah menyelesaikan pekerjaan, tetapi dengan adanya komputer seseorang menggunakannya pada hal-hal yang baik atau hal-hal yang buruk. Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer.

Tindak pidana cyber crime di Indonesia telah diatur Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kejahatan siber (*cyber crime)* merupakan perkembangan dari computer crime (Hutabarat, 2024). *Cyber crime* dan *cyber law* dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah menimbulkan korban, bukan hanya pada kalangan remaja namun disemua usia. Hal tersebut mengharuskan satuan kepolisian untuk segera bertindak dalam menangani kasus *cyber crime* (kejahatan dunia maya) yang cakupan kejahatannya sangat luas bahkan tidak terbatas. *Cyber crime* adalah kejahatan yang dilakukan oleh seseorang, sekelompok orang dan korporasi (badan hukum) dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Kejahatan ini terjadi didunia maya (virtual) sehingga mempunyai karakteristik yang berbeda dengan kejahatan tradisional.

Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (user) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer. Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber (Dermawan & Akmal. 2024). Istilah "hukum siber diartikan dari kata *cyber law*. Saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi, istilah lain yang digunakan adalah hukum dunia maya *(virtual word law),* hukum teknologi informasi *(law of information technology).* Istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual atau maya. Kemudian setelah itu, muncul istilah baru dari kejahatan komputer yaitu *Cyber crime. Cyber Crime* merupakan perkembangan dari computer crime. *Cyber crime* dan *cyber law* dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah banyak menjatuhkan korban, bukan hanya pada kalangan remaja namun disemua usia. Hal tersebut mengharuskan satuan kepolisian untuk segera bertindak dalam menangani kasus *cyber crime* (kejahatan dunia maya) yang cakupan kejahatannya sangat luas bahkan tidak terbatas. Cara pandang konvensional terhadap tindak pidana *cyber crime* akan menimbulkan kesulitan dan ketimpangan dalam proses penyelidikan, penyidikan dan pembuktian dimana proses tersebut tidaklah sama dengan proses penyelidikan, penyidikan dan pembuktian pada kasus-kasus tindak pidana konvensional, namun sikap positif tetap harus kita ambil terhadap Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai payung hukum

dalam dunia *Cyber Crime*, dengan harapan dapat menjadi acuan dan salah satu literatur undang-undang dalam hal penegakan *cyber law* di Indonesia.

Dalam penanganan kasus *cyber crime* pula diharapkan kemaksimalan dari pihak kepolisian untuk menghindari agar kasus *cyber crime* yang telah terjadi dapat begitu saja terlepas dari pengawasan hukum, *Cyber crime* memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cyber crime*, pemahaman dan pengetahuan ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan kejahatan *cyber crime* tersebut.

Peninjauan masalah kebijakan kriminalisasi dalam Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronikini merupakan tahap yang paling strategis dari keseluruhan perencanaan proses fungsionalisasi hukum pidana atau proses penegakan hukum pidana dalam rangka penanggulangan kejahatan *cyber crime.* Dengan demikian, peninjauan kembali *(review)* terhadap kebijakan kriminalisasi kejahatan teknologi informasi *(cyber crime)* dalam undang-undang ITE ini harus pula difokuskan pada ketiga bidang kebijakan di atas. Dengan meninjau ketiga hal tersebut dalam undang-undang ini, diharapkan dapat menganalisis fungsionalisasi hukum pidana dalam tahap formulasi sehingga dapat mengetahui dasar pertimbangan pembuat undang-undang dalam menyusun kebijakan kriminalisasi Selain itu, juga dapat mengetahui letak kelemahan-kelemahan kriminalisasi *cyber crime* dalam UU ITE yang perlu diperhatikan oleh aparat penegak hukum yang mengimplementasikan undang-undang ini (Laksana, 2019).

Berdasarkan obserfasi awal di Polda Sulsel, bahwa terdapat beberapa kasus *cyber crime* yang pernah ditangani oleh pihak kepolisian Makassar, sebagai contoh kasus peretasan kartu debit, Tim *Cyber Crime* Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Sulawesi Selatan mengejar empat peretas kartu debit yang mencuri uang nasabah, setelah sebelumnya menangkap seorang pelaku kejahatan tersebut. "*Pelaku 'hacker' (peretas) ini diamankan satu orang, tapi masih ada empat pelaku lain di kejar, termasuk bos 'hacker'-nya. Mereka dimasukkan dalam daftar pencarian orang (DPO),*" Ujar Direktur Reskrimsus Polda Sulsel Kombes Pol Helmi Kwarta di Makassar, Jumat (9/6).

Dalam kasus tersebut Seorang peretas atau bagian sindikat kejahatan itu, yang telah ditangkap berinisial MM. Dan Polisi telah mengetahui identitas empat peretas lain yang buron, yakni H (bos), HPS, THS, dan MS (anak buah). Dalam kasus tersebut para peretas mencuri saldo nasabah kartu debit, Mastercard, dengan masuk sistem, kemudian ke akun seseorang yang memiliki kartu kredit dengan menggunakan aplikasi tertentu. "Dari aplikasi itu dia bisa mengakses akun seseorang yang mempunyai uang di kartu debit, sehingga dia bisa menggunakan kartu tersebut. Sementara pemilik tidak tahu kalau digunakan oleh pelaku,"

Modus operandi mereka yaitu H selain bos sindikat itu juga berperan mengumpulkan data-data surat elektronik berdasarkan daftar email korban yang dijadikan data target pengelabuan di laptop MM. Selanjutnya, HPS menggunakan

perangkat lunak *Heart Sender* V mengirimkan email pengelabuan kepada korban atau pemilik email yang masuk daftar tersebut, dengan menargetkan pengguna situs https://login.northlane.com/ untuk diambil data kredensial yang sensitif, seperti "username", kata kunci, email, paspor, dan data kartu debit tersebut. Setelah calon korban mengisi data kredensial, THS mengecek email korban. Selanjutnya, MM diberikan "username" dan kata kunci oleh H serta data kartu debit itu milik orang lain untuk dicek isi saldo, seperti nomor kartu dan kode pengamanan. Selanjutnya akan muncul saldo kartu debit itu milik korban. Tersangka MM lalu menyimpan data tersebut ke notepad dan memasukkan jumlah saldo. Saat H meminta data itu, ia memberikannya. Pelaku lainnya, MS, lalu memanfaatkan data kredensial untuk transaksi, selanjutnya mencairkan saldo kartu debit serupa milik orang lain, dari warga negara asing dengan berbagai cara, seperti bertransaksi koin *Cryptocurrency di platform Paxful*, mencairkan lewat *situs Western Union dan Remitly* untuk mendapatkan keuntungan pribadi. Tersangka MM menjalankan aksi itu sejak Maret 2021 hingga 20 April 2023 dan telah mendapatkan keuntungan pribadi sekitar Rp100 juta. Tersangka dijerat Pasal 46 Ayat 1 jo Pasal 30 Ayat 1 dan atau Pasal 46 Ayat 2 jo Pasal 30 Ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) jo Pasal 55 Ayat 1 ke-1 KUHP. Contoh lain kejahatan yang terjadi dimasyarakat adalah pencemaran nama baik melalui sosial media, Adapun Pencemaran nama baik adalah tindakan yang termasuk dalam kategori penghinaan, merendahkan, ataupun menyebarkan informasi yang tidak benar terkait reputasi seseorang, kelompok, ras, agama, ataupun golongan tertentu (Djanggih & Hipan. 2018). Tentunya hal ini sangat mengancam masyarakat. Oleh karena itu penulis tertarik untuk membahas kasus *Cyber crime* yang terjadi dalam masyarakat.

METODE PENELITIAN

Tipe penelitian yang digunakan dalam penelitian ini yakni tipe penelitian yang mengidentifikasi hukum yang terdapat dalam masyarakat dengan maksud untuk mengetahui gejala-gejala lainnya sehingga menghasilkan gabungan antara teori dan praktek lapangan, Sesuai dengan jenis penelitian yang berupa penelitian hukum empiris, maka metode pendekatan yang digunakan dalam penelitian ini adalah metode pendekatan yuridis empiris, karena mengacu kepada efektivitas pelaksanaan hukum dan norma-norma tertulis yang dibuat dan diundangkan oleh lembaga atau pejabat negara yang berwenang dalam hal ini mengenai pelaksanaan Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lokasi penelitian yang dimaksud adalah di Polda Sulsel yang menerima laporan serta melakukan penyelidikan sehingga dapat dipastikan bahwa pada instansi tersebut tersedia cukup (data sekunder) untuk dijadikan bahan analisis dari Penelitian ini.

PEMBAHASAN

A. Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar

Dalam menanggulangi terjadinya kejahatan, pihak kepolisian telah melakukan berbagai Upaya untuk menangani terjadinya kejahatan dunia maya, dengan menghimbau masyarakat melalui media elektronik dan sosial media. Adapun Data

Tindak Pidana Penghinaan Pencemaran Nama Baik (ITE) Pada Subdit V Ditreskrimsus Polda Sul-sel pada tahun 2021-2023.

Tabel 1. Data Tindak Pidana Penghinaan Pencemaran Nama Baik

NO	TAHUN	CT	CC	LIDIK	RJ	P21 / TAHAP II
1.	2021	16	12	4	3	9
2.	2022	86	30	66	8	22
3.	2023	34	12	22	7	5
JUMLAH		113	48	75	14	34

Sumber data: Polda Sulsel 2024

Dari data di atas dapat disimpulkan kejahatan dalam dunia maya terjadi di setiap tahunnya. Adapun dari data diatas bentuk tindak pidana pencemaran nama baik yang sering terjadi di setiap tahunnya. UU ITE mengatur perlindungan berbagai kegiatan yang menggunakan internet, baik itu untuk mendapatkan informasi maupun melakukan transaksi. Dalam undang-undang ini juga dijelaskan sanksi yang diberikan kepada orang yang menyalahgunakan internet, termasuk melakukan kejahatan dan menyebarkan berita palsu.

Berdasarkan Pasal 1 butir 5 KUHAP menegaskan penyelidikan. Tindakan penyelidikan penekanannya diletakkan pada tindakan mencari dan menemukan suatu peristiwa yang dianggap atau diduga sebagai tindak pidana. Pada penyidikan, titik berat tekanannya diletakkan pada tindakan mencari serta mengumpulkan bukti.Supaya tindak pidana yang ditemukan dapat menjadi terang.Agar dapat menemukan dan menentukan pelakunya. Antara penyelidikan dan penyidikan adalah dua fase tindakan yang berwujud satu. Antara keduanya saling berkaitan guna dapat diselesaikan pemeriksaan suatu peristiwa pidana. Adapun Fungsi penyidik dilakukan sebelum dilakukan penyelidikan hanya bertugas untuk mengetahui dan menentukan peristiwa apa yang sesungguhnya telah terjadi dan bertugas membuat berita acara serta laporannya nantinya merupakan dasar permulaan penyidikan.

Menanggapi hal tersebut di atas, menurut penyidik dalam wawancara yang dilakukan peneliti, penyidik menyatakan bahwa secara umum proses penyidikan kejahatan *Cyber Crime* sama dengan proses penyidikan kejahatan konvensional lainnya. Bedanya hanya dari segi proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. Terlihat bahwa penanganan tindak kejahatan cyber crime sedikit rumit dibandingkan kejahatan konvensional, sebab terlebih dahulu harus berkoordinasi dengan beberapa pihak tertentu untuk mendapatkan kepastian bahwa hal tersebut benar-benar merupakan tindak kejahatan pidana atau bukan. Sementara dalam menetapkan tersangka kejahatan cyber crime, memiliki tingkat kesulitan yang lebih rendah dibanding kejahatan konvensional, dengan melihat barang bukti berupa nomor handphone atau alamat sosial media yang dimiliki pelaku dan tentunya dengan barang bukti tersebut maka akan tertuju secara langsung kepada pihak yang melakukan tindakan kejahatan. (Wawancara : Januari 2024).

