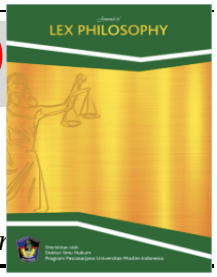
Journal of Lex Philosophy (JLP)
Volume 5, Nomor 2, Desember 2024
P-ISSN: 2722-1237, E-ISSN: 2722-2020
Website: http: pasca-umi.ac.id/index.php/jlp
This work is licensed under a Creative Commons Attribution 4.0 International Licer



Implementasi UU ITE Dalam Rangka Pemberantasan Tindak Pidana Pemerasan Dalam Dunia Digital

Ainun Jariah A. Kadir[1], Mulyati Pawennei[2] & Asriati[2]

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

Submitted: 1 Nopember 2024; Revised: 16 Desember 2024; Accepted: 31 Desember 2024

ABSTRAK
Tujuan penelitian menganalisis implementasi UU ITE dalam rangka pemberantasan tindak pidana pemerasan dalam dunia digital; (2) Untuk mengetahui dan menganalisis kebijakan penegakan hukum terkait UU ITE dalam rangka pemberantasan tindak pidana pemerasan dalam dunia digital. Penulisan ini menggunakan metode penelitian hukum Normatif Hasil penulisan menunjukkan bahwa implementasi UU ITE dalam rangka pemberantasan tindak pidana pemerasan dalam dunia digital di perlukan upaya responsif dari para penegak hukum, upaya yang dapat dilakukan yaitu Upaya Represif dan Upaya Preventif. Kebijakan penegakan hukum terkait UU ITE dalam rangka pemberantasan tindak pidana pemerasan dalam dunia digital yaitu menjerat pelaku dengan Pasal 27 ayat (4). Dan ancaman pidana pelaku yang terbukti melanggar pasal ini yaitu pada Pasal 45 ayat (4).

Kata Kunci: *Pemberantasan; Pemerasan; Digital*

ABSTRACT
The research objective is to analyze the implementation of the ITE Law in the context of eradicating criminal acts of extortion in the digital world; (2) To understand and analyze law enforcement policies related to the ITE Law in the context of eradicating criminal acts of extortion in the digital world. This writing uses the Normative legal research method. The results of the writing show that the implementation of the ITE Law in the context of eradicating criminal acts of extortion in the digital world requires responsive efforts from law enforcers, efforts that can be taken are Repressive Efforts and Preventive Efforts. The law enforcement policy related to the ITE Law in the context of eradicating criminal acts of extortion in the digital world is to ensnare perpetrators under Article 27 paragraph (4). And the criminal threat for perpetrators who are proven to have violated this article is Article 45 paragraph (4).

Keywords: *Eradication; Extortion; Digital*

PENDAHULUAN

Kemajuan teknologi yang sangat pesat, dan adanya teknologi yang canggih serta modern sengaja diciptakan oleh manusia untuk mempermudah pekerjaan maupun mengakses segala informasi dan ilmu pengetahuan, sehingga dalam pekerjaannya manusia dapat menyelesaikannya dalam waktu singkat, perkembangan teknologi informasi dan komunikasi yang sangat cepat ini telah mempengaruhi perkembangan manusia di dunia (Ridwan, Masrul & Juhaepa, 2018). Teknologi informasi diyakini akan membawa manfaat dan kepentingan yang besar bagi negara-negara di dunia. Hal yang menjadikan teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia. Selain itu teknologi informasi mampu menghasilkan produk-produk teknologi informasi itu sendiri, seperti komputer, modem, serta sarana-sarana lain untuk membangun jaringan internet dan sebagainya (Cholik, 2021).

Kehidupan manusia di zaman sekarang ini sangat bergantung pada teknologi. Di satu sisi,teknologi dapat membawa banyak dampak positif, seperti adanya *E-mail, E-commerce, Cyber bank, Online Business, Internet Banking*, dan sebagainya. Namun, di sisi lain juga membawa dampak negatif dengan munculnya *cyber crime* (Sari, 2021). Dinamika kemajuan teknologi informasi dan komunikasi dalam masyarakat saat ini selain memberikan dampak positif, juga memberikan dampak negatif dari akibat ketidaksesuaian penggunaannya yang mengakibatkan timbulnya suatu kejahatan yang dikenal dengan istilah kejahatan siber (Ashady, 2024).

Produk Teknologi Informasi dan Komunikasi yang memudahkan setiap orang untuk memperoleh dan menyebar luaskan informasi dengan cepat, murah dan menjangkau wilayah yang sangat luas ialah Internet. Pemanfaatan internet tidak selalu membawa dampak positif akan tetapi juga dampak negatif. Salah satu dampak negatif dalam penggunaan internet adalah penyebaran informasi bermuatan pornografi melalui internet (Tarigan, Akhyar & Mustamam, 2023). Dengan adanya penyalahgunaan teknologi pada media elektronik maka telah menciptakan banyak bentuk kejahatan salah satunya ialah penyebaran pornografi di media elektronik. Pornografi di media elektronik adalah konten pornografi yang dimuat secara digital, salah satunya melalui jaringan internet. Pornografi berasal dari dua suku kata, yakni pornos dan grafi. *Pornos* yaitu perbuatan asusila yang berhubungan dengan seksual, atau perbuatan yang bersifat fulgar tidak senonoh atau cabul, sedangkan grafi adalah gambar atau tulisan, dan dalam arti luas grafi termasuk benda –benda patung yang isi atau artinya menunjukan atau menggambarkan suatu yang bersifat asusila atau menyerang rasa kesusilaan orang lain (Muqsit, Wijaya & Widianto, 2023).

Secara sederhana pornografi merupakan segala konten yang memuat kecabulan dan eksploitasi seksual yang melanggar norma sosial. Pornografi dapat berupa gambar, foto, tulisan, suara, animasi, kartun, percakapan, gerak tubuh, dan pertunjukan di muka umum. Ada beberapa syarat yang perlu ada agar wujud perbuatan mengupload atau menyiarkan selesai, yaitu sebagai berikut:

1. Telah ada wujud konkretnya, seperti mengumumkan, mengirimkan, mempertontonkan telah selesai dilakukan.
2. Pornografi yang disiarkan telah diketahui dilihat atau di dengar orang banyak (umum).
3. Orang banyak mengetahui atau mendengar pornografi disebabkan langsung

oleh perbuatan menyiarkan yang dilakukan oleh pengupload,bukan sudah diketahui sebelumnya.

Salah satu dampak buruk dari Internet ialah pelaku kejahatan memanfaatkan internet sebagai alat untuk melakukan kejahatannya. Seperti pertama, sebagai alat teror untuk meneror seseorang. Kedua, mempublikasikan hal-hal yang berbau asusila, pornografi, perjudian. Ketiga, hacker yang menerobos masuk sistem orang lain dengan tanpa hak dan atau melawan hukum. keempat, dan juga banyaknya kasus penipuan yang terjadi secara online.

Secara hukum maka, perbuatan tersebut melanggar Pasal 27 ayat (4) Undang Undang Namor 11 Tahun 2008 *jo* Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU ITE) yakni: "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" (Djanggih,& Qamar, 2018). Pelanggaran terhadap Pasal 27 ayat (4) UU ITE ini diancam dengan pidana yang diatur dalam Pasal 45 ayat (4) UU ITE, yaitu: "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikandan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana kurungan paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1 miliar" (Gumbira, 2020).

Ketentuan Pasal 27 ayat (4) UU ITE, sama seperti ketentuan dalam Pasal 27 UU ITE lainnya yakni merujuk pada KUHP. Ketentuan pada ayat (4) ini merujuk pada Pasal 368 dan Pasal 369 KUHP tentang Pemerasan dan Pengancaman. Sementara itu, perilaku merekam kegiatan seksualnya itu sendiri sama dengan perbuatan yang dilarang berlandaskan Pasal 4 ayat (1) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi yang berbunyi: "Setiap orang dilarang menciptakan, mlaksanakan, memperbanyak, mengulang, menyebarluaskan, menyiarkan, mengimpor, memperdagangkan, menawarkan, memperjual belikan, menyewakan, atau menjanjikan pornografi (Hidayat, *et, al,* 2023).

METODE PENELITIAN

Penulis akan melakukan penelitian berdasarkan penelitian hukum dengan melalui berbagai bahan kepustakaan. Penelitian hukum yang dimaksud adalah penelitian di bidang hukum yang dilatar belakangi oleh adanya kesenjangan antara *das sollen* dengan *das sein*.[81] Dalam studi kepustakaan Ini diharapkan agar dapat memberi sudut pandang yang lebih luas. Selain penelaahan terhadap buku-buku kepustakaan, sehingga ditemukan suatu asas hukum yang berupa dogma/dokrin hukum yang akan menjawab pertanyaan sesuai dengan pokok permasalahan dalam penelitian ini.

PEMBAHASAN

A. Implementasi UU ITE Dalam Rangka Pemberantasan Tindak Pidana Pemerasan Dalam Dunia Digital

Era globalisasi saat ini semakin berkembang pesat ditandai semakin banyaknya aspek kehidupan manusia yang dapat dilakukan melalui teknologi informasi.

Perkembangan tersebut dapat menjadi pisau bermata dua yang memberikan dampak baik yang bermanfaat dan dampak buruk yang dapat menjerat perilaku-perilaku menyimpang. Salah satunya adalah penyalahgunaan penggunaan internet yang dapat memberikan kerugian. Sisi buruk dari teknologi menyebabkan semakin mudahnya seseorang melakukan kejahatan menggunakan teknologi informasi yang biasa dikenal dengan kejahatan siber (*cybercrimes*) (Haqqi & Wijayati, 2019).

Penggunaan istilah *cybercrime* dalam penulisan ini eratkaitannya dengan dunia digital sehingga penulis menggunakan istilah *cybercrime* karena *cybercrime* sendiri merupakan segala bentuk kejahatan yang terjadi di dunia maya, dan dunia digital itu sendiri merupakan dunia yang terbentuk dari perkembangan teknologi informasi dan komunikasi, khususnya teknologi komputer yang terhubung internet. Maka dari pada itu penggunaan istilah *cybercrime* dapat dihubungkan dengan penggunaan istilah dunia digital.

Polri dalam hal ini unit *cybercrime* menggunakan parameter berdasarkan dokumen kongres PBB:*The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah Cyber Crime:

Pertama, cyber crime in a narrow sense (dalam arti sempit) disebut *computer crime: any illegal behaviour directed by means of electronic operation that target the security of computer system and the data processed by them.*

Kedua, cyber crime in a broader sense (dalam arti luas) disebut *computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.*

Indonesia belum memiliki Undang-Undang khusus/cyber law yang mengatur mengenai *cybercrime*, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku cybercrime terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut (Sumadi, 2015). *Computer viruses* atau Virus kompute merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus murni hanya dapat menyebar dari sebuah komputer ke komputer lainnya (dalam sebuah bentuk kode yang bisa dieksekusi).ketika inangnya diambil ke komputer target, contohnya ketika user mengirimnya melalui jaringan atau internet, atau membawanya dengan media lepas (*floppy disk, cd, dvd, atau usb drive*). Virus bisa bertambah dengan menyebar ke komputer lain dengan mnginfeksi *file* pada *network file system* (sistem file jaringan) atau sistem file yang diakses oleh komputer lain.

Contoh kejahatan yang menjadikan jaringan komputer atau divais sebagai alat yaitu: *Cyber stalking* (Pencurian dunia maya), Penipuan dan pencurian identitas, *Phishing scam*, Perang informasi (*Information warfare*). *Cyber stalking* (Pencurian dunia maya) *Cyberstalking* adalah penggunaan internet atau alat elektronik lainnya untuk menghina atau melecehkan seseorang, sekelompok orang, atau organisasi.

Hal ini termasuk tuduhan palsu, memata-matai, membuat ancaman, pencurian

Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer independen atau divais.Contoh kejahatan yang target utamanya adalah jaringan komputer atau divais yaitu: *Malware (malicious software / code), Denial-of-service (DOS) attacks, Computer viruses.*

Penipuan dan pencurian identitas Pencurian identitas adalah menggunakan identitas orang lain seperti KTP, SIM, atau paspor untuk kepentingan pribadinya, dan biasanya digunakan untuk tujuan penipuan. Umumnya penipuan ini berhubungan dengan Internet, namun sering huga terjadi di kehidupan sehari-hari. Misalnya penggunaan data yang ada dalam kartu identitas orang lain untuk melakukan suatu kejahatan. Pencuri identitas dapat menggunakan identitas orang lain untuk suatu transaksi atau kegiatan, sehingga pemilik identitas yang aslilah yang kemudian dianggap melakukan kegiatan atau transaksi tersebut.

Phishing scam, *phising* (Indonesia: pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah *phishing* dalam bahasa Inggris berasal dari kata fishing (memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.

Perang informasi (*Information warfare*) Perang Informasi adalah penggunaan dan pengelolaan informasi dalam mengejar keunggulan kompetitif atas lawan.perang Informasi dapat melibatkan pengumpulan informasi taktis, jaminan bahwa informasi sendiri adalah sah, penyebaran propaganda atau disinformasi untuk menurunkan moral musuh dan masyarakat, merusak kualitas yang menentang kekuatan informasi dan penolakan peluang pengumpulan-informasi untuk menentang kekuatan. Informasi perang berhubungan erat dengan perang psikologis. Contohnya ketika seseorang mencuri informasi dari situs, atau menyebabkan kerusakan computer atau jaringan komputer. Semua tindakan ini adalah virtual (tidak nyata) terhadap informasi tersebut hanya ada dalam dunia digital, dan kerusakannya dalam kenyataan, tidak ada kerusakan fisik nyata kecuali hanya fungsi mesin yang bermasalah.Komputer dapat dijadikan sumber bukti. Bahkan ketika komputer tidak secara langsung digunakan untuk kegiatan kriminal, komputer merupakan alat yang sempurna untuk menjaga record atau catatan, khususnya ketika diberikan tenaga untuk mengenkripsi data. Jika bukti ini bisa diambil dan didekripsi, ini bisa menjadi nilai bagi para *investigator criminal*.

Tindak Pidana Pemerasan Dalam KUHP

Tindak pidana pemerasan merupakan salah satu perbuatan pidana yang diatur dalam Kitab Undang-undang Hukum Pidana (KUHP), Seperti yang kita ketahui bersama bahwa dasar hukum yang berlaku di Indonesia dan paling banyak digunakan untuk memutus suatu perkara pidana adalah Kitab Undang-Undang Hukum Pidana. Dalam sebagian besar kasus yang tejadi dalam ruang lingkup hukum pidana, hakim mengadili terdakwanya menggunakan Pasal yang terdapat

dalam KUHP (Sari, Gita & Lumbanraja, 2019).

Peraturan hukum positif utama yang berlaku di Indonesia adalah KUHP, dimana KUHP sendiri merupakan kodifikasi dari hukum pidana dan berlaku untuk semua golongan penduduk, yaitu golongan timur asing, bumiputera, dan Eropa. Dengan demikian dapat dikatakan ada suatu bentuk kesamaan atau keseragaman dalam peraturan hukum pidana yang berlaku di Indonesia KUHP mempunyai aturan yang digunakan dalam tindak pidana Pemerasan, baik yang dilakukan secara sendiri maupun yang dilakukan secara bersama-sama, dimana yang disoroti oleh hukum pidana tidak hanya mengenai tindak pidana pemerasannya saja, melainkan juga mengenai kebersamaan beberapa orang untuk melakukan tindak pidana tersebut. Terdapat 2 pasal yang bisa dikenakan dalm kasus tersebut, yaitu Pasal 368 ayat (1) KUHP dan Pasal 55 ayat (1) KUHP.

Berikut akan penulis sebutkan bunyi redaksional dari Pasal 368 ayat (1) KUHP "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan, untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya memberi hutang maupun menghapuskan piutang diancam, karena pemerasan dengan pidana penjara paling lama sembilan tahun".

Pasal 55 ayat (1) KUHP " dipidana sebagai pembuat (dader) sesuatu perbuatan pidana:

Ke-1. Mereka yang melakukan, yang menyuruh lakukan dan yang turut serta melakukan perbuatan. Ke-2. Mereka yang dengan memberi atau menjanjikan sesuatu, dengan menyalah gunakan kekuasaan atau martabat, dengan kekerasan, ancaman, atau penyesatan, atau dengan memberi kesempatan, sarana atau keterangan, sengaja menganjurkan orang lain supaya melakukan perbuatan"

Pasal 368 ayat 1 : Barang siapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hukum memaksa orang lain dengan kekerasan maupun ancaman kekerasan, supaya orang itu memberikan barang yang sama sekali atau sebagiannya termasuk kepunyaan orang itu sendiri, kepunyaan orang lain, atau supaya orang itu membuat hutang atau menghapus piutang dihukum penjara paling lama sembilan tahun.

Kejadian ini disebut sebagai *afpersing* atau pemerasan dengan kekerasan. Dimana hal yang dilakukan oleh orang yang dikatakan sebagai pemeras adalah:

1). Memaksa orang lain, Yaitu melakukan tekanan kepada orang lain, sehingga orang itu melakukan sesuatu yang berlawanan dengan kehendaknya sendiri.
2) Memberikan barang yang sama sekali atau sebagiannya termasuk kepunyaan orang itu sendiri, kepunyaan orang lain, atau supaya orang itu membuat hutang atau menghapus piutang. Disini yang disebut sebagai barang adalah segala sesuatau yang berwujud dan tidak selalu mempunyai nilai ekonomis. Hewan juga merupakan hal yang dapat disebut sebagai barang dalam pengertian ini, karena hewan dapat digunakan sebagai objek perbuatan pidana pemerasan oleh seseorang kepada orang lain. Sedangkan pengertian miliknya sendiri atau sebagian milik orang lain dapat diartikan sebagai barang yang mempunyai dua pemilik, dan kemudian salah seorang pemiliknya memaksa

pemilik yang satunya untuk meyerahkan barang itu sepenuhnya kepadanya, sehingga kepemilikkan barang itu mutlak miliknya dan tidak perlu ia bagi dengan orang lain.

3) Memaksa orang lain dengan.
   Memaksakan kehendak kepada orang lain untuk melakukan apa yang diperintahkannya, hal ini dapat dikatakan sebagai melawan hak dari orang yang dipaksanya. Melawan hak sendiri merupakan suatu perbuatan yang melawan hukum, karena seseorang tidak dapat begitu saja memaksakan suatu hal kepada orang alian, karena hal ini melanggar hak asasi dari korbannya tersebut.
4) Menggunakan kekerasan atau ancaman kekerasan.
   Melakukan kekerasan artinya mempergunakan tenaga atau kekuatan jasmani yang tidak kecil secara tidak sah, misalnya dengan memukul tangan, menyepak, menendang dan berbagai perbuatan fisik yang lain baik secara tangan kosong atau dengan segala macam senjata. Kekerasan dapat pula dipersamakan dengan membuat orang lain dalam keadaan tidak berdaya, yang artinya tidak mempunyai kekuatan atau tenaga sama sekali, sehingga tidak dapat mengadakan perlawanan sedikitpun. Misalnya dengan mengikat tangan dan kaki menggunakan tali atau dengan mengurung korbannya di kamar, atau dengan memberikan suntikan yang dapat melumpuhkan orang tersebut. Orang yang tidak berdaya itu masih dapat mengetahui apa yang terjadi atas dirinya.

Tindak Pidana Pemerasan Dalam UU ITE

Seiring dengan perkembangan zaman, dan dalam mengatur *cyber space* dan *cyber crime* telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam Undang- Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disingkat UU ITE). UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi. Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di cyber space.

Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan " Setiap orang berhak untuk mencari, memperoleh, memiliki, meyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia". Tindakan-tindakan cyber crime yang dimuat dalam Undang- undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu, sebagai berikut : 1)Tindakan yang melanggar kesusilaan Dalam Pasal 27 ayat (1) UU Nomor 11 Tahun 2008 disebutkan "Setiap orang dengan sengaja dan tanpa hak mendistribusikan danatau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik

yang memiliki muatan yang melanggar kesusilaan", tetapi dalam pasal tersebut tidak dijelaskan mengenai perbuatan yang memiliki muatan yang melanggar kesusilaan.

Sementara dalam konteks perbuatan yang melanggar kesusilaan melalui media elektronik, terdapat beberapa tindakan yang tergolong dalam Pasal 27 ayat (1) UU ITE salah satunya yaitu *cyber* pornografi dan prostitusi online. Tindak pidana ini akan semakin berat hukumannya apabila dilakukan terhadap anak di bawah umur. Salah satu permasalahan yang ditimbulkan dari kemajuan teknologi informasi melalui jaringan internet adalah beragamnya situs yang menampilkan adegan pornografi. Seolah-oleh sekarang ini, sulit sekali memproteksi jaringan internet dari serbuan pebisnis hiburan yang menjual pornografi (Putra, 2015).

Selain *cyber* pornografi, melakukan pengancaman dan pemerasan melalui dunia digital juga merupakan perbuatan tindak pidana yang diatur dalam UU ITE pada Pasal 27 ayat (4) yang menybutkan bahwa "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" (Ersya, 2017).

Kejahatan pemerasan dan pengancaman melalui dunia digital merupakan perbuatan melawan hukum, banyak aturan yang mengatur mengenai kejahatan pemerasan dan pengancaman melalui dunia digital sehingga hal tersebutlah terkadang menjadi faktor ketidaktahuan masyarakat dikarenakan kurangnya minat baca masyarakat, sehingga pemerintah maupun aparat penegak hukum perlu mengadakan sosialisasi agar masyarakat mengetahui bahwa adanya peraturan yang mengatur mengenai dampak jika melakukan kejahatan pemerasan dan pengancaman melalui media elektronik yang terdapat di Undang-Undang (Dermawan & Akmal, 2020).

Faktor sarana dan fasilitas yang ada sangat berpengaruh dalam menunjang perbuatan jahat tersebut. Di zaman globalisasi seperti sekarang ini kemajuan teknologi memang sangat berpengaruh di kehidupan manusia, hampir semua orang mengetahui apa media internet tersebut. Media internet sebagai media komunikasi dijadikan alat untuk mempermudah pelaku melakukan pengancaman dan pemerasan, karena menggunakan media elektronik ini dapat mengefektifkan dan mengefisiensikan waktu sehingga seseorang dapat melakukan dengan siapapun dan kapanpun (Sa'idah, Santi & Suryanto, 2021).

Faktor kurangnya kontrol sosial dari keluarga, masyarakat, dan pemerintah. Kontrol dari pihak keluarga dan masyarakat menjadi suatu komponen yang harusnya berjalan dengan baik. Kontrol yang dilakukan oleh keluarga dan masyarakat tersebut seharusnya menjadi faktor utama dalam melakukan upaya penanggulangan yang bersifat preventif. Faktor keluarga yang di dalamnya tidak memiliki suasana keharmonisan merupakan pendorong seseorang untuk tidak peduli terhadap keluarganya. Sehingga tidak ada perhatian khusus terhadap masalah apa yang sedang dialami keluarganya dan lebih mementingkan kepentingan dirinya sendiri.

Faktor lain yang memicu kejahatan pemerasan dan pengancaman melalui media sosial adalah karena ketidak tauannya pelaku terhadap hukuman yang akan

didapatkan setelah melakukan tindak pidana tersebut. Kejahatan pemerasan dan pengancaman melalui media elektronik bertentangan atau tidak sesuai dengan dengan Pasal 45 ayat (4) UU ITE, setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Berdasarkan ketentuan tersebut bahwa ancaman pidana penjara selama enam tahun ternyata tidak juga dapat menyurutkan perbuatan daripada pelaku kejahatan tersebut.

Menurut penulis ketentuan mengenai pemerasan yang diatur dalam peraturan perundang-undangan dapat dilaksanakan berdasarkan KUHP dan juga UU ITE, dalam KUHP Pasal 368 menyebutkan bahwa "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan, untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya memberi hutang maupun menghapuskan piutang, diancam, karena pemerasan dengan pidana penjara paling lama sembilan tahun", sedangkan dalam UU ITE Pasal 27 ayat (4) menyebutkan bahwa " 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" dan aturan mengenai hukumannya diatur dalam Pasal 45 ayat 4 yaitu dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Berdasarkan ke-dua Pasal tersebut mengatur terkait tindak pidana pemerasan, akan tetapi dalam KUHP hanya mengatur tindak pidana pemerasan secara umum (*lex generali)* sedangkan dalam UU ITE mengatur secara explisit tindak pidana pemerasan secara khusus (*lex specialis)*. Apabila merujuk Pasal 63 ayat 2 KUHP yang menyebutkan bahwa "Jika suatu perbuatan masuk dalam suatu aturan pidana yang umum, diatur pula dalam aturan pidana khusus, maka yang khusus itulah yang diterapkan. Secara aturan berdasarkan pada Pasal 63 ayat 2 KUHP, tindak pidana pemerasan dalam dunia digital (elektronik) maka aturan yang dapat dilaksanakan yaitu dalam Pasal 27 ayat (4) dan Pasal 45 ayat (4) UU ITE. Maka dalam upaya mengimplementasikan UU ITE sebagai bentuk pemberantasan tindak pidana pemerasan dalam dunia digital diperlukan kerja sama dan *supporting* dengan berbagai pihak, baik dari aparat penegak hukum dan juga dari kalangan masyarakat hukum. Dan untuk mengimplementasikan pemberantasan tindak pidana pemerasan dalam dunia digital maupun media elektronik dan media sosial maka dibutuhkan upaya represif dan upaya preventif.

Upaya repsresif dapat dilakukan melalui upaya dalam penanggulangan kejahatan yang lebih menitikberatkan pada sifat pemberantasan sesudah kejahatan itu terjadi, upaya represif dapat dilakukan dengan penyelidikan oleh pihak kepolisian, melakukan penindakan terhadap pelaku kejahatan, melakukan penyidikan terhadap pelaku.

Tahap penyelidikan merupakan tahap pertama yang dilakukan penyelidik dalam

melakukan penyelidikan tindak pidana serta tahap tersulit dalam proses penyidikan, hal ini disebabkan dalam tahap ini penyelidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebabsebab dari tindak pidana tersebut dalam upaya penanggulangan. Dalam penyelidikan kasus pemerasan dan pengancaman melalui media sosial, pihak kepolisian banyak mengalami kendala dan kesulitan, karena kasus yang berhubungan dengan kejahatan dunia maya penanganannya berbeda dengan kasus tindak pidana biasa atau konvensional. Apalagi pelaku kejahatan tersebut bisa melakukan aksinya kapan saja tanpa sepengetahuan orang lain dan menggunakan akun palsu, Langkah-langkah yang dilakukan pihak kepolisian adalah melakukan pemeriksaan misalnya di warnet yang biasanya digunakan oleh pelaku kejahatan, sekaligus mengumpulkan bukti, melacak, dan melakukan penyitaan terhadap bukti elektronik seperti hard disk, melakukan pengungkapan atau penahanan berdasarkan bukti permulaan atau alat bukti yang cukup.

Upaya penindakan yang dilakukan pihak kepolisian dalam penanggulangan tindak pidana pemerasan dan pengancaman melalui dunia digital sangat penting. Upaya pemberantasannya tidak hanya dengan penindakan saja memang sedikit mengalami kesulitan karena pelaku kejahatan dunia maya dapat melakukan aksinya dimana saja, tanpa sepengetahuan orang lain maka perlu adanya kerjasama yang baik antara kepolisian dengan masyarakat.

Penyidikan yang dilakukan oleh pihak kepolisian tidak mengenal batas wilayah. Oleh karena itu perlu kerjasama dengan aparat penegak hukum yang lain. Karena hal tersebut sangat penting dilakukan dalam mengumpulkan barang bukti, penyitaan terhadap bukti elektronik pelaku kejahatan cyber crime. Hal ini membuktikan bahwa peraturan perundang- undangan yang sudah ada sudah cukup baik pada kenyataannya, namun terkadang kurang maksimal dalam melakukan penanganan yang ketat, sehingga masih saja terjadi adanya tindak pidana pemerasan dan pengancaman melalui media elektronik.

Upaya preventif dilalukan dengan cara tindakan pencegahan dalam menangani pelanggaran norma-norma yang berlaku yakni dengan mengusahakan agar faktor niat dan kesempatan tidak bertemu sehingga situasi keamanan dan ketertiban masyarakat tetap terpelihara aman dan terkendali. Upaya preventif yang dilakukan oleh aparat kepolisian yaitu memberikan himbauan kepada masyarakat dengan melakukan sosialisasi kepada masyarakat tentang tindak pidana pemerasan dan pengancaman melalui media sosial agar dapat menanggulangi tindak pidana pemerasan dan pengancaman melalui media digital, media elektronik dan media sosial.

Selain upaya represif dan upaya preventif yang dapat dilakukan, implementasi UU ITE untuk pemberantasan tindak pidana pemerasan juga dibutuhkan peningkatan sarana dan fasilitas penegak hukum yang memadai, Penegakan hukum terhadap *cyber crime* mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud. Penentuan waktu dan tempat terjadinya *cyber crime* ditentukan saat kapan alat itu bekerja efektif, oleh sebab itu analisis telematika sangat diperlukan dalam mengungkap kejahatan ini. Untuk menelusursi, mendeteksi dan menanggulangi kejahatan ini caranya sangat tergantung aplikasi dan topologi jaringan yang

dipakai. Sebagian aplikasinya ada di *gnacktrack* dan *backtrack*. Hal ini menggambarkan bahwa sarana dan fasilitas yang memadai menjadi hal yang penting dalam proses penegakan hukum. Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau halhal itu tidak terpenuhi maka mustahil penegakan hukum akan mencapai tujuannya.

B. Kebijakan Penegakan Hukum Terkait UU ITE Dalam Rangka Pemberantasan Tindak Pidana Pemerasan Dalam Dunia Digital

Hukum pidana secara umum mengandung setidaknya dua jenis norma, yakni norma yang harus selalu dipenuhi agar suatu tindakan dapat disebut sebagai tindak pidana, dan norma yang berkenaan dengan ancaman pidana yang harus dikenakan bagi pelaku dari suatu tindak pidana. Secara terinci undang-undang hukum pidana telah mengatur tentang:

1) bilamana suatu pidana dapat dijatuhkan bagi seorang pelaku,
2) Jenis pidana yang bagaimanakah yang dapat dijatuhkan bagi pelaku tersebut,
3) Untuk berapa lama pidana dapat dijatuhkan atau berapa besarnya pidana denda yang dapat dijatuhkan, dan
4) Dengan cara bagaimanakah pidana harus dilaksanakan.

Sudah umum diketahui bahwa tindak pidana merupakan pelanggaran atas kepentingan negara sebagai representasi kepentingan publik. Hal ini kemudian menjadi dasar kewenangan bagi negara untuk menentukan, membuat peraturan, menuntut, dan menghukum seseorang yang melanggar peraturan/hukum pidana. Hal ini diperkuat oleh pengklasifikasian ilmu hukum di mana hukum pidana adalah bagian dari hukum publik yang tidak membolehkan campur tangan individu.

Di sinilah letak pentingnya kebijakan negara dalam kaitannya dengan penetapan aturan perundang-undangan hukum pidana. Dalam menentukan suatu tindak pidana digunakan kebijakan hukum pidana. Penegakan hukum pidana merupakan salah satu bentuk dari upaya penanggulangan kejahatan. Penggunaan hukum pidana sebagai alat untuk penanggulangan kejahatan merupakan bagian dari kebijakan kriminal. Upaya penanggulangan kejahatan dengan hukum pidana tersebut dilakukan dalam rangka untuk mencapai tujuan akhir dari kebijakan kriminal itu sendiri, yaitu memberikan perlindungan masyarakat agar tercipta ketertiban dan kesejahteraan. Upaya untuk mencegah dan menanggulangi kejahatan dengan menggunakan sarana hukum pidana disebut juga dengan istilah penal *policy* atau kebijakan penal. Kebijakan hukum pidana tidak hanya sebatas membuat suatu peraturan perundang-undangan yang mengatur hal-hal tertentu. Tetapi lebih dari itu, kebijakan hukum pidana memerlukan pendekatan yang menyeluruh yang melibatkan berbagai disiplin ilmu hukum selain ilmu hukum pidana serta kenyataan di dalam masyarakat sehingga kebijakan hukum pidana yang digunakan tidak keluar dari konsep yang lebih luas yaitu kebijakan sosial dan rencana pembangunan nasional dalam rangka mewujudkan kesejahteraan masyarakat.

Sudarto menjelaskan, sebagaimana dikutip Barda NawawiArief, bahwa kebijakan penal mempunya dua arti, yaitu arti sempit yang memiliki cakupan keseluruhan asas dan metode yang menjadi dasar dari reaksi terhadap pelanggaran hukum yang berupa pidana; dan arti luas yang mencakup keseluruhan fungsi dari aparatur penegak hukum termasuk di dalamnya cara kerja dari pengadilan dan polisi.

Masalah kebijakan hukum pidana bukanlah semata-mata pekerjaan pembuatan perundang-undangan semata. Dalam hal pembuatan perundang-undangan pidana, hal ini selain dapat dilakukan secara yuridis normatif dan sistematik-dogmatik, juga memerlukan pendekatan yuridis faktual yang dapat berupa pendekatan sosiologis, historis dan komparatif, bahkan memerlukan pula pendekatan komprehensif dari berbagai disiplin sosial lainnya dan pendekatan integral dengan pidana".

Kebijakan dalam upaya penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana). Penegakan hukum pidana tidak bisa dilepaskan dari kebijakan yang dibuat oleh negara dalam rangka menegakkan aturan demi terwujudnya kemaslahatan bersama, sehingga dengan demikian, kebijakan hukum pidana sering juga dikatakan sebagai bagian dari kebijakan penegakan hukum (law enfocement policy).

Di samping itu, usaha penanggulangan kejahatan melalui pembuatan undang-undang (hukum) pidana pada hakikatnya juga merupakan bagian integral dari usaha perlindungan masyarakat (*social defence*), dan usaha mencapai kesejahteraan masyarakat (*social welfare*), sehingga wajar pulalah apabila kebijakan hukum pidana juga merupakan bagian integral dari kebijakan sosial (*social policy*). Kebijakan sosial (*social policy*) itu sendiri dapat diartikan sebagai segala usaha yang rasional untuk mencapai kesejahteraan masyarakat dan sekaligus mencakup perlindungan masyarakat. Jadi, di dalam pengertian *social policy* sekaligus tercakup di dalamnya *social welfare policy* dan *social defence policy*.

Banyak kalangan menilai bahwa masyarakat Indonesia pada umumnya tidak merasa keberatan dan tidak merasa terbebani dengan adanya kebijakan penanggulangan kejahatan melalui sarana hukum pidana, meskipun sifat dari hukum pidana lebih menekankan aspek represif dari pada preventif. Sikap bangsa Indonesia dalam menerima kebijakan ini terlihat daripraktik perumusan dan penetapan perundang-undangan oleh wakil-wakil rakyat selama ini yang menunjukkan bahwa penggunaan hukum pidana merupakan bagian dari kebijakan atau politik hukum yang dianut di Indonesia. Penggunaan hukum pidana dianggap sebagai hal yang wajar dan normal, seolah-olah eksistensinya tidak lagi dipersoalkan. Namun demikian, yang menjadi masalah adalah garis-garis kebijakan atau pendekatan bagaimanakah yang sebaiknya ditempuh dalam menggunakan hukum pidana itu.

Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara (*borderless*). Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang dalam pengembangannya akan merasakan

kecenderungan timbulnya neokolonialisme. Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara. Jaringan informasi melalui komputer (*interconnected computer networks*) dapat digolongkan dalam tiga istilah yaitu ekstranet, intranet dan internet. Intranet adalah "*a private network belonging to an organization, usually a corporation, accessible only by the organization's members, employes, or others with authorization* dan ekstranet adalah "*a fancy way of saying that a corporation has opened up portions of its intranet to authorized users outside the corporation*.

Saat ini Indonesia telah memiliki cyber law untuk mengatur dunia maya berikut sanksi bila terkaji *cybercrime* baik di wilayah Indonesia maupun di luar wilayah hukum Indonesia yang akibatnya dirasakan di Indonesia. *Cybercrime* terus berkembang seiring dengan revolusi teknologi informasi yang membalikkan paradigma lama terhadap kejahatan konvensional ke arah kejahatan virtual dengan memanfaatkan instrumen elektronik tetapi akibatnya dapat dirasakan secara nyata. Penanggulangan *cybercrime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundangundangan.Terdapat beberapa perundangundangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan Internet sebelum disahkannya UU ITE.

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), di samping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi "gaptek" hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan Internet. Berdasarkan data Polri, kasus kejahatan dunia maya yang terjadi selama kurun waktu 4 (empat) tahun dari tahun 2019 sampai dengan tahun 2023, terdapat 48 (empat puluh delapan) kasus. Dari 48 (empat puluh delapan) kasus yang dilaporkan tersebut, 25 (dua puluh lima) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum.

Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organism' yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapai tujuannya. Dalam konsep keamanan masyarakat modern, sistem keamanan bukan lagi tanggung jawab penegak hukum semata, namun menjadi tanggung jawab bersama seluruh elemen masyarakat. Dalam pandangan konsep in masyarakat di samping sebagai objek juga sebagai subjek. Sebagai subjek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa kegiatan internet dan media lainnya. Sebagai objek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi Internet.

UU ITE dalam Regulasi mengenai pemakaian Teknologi Informasi dan Komunikasi (TIK) sudah ditetapkan secara jelas setelah diberlakukannya UU ITE, Namun, dengan meningkatnya penggunaan internet di masyarakat, terutama dalam penggunaan media sosial, kasus- kasus terkait informasi serta transaksi elektronik juga semakin banyak terjadi. Kondisi ini menjelaskan bahwa berbagai kasus ITE

yang tinggi umumnya melibatkan berbagai pasal yang banyak digunakan, contohnya pencemaran nama baik dan penyebaran berita palsu (*hoax*). Namun penting dicatat bahwa kasus-kasus terkait ITE juga bervariasi, tidak hanya terbatas pada pencemaran nama baik atau penyebaran berita palsu. Tindakan yang tak diperbolehkan menurut Undang-Undang ITE didasari Pasal 27 hingga Pasal 37. Namun, secara lebih terinci, larangan konkret diatur hanya dari Pasal 27 hingga Pasal 35 dalam Undang-Undang ITE. Salah satu tujuan dari pembentukan UU ITE adalah untuk menyokong perkembangan teknologi informasi dengan menyusun kerangka hukum yang tepat, yang mengatur penggunaannya untuk memastikan keamanan dan mencegah penyalahgunaan, sambil tetap mempertimbangkan berbagai nilai agama serta budaya sosial masyarakat Indonesia. Secara keseluruhan, keberadaan UU ITE memiliki beberapa manfaat potensial jika diterapkan dengan tepat. Terdapat manfaat UU ITE, seperti:[120]

1) Kejelasan hukum dalam transaksi elektronik
2) Mendorong pertumbuhan ekonomi di Indonesia.
3) Kontribusi dalam pencegahan kejahatan internet
4) Perlindungan masyarakat.

Pemerintah membuat SKB (Surat Keputusan Bersama) UU ITE untuk membantu penegak hukum menjalankan pekerjaan mereka. Namun, ada beberapa kategori dan kondisi yang memungkinkan pemerintah tak memperhatikan SKB tersebut. Pemerintah harus menyiapkan perubahan pada Undang-undang Informasi Teknologi Elektonik menggunakan pertimbangan semua pendapat masyarakat serta stakeholderdengan efektif. Ini juga harus mempertahankan aspirasi Pasal 28 D ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945, yang menjelaskan apabila tiap manusia memiliki hak atas pengakuan, jaminan, perlindungan, hingga kepastian juga perlakuan hukum yang adil di hadapan hukum.

Materi UU ITE terbagi dua, yaitu: pengaturan transaksi elektronik dan informasi elektronik, serta pengaturan pelanggaran yang tak diperbolehkan dan diancam hukuman pidana (*cybercrime*). Selain itu, UU ITE adalah pengaturan tindak pidana siber pada Undang-Undang pertama di Indonesia. Pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia. perlu diperhatikan sisi perlindungan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata- mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada menigikan

kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Perluasan pengaturan yurisdiksi ekstrateritorial dalam tindak pidana teknologi informasi dimaksudkan untuk melindungi jaringan komunikasi/informasi yang saat ini telah menjadi kepentingan intemasional/global. Pengaturan yurisdiksi ekstrateritorial sama dengan prinsip atau azas ubikuitas, alasannya saat ini semakin marak terjadi cybercrime seiring dengan pertumbuhan penggunaan internet. Yang dimaksud dengan prinsip atau azas ubikuitas adalah prinsip yang mengatakan bahwa delik-delik yang dilakukan atau terjadi di sebagian wilayah teritorial negara sebagian di luar wilayah teritorial suatu negara (ekstrateritorial) harus dapat dibawa ke dalam yurisdikgi setiap negara yang terkait.

Berdasarkan Pasal 2 dan penjelasan UUITE pada dasarnya tetap didasarkan pada asas teritorial (pasal 2-5 KUHP), asas personal/nasional aktif (pasal 7 KUHP), dan asas universal (pasal 8 KUHP), hanya ada perubahan dan perkembangan formulasinya yaitu:

1) Memuat ketentuan tentang lingkup yurisdiksi yang bersifat transnasional dan internasional serta memuat ketentuan khusus terhadap tindak pidana teknologi informasi.
2) Subjek hukum tidak hanya terhadap perorangan baik warga negara Indonesia ataupun warga negara asing tetapi juga 'terhadap badan hukum asing (koorporasi).

Pelaku yang melanggar UU ITE dapat dijerat pidana meskipun berada di luar negeri, karena sifat UU ITE yang *borderless*. Kebijakan penegak hukum untuk pemerasan yang melanggar UU ITE adalah dengan menjerat pelaku dengan Pasal 27 ayat (4). Dan ancaman pidana pelaku yang terbukti melanggar pasal ini yaitu pada Pasal 45 ayat (4) dapat dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar. UU ITE merupakan salah satu upaya untuk menanggulangi tindak pidana yang berkaitan dengan teknologi. Tindak pidana konvensional yang diatur dalam KUHP dirumuskan ulang dalam UU ITE dengan menambahkan unsur ruang lingkup dan perbuatan di ranah teknologi.

KESIMPULAN

1. Implementasi UU ITE dalam rangka pemberantasan tindak pidana pemerasan dalam dunia digital di perlukan upaya responsif dari para penegak hukum, upaya yang dapat dilakukan yaitu Upaya Represif dan Upaya Preventif. Upaya repsresif dapat dilakukan melalui upaya dalam penanggulangan kejahatan yang lebih menitikberatkan pada sifat pemberantasan sesudah kejahatan itu terjadi, upaya represif dapat dilakukan dengan penyelidikan oleh pihak kepolisian, melakukan penindakan terhadap pelaku kejahatan, melakukan penyidikan terhadap pelaku. Upaya preventif dilalukan dengan cara tindakan pencegahan dalam menangani pelanggaran norma-norma yang berlaku yakni dengan mengusahakan agar faktor niat dan kesempatan tidak bertemu sehingga situasi keamanan dan ketertiban masyarakat tetap terpelihara aman dan terkendali. Upaya preventif yang dilakukan oleh aparat kepolisian yaitu memberikan himbauan kepada masyarakat dengan melakukan sosialisasi kepada masyarakat

tentang tindak pidana pemerasan dan pengancaman melalui media sosial agar dapat menanggulangi tindak pidana pemerasan dan pengancaman melalui media digital, media elektronik dan media sosial. Selain upaya represif dan upaya preventif yang dapat dilakukan, implementasi UU ITE untuk pemberantasan tindak pidana pemerasan juga dibutuhkan peningkatan sarana dan fasilitas penegak hukum yang memadai, Penegakan hukum terhadap *cyber crime* mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud..

2. Kebijakan penegak hukum untuk pemerasan yang melanggar UU ITE adalah dengan menjerat pelaku dengan Pasal 27 ayat (4). Dan ancaman pidana pelaku yang terbukti melanggar pasal ini yaitu pada Pasal 45 ayat (4) dapat dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar. UU ITE merupakan salah satu upaya untuk menanggulangi tindak pidana yang berkaitan dengan teknologi. Tindak pidana konvensional yang diatur dalam KUHP dirumuskan ulang dalam UU ITE dengan menambahkan unsur ruang lingkup dan perbuatan di ranah teknologi.

SARAN

1. Agar masyarakat sadar akan hukum juga merupakan salah satu aspek penting untuk melaraskan tujuan agar tercapainya pemberantasan cyber crime yang marak terjadi.
2. Aparat penegak hukum hendaknya meningkatkan sarana dan fasilitas yang lebih baik lagi dalam hal mencari pembuktian guna peningkatan kemampuan dibidang teknologi informasi dan komunikasi sebagai penunjang efektivitas penanganan terhadap pelaku pemerasan melalui media elektronik. Serta memberikan sanksi hukum dengan sebaik dan seoptimal mungkin dimana tidak hanya sesuai dengan KUHP tetapi lebih mengutamakan UU ITE.

DAFTAR PUSTAKA

Ashady, S. J. (2024). Cybercrime sebagai Kejahatan Dunia Maya dalam Perspektif Hukum dan Masyarakat. *Juridische: Jurnal Penelitian Hukum*, *1*(2), 34-46.

Cholik, C. A. (2021). Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang. *Jurnal Fakultas Teknik UNISA Kuningan*, *2*(2), 39-46.

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.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50-62.

Gumbira, S. W. (2020). Problematika Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Dalam Menanggulangi Cyberbullying Di Sosial Media Pasca Judicial Review Mahkamah Konstitusi RI. *Jurnal Pro Justice: Kajian Hukum dan Sosial*, *1*(1), 50-71.

Haqqi, H., & Wijayati, H. (2019). *Revolusi industri 4.0 di tengah society 5.0: sebuah integrasi ruang, terobosan teknologi, dan transformasi kehidupan di era disruptif*. Anak Hebat Indonesia.

Hidayat, S., Haris, O. K., Safiuddin, S., & Gaisar, M. A. B. (2023). Kebijakan Formulasi Kejahatan Sekstorsi dalam Sistem Pidana Indonesia. *Halu Oleo Legal Research*, *5*(2), 662-674.

Muqsit, I. M., Wijaya, A. U., & Widianto, R. M. (2023). Perlindungan Hukum Terhadap Pelaku Pornografi. *Jurnal Ilmu Hukum Wijaya Putra*, *1*(1), 25-34.

Putra, E. N. (2015). Kejahatan Tanpa Korban Dalam Kejahatan Cyberporn. *Jurnal Cakrawala Hukum*, *6*(1), 1-12.

Ridwan, H., Masrul, M., & Juhaepa, J. (2018). Komunikasi Digital Pada Perubahan Budaya Masyarakat E-Commerce Dalam Pendekatan Jean Baudrillard. *Jurnal Riset Komunikasi*, *1*(1), 99-108.

Sa'idah, F. L., Santi, D. E., & Suryanto, S. (2021). Faktor produksi ujaran kebencian melalui media sosial. *Jurnal Psikologi Perseptual*, *6*(1), 1-15.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58-77.

Sari, I. D. M., Gita, H., & Lumbanraja, A. D. (2019). Analisis Kebijakan Hukum Pidana Terhadap Delik Perbuatan Tidak Menyenangkan. *Jurnal Pembangunan Hukum Indonesia*, *1*(2), 171-181.

Sumadi, H. (2015). Kendala dalam menanggulangi tindak pidana penipuan transaksi elektronik di Indonesia. *Jurnal Wawasan Yuridika*, *33*(2), 175-203.

Tarigan, A. J., Akhyar, A., & Mustamam, M. (2023). Perlindungan Hukum Terhadap Korban Pornografi Dalam Media Sosial Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Ilmiah METADATA*, *5*(1), 196-210.

.