# EFEKTIVITAS UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DALAM MENANGGULANGI KEJAHATAN SIBER DI INDONESIA

**DANEL ADITIA SITUNGKIR**
Fakultas Hukum Universitas Sumatera Barat

***Abstract****: The Electronic Information and Transactions Law (UU ITE) is indeed an essential legal instrument needed to address cybercrime. However, to maximize its effectiveness, corrective measures are required, including legal revisions, strengthening of human resources, updating legal infrastructure, and long-term educational strategies involving all elements of society. In the future, the UU ITE is expected to function not merely as a punitive tool, but also as a catalyst for realizing a democratic, just, and human rights-respecting digital governance system. The ideal model of UU ITE effectiveness in combating cybercrime is not solely about legal enforcement, but more profoundly about balancing legal certainty, justice, human rights protection, and technological advancement. The state must be present not to intimidate digital citizens, but to protect them from real threats in cyberspace. Within the broader framework of national development, the existence of an ideal cyber legal model becomes a crucial foundation for achieving a sovereign, fair, and humane digital Indonesia.*
***Keywords****: UU ITE, Cybercrime, Indonesia.*

**Abstrak:** UU ITE sejatinya merupakan perangkat hukum yang penting dan dibutuhkan dalam menghadapi kejahatan siber. Namun agar efektivitasnya semakin maksimal, diperlukan langkah-langkah korektif berupa revisi, penguatan sumber daya, pembaruan infrastruktur hukum, serta strategi edukatif jangka panjang yang melibatkan seluruh elemen bangsa. Ke depan, UU ITE diharapkan tidak hanya menjadi instrumen pemidanaan, tetapi juga menjadi katalisator dalam mewujudkan tata kelola dunia digital yang demokratis, berkeadilan, dan menjunjung tinggi hak asasi manusia. Model ideal efektivitas UU ITE dalam menanggulangi kejahatan siber bukan hanya berbicara soal ketegasan hukum, tetapi lebih jauh tentang keseimbangan antara kepastian hukum, keadilan, perlindungan hak asasi manusia, dan kemajuan teknologi. Negara harus hadir bukan untuk menakut-nakuti warga digital, melainkan untuk melindungi mereka dari ancaman yang nyata di ruang siber. Dalam kerangka besar pembangunan nasional, keberadaan model hukum siber yang ideal menjadi fondasi penting menuju Indonesia digital yang berdaulat, adil, dan manusiawi.
**Kata Kunci:** UU ITE, Kejahatan Siber, Indonesia.

## A. Pendahuluan

Penanggulangan *cyber crime* di Indonesia bertumpu pada Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Sebagai regulasi utama dalam pengaturan aktivitas di ruang digital, UU ITE telah mencakup sejumlah pasal yang mengatur tindak pidana terkait penyebaran berita bohong, penghinaan, pencemaran nama baik, peretasan, akses ilegal, dan penyebaran konten yang melanggar kesusilaan (Hidayat¸2025). Namun, pada tataran praktik, sering kali terjadi tarik ulur antara perlindungan kebebasan berekspresi dan penegakan hukum. Beberapa ketentuan dianggap multitafsir dan berpotensi digunakan untuk membungkam kritik terhadap pemerintah maupun aktor-aktor berkuasa. Hal ini menjadi salah satu indikator bahwa efektivitas hukum pidana, khususnya dalam konteks kejahatan siber, tidak bisa dilepaskan dari

konteks politik hukum dan budaya penegakan hukum di Indonesia.

Meskipun telah dilakukan beberapa revisi terhadap Undang-Undang Informasi dan Transaksi Elektronik, tantangan dalam penerapan norma hukum di lapangan masih sangat nyata. Salah satu persoalan utama adalah bagaimana substansi hukum yang tertuang dalam UU ITE mampu menjawab realitas kejahatan digital yang berkembang sangat cepat dan dinamis. Fenomena kejahatan siber memiliki karakteristik yang unik, antara lain tidak mengenal batas teritorial, bersifat anonim, dan menggunakan teknologi canggih yang sulit dilacak oleh aparat penegak hukum konvensional. Dalam kondisi ini, efektivitas suatu undang-undang tidak hanya ditentukan oleh eksistensinya secara normatif, melainkan juga oleh sejauh mana perangkat hukum tersebut dapat diimplementasikan secara operasional dan memberi dampak nyata dalam mencegah dan menanggulangi kejahatan siber.