Sebagaimana kasus pencemaran nama baik yang banyak ditangani oleh pihak kepolisian. Perbuatan tersebut dilakukan pelaku melalui media internet dengan

menyebarkan berita bohong/tidak benar dan berita yang bersifat rahasia sehingga berakibat mencemarkan nama baik orang lain atau instansi tertentu. Perbutan pelaku tersebut merupakan pelanggaran terhadap ketentuan Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pasal 27 ayat 3 dan lebih jelas diatur dalam KUHP pasal 310 tentang penghinaan. Dalam proses penyidikannya harus melibatkan saksi ahli bahasa untuk mengetahui apakah konteks bahasa yang digunakan oleh pelaku adalah tindak pidana atau bukan. Namun berdasarkan hasil wawancara, pihak kepolisian Polda Sulsel tidak dapat memberikan informasi terkait proses penangkapan pelaku pada kasus Cyber Crime dalam hal ini pencemaran nama baik yang berhasil diselesaikan oleh pihak epolisian karena bersifat rahasia.

Dalam proses penyidikan kasus ini, dilakukan berdasarkan ketentuan dalam UU ITE pasal 42 yang menegaskan "penyidikan terhadap tindak pidana sebagaimana yang dimaksud dalam Undang-undang ini dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam undang-undang ini". Dalam KUHAP diatur pada BAB penyidikan pasal 107, dan ini sebagaimana diatur pula pada pasal 43 UU ITE, bahwa selain penyidik pejabat polisi Negara Republik Indonesia, juga bekerja sama dengan pejabat pegawai Negeri sipil. Sementara dalam hal penggeledahan, pihak kepolisian harus mendapatkan izin dari ketua pengadilan. Sebagaimana yang terdapat pada pasal 43 ayat 3 (UU) Nomor 1 Tahun 2024 tentang ITE yang menerangkan bahwa "penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketuan pengadilan setempat" Hal ini juga sebagaimana yang terdapat pada pasal 33 ayat 1 KUHAP. Proses ini dilakukan untuk kepentingan penyidikan dengan tetap memperhatikan perlindungan terhadap privasi, kerahasiaan dan kelancararan layanan publik sebagaimana diatur dalam pasal 43 (2) UU ITE.

Dengan demikian, proses penyidikan yang dilakukan oleh pihak kepolisian Polda Sulsel menggunakan payung hukum dari (UU) Nomor 1 Tahun 2024 tentang informasi dan transaksi elektronik, namun dalam pelaksanaannya tidak dapat terlepas dari ketentuan KUHP dan KUHAP, dan beberapa pasal dalam UU ITE tetap mempertimbangkan ketentuan dalam KUHAP karena ada hal-hal yang tidak diatur dalam UU ITE namun diatur dalam KUHP dan KUHAP. Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena belum samanya persepsi diantara aparat penegak hukum, barang bukti digital adalah barang bukti dalam kasus *cybercrime* yang belum memiliki rumusan yang jelas dalam penentuannya sebab digital *evidence* tidak selalu dalam bentuk fisik yang nyata. Misalnya untuk kasus pembunuhan sebuah pisau merupakan barang bukti utama dalam melakukan pembunuhan sedangkan dalam kasus *cybercrime* barang bukti utamanya adalah komputer tetapi komputer tersebut hanya merupakan fisiknya saja sedangkan yang utama adalah data di dalam hard disk komputer tersebut yang berbentuk file, yang apabila dibuat nyata dengan print membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut dalam bentuk compact disc 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 (Wawancara : Januari 2024).

Dari seluruh laporan kasus cyber crime yang masuk, 90% adalah kasus pencemaran nama baik yang mana merupakan delik aduan sehingga kasus tersebut bisa saja ditarik. Namun, sejauh ini semua kasus cyber crime yang masuk di Polda Sulsel dibawa ketahap pengadilan. Informasi yang kami dapatkan di atas, dalam hal bentuk penyelesaiannya sebagaimana yang diatur dalam (UU) Nomor 1 Tahun 2024 tentang ITE pada pasal 38- 39. Bahwa setiap orang yang menjadi korban dari tindak pidana cyber crime dapat melakukan gugatan. Namun selain dari gugatan perdata tersebut, peyelesaian kasus dapat pula dilakukan arbitrase yaitu usaha perantara dalam meleraikan sebuah sengketa atau dengan kata lain kedua pihak telah berdamai.

Hal ini dapat terjadi karena kasus cyber crime dalam hal pencemaran nama baik adalah delik aduan yang berarti delik yang hanya bisa diproses apabila ada pengaduan atau laporan dari orang yang menjadi korban tindak pidana. Dalam delik aduan, penuntut terhadap delik tersebut digantungkan pada persetujuan dari yang dirugikan. Pada delik aduan ini korban tindak pidana dapat mencabut laporannya kepada pihak yang berwenang apabila diantara mereka telah terjadi suatu perdamaian. Delik aduan ini banyak diatur dalam KUHAP seperti pasal 310 tentang pencemaran nama baik, pasal 355 tentang perbuatan yang tidak menyenangkan, dan pasal 284, 287, 289 tentang kejahatan asusila. Dan ketentuan seperti ini tidak diatur dalam UU ITE.

Adapun Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar melalui:

1. Upaya Pre-emtif

Upaya yang dilakukan untuk menghilangkan penyebab kejahatan. Upaya ini dilakukan untuk menghilangkan faktor penyebab yang mendorong terjadinya kejahatan tersebut. Adapun tanggapan responden terhadap upaya yang dilakukan pihak kepolisian dalam menanggulangi penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar.

Tabel 2 Tanggapan Responden Terhadap Upaya Yang Dilakukan Pihak Kepolisian Dalam Menanggulangi Penyalahgunaan Informasi Dan Transaksi Elektronik Di Kota Makassar

No	Tanggapan Responden	Frekuensi	Presentase
1	Efektif	10	50,00
2	Kurang efektif	9	45.00
3	Tidak efektif	1	5.00
	Jumlah	20	100

Sumber data: Kuisioner tahun 2024

Berdasarkan data pada tabel diatas menunjukkan bahwa jawaban responden tentang Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar ditanggapi bervariatif, yaitu: 10 Orang responden (50,00%) menyatakan efektif, kemudian 9 Orang responden (45.00%) menyatakan kurang efektif, sedangkan 1 orang responden (5,00%) menyatakan tidak efektif. Dari data tersebut, dapat dikatakan bahwa Fungsi Kepolisian dalam penyidikan

penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar melalui Upaya Pre-emtif belum sepenuhnya terlaksana secara efektif. Oleh karena itu, proses penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar tersebut masih perlu diberi terobosan agar dapat lebih efektif guna mendukung terwujudnya penegakan hukum yang maksimal.

Tindakan pre-emtif merupakan langkah awal yang dilakukan polisi untuk mencegah tindak pidana. Upaya yang dilakukan sebagai bagian dari pemberantasan kejahatan yang bertujuan untuk menanamkan nilai-nilai/norma-norma yang baik dan menjamin bahwa norma-norma tersebut tertanam dalam diri seseorang maupun masyarakat. Adapun Langkah yang dapat di laksanakan dengan melakukan kegiatan sosialisasi dan himbauan kepada Masyarakat agar dapat berhati-hati serta selektif menggunakan transaksi elektronik di era digital ini.

1. Melakukan tindakan atau upaya Preventif

Upaya preventif merupakan suatu upaya yang sangat mudah dilakukan karena dapat dilakukan oleh siapa saja bagi mereka yang dapat memberikan pengetahuan-pengetahuan tentang pencegahan suatu kejahatan. Dalam upaya preventif yang paling diutamakan adalah menghilangkan suatu kesempatan untuk melakukan suatu kejahatan.

Adapun tanggapan responden terhadap upaya yang dilakukan pihak kepolisian dalam menanggulangi penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar

Tabel 3 Tanggapan Responden Terhadap Upaya Yang Dilakukan Pihak Kepolisian Dalam Menanggulangi Penyalahgunaan Informasi Dan Transaksi Elektronik Di Kota Makassar

No	Tanggapan Responden	Frekuensi	Presentase
1	Efektif	8	40,00
2	Kurang efektif	8	40.00
3	Tidak efektif	4	20.00
	Jumlah	20	100

Sumber data: Kuisioner tahun 2024

Berdasarkan data pada tabel diatas menunjukkan bahwa jawaban responden tentang Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar ditanggapi bervariatif, yaitu: 8 Orang responden (40,00%) menyatakan efektif, kemudian 8 Orang responden (40.00%) menyatakan kurang efektif, sedangkan 4 orang responden (20,00%) menyatakan tidak efektif. Dari data tersebut, dapat dikatakan bahwa Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar melalui Upaya Preventif belum sepenuhnya terlaksana secara efektif. Oleh karena itu, proses penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar tersebut masih perlu diberi terobosan agar dapat lebih efektif guna mendukung terwujudnya penegakan hukum yang maksimal. Adapun Fungsi Kepolisian dalam pencegahan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar yaitu Memberikan Perlindungan, Pengayom dan Pelayanan Pada Masyarakat dengan melakukan kegiatan pencegahan dengan cara melalui Patroli Cyber, serta

edukasi terhadap masyarakat dan Menegakkan Hukum melalui tindakan.

2. Upaya Represif

Upaya represif merupakan upaya terakhir yang di lakukan setelah upaya pre-emtif dan preventif. Upaya ini dilakukan pada saat telah terjadi tindak pidana/kejahatan tindakan ini disebut sebagai penegakan hukum (law enforcement) dengan menjatuhkan hukuman sesuai dengan sanksi yang telah ditentukan. Adapun yang dapat melakukan upaya represif ini hanya orang-orang tertentu saja. yakni, mulai dari pihak kepolisian, kejaksaan, kehakiman, sampai lembaga pemasyarakatan. Selain itu, upaya penegakan hukum juga termasuk dalam bidang kebijakan sosial, karena tujuannya adalah untuk mencapai kesejahteraan masyarakat secara umum, yaitu segala usaha rasional untuk mencapai kesejahteraan masyarakat. Bentuk yang pertama adalah bersifat represif yang menggunakan sarana penal, yang sering disebut sebagai sistem peradilan pidana (criminal justice system). Dalam hal ini secara luas sebenarnya mencakup pula proses kriminalisasi. Yang kedua berupa usaha-usaha prevention without punishment (tanpa menggunakan sarana penal) dan yang ketiga adalah mendayagunakan usaha-usaha pembentukan opini masyarakat tentang kejahatan dan sosialisasi hukum melalui media massa secara luas.

Adapun tanggapan responden terhadap upaya yang dilakukan pihak kepolisian dalam menanggulangi penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar

Tabel 4 Tanggapan Responden Terhadap Upaya Yang Dilakukan Pihak Kepolisian Dalam Menanggulangi Penyalahgunaan Informasi Dan Transaksi Elektronik Di Kota Makassar

No	Tanggapan Responden	Frekuensi	Presentase
1	Efektif	10	50,00
2	Kurang efektif	10	50.00
3	Tidak efektif	-	-
	Jumlah	20	100

Sumber data: Kuisioner tahun 2024

Berdasarkan data pada tabel diatas menunjukkan bahwa jawaban responden tentang Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar ditanggapi bervariatif, yaitu: 10 Orang responden (50,00%) menyatakan efektif, kemudian 10 Orang responden (50.00%) menyatakan kurang efektif, sedangkan tidak ada menyatakan tidak efektif. Dari data tersebut, dapat dikatakan bahwa Fungsi Kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar melalui Upaya Represif belum sepenuhnya terlaksana secara efektif. Oleh karena itu, proses penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar tersebut masih perlu diberi terobosan agar dapat lebih efektif guna mendukung terwujudnya penegakan hukum yang maksimal.

Adapun bentuk Penanggulangan dengan upaya refresif untuk menindak para pelaku sesuai dengan perbuatannya dan memberi edukasi atas perbuatan yang dilakukannya sehingga mereka sadar bahwa perbuatan yang dilakukannya adalah perbuatan melanggar hukum dan merugikan Masyarakat. Pencegahan refresif yang dilakukan oleh kepolisian dalam penanggulangan tindak pidana pelaku pencemaran nama baik melalui media sosial adalah dengan cara melakukan penegakan hukum terhadap pelaku tersebut. Dengan demikian diharapakan agar Masyarakat dan pihak kepolisian dapat bekerja sama untuk menanggulangi kejahatan siber yang sampai sekarang masih terjadi di tengah-tengah Masyarakat.

B. Faktor-faktor yang mempengaruhi Fungsi kepolisian dalam penyidikan penyalahgunaan Informasi dan Transaksi Elektronik di Kota Makassar

Ada beberapa faktor yang dapat menyebabkan kejahatan siber menjadi lebih mudah terjadi. Beberapa faktor tersebut tentunya sangat beragam sehingga memungkinkan serangan terjadi. Berikut adalah beberapa faktor yang dapat mempermudah terjadinya kejahatan siber:

1. Kerentanan Sistem Keamanan

Kejahatan siber sering terjadi karena adanya kerentanan atau celah dalam sistem keamanan. Apalagi tak semua orang menjadikan keamanan sebagai prioritas. Bahkan ada juga yang mengabaikan sistem keamanan dan tidak memperbaharuinya secara teratur. Jika perangkat lunak atau sistem operasi tidak diperbarui secara teratur, kelemahan keamanan tertentu bisa dieksploitasi oleh penjahat siber. Akibatnya kejahatan siber menjadi sulit untuk dihindari.

2. Kurangnya Kesadaran Keamanan

Sampai saat ini masih banyak orang yang belum menyadari dan memahami bahaya dunia digital. Kurangnya pemahaman dan kesadaran mengenai praktik keamanan digital dapat membuat individu atau organisasi mengabaikan masalah keamanan dasar seperti memperbarui kata sandi. Tak jarang banyak individu maupun organisasi asal klik tautan yang muncul meski mencurigakan tanpa memahami resiko keamanannya. Individu seperti inilah yang biasanya lebih rentan mengalami kejahatan siber. Hal ini karena tanpa sadar telah memudahkan para penjahat siber melakukan aksinya.

3. Kemajuan Teknologi

Kemajuan teknologi memang semakin pesat. Keuntungan yang bisa diberikan oleh kemajuan ini juga sangat signifikan. Sayangnya meskipun teknologi memberikan banyak keuntungan, kemajuan teknologi juga dapat membuka pintu bagi penjahat siber. Perkembangan dalam kecerdasan buatan dan teknologi lainnya dapat digunakan untuk mengembangkan serangan yang lebih canggih dan sulit dideteksi. Terlebih jika tidak diiringi dengan pengembangan cara mengatasi serangan tersebut maka kejahatan siber bisa jadi akan semakin berkembang.

4. Anonimitas di Internet

Anonimitas yang diberikan oleh internet dapat memotivasi penjahat siber untuk melakukan tindakan tanpa takut terkena sanksi hukum. Kemampuan untuk menyembunyikan identitas para ini membuatnya sulit untuk dilacak. Bahkan untuk

menangkap pelaku kejahatan siber tergolong hampir mustahil. Jika bisa pun sudah pasti akan memerlukan waktu yang sangat lama.

5. Eksploitasi Manusia (Social Engineering)

Penjahat siber sering menggunakan teknik sosial untuk memanipulasi individu atau karyawan agar memberikan informasi rahasia atau mengakses sistem yang aman. Kurangnya kesadaran terhadap teknik social engineering dapat membuat serangan semacam itu lebih berhasil dan mudah dilakukan.

6. Kurangnya Hukuman yang Tegas

Faktor penyebab kejahatan siber semakin mudah dan marak terjadi tentunya tak lepas dari lemahnya hukum yang ada. Memang seperti di Indonesia sendiri sudah ada pasal tersendiri mengenai kejahatan ini. Namun dalam prakteknya penanganan tentang kasus ini masih terbilang kurang. Inilah yang akhirnya membuat penjahat siber untuk terus melakukan serangan tanpa takut ditangkap atau dihukum.

7. Ketergantungan pada Teknologi

Semakin banyaknya organisasi dan individu yang bergantung pada teknologi digital meningkatkan potensi serangan siber. Ketergantungan ini membuat banyak target yang menarik bagi penjahat siber yang mencari keuntungan finansial atau ingin menciptakan kerusakan.

8. Identitas Pengguna

Faktor penyebab cyber crime lainnya adalah terkait identitas pengguna. Fitur-fitur yang mempermudah manipulasi privasi di platform media sosial seringkali dimanfaatkan oleh pengguna dengan niat yang tidak baik. Tidak hanya itu, data pengguna lain juga rentan terhadap pencurian memberikan peluang bagi pelaku kejahatan siber untuk melakukan manipulasi maupun kejahatan terhadap korban.

9. Replikasi Aset Informasi

Pengguna media sosial dengan mudah dapat mereplika atau menggandakan aset informasi sehingga memberi peluang terjadinya kejahatan siber. Hal ini biasanya terjadi karena fitur penghapusan atau yang dikenal sebagai ‘delete button’ di dunia internet tidak tersedia.

10. Lokasi

Faktor selanjutnya yang bisa memicu munculnya ancaman serangan kejahatan siber adalah lokasi , lokasi bisa dideteksi dengan mudah di media sosial. Hal ini sama saja dengan memberi kemudahan untuk pemalsuan dan menjadi awal terjadinya kejahatan siber. Dengan lokasi ini orang asing bisa dengan mudah mengetahui lokasi hingga Alamat rumah kita. Informasi lokasi tersebut kemudian bisa disalahgunakan untuk melakukan kejahatan siber.

11. Motivasi Finansial

Motivasi Finansial juga bisa menjadi faktor penyebab kejahatan siber. Hal ini karena banyak sekali serangan siber dilakukan dengan tujuan mendapatkan keuntungan finansial. Untuk itulah pelaku kejahatan siber ini sampai nekat melakukan pencurian data pribadi, peretasan rekening bank, atau ransomware. Pelaku kejahatan siber ini bahkan tidak akan peduli pada kerugian yang dialami korbannya asalkan mendapat

keuntungan finansial. Inilah kenapa kejahatan siber bisa menjadi kerugian yang sangat besar untuk para korbannya.

12. Kondisi Lingkungan Digital yang Dinamis

Lingkungan digital yang terus berkembang dan berubah dengan cepat memberikan peluang bagi penjahat siber untuk mengeksploitasi celah keamanan yang baru muncul. Inilah yang kemudian membuat kejahatan siber semakin meningkat dan sulit dihentikan.

Memahami faktor-faktor ini penting untuk mengembangkan strategi keamanan yang lebih efektif dan mengurangi risiko terhadap kejahatan siber. Selain itu tentunya kita juga harus bertindak baik itu melakukan antisipasi atau mulai melindungi diri agar terhindar dari kejahatan siber. Adapun cara untuk melindungi diri bisa mulai kita lakukan dengan tidak sembarangan memberikan informasi pribadi. Selalu waspada ketika memasukan informasi penting seperti nomor KTP, tanggal lahir maupun nomor telepon di suatu aplikasi atau situs web.

Disamping itu juga perlu menggunakan kata sandi yang kuat dan berbeda untuk setiap akunnya. Selalu perbarui perangkat lunak keamanan atau antivirus di komputer. Dalam hal ini kita juga tidak boleh asal mengklik tautan atau lampiran yang mencurigakan. Dengan melakukan antisipasi dan melindungi diri maka resiko menjadi korban serangan siber bisa diminimalisir. Selain itu hal yang dapat kita lakukan yaitu untuk menggunakan konektivitas dan sistem penyimpanan yang aman agar informasi pribadi lebih terlindungi.

(Wawancara dengan penyidik januari 2024). Hasil wawancara peneliti kepada penyidik mengenai kendala yang dihadapi oleh pihak penyidik Polda Sulsel dalam Penyidikan Tindak Pidana Cyber Crime adalah sebagai berikut:

1. Kendala Internal, kendala yang dihadapi adalah pada pelakunya saksi dari kasus serta tidak adanya unit khusus menangani masalah kejahatan dunia maya yang kita kenal dengan unit cyber crime, sementara pihak penyidik terkadang sulit mengetahui keberadaan pelaku sekalipun menggunakan teknologi. Selanjutnya berdasarkan wawancara tersebut, penelti merangkum beberapa kendala yaitu:
   a. Kurangnya saksi ahli, dalam hal ini saksi ahli gambar dan saksi ahli bahasa.
   b. Sulit memperoleh saksi kejahatan.
   c. Keberadaan pelaku yang sulit dideteksi sekalipun menggunakan teknologi.
2. Kendala Eksternal
   a. Izin ketua pengadilan untuk penggeledahan dan penyitaan serta izin melalui penuntut umum dari ketua pengadilan untuk penangkapan dan penahanan.
   b. Masyarakat yang kurang memahami masalah tindak pidana Cyber Crime dianggap sebagai bukan kejahatan.

Faktor teknologi, mengenai kemajuan teknologi informasi yang ada saat ini. Kemajuan teknologi mempengaruhi dalam menemukan alat bukti khususnya menganai data elektronik dari suatu pembuktian tindak pidana Cyber Crime. Menurut Soerdjono Soekanto, ada lima faktor yang sangat mempengaruhi dalam penegakan hukum diantara beberapa faktor saling berkaitan satu dengan yang lainnya, oleh karena itu merupakan esensi dari penegakan hukum serta merupakan esensi dari penegakan hukum. Adapun kelima faktor yang dimaksud adalah sebagai berikut:

1. Faktor Hukum (substansi hukum) Dalam upaya penegakan hukum diperlukan adanya keserasian antara berbagai peraturan perundang-undangan yang berbeda derajatnya. Ketidak cocokan itu bisa terjadi misalnya antara peraturan yang tertulis dengan yang tidak tertulis, antara undang-undang yang derajatnya lebih tinggi dengan peraturan yang lebih rendah, antara undang-undang yang bersifat khusus dengan yang bersifat umum, dan antara undang-undang yang berlaku belakangan dengan yang berlaku terdahulu.Semuanya ini dapat mempengaruhi masalah penegakan hukum karena tujuan dibentuknya suatu peraturan adalah untuk memberikan kepastian hukum, kemanfaatan dan keadilan. Untuk itu maka demi menghindari agar jangan sampai terjadi suatu peraturan tidak berlaku secara efektif di masyarakat maka perlu diperhatikan asas dan tujuan dari undang-undang itu sendiri.
2. Faktor Penegak Hukum Atau Struktur Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan cyber crime, dimana kemampuan penyidik sangat dibutuhkan untuk mengungkap kasus-kasus cyber crime. Adanya unit cybercrime dilingkungan kepolisian membuktikan bahwa dibutuhkannya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya, oleh karena itu dibutuhkaannya pendidikan khusus untuk memberikan pengetahuan terkait cyber kepada para penyidik yang khusus menangani masalah cyber crime. Dalam berfungsinya hukum, mentalitas atau keperibadian petugas penegak hukum memainkan peran penting, apabila peraturan sudah baik, tetapi kualitas petugas kurang baik maka akan menimulkan masalah oleh karena itu salah satu kunci keberhasilan dalam penegakan hukum adalah mentalitas atau keperibadian penegak hukum. Menurut J.E. Sahetapy, yang mengatakan bahwa "dalam rangka penegakan hukum dan implementasi penegakan hukum bahwa penegakan keadilan tanpa kebenaran adalah suatu kebijakan, penegakakan kebanaran tanpa kejujuran adalah suatu kemunafikan, dalam kerangka penegakan hukum oleh setiap lembaga penegakan hukum, keadilan dan kebenarannya harus dinyatakan, harus terasa dan terlihat, serta harus diaktualisasikan".
3. Penegakan hukum di dalam masyarakat selain dipengaruhi oleh peraturan perundang-undangan (kaidah-kaidah) juga ditentukan oleh para penegak hukum, sering terjadi beberapa peraturan tidak dapat terlaksana dengan baik dikarenakan ada penegak hukum yang tidak melaksanakan suatu peraturan dengan cara semestinya. Menurut Soerjono Soekanto , secara sosiologis maka setiap penegak hukum tersebut mempunyai kedudukan (status) dan peran (role). Kedudukan sosial merupakan posisi tertentu di dalam struktur kemasyarakatan, yang mungkin tinggi, sedang dan rendah.Kedudukan tersebut sebenarnya merupakan suatu wadah yang isinya adalah hak-hak dan kewajiban-kewajiban tertentu.Suatu hak sebenarnya merupakan wewenang untuk berbuat atau tidak berbuat, sedangkan kewajiban adalah beban atau tugas.

   Seorang penegak hukum, sebagimana halnya dengan warga-warga masyarakat lainnya, lazimnya mempunyai beberapa kedudukan dan peranan sekaligus. Dengan demikian tidaklah mustahil, bahwa antara berbagai kedudukan dan peranan timbul konflik.Kalau di dalam kenyataanya terjadi suatu kesenjangan antara peranan yang seharusya dengan peranan yang sebenarnya dilakukan atau

peranan aktual, maka terjadi kesenjangan peranan. Terkait masalah penegak hukum, menurut Penyidik Polda Sulsel, mengemukakan bahwa penyidik khususnya cyber crime dalam penindakan sudah sangat efektif, tindakan penyelidikan untuk menentukan apakah sebuah peristiwa merupakan sebuah peristiwa pidana merupakan sebuah kewajiban bagi pejabat yang berwenang ketika menerima sebuah laporan dari masyarakat sebagaimana yang dimaksud dalam Pasal 102 Ayat (1) KUHAP, yaitu : "Penyelidik yang mengetahui, menerima laporan atau pengaduan tentang terjadinya suatu peristiwa yang patut diduga merupakan tindak pidana wajib segera melakukan tindakan penyelidikan yang diperlukan."(Wawancara Januari 2024).

4. Faktor Sarana atau Fasilitas Dalam mengungkap kasus-kasus cyber crime dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian. Fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital serta merekam dan menyimpan bukti-bukti yang berupa soft copy (gambar, program, html, suara, dan lain sebagainya). Komputer forensik merupakan salah satu cabang ilmu forensic yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital.Komputer forensic dikenal sebagai digital forensic. Adapun tujuannya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian ataupelanggaran keamanan dari sistem informasi. Berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum. Contohnya, melalui Internet Forensik, kita dapat megetahui siapa saja orang yang mengirim email kepada kita, kapan dan dimana keberadaan pengirim. Dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi IP Address, komputer yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada website kita tersebut. Kemampuan digital forensik menggunakan fasilitas yang hanya dimiliki oleh laboratorium forensik komputer. Terkait dengan hal tersebut unit cyber crime polda sulsel belum memiliki fasilitas berupa laboratorium forensic komputer, yang mengakibatkan terkendalanya upaya penanggulangan cyber crime di wilayah hukum Polda Sulsel . Dengan kurangnya fasilitas mapun sarana pendukung maka penegakan hukum akan menjadi terhambat dan tentunya para aparat penegak hukum tidak dapat memaksimalkan perannya secara aktual. Sarana atau fasilitas yang cukup ampuh di dalam penegakan hukum bisa dalam bentuk kepastian dalam penanganan perkara maupun kecepatan memproses perkara tersebut, karena dampaknya disini akan lebih nyata apabila dibanding dengan peningkatan sanksi negatif belaka. Apabila tingkat kepastian dan kecepatan penanganan perkara ditingkatkan, maka sanksi-sanksi negatif akan mempunyai efek menakutkan sehingga akan dapat mencegah peningkatan kejahatan maupun residivisme.

5. Faktor Masyarakat dan Lingkungan Masyarakat dan lingkungan merupakan faktor utama yang sangat berpengaruh terhadap penegakan hukum di Indonesia karena berkaitan erat dengan kesadaran masyarakat mengenai hak dan kewajibannya di depan hukum. Kesadaran hukum masyarakat adalah merupakan keseluruhan yang mencakup pengetahuan tentang hukum, penghayatan fungsi hukum dan ketaatan pada hukum. Sebaik apapun suatu

peraturan maupun aparat pelaksananya bila kesadaran masyarakat akan hukum rendah maka penegakan hukum akan terhambat. Dalam kasus kekerasan pada anak tak jarang kita jumpai bahwa aktor utama yang cukup berperan disini adalah masyarakat dan lingkungan.

Faktor Kebudayaan atau Kultur Legal Culture atau budaya hukum pada dasarnya mencakup nilai-nilai yang mendasari hukum yang berlaku, dan nilai-nilai mana merupakan konsepsi-konsepsi abstrak tentang apa yang dianggap baik sehingga patut untuk dipatuhi dan apa yang dianggap buruk sehingga harus dihindari. Dalam penegakan hukum nilai-nilai kultur tersebut diatas dapat dijabarkan dalam kaidah-kaidah dan pandangan yang mantap dalam sikap dan tindakan sebagai rangkaian nilai akhir untuk menciptakan suatu pembaharuan sosial, memelihara dan mempertahankan kontrol sosial guna tercipta kedamaian dalam pergaulan hidup masyarakat. Budaya hukum yang baik akan menciptakan suatu tatanan masyarakat yang baik pula. Seringkali paradigma seperti ini tidak dipahami dan diresapi oleh masyarakat, apalagi yang memiliki latar belakang pendidikan rendah.

KESIMPULAN

1. Efektivitas penyidikan oleh Kepolisian terhadap penyalahgunaan Informasi dan Transaksi Elektronik (ITE) masih kurang efektif karena beberapa hal sebaga berikut: Laju pertumbuhan cyber crime yang begitu pesat, yang disebabkan oleh Faktor Ekonomi, Faktor Lingkungan, Faktor Sosial Budaya, dan Faktor Intelektual. Masyarakat dan penegak hukum diharapkan dapat bekerja sama dalam memberantas kejahatan siber agar di era digital ini kejahatan tersebut dapat berkurang sehingga pemanfaatan teknologi dapat digunakan dengan baik dari segi aspek positifnya.
2. Faktor-faktor yang menjadi kendala yang dihadapi oleh pihak Kepolisian dalam penyidikan tindak pidana penyalahgunaan Informasi dan Transaksi Elektronik (ITE): Aspek Penyidik, kemampuan dan skill penyidik sangat dibutuhkan untuk mengungkap kasus-kasus penyalahgunaan Informasi dan Transaksi Elektronik (ITE), Aspek alat bukti, karena alat bukti elektronik yang berupa data-data tersebut rentang untuk diubah atau dihapus sehingga menyulitkan dalam pengumpulan bukti dan Aspek Fasilitias, dalam mengungkap kasus-kasus cyber crime dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian.

SARAN

1. Pemerintah diharapkan meningkatkan dalam membantu upaya penanggulangan dengan cara menyediakan lapangan kerja yang layak untuk sumber daya manusia yang belum terpakai agar kemampuan mereka tidak lagi disalahgunakan untuk melakukan kejahatan, juga harus memperhatikan aturan-aturan terkait informasi dan transaksi elektronik guna mengurangi celah hukum yang dapat timbul, dan pemerintah harus menyediakan fasilitas yang mampu mendukung upaya penindakan penyalahgunaan informasi dan transaksi elektronik (ITE).
2. Perlunya Serta peran Masyarakat untuk memberantas kejahatan siber dengan cara untuk melindungi diri bisa mulai kita lakukan dengan tidak sembarangan memberikan informasi pribadi. Selalu waspada ketika memasukan informasi penting seperti nomor KTP, tanggal lahir maupun nomor telepon di suatu

aplikasi atau situs web. Disamping itu juga perlu menggunakan kata sandi yang kuat dan berbeda untuk setiap akunnya. Selalu perbarui perangkat lunak keamanan atau antivirus di komputer. Dengan melakukan antisipasi dan melindungi diri maka resiko menjadi korban serangan siber bisa diminimalisir. Selain itu hal yang dapat kita lakukan yaitu untuk menggunakan konektivitas dan sistem penyimpanan yang aman agar informasi pribadi lebih terlindungi.

3. Pengguna internet di himbau untuk lebih berhati-hati dalam mengakses layanan Internet dan memastikan bahwa media yang mereka akses dapat dipercaya sebelum memberikan data atau informasi apa pun. Hal ini bertujuan untuk mencegah segala bentuk kejahatan. Serta diharpkan peran serta masyarakat dalam membantu penegakan hukum terkait cyber crime, dengan melaporkannya keaparat kepolisian jika melihat atau pun menjadi korban penyalahgunaan informasi dan transaksi elektronik (ITE).

DAFTAR PUSTAKA

Arif, M. (2021). Tugas dan fungsi kepolisian dalam perannya sebagai penegak hukum menurut Undang-Undang Nomor 2 Tahun 2002 tentang kepolisian. *Al-Adl: Jurnal Hukum*, *13*(1), 91-101.

Bahri, I. S. (2023). *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023)*. Bahasa Rakyat.

Dermawan, A., & Akmal, A. (2020). Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi. *Journal of science and social research*, *2*(2), 39-46.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Djanggih, H. (2018). The phenomenon of cyber crimes which impact children as victims in Indonesia. *Yuridika*, *33*(2), 212-231.

Djanggih, H., & Hipan, N. (2018). Pertimbangan Hakim dalam Perkarapencemaran Nama Baik Melalui Media Sosial (Kajian Putusan Nomor: 324/Pid./2014/PN. SGM). *Jurnal Penelitian Hukum De Jure*, *18*(1), 93-102.

Hutabarat, S. A. (2024). Kajian Kebijakan Hukum Pidana Terhadap Kejahatan Di Media Sosial. *Judge: Jurnal Hukum*, *5*(01), 12-15.

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Times*, *5*(2), 35-42.

Laksana, A. W. (2019). Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif. *Jurnal Hukum*, *35*(1), 52-76.

Nashihin, H., Baroroh, A., & Ali, A. (2020). Implikasi hukum teknologi informasi dalam perkembangan teknologi pendidikan islam (Telaah atas Hukum Moore, Hukum Metcalfe, dan Hukum Coase). *At Turots: Jurnal Pendidikan Islam*, *2*(2 Desember), 136-147.

Ramadhan, A. (2021). Diskresi Penyidik Polri Sebagai Alternatif Penanganan Perkara Pidana. *Lex Renaissance*, *6*(1), 25-41.

Sugianto, Q. F. (2019). Peluang dan Tantangan Calon Notaris Dalam Menghadapi Perkembangan Disrupsi Era Digital. *Notarius*, *12*(2), 656-668.

.

.