SKRIPSI

PELANGGARAN ETIKA DALAM LINGKUP KEJAHATAN CYBER DI INDONESIA

Disusun untuk memperoleh gelar Sarjana Hukum

Oleh

Yulio Dharma Panji Pratama

18.0201.0102

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH MAGELANG

2025

BAB 1

PENDAHULUAN

A. Latar Belakang Masalah

Pada zaman modern sekarang ini teknologi semakin berkembang Dimana kita tahu bahwa untuk berkomunikasi maupun mencari informasi dapat dilakukan dengan cepat dan tepat.(Tamimi & Munawaroh, 2024) Kemajuan ini, teknologi dapat memperlancar dan memudahkan kita tanpa terhalang jarak, ruang, maupun waktu. Dengan menggunakan internet sebagai salah satu produk utamanya dalam kemajuan teknologi tersebut yang di lakukan oleh penggunanya sesuai dengan kebutuhannya seperti, Pendidikan, bisnis, Pemerintahan, serta juga dapat digunakan untuk hiburan. Namun, di sisi lain dalam kemajuan teknologi ini menimbulkan berbagai permasalahan baru, salah satunya meningkatnya kejahatan cyber. (Fuady, 2005)

Dengan media sosial sebagai alat menghubungkan seseorang untuk dapat berinteraksi maupun komunikasi antar jarak yang jauh maupun dekat. Media sosial merupakan media dimana kita dapat mengirim, membuat, mendapatkan sesuatu yang di inginkan seperti salah satu contoh membuat konten kepada khalayak ramai. (Jurnalistik et al., 2021)

Selain pemanfaatan suatu kegiatan di media sosial tidak jarang juga di temukan penyalahgunaan dalam menyebarkan informasi yang memungkinkan akan terjerat masalah hukum akibat penyebaran informasi palsu yang pastinya itu melanggar etika.(Basuki, 2019)

Hal itu memerlukan adanya etika dalam bermedia sosial supaya terhindar oleh pelanggaran hukum bahkan pelanggaran etika dalam ber interaksi di dunia cyber.(Turnip & Siahaan, 2021)

Kejahatan cyber merupakan kejahatan yang di lakukan melalui media teknologi yang berupa peretasan (hacking), pencurian data pribadi, penipuan online, penyebaran hoaks, dan berbagai pelanggaran hukum lainnya. Selain dalam sisi hukum melanggar , penting juga untuk menelaah kejahatan cyber dari sudut pandang etika. (Umam, 2019)

Dengan menggunakan jaringan internet melalui smartphone, komputer dan juga alat media lain dapat memunculkan berbagai perilaku suatu pengguna cyber untuk melakukan kejahatan yang sering di sebut *cybercrime*. (Ariyaningsih et al., 2023) *Cybercrime* mempunyai dua kategori yaitu *cybercrime* dalam makna sempit dan *cybercrime* dalam makna luas. *Cybercrime* dalam makna sempit yaitu kejahatan dalam sistem komputer . Sedangkan dalam makna luasnya cybercrime yaitu kejahatan terhadap sistem atau jaringan komputer dengan menggunakan sarana komputer.(Habibi & Liviani, 2020)

Pada kejahatan cyber pada dasarnya suatu Tindakan melanggar hukum. Tanpa di sadari oleh para pelaku pengguna cyber itu bahwa tindakanya juga merupakan pelanggaran etika. Maka demikian kejahatan cyber menjadi aspek yang sering di abaikan oleh Sebagian Masyarakat . Para pelaku tidak menyadari bahwa tindakanya melanggar norma dan nilai moral. Seperti Tindakan memanipulasi informasi, menyebarkan data pribadi orang lain tanpa izin, berkomentar tidak baik terhadap pengguna cyber yang lain,

dan masih banyak lagi. (Enjelina et al., 2025)Maka dapat kita garis bawahi bahwa Tindakan tersebut bukan hanya pelanggaran hukum saja, tetapi juga merupakan pelanggaran etika dalam dunia cyber.

Kejahatan cyber harus di atasi dengan Upaya hukum pidana, termasuk dalam hal pembuktian. Sebab oleh fakta bahwa penegakan hukum pidana, seseorang dapat dianggap bersalah atau tidak,selain berdasarkan undang-undang yang ada sebelumnya (asas legalitas), juga harus di dukung oleh bukti yang sah untuk dapat dipertanggungjawabkan (unsur kesalahan). Seperti bunyi Pasal 1 Ayat (1) asas legalitas dalam hukum pidana (KUHP). (Enjelina et al., 2025) ” *Nullum delictum nulla poena sine praevia lege poenali.”* Artinya “ Tiada tindak pidana,tidak ada pidana,tanpa adanya aturan hukum pidana terlebih dahulu.”

Dalam Masyarakat pada bentuk kejahatan cyber di bagi dengan tiga macam kualifikasi umum yaitu :

1. Kejahatan dunia maya yang berkaitan dengan kerahasiaan,integritas dan keberadaan data serta sistem komputer.
2. Kejahatan dunia maya yang menggunakan komputer sebagai alat kejahatan.
3. Kejahatan dunia maya yang berkaitan dengan isi atau muatan data maupun sistem komputer.

Di Indonesia ini pengguna pengguna internet atau media sosial sudah mencapai 63 juta orang. Selain itu 95 persen dari pengguna menggunakan internet untuk jejaring sosial.(Subagyo, 2015)

Bahkan untuk menjalankan tugasnya Pemerintahan serta jajaranya juga menggunakan media dengan menggunakan aplikasi seperti isntagram, tiktok, tweeter dan aplikasi yang lain. Dari beberapa media tersebut maka tidak mengecilkan kemungkinan untuk terjadi ancaman kejahatan cyber berupa hacking contohnya. Dimana para pelaku hacking bertindak untuk mendapatkan atau mengetahui rahasia-rahasia pribadi maupun komunitas atau instansi negara.(Rashid & Rashid, 2023)

Maka Indonesia perlu mempercepat penerapan undang-undang keamanan Cyber untuk menciptakan landasan hukum.dengan undang-undang tersebut guna mendorong suatu strategi keamanan cyber yang komprehensif untuk mengutamakan fungsi BSSN. (Rahmadiani et al., 2019)

Sejak tahun 2019 kementerian komunikasi dan informatika (KOMINFO) mencatat 29 lembaga dan perusahaan yang menjadi sasaran kejahatan cyber berupa kebocoran data, termasuk badan penyelenggara jaminan sosial (BPJS) kesehatan.Dengan kasus tersebut dari 21 kasus telah berhasil di selesaikan oleh Kominfo. Penyebab dari terjadinya kebocoran data dikarenakan sistem keamanan yang mudah di retas serta kurangnya integritas sumber daya manusia yang bekerja sama dengan pelaku peretasan.(Oktaviani et al., 2021)

Dalam kasus peretasan terdapat ketentuan khusus yang mengatur tindak pidana pada pasal 30 ayat 1,2 dan 3 UU ITE. (Republik Indonesia, 2008) Disitu menjelaskan bahwa setiap orang yang mencoba masuk pada sistem elektronik orang lain secara sengaja tanpa hak melawan hukum.

Dari sisi hukum mungkin kita lihat melanggar namun dalam pandakangan etika tetap melanggar karena seringkali menjadi aspek yang di abaikan para pelaku yang dimana tindakanya tidak hanya melanggar hukum saja namun juga melanggar norma dan nilai moral. Meskipun di Indonesia pemerintah telah menerapkan Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) serta melakukan berbagai upaya penegakan hukum ,kenyataanya kejahatan cyber dan pelanggaran etika di dunia cyber masih terus terjadi.

Terorisme cyber merupakan kejahatan menggunakan sarana internet dengan mengakibatkan ancaman,gangguan keamanan,dan mengakibatkan kerugian materiil maupun nonmateriil.pelaku dalam hal ini dapat perorangan maupun kelompok, korporasi, badan hukum. (Agustus, 2024)

Meningkatnya Cybercrime di Indonesia telah menjadikan pemerintah dan aparat hukum melakukan beberapa antisipasi melalui perubahan Undang-undang sesuai perkembangan teknologi. Seperti pemberian etika komputer di Perguruan Tinggi dan Pemahaman tentang kesadaran keamanan berinternet kepada para penggunanya. Namun tetap saja semua kembali kepada masing-masing pengguna teknologi informasi ini tentang sadar pentingnya mengamankan data-data dan aktifitasnya.tetapi sayangnya tingkat kepedulian pengguna dalam menjaga keamanan TI masih belum tinggi. (Chintia et al., 2019)

Dalam hal ini perlunya sosialisasi dari pemerintah kepada masyarakat akan bahaya cyber (Pertiwi et al., 2024) guna menghindari kejadian yang tidak diinginkan dikemudian hari.(Bupu et al., 2024)

Kejahatan cyber tidak hanya melanggar hukum formal namun juga melanggar norma dan prinsip etika yang seharusnya menjadi landasan dalam berinteraksi di ruang digital .terdapat beberapa yang kita temui dalam tindakan tidak etis di dunia maya terdapat tindakan yang secara hukum belum di atur atau sulit di buktikan namun secara moral dan etika jelas keliru seperti penyebaran hoaks, doxing (membuka identitas seseorang secara tidak izin), atau mengakses data pribadi. Dalam etika tindakan menyimpang dalam dunia maya mencerminkan bahwa rendahnya kesadaran moral sebagian pengguna terhadap nilai-nilai tanggungjawab, kejujuran, dan penghormatan terhadap privasi orang lain. Namun banyak pengguna *cyber* yang menganggap dunia maya sebagai ruang bebas tanpa aturan sehingga mereka dapat bertindak tanpa mempertimbangkan dampak terhadap orang lain.Dalam beberapa kasus pelaku kejahatan cyber tidak merasa bersalah secara moral karena kurangnya pemahaman etika digital. (Turnip & Siahaan, 2021). Hal ini menunjukan bahwa penegakan hukum tidaklah cukup harus ada pendekatan etis memahami dan menanggulangi kejahatan cyber tersebut.

Etika menjadi landasan moral dalam menentukan salah dan benar terutama dalam dunia tanpa batas seperti internet. Dimana aturan hukum belum bisa menjangkau secara menyeluruh, etika dapat menjadi panduan tindakan yang bertanggungjawab atas perlakuanya. (Basuki, 2019)

Maka pentingnya untuk mengkaji kejahatan cyber tidak hanya dari sisi yuridis,tetapi juga dari perspektifetika normatif, seperti deontologi, utilitarianisme, dan etika kebajikan. (Weruin, 2019)

Oleh karena itu, maka penelitian ini akan mengulas dan menganalisis bentuk-bentuk pelanggaran etika dalam kejahatan cyber, serta mencari solusi berbasis moral dalam bernegara yang sehat.penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan literasi etika digital di indonesia. (Amirulkamar, 2024)

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan tersebut, dirumuskan permasalahan sebagai berikut:

Apa saja bentuk pelanggaran etika dalam kejahatan *cyber*?

C. Tujuan penelitian

Tujuan dari penelitian ini diharapkan mampu memberikan arah yang jelas terkait dengan langkah yang akan dilakukan dalam penelitian ini, serta memberikan batasan-batasan dalam penelitian ini. Adapun tujuan yang ingin dicapai oleh penulis dalam penelitian ini :

1. Untuk menganalisis identifikasi analisis hukum terhadap kejahatan cyber yang rentan terjadi di kalangan hidup manusia.
2. Untuk mengetahui faktor apa saja yang mengakibatkan maraknya kejahatan cyber
3. Untuk memberikan upaya dalam menangani kejahatan cyber.

D. Manfaat Penelitian

Dalam penelitian tentunya sangat diharapkan adanya manfaat dan kegunaan yang dapat diambil dalam penelitian tersebut. Adapun manfaat yang didapat dari penelitian ini :

1. Manfaat Teoritis
    a. Hasil penelitian ini dapat memberikan kontribusi terhadap penelitian sejenis di masa mendatang, sehingga dapat digunakan sebagai referensi bagi mahasiswa yang tertarik untuk melanjutkan penelitian mengenai isu yang dibahas dalam proposal ini.
    b. Hasil penelitian ini juga bermanfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang hukum pidana lintas terkait kejahatan cyber
2. Manfaat Praktis
    a. Temuan dari penelitian ini dapat menjadi referensi bagi aparat penegak hukum dalam menjalankan penegakan hukum terhadap Tindakan kejahatan cyber.
    b. Diharapkan, hasil penelitian ini dapat memperluas pemahaman tentang pentingnya penguatan penegakan hukum terhadap kejahatan cyber.

BAB II

TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Dalam penelitian (Primawati, 2016) yang berjudul Etika IT Di Indonesia Studi Kasus:Cybersquatting Pada Domain PT. Mustika Ratu . Jurnal ini membahas mengenai permasalahan kode etik dalam tekhnologi informasi di Indonesia. Dia mengatakan bahwa perkembangan teknologi informasi telekomunikasi media serta informasi . Ialah internet dengan berbasis website menjadi hal yang cukup kompleks untuk di miliki setiap perusahaan agar keberadaan bisnisnya mencakup seluruh duina. Dengan mengaktifkan layanan internet wajib membuat nama domain mengidentifikasikan keberadaan perusahaan tersebut. Dalam kasus mustika-ratu.com peneliti berpendapat bahwa pihak lain yang mendaftarkan domain mustika-ratu.com belum tentu bersalah jika tidak merugikan pihak pemilik awal. Maka untuk menghindar dari pelanggaran etika seperti itu perusahaan perlu waspada khususnya dalam mendaftar nama domain yang harus mempunyai pengetahuan yang luas tentang domain pada dunia cyber. Kesimpulanya bahwa dunia internet rawan terjadi kejahatan cyber.cyberquatting salah satu pelanggaran etika IT dan juga kejahatan cyber.

Penelitian selanjutnya (Rusdiyanto et al., 2024) berjudul Penipuan Menggunakan Media Internet Berupa Jual Beli Online membahas tentang bagaimana hukum indonesia mengatur tindak pidana penipuan dalam ranah kejahatan cyber yang terjadi dalam aktifitas jual beli online. Pada penelitianya

juga mengkaji peraturan-peraturan yang di gunakan oleh aparat penegak hukum dalam menanggulangi kejahatan tersebut. Metode penelitian tersebut dengan hukum normatif. Dengan hasil penelitian menunjukan bahwa penipuan secara online dengan sarana yang di gunakan yaitu melalui sistem elektronik seperti komputer,dan peragkat yang lainya. Perilaku tersebut dapat di jerat melalui undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik (UUITE) pelaku dapat dikenakan pasal 378 KUHP tentang penipuan dan juga pasal 28 ayat 1 UU ITE tentang penyebaran informasi bohong atau menyesatkan yang dapat merugikan konsumen. Penelitian ini berpedoman dengan aspek hukum saja.sedangkan penilitian saya tidak hanya tertuju dengan nilai hukum namun juga nilai etika pada pelaku kejahatan cyber.

Penelitian selanjutnya (Salim & Hakim, 2024) dengan jurnalnya yang berjudul Penurunan Etika Sebagai Dampak Kejahatan Siber Terhadap Generasi Muda Di Indonesia. Peneliti ini bertujuan menganalisis bagaimana serangan *cyber* memengaruhi nilai-nilai etika di kalangan remaja dan mahasiswa.peneliti menggunakan metode kualitatif untuk menganalisis pengalaman generasi muda terhadap ancaman *cyber*.Data yang di cakup tanggapan terhadap cyberbullying,penipuan online,dan ekploitasi digital.dengan hasil menunjukan kejahatan *cyber* merusak integritas moral dan memicu penurunan etika dalam perilaku online dan ofline. Dalam menanggapi hal ini perlu kolaboratif bagi pemerintah, pendidikan, dan masyarakat untuk meningkatkan kesadaran dan pendidikan digital untuk melindungi integritas etika generasi muda.

Dapat di simpulkan bahwa adanya tindakan pencegahan dan pendidikan yang holistik untuk mengatasi dampak negatif kejahatan *cyber* terhadap etika remaja di indonesia. Penelitian ini sama dengan penelitian saya dimana etika dalam perilaku di dunia *cyber* ini memang mempunyai ancaman yang luar biasa. Yang dapat merugikan pihak korban secara materiil atau nonmateriil.

Penelitian selanjutnya (Hafidz, 2021) Dalam jurnal yang berjudul Penyebaran Screenshot Whatsapp dalam Perspektif Etika dan Hukum Pidana. Ini merupakan jenis penelitian hukum normatif atau yuridis normatif, dengan pendekatan perundang-undangan. Penelitian ini bersifat deskriptif analisis dengan menggunakan data sekunder yang di peroleh melalui studi kepustakaan, kemudian di analisis secara kualitatif. Pada jurnalnya menghasilkan bahwa penyebaran screenshot whatsapp dalam perspektif etika, termasuk tindakan tidak etis atau tidak baik jika dilakukan tanpa izin atau persetujuan dari orang yang terlibat dalam percakapan. Dalam persektif hukum pidana maka termasuk ke dalam pencemaran nama baik, karena terdapat data pribadi seseorang atau mengandung privasi orang lain. Berdasarkan ketentuanya Pasal 27 ayat 3 undang-undang no 19 tahun 2016 tentang setiap orang dengan sengaja tanpa hak mendistribusikn atau mentransmisikan atau membuat dapat di aksesnya informasi elektronik dan dokumen elektronik yang mengandung penghinaan atau pencemaran nama baik. Dalam penelitian di atas sama dengan penelitian yang saya ambil karena *cybercrime* tidak hanya tertuju pada kepastian hukum saja namun juga nila etika moral.

Pada penelitian terakhir (Riskiyadi et al., 2021) Dengan judul jurnal *cybercrime* dan *cybersecurity* pada fintech: Sebuah Tinjauan Pustaka Sistematis. Penelitian ini bertujuan untuk mengetahui tantangan *cybercrime* yang di hadapi di industri fintech dengan menggunakan *cybersecurity* sebagai penangulangan tantangan tersebut. Penelitian ini menggunakan metode tinjauan Pustaka sistematis dari berbagai artikel yang membahas *cyber* dan *cybersecurity*. Hasil penelitianya menunjukan bahwa masalah *cybercrime* pada fintech meliputi regulasi *cybercrime* yang belum kuat, pencurian data dan informasi serta pencurian kekayaan intelektual sehingga dapat memberikan dampak pada reputasi fintech.

Pada penelitian di atas meneliti ancaman pada *cybecrime* dan sebaiknya dengan penelitian yang sedang saya lakukan harus memberikn teori yang lebih relevasn seperti menambahkan aspek hukum dan nilai etikanya.

B. Kerangka Teori

Kerangka teori merupakan landasan konseptual dalam menganalisis fenomena perilaku pengguna cyber yang melanggar hukum dan etika.teori yang dapat di gunakan sebagai pisau analisis dalam penelitian sebagai berikut :

Teori Perilaku Sosial

Teori ini menjelaskan perilaku individu terbentuk dan interkasi sosial dan pengaruh lingkungan. Dalam dunia maya ,media sosial sebagai ruang interaksi digital yang membentuk pola atau perilaku baru sesorang yang artinya konsep teori disinhibisi online (Online Disinhibition Effect) (KHADAFI, 2023) dengan kata lain fenomena yang muncul dalam perilaku

sesorang melakukan atau mengatakan hal-hal di dunia maya tetapi tidak dilakukan di dunia nyata. Teori ini terjadi karena mereka merasa lebih bebas mengekspresikan diri dan kurang terikat oleh aturan sosial.

Teori Etika

Etika dalam bahasa Yunani *ethos* yang berarti watak kesusilaan atau adat.(Basri et al., 2024) Sedangkan moral dari kata mores yang berarti cara hidup atau adat. Perbedaan keduanya jika moral suatu perbuatan yang sedang di nilai baik atau buruk. Sedangkan etika adalah pengkajian secara mendalam tentang perbuatan yang ada, jadi etika adalah suatu cabang dalam ilmu filsafat yang membahas system nilai yang berlaku yang bersifat kritis dan rasional.secara hukum etika merupakan prinsip moral dari perilaku yang mencakup kejujuran, integritas, dan tanggungjawab. Dalam kejahatan *cyber* etika menjadi penting di evaluasi dari tindakan-tindakan di ruang digital, Tetapi secara moral patut di pertanyakan. Teori etika mempunyai beberapa macam yaitu:

a. Etika Deontologi (etika kewajiban)

   Etika deontologi merupakan etika yang menyatakan bahwa moralitas suatu tindakan ditentukan oleh apakah tindakan tersebut sesuai dengan kewajiban yang berlaku, bukan oleh konsekuensi atau hasilnya. Seperti halnya pada *cybercrime* tindakan seperti peretassan data dianggap salah karena melanggar hak dan martabat orang lain. Yang akan berdampak buruk pada orang tersebut. Lebih jelasnya tindakan tersebut di anggap melanggar karena mengabaikan kewajiban untuk menghormati sesama

b. Etika Utilitarisme (Etika Konsekuensialis)

Etika Utilitarianisme merupakan etika yang menempatkan tindakan yang baik sebagai tindakan yang memberikan manfaat terbesar bagi orang banyak. Yang berarti tindakan yang memaksimalkan kebahagiaan dan kesejahteraan bagi semua pihak yang terkena dampak. Dalam kejahatan *cyber* kita dapat melihat seperti penyebaran hoaks yang menimbulkan kepanikan bagi banyak korban, terutama kepercayaan dalam publik. Tetapi menguntungkan bagi pelaku tindak kejahatan tersebut.

c. Etika Sosial Dan Etika Profesi

Etika Sosial merupakan prinsip moral yang mengatur perilaku manusia dalam relasi sosial, serta bagaimana nilai-nilai moral tersebut diterapkan dalam struktur, sistem, isudan komunitas sosial. lebih jelasnya individu seharusnya berinteraksi dengan orang lain dalam masyarakat dengan menghormati hak, kewajiban, dan keadilan. Sedangkan Etika Profesi merupakan seperangkat nilai, prinsip, dan norma moral yang mengatur perilaku dan tindakan individu dalam konteks profesinya. Ini adalah panduan moral dimana profesional dalam mengambil keputusan yang tepat, bertanggungjawab, dan etis dalam melaksanakan tugas mereka. Etika ini juga menjaga integritas, transparansi, dan akuntabilitas dalam menjalankan tugas, serta mencegah praktik gratifikasi, korupsi, dan penyalah gunaan wewenang. Hal ini dapat di contohkan dalam kejahatan *cyber* seperti bocornya informasi rahasia perusahaan itu melanggar etika sosial maupun etika profesi karena merugikan banyak pihak dan merusak kepercayaan publik.

Teori Kejahatan Cyber *(Cybercrime)*

Cybercrime merupakan kejahatan yang dilakukan dengan menggunakan komputer atau jaringan komputer sebagai alat atau sasaran untuk mencapai tujuan ilegal. Tindakan ini melibatkan pencurian data, perusakan sistem, penipuan, atau penyalahgunaan informasi yang di simpan. Kegiatan ini berdampak kerugian finansial, kehilangan data pribadi, kerusakan reputasi, dan bahkan dapat mengancam keamanan nasional.

Menurut Andi Hamzah (1989) *cybercrime* adalah kejahatan di bidang komputer yang secara umum dapat di artikan sebagai penggunaan komputer secara ilegal.(Sugiaryo, 2010)

Menurut Widodo Cybercrime adalah kegiatan yang dilakukan sesorang atau sekelompok orang atau badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan.(Mohd. Yusuf DM et al., 2022)

Menurut Murti (2005) istilah untuk menggambarkan tindakan kejahatan dengan menggunakan media komputer atau internet.

Menurut Gregory (2015) bentuk kejahatan virtual yang memanfaatkan media komputer yang terhubung dengan internet.

Menurut Aldrich & Duffield (2014) kejahatan *cyber* yang melibatkan pengguna TIK dengan tujuan mengganggu, merampas, dan, merusak sebuah data.

Secara ringkas di artikan bahwa cybercrime merupakan tindakan ilegal yang terjadi di dunia maya mulai dari, peretasan sistem komputer, pencurian data, penipuanonline, dan penyebaran malware.

Cybercrime mempunyai karakteristik meliputi ruang lingkup global yang melintas batas negara, tidak mudah dideteksi, melibatkan teknologi canggih, dan dilakukan secara online.

Kejahatan siber (*cybercrime*) merupakan istilah umum untuk berbagai kegiatan kriminal yang di lakukan menggunakan komputer atau jaringan internet. Jenis kegiatan kriminal ini meliputi:

- *Phising*

  Kegiatan ini merupakan Tindakan pidana pasal 378 KUHP tentang penipuan dan UU No 11 tahun 2008. Penipuan online yang bertujuan untuk mencuri data pribadi, seperti nomor kartu kredit, pin, atau pasword, dengan motif pelaku menyamar sebagai lembaga atau perusahaan yang terpercaya.

- *Hacking*

  Kegiatan ini Tindakan pidana pasal 30 UU ITE tentang peretasan sistem komputer atau jaringan tanpa izin dengan tujuan mencuri data atau merusak sistem

- *Ransomware*

  Kegiatan ini dengan memblokir akses, menghancurkan, atau menerbitkan data penting korban. Tetapi kegiatan ini harus mempunyai syarat supaya tidak melakukan kriminal tersebut dengan membayarkan uang tebusan kepada pelaku.

- *Cyberbullying*

  Kegiatan ini merupakan perundungan atau penindasan yang bersifat online melalui internet. Tindakan ini berupa hinaan, ancaman,

pelecehan, atau penyebaran informasi palsu bahkan informasi terkadang ada yang bersifat memalukan.

Aspek hukum *cybercime* di atas di atur oleh UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) dan KUHP (Kitab Undang-Undang Hukum Pidana). UU ITE mengatur Tindakan pidana khusus terjadi di dunia maya, sementara KUHP mengatur tindak pidana secara umum yang dapat terjadi melalui elektronik.

Dengan teori di atas dalam era modern ini semua kegiatan yang memudahkan semua orang untuk beraktifitas yang menghasilkan keuntungan maupun kerugian . Dalam etika di dunia maya tidak semua bermasalah pada hukum,misalnya penyebaran hoaks walaupun belum tentu terjerat hukum akan tetapi secara etika di anggap Tindakan yang tidak bermoral karena merugikan orang lain.

Selanjutnya pada teori *cybercrime* di atas menjelaskan karakteristik, serta dampak kejahatan yang terjadi di sarana teknologi informasi saat ini dalam mengidentifikasi perbuatan melawan hukum yang di lakukan menggunakan sarana computer atau jaringan internet. Teori keduanya merupakan fenomena kejahatan yang terjadi dengan pertimbangan dimensi hukum dan etika guna mendukung pencegahan dan penanggulangan *cybercrime*.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian yang akan dipergunakan adalah penelitian yuridis normatif (legal research) Penelitian hukum normatif pada umumnya dapat di sebut penelitian hukum doktriner maupun penelitian hukum kepustakaan. (Ersya, 2017)

Penelitian hukum normatif merupakan suatu cara untuk menemukan kebenaran dari sisi normatif berdasarkan logika dan ilmu hukum. Yang ada dan dasarnya pada peraturan-peraturan yang tertulis dan juga bahan hukum yang lain. Penelitian normatif mengkaji norma hukum positif yang bertujuan menganalisis dan memahami kejahatan *cyber* dari perspektif etika dalam hukum.

B. Pendekatan Penelitian

Pendekatan Penelitian yang dilakukan yitu dengan menggunakan:

1. Pendekatan Perundang-undangan (Statue Approach)

   Yang bisa di artikan dengan metode pendekatan menggunakan undang-undang.(Benuf et al., 2019)dengan metode menelaah undang-undang dan regulasi yang bersangkutan atau mengkaji peraturan perundang-undangan seperti UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), KUHP, dan peraturan terkait lainya.

2. Pendekatan Kasus (Case Approach)

Pada penelitisn normatif menggunakan kasus terkait kejahatan *cyber* yang telah di proses secara hukum untuk melihat norma dan pertimbangan etis.

C. Objek Penalitian

Objek Penelitian ini adalah norma hukum yang mengatur kejahatan *cyber* serta konsep etika yang berkaitan dengan tindakan dalam ruang digital. Penelitian ini juga mengkaji relevansi dan efektivitas penerapan etika dalam menanggulangi kejahatan *cyber*.

D. Sumber Data

Dalam memecahkan permasalahan hukum di butuhkan sumber hukum agar memudahkan penulis. Sumber data yang telah di peroleh akan di olah dalam penilitian hukum normatif dengan menggunakan bahan hukum primer yang terdiri dari peraturan perundang -undangan dan putusan hakim, serta bahan hukum sekunder yang berupa bahan yang memberikan penjelasan hukum. Dan taklupa penulis juga menggunakan bahan hukum tersier. Berikut adalah bahan hukumnya:

1) Bahan Hukum Primer

Di dalam penelitian ini penulis mengkaji ketentuan pada perundang-undangan dan putusan pengadilan yang terkait dengan kasus kejahatan *cyber*. Yang meliputi:

a. Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik yang telah mengalami perubahan melalui Undang-Undang No 19 Tahun 2016 dan Undang-Undang No 1 Tahun 2024.

b. Kitab Undang-Undang Hukum Pidana (KUHP)

2) Bahan Hukum Sekunder

Bahan hukum sekunder merupakan penjelasan bahan hukum primer dengan menggunakan buku, tulisan ilmiah dan laporan lain yang berkaitan dengan materi penelitian.

3) Bahan Hukum Tersier

Yaitu bahan hukum yang meberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder yang ada atas kamus hukum.

E. Teknik Pengambilan Data

Penelusuran bahan hukum primer,sekunder,dan tersier dapat dilakukan melalui studi kepustakaan (library research) maupun studi dokumentasi terhadap bahan hukum dan informasi hukum serta perpustakaan-perpustakaan pada instansi yang terkait dan juga melalui penelusuran internet. Bahan hukum primer dan sekunder dalam pencarian yang terkait tentang urgensi terkait kejahatan *cyber* dalam pandangan etika.

F. Teknik Analisis Data

Data yang diperoleh selanjutnya akan di analisis secara kualitatif dengan mereduksi data agar sesuai dengan topik yang di teliti, dan menyajikanya secara deskriptif, lalu mengambil kesimpulan berdasarkan data yang telah disajikan secara deduktif yang artinya deskriptif kualitatif.

BAB V

PENUTUP

A. Kesimpulan

Etika merupakan seperangkat nilai moral dan prinsip yang mengatur perilaku manusia dalam kehidupan bermasyarakat. Dalam perkembangan teknologi muncullah etika digital yaitu merupakan panduan perilaku yang menekankan tanggung jawab individu dalam menggunakan teknologi informasi secara bijak dan tanggung jawab. Etika digital juga menjadi sangat penting karena aktivitas di dunia digital memiliki dampak nyata terhadap individu maupun masyarakat. Di dalam etika digital memiliki mempunyai prinsip-prinsip seperti integritas, privasi, keadilan, dan tanggung jawab. Prinsip tersebut sejalan dengan asas hukum dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), seperti asas kepastian hukum, keadilan, kepatutan, kebebasan yang bertanggungjawab, dan perlindungan terhadap hak asasi manusia. Dengan memahami dan menerapkan etika digital, masyarakat dapat menciptakan ruang digital yang sehat, aman, dan beradab. Etika digital tidak hanya soal hukum tapi juga cerminan karakter dan serta tanggung jawab individu dalam kehidupan digital.

B. Saran

Berdasarkan hasil penelitian dan pembahasan mengenai pentingnya etika dalam konteks Undang-undang Informasi dan Transaksi Elektronik (UU ITE), maka saya memberikan saran sebagai berikut :

1. Bagi Masyarakat Umum

Diharapkan masyarakat lebih meningkatkan literasi digital, terutama dalam memahami etika berkomunikasi dan berperilaku di dunia maya. Pengguna media sosial dan penyelenggara platform seharusnya mempunyai kesadaran akan tanggung jawab sosial dan hukum agar terhindar dari pelanggaran etika maupun pelanggaran hukum.

2. Bagi Pemerintah dan Pembuat Kebijakan

Perlu adanya pembaharuan dan sosialisasi berkala terutama pada UU ITE agar Masyarakat memahami batasan perilaku supaya tidak terjerat dalam hukum maupun dampak sosial terhadap pelanggaran etika. Pemerintah juga di sarankan untuk menyediakan edukasi publik yang lebih massif terkait etika digital, misalnya melalui kampanye digital, kurikulum pendidikan, maupun pelatihan kepada Masyarakat.

3. Bagi Institusi Pendidikan

Sebaiknya pendekatan dan pemahaman tentang etika digital harus di masukan secara formal ke dalam kurikulum, sebab hal ini bertujuan agar generasi muda mengenal etika digital yang baik dan benar seperti apa. Dan juga mengurangi adanya pelanggaran etika yang sering terjadi di media sosial.

4. Bagi Peneliti Selanjutnya

Disarankan untuk mengkaji lebih dalam menegenai efektivitas penerapan etika digital dalam kehidupan bermasyarakat serta dampak hukum maupun sosialnya .Peneliti selanjutnya juga dapat menambahkan aspek supaya dapat memberikan kontribusi lebih komprehensif.

DAFTAR PUSTAKA

Achmad, G. H. (2022). Pemikiran Filsafat Etik Immanuel Kant dan Relevansinya dengan Akhlak Islam. *Alsys*, *2*(2), 324–339. https://doi.org/10.58578/alsys.v2i2.310

Agustus, N. (2024). *Pertanggungjawaban Pidana Pelaku Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional perbuatan , namun tujuannya sama dengan terorisme konvensional . Bentuk-bentuk terorisme a . Tinjauan Umum Pertanggungjawaban Pidana Dalam cambridge dictionary , perta*. *1*(4), 180–199.

Amirulkamar, S. (2024). *Dampak literasi digitalterhadap pelayanan publik di indonesia dalam perspektif etika*. *5*(1), 87–94.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Basri, H. H., Heliwasnimar, H., & Ardimen, A. (2024). Etika dan Moral Dalam Ilmu Pengetahuan. *Indonesian Research Journal on Education*, *4*(1), 343–351. https://doi.org/10.31004/irje.v4i1.494

Basuki, S. (2019). Etika Informasi. *Pustakawan*, *26*(1), 4–11.

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Bupu, A. G., Medan, K. K., & Amalo, H. (2024). Analisis Yuridis Cyber Crime Pembobolan Dana Nasabah pada Aplikasi Mobile Banking dengan Modus Pembobolan Jalur Undangan Pernikahan Palsu. *Jurnal Ilmu Hukum dan Sosial*, *2*(2), 367–383. https://doi.org/10.51903/hakim.v2i2.1829

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati S.Kom., M.Sc.Eng, N. A. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology*, *2*(2), 65. https://doi.org/10.26740/jieet.v2n2.p65-69

Enjelina, D., Natalia, S. H. L., & Suryawati, P. S. M. (2025). *Pelanggaran Etika Dalam Media Sosial*. *2*(1), 174–180.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *August 2017*, 50–62. https://doi.org/10.24036/8851412020171112

Fuady, M. E. (2005). Internet: Teknologi Pencipta Dunia "Cyber." *MediaTor*, *Vol.6*(No.2), 255–264. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hafidz, J. (2021). Penyebaran Screenshot Whatsapp dalam Perspektif Etika dan Hukum Pidana. *Jurnal Cakrawala Informasi*, *1*(1), 58–73. https://doi.org/10.54066/jci.v1i1.213

Jurnalistik, I. K., Dakwah, F., & Gunung, U. I. N. S. (2021). *Media Sosial Sebagai Sarana Penyebarluasan Berita*. *6*(September), 247–266.

KHADAFI, M. R. (2023). *Kajian Disinhibisi Online Di Media Sosial (Studi Kasus Kreator Konten Kritik Sosial Di Media Sosial Tiktok)*. 110.

Made Wisnu A. S., I Wayan Gde Wiryawan, & Kt. Sukawati Lanang P. P. (2021). Faktor Penyebab Terjadinya Kejahatan Cyber Crime Yang Dilakukan Oleh Orang Asing Di Bali Ditinjau Dari Perspektif Kriminologi. *Jurnal Yusthima*, *1*(01), 58–70. https://doi.org/10.36733/yusthima.v1i01.2984

Mohd. Yusuf DM, Vivi Yola, Destin Maiharani, & Egi Dwi. (2022). Analisis Terhadap Modus-Modus Dalam Hukum Cyber Crime. *Jurnal Hukum, Politik Dan Ilmu Sosial*, *1*(2), 64–70. https://doi.org/10.55606/jhpis.v1i2.725

Oktaviani, S., Dewata, Y. J., & Fadlian, A. (2021). Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite. *De Juncto Delicti: Journal of Law*, *1*(2), 146–157. https://doi.org/10.35706/djd.v1i2.5732

Pertiwi, N. A. S., Fitri Umardiyah, Mansyur, M. N., Munir, M., Sapi'i, I., Sholichah, A., & Fudlah, T. N. (2024). Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4.0. *Jumat Informatika: Jurnal Pengabdian Masyarakat*, *5*(1), 49–55. https://ejournal.unwaha.ac.id/index.php/abdimas_if/article/view/4525

Primawati, A. (2016). Etika It Di Indonesia Studi Kasus: Cybersquatting Pada Domain Pt. Mustika Ratu. *Simetris : Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *7*(1), 421. https://doi.org/10.24176/simet.v7i1.534

Purba, R. T. (2022). Perkembangan Moral Menurut Kohlberg Dan Implementasinya Dalam Perspektif Kristen Terhadap Pendidikan Moral Anak Di Sekolah Dasar. *Aletheia Christian Educators Journal*, *3*(1), 11–20. https://doi.org/10.9744/aletheia.3.1.11-20

R, I. (2003). Jurisdiksi Dunia Maya (Cyberspace) Dalam Sistem Hukum Nasional Abad XXI. *Jurnal Hukum IUS QUIA IUSTUM*, *10*(24), 119–127. https://doi.org/10.20885/iustum.vol10.iss24.art10

Rahmadiani, A., Mantovani, A. P. K., Hariz, S. U., Haryanto, J., & Aidad, F. F. (2019). Strategi Keamanan Siber Indonesia Rekomendasi Rencana Aksi Dan Implementasi. *Center for Digital Society*, *1*(69), 5–24.

Rashid, F., & Rashid, S. (2023). Cyber Laws. *Digital Freedom*, 85–133. https://doi.org/10.1201/9781003403784-3

Republik Indonesia. (2008). Undang-Undang tentang Informasi dan Transaksi Elektronik. *Bi.Go.Id*, *September*, 1–2. https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen dan Organisasi*, *12*(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528

Rusdiyanto, D., Siwi, D. R., Fitriana, G., Fitri, A., & Jainah, Z. O. (2024). Penipuan Menggunakan Media Internet Berupa Jual-Beli Online. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*, *II*(4), 277–285. https://doi.org/10.24252/iqtishaduna.vi.43808

Salim, L., & Hakim, N. (2024). *Penurunan Etika Sebagai Dampak Kejahatan Siber Terhadap Generasi Muda di Indonesia*. *2*(1), 628–636.

Subagyo, A. (2015). Sinergi dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Warfare Threat. *Jurnal Pertahanan*, *5*(1), 89–107.

Sugiaryo. (2010). KEBIJAKAN REGULASI HUKUM PIDANA DALAM MENANGANI KEJAHATAN TEKNOLOGI INFORMASI Oleh : Sugiaryo (Staf Pengajar UNISRI Surakarta). *Jurnal Serambi Hukum*, *04*(02).

SUYONO, S. (2022). Kajian Literatur: Konsep Integritas Bagi Asn. *CENDEKIA: Jurnal Ilmu Pengetahuan*, *2*(3), 247–260. https://doi.org/10.51878/cendekia.v2i3.1479

Talumedun, G. J., Gosal, R., & Kimba, A. (2019). Penonaktifan Sementara Sri Wahyumi Maria Manalip, SE Bupati Kabupaten Kepulauan Talaud hasil pemilihan tahun 2014 sampai 2019. *Eksekutif : Jurnal Jurusan Ilmu Pemerintahan*, *1*. https://ejournal.unsrat.ac.id/index.php/jurnaleksekutif/article/view/21558%0Ahttps://ejournal.unsrat.ac.id/index.php/jurnaleksekutif/article/download/21558/21264

Tamimi, F., & Munawaroh, S. (2024). *Teknologi Sebagai Kegiatan Manusia Dalam Era Modern Kehidupan Masyarakat*. *2*(3), 66–74.

https://doi.org/10.61132/saturnus.v2i3.157

Taufik, M. (2018). Etika Plato dan Aristoteles: Dalam Perspektif Etika Islam. *Refleksi Jurnal Filsafat dan Pemikiran Islam*, *18*(1), 27–45. https://doi.org/10.14421/ref.v18i1.1855

Timoty Agustian Berutu, Dina Lorena Rea Sigalingging, Gaby Kasih Valentine Simanjuntak, & Friska Siburian. (2024). Pengaruh Teknologi Digital terhadap Perkembangan Bisnis Modern. *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, *2*(3), 358–370. https://doi.org/10.61132/neptunus.v2i3.258

Turnip, E. Y., & Siahaan, C. (2021). Etika Berkomunikasi dalam Era Media Digital. *Jurnal Ekonomi, Sosial & Humaniora*, *3*(4), 1–8. https://www.jurnalintelektiva.com/index.php/jurnal/article/view/659

Umam, M. S. (2019). Orientasi Etika dan Cyber Security Awareness (Studi Kasus pada UMKM di Bantul). *Akmenika: Jurnal Akuntansi dan Manajemen*, *13*(2), 283–291. https://doi.org/10.31316/akmenika.v16i2.394

Weruin, U. U. (2019). Teori-Teori Etika Dan Sumbangan Pemikiran Para Filsuf Bagi Etika Bisnis. *Jurnal Muara Ilmu Ekonomi dan Bisnis*, *3*(2), 313. https://doi.org/10.24912/jmieb.v3i2.3384

Widiyanto, D., & Istiqomah, A. (2023). Pendidikan Kewarganegaraan Sebagai Wahana Pendidikan Demokrasi. *Jurnal Pendidikan*, *32. No.1*(1), 1–10. http://journal.univetbantara.ac.id/index.php/jp/article/view/2826