Revisi ini belum sepenuhnya menyelesaikan persoalan. Dalam praktiknya, masih terdapat celah hukum yang memungkinkan pelaku kejahatan siber lolos dari jerat hukum karena terbatasnya alat bukti digital, kurangnya pemahaman aparat penegak hukum terhadap teknologi informasi, serta minimnya kerja sama lintas negara untuk menghadapi kejahatan siber lintas batas. Hal ini menunjukkan bahwa efektivitas UU ITE sangat bergantung pada tiga aspek utama, yaitu substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*). Jika salah satu dari ketiganya lemah, maka implementasi undang-undang tersebut tidak akan mencapai hasil yang optimal.

UU ITE telah cukup komprehensif dalam menjangkau berbagai bentuk pelanggaran yang dilakukan melalui media elektronik. Namun demikian, ketentuan yang bersifat umum sering kali menghadirkan tantangan dalam proses pembuktian hukum, apalagi dalam kasus-kasus yang memerlukan pendekatan forensik digital tingkat lanjut. Sebagai contoh, dalam kasus peretasan situs pemerintah atau penyebaran malware, identifikasi pelaku sering kali sulit dilakukan karena pelaku menggunakan teknik penyamaran (*obfuscation*) atau menyembunyikan identitas melalui jaringan anonim (seperti VPN atau dark web). Untuk itu, penguatan regulasi harus diikuti dengan instrumen turunan yang memberikan pedoman teknis, termasuk tata cara penyitaan barang bukti digital, prosedur pengumpulan log data, hingga mekanisme koordinasi lintas Lembaga (Kang, 2018).

Dari sisi struktur hukum, tantangan terbesar adalah ketidaksiapan aparat penegak hukum menghadapi kompleksitas kejahatan siber. Meskipun beberapa satuan tugas siber telah dibentuk di lingkungan kepolisian dan kejaksaan, jumlah personel yang terlatih dan memiliki latar belakang IT masih sangat terbatas. Ketimpangan ini menyebabkan penanganan perkara sering kali mengalami keterlambatan atau bahkan tidak dapat ditindaklanjuti karena tidak ditemukan cukup bukti elektronik yang sah secara hukum. Di sisi lain, lembaga peradilan juga menghadapi tantangan serupa. Banyak hakim yang belum memiliki pemahaman yang memadai tentang dinamika kejahatan digital, sehingga putusan yang dihasilkan terkadang tidak mencerminkan keadilan substantif.

Budaya hukum masyarakat juga menjadi faktor penentu dalam efektivitas UU ITE. Rendahnya kesadaran masyarakat terhadap bahaya kejahatan siber, serta minimnya literasi digital, menyebabkan sebagian besar pengguna internet di Indonesia mudah menjadi korban atau bahkan pelaku kejahatan digital tanpa disadari. Praktik menyebarkan informasi yang belum terverifikasi, mengakses situs terlarang, atau menggunakan perangkat lunak bajakan merupakan hal yang dianggap biasa dalam kehidupan digital masyarakat Indonesia. Oleh karena itu, selain penegakan hukum yang tegas, dibutuhkan juga pendekatan edukatif dan preventif yang berkesinambungan (Judhariksawan, 2019). Pemerintah harus aktif melibatkan lembaga pendidikan, organisasi masyarakat sipil, serta media massa dalam membangun budaya digital yang sehat dan bertanggung jawab.

Efektivitas UU ITE juga harus dinilai dari keberhasilan negara dalam menjamin keadilan hukum bagi korban kejahatan siber. Dalam beberapa kasus, korban kejahatan digital, seperti korban penipuan daring atau doxing, mengalami kesulitan dalam mengakses keadilan karena proses hukum yang panjang, rumit, dan mahal. Hal ini menunjukkan bahwa sistem hukum masih belum sepenuhnya berpihak kepada masyarakat sebagai pencari keadilan. Oleh karena itu, perlu dilakukan reformasi menyeluruh terhadap mekanisme penegakan hukum, termasuk penyederhanaan prosedur pelaporan, pembentukan unit layanan terpadu untuk korban kejahatan siber, serta penyediaan bantuan hukum bagi masyarakat yang membutuhkan.

Efektivitas UU ITE harus dinilai dalam konteks perkembangan global. Mengingat kejahatan siber bersifat transnasional, maka instrumen hukum nasional perlu diselaraskan dengan hukum internasional dan standar global. Kerja sama antarnegara melalui mekanisme ekstradisi, pertukaran intelijen digital, dan penyelarasan norma pidana menjadi sangat penting. Sayangnya, hingga kini Indonesia belum meratifikasi beberapa konvensi penting seperti *Budapest Convention on Cybercrime*, yang padahal dapat memberikan landasan kuat bagi kerja sama internasional dalam menangani kejahatan digital lintas batas (Maskun¸2013). Oleh karena itu, penguatan posisi Indonesia dalam forum internasional terkait keamanan siber harus menjadi bagian dari strategi nasional dalam mengefektifkan UU ITE.

Efektivitas UU ITE juga sangat dipengaruhi oleh dinamika politik dan sosial. Dalam konteks demokrasi, terdapat kekhawatiran bahwa UU ITE digunakan sebagai alat untuk mengontrol opini publik dan membungkam kritik terhadap pemerintah. Penggunaan pasal-pasal tertentu, seperti pasal penghinaan atau pencemaran nama baik, sering kali menuai kritik karena dianggap membatasi kebebasan berekspresi yang dijamin oleh konstitusi. Oleh karena itu, efektivitas UU ITE tidak boleh hanya diukur dari kuantitas penindakan, tetapi juga dari kualitas perlindungan hak-hak sipil yang dijamin dalam negara hukum. Dalam hal ini, reformulasi pasal-pasal multitafsir dalam UU ITE menjadi sangat urgen agar hukum benar-benar menjadi alat perlindungan dan keadilan bagi semua pihak.

Penting juga untuk menyoroti bagaimana UU ITE diimplementasikan dalam konteks platform digital global. Banyak konten ilegal atau pelanggaran hukum yang terjadi melalui platform media sosial yang berbasis di luar negeri, seperti Facebook, Instagram, X (Twitter), dan TikTok. Penegakan hukum terhadap platform tersebut sering kali terkendala oleh yurisdiksi dan keterbatasan kerja sama hukum internasional. Oleh karena itu, efektivitas UU ITE membutuhkan dukungan dari kerja sama antara pemerintah dan penyedia platform global dalam rangka memperkuat regulasi konten dan mempercepat proses take-down terhadap konten ilegal. Perlu dibangun mekanisme yang jelas dan transparan mengenai tanggung jawab platform digital dalam menjaga ruang siber Indonesia agar tetap aman dan sehat.

Namun demikian, efektivitas UU ITE masih menghadapi berbagai tantangan yang harus segera diatasi agar implementasinya benar-benar mampu menjawab kompleksitas kejahatan siber di era digital. Salah satu tantangan utama adalah terkait dengan multitafsir sejumlah pasal yang dinilai terlalu umum atau bersifat "karet". Hal ini menyebabkan ketidakpastian hukum dan membuka peluang terjadinya kriminalisasi terhadap ekspresi yang sah, seperti kritik terhadap pemerintah atau diskusi publik yang bersifat sensitive (Warren¸2020). Kasus-kasus yang menyangkut pasal pencemaran nama baik, ujaran kebencian, dan penyebaran informasi yang meresahkan masyarakat sering kali menjadi kontroversial karena dianggap mengekang kebebasan berekspresi.

Tantangan lainnya adalah kurangnya pemahaman aparat penegak hukum terhadap substansi dan filosofi UU ITE. Banyak kasus yang ditangani tidak menunjukkan kesesuaian antara jenis pelanggaran dengan pendekatan hukum yang digunakan. Hal ini disebabkan

oleh kurangnya pelatihan dan pemutakhiran pengetahuan aparat terhadap perkembangan dunia digital yang sangat dinamis. Oleh karena itu, peningkatan kapasitas aparat dalam memahami aspek teknis dan yuridis dari kejahatan siber merupakan prasyarat utama agar UU ITE dapat diterapkan secara tepat dan tidak disalahgunakan.

Efektivitas UU ITE juga tergantung pada kesiapan infrastruktur teknologi yang dimiliki negara. Tanpa dukungan sistem pelacakan digital, forensik siber, dan basis data intelijen elektronik yang memadai, penegakan hukum terhadap pelanggaran di ruang siber akan lambat dan tidak optimal. Selain itu, masih terdapat hambatan dalam kerja sama lintas batas (*cross-border enforcement*), terutama jika pelaku berada di luar negeri atau menggunakan server asing yang tidak terjangkau yurisdiksi nasional. Oleh karena itu, kerja sama internasional menjadi penting untuk mendukung penegakan hukum yang efektif terhadap kejahatan siber lintas negara.

Evaluasi terhadap efektivitas UU ITE harus pula mempertimbangkan aspek perlindungan korban dan pemulihan kerugian akibat kejahatan siber. Selama ini, perhatian terhadap hak korban masih kurang mendapat porsi dalam sistem hukum siber di Indonesia. Misalnya, korban penyebaran konten pribadi atau pemerasan berbasis digital sering kali tidak mendapatkan akses keadilan secara cepat dan memadai. Oleh karena itu, reformasi kebijakan hukum harus mengintegrasikan pendekatan berbasis korban (*victim-centered approach*), termasuk melalui mekanisme pemulihan, pendampingan hukum, dan kompensasi (Kartiko, 2023).

Selain memperkuat substansi UU ITE, efektivitas penanggulangan kejahatan siber juga ditentukan oleh sinergi antarlembaga. Koordinasi antara Kementerian Komunikasi dan Informatika (Kominfo), Kepolisian, Kejaksaan, serta Badan Siber dan Sandi Negara (BSSN) harus lebih solid dan terstruktur. Dibutuhkan sistem kerja terpadu berbasis data bersama (shared intelligence system) untuk mempercepat proses identifikasi pelanggaran dan eksekusi penindakan. Pembentukan satuan tugas khusus yang bersifat lintas sektoral dapat memperkuat efektivitas implementasi UU ITE dalam menghadapi beragam ancaman digital secara komprehensif. Literasi digital harus terus ditingkatkan agar masyarakat tidak hanya menjadi pengguna pasif, tetapi juga aktor aktif dalam menjaga ruang digital yang sehat. Kampanye publik tentang etika digital, bahaya penyebaran hoaks, serta tata cara pelaporan pelanggaran siber perlu dilakukan secara masif dan berkelanjutan. Keterlibatan komunitas, akademisi, dan media dalam memberikan edukasi serta menjadi jembatan komunikasi antara masyarakat dan aparat penegak hukum akan sangat membantu menciptakan ekosistem digital yang inklusif dan bertanggung jawab.

**B. Metodologi Penelitian**

Peneltian ini menggunakan penelitian hukum normatif dengan membahasa rumusan masalah sebagai berikut: Bagaimana Efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam Menanggulangi Kejahatan Cyber di Indonesia? Bagaimana Model Ideal Efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam Menanggulangi Kejahatan Cyber di Indonesia?

## C. Hasil dan Pembahasan

### Efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam Menanggulangi Kejahatan Cyber di Indonesia

UU ITE yang pertama kali disahkan pada tahun 2008 melalui Undang-Undang Nomor 11 Tahun 2008 merupakan tonggak penting dalam pembentukan sistem hukum di bidang teknologi informasi dan komunikasi. Undang-undang ini dirancang untuk menjawab tantangan hukum akibat transformasi digital yang telah mengubah cara manusia berinteraksi, melakukan transaksi, dan berkomunikasi (Kurniawan, 2014). Seiring

perkembangannya, UU ITE mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 dan yang terbaru, Undang-Undang Nomor 1 Tahun 2024.

UU ITE mengatur berbagai bentuk kejahatan siber seperti:

1) Akses ilegal terhadap sistem elektronik (*hacking*),
2) Intersepsi ilegal,
3) Pemalsuan dokumen digital,
4) Penyebaran konten ilegal (hoaks, pornografi, ujaran kebencian),
5) Penipuan online,
6) Pelanggaran data pribadi, dan
7) berbagai bentuk gangguan terhadap sistem elektronik.

Pasal-pasal penting yang digunakan untuk menindak kejahatan siber di antaranya adalah Pasal 27–29 (tentang konten ilegal), Pasal 30–32 (tentang akses ilegal dan manipulasi data), serta Pasal 35–36 (tentang manipulasi informasi atau sistem elektronik untuk keuntungan pribadi atau orang lain). Sejak diberlakukan, UU ITE telah menjadi instrumen hukum utama dalam menanggulangi kejahatan siber. Beberapa indikator keberhasilannya adalah, sebagai berikut (Harahap, 2012):

1) Peningkatan Kasus yang Diungkap Kepolisian Republik Indonesia melalui Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri telah berhasil mengungkap ribuan kasus setiap tahun yang berkaitan dengan pelanggaran UU ITE, termasuk penipuan daring, penyebaran konten kebencian, dan eksploitasi seksual anak.
2) Pemberlakuan Asas Ekstrateritorial. UU ITE memungkinkan negara untuk menindak pelaku kejahatan siber yang tidak berada di wilayah hukum Indonesia apabila perbuatannya berdampak di dalam negeri, sehingga memperluas cakupan penegakan hukum.
3) Koordinasi Lintas Lembaga. Terdapat kerja sama antara Kementerian Komunikasi dan Informatika (Kominfo), Kepolisian, BSSN, dan Kejaksaan dalam melakukan patroli siber, memblokir konten berbahaya, serta memproses hukum pelaku.
4) Pemblokiran dan Takedown Konten Ilegal. Kominfo secara aktif melakukan pemutusan akses terhadap konten negatif. Misalnya, situs pornografi, penyebaran hoaks, dan perjudian daring secara rutin diblokir.

Meski mencatatkan sejumlah keberhasilan, efektivitas UU ITE masih menghadapi beberapa kelemahan dan tantangan berikut (Sinaga,2020):

1) Pasal-Pasal yang Bersifat Karet dan Multitafsir. Beberapa pasal seperti Pasal 27 ayat (3) tentang pencemaran nama baik sering digunakan untuk melaporkan warga yang menyampaikan kritik, sehingga berpotensi membungkam kebebasan berekspresi. Hal ini menimbulkan ketakutan di masyarakat dan bertentangan dengan prinsip demokrasi.
2) Kriminalisasi Berlebihan. UU ITE sering dipakai sebagai alat untuk melakukan kriminalisasi terhadap aktivitas bermedia sosial yang sejatinya bukan tindak pidana berat. Hal ini menyebabkan overkriminalisasi, yang menguras energi aparat dan menimbulkan ketidakpercayaan publik.
3) Keterbatasan Sumber Daya Aparat Penegak Hukum. Tidak semua aparat penegak hukum memiliki kompetensi dalam mendeteksi, menyelidiki, dan mengadili kejahatan siber. Kejahatan digital membutuhkan keahlian khusus seperti digital forensics, manajemen data, dan pemahaman struktur jaringan global.
4) Kurangnya Infrastruktur Teknologi. Untuk menelusuri pelaku kejahatan siber dibutuhkan perangkat teknologi yang canggih dan basis data yang saling

terkoneksi. Banyak instansi hukum yang masih belum dilengkapi infrastruktur penunjang penegakan hukum siber secara maksimal.

5) Rendahnya Literasi Digital Masyarakat. Sebagian besar masyarakat Indonesia masih belum memahami batasan hukum dalam menggunakan media sosial. Kurangnya kesadaran ini memperbesar potensi pelanggaran UU ITE secara tidak sengaja.

Sejumlah upaya telah dilakukan untuk memperbaiki kelemahan dalam UU ITE, termasuk melalui revisi pada tahun 2016 dan 2024. Namun, masih terdapat kebutuhan akan reformulasi lebih lanjut, antara lain:

1) Pemisahan antara tindak pidana murni dan pelanggaran etik/kesusilaan agar tidak semua pelanggaran siber dijerat dengan hukum pidana, namun bisa diselesaikan secara administratif atau perdata.
2) Perumusan pasal secara lebih presisi dengan menambahkan unsur "niat jahat" (*mens rea*) dan "akibat nyata" untuk menghindari multitafsir.
3) Penguatan mekanisme *restorative justice* dalam kasus yang tidak menimbulkan dampak signifikan, seperti adu domba antarpihak yang dapat didamaikan tanpa proses pidana.
4) Peningkatan akuntabilitas aparat penegak hukum melalui pengawasan dari lembaga pengawas independen agar tidak terjadi penyalahgunaan kekuasaan.

Efektivitas UU ITE juga sangat tergantung pada peran aktif berbagai elemen dalam penerapannya (Didik, 2007):

1) Pemerintah. Harus memastikan sinkronisasi kebijakan nasional dan regulasi sektoral serta menyiapkan anggaran untuk peningkatan infrastruktur dan sumber daya manusia.
2) Aparat Penegak Hukum. Harus diberikan pelatihan berkala, pembaruan perangkat digital, serta pedoman etik dalam menangani kasus UU ITE.
3) Sektor Swasta dan Platform Media Sosial. Harus dilibatkan dalam upaya deteksi dini, pelaporan konten ilegal, serta perlindungan data pengguna. Tanggung jawab bersama (*co-regulation*) antara negara dan penyedia platform perlu ditingkatkan.
4) Masyarakat Sipil dan Media. Berperan sebagai pengawas independen dan pendidik publik. Kampanye literasi digital, pelatihan warga net, serta advokasi terhadap korban pelanggaran siber menjadi bagian penting dalam membentuk ekosistem digital yang sehat.

UU ITE hadir sebagai respon negara terhadap dinamika perkembangan teknologi informasi yang sangat pesat. Perkembangan dunia digital telah melahirkan beragam bentuk interaksi sosial baru, termasuk potensi kejahatan siber yang tak terbendung. UU ITE menjadi payung hukum utama dalam mengatur dan menanggulangi berbagai tindak pidana yang muncul di ranah digital seperti penyebaran informasi palsu (hoaks), penipuan daring, peretasan sistem elektronik, ujaran kebencian, hingga pelanggaran terhadap data pribadi.

UU ITE telah membawa dampak signifikan dalam proses penegakan hukum terhadap kejahatan siber. Sejumlah kasus besar berhasil diungkap oleh aparat penegak hukum dengan berlandaskan pada ketentuan dalam UU ITE. Kepolisian, melalui Direktorat Tindak Pidana Siber Bareskrim Polri, mampu mengungkap ribuan kasus kejahatan digital setiap tahunnya. Selain itu, kewenangan Kominfo untuk memblokir situs dan konten ilegal telah menjadi langkah konkret negara dalam menjaga ruang digital dari konten-konten yang meresahkan masyarakat. Hal ini mencerminkan bahwa UU ITE telah menjadi instrumen legal yang cukup efektif dari segi pencegahan dan penindakan (Dikdik, 2009).

Efektivitas UU ITE juga menyisakan berbagai persoalan yang perlu dievaluasi secara mendalam. Salah satu kritik utama terhadap UU ini adalah keberadaan sejumlah pasal yang dinilai multitafsir dan rentan digunakan secara sewenang-wenang. Pasal 27 ayat (3) tentang pencemaran nama baik, misalnya, kerap dijadikan alat kriminalisasi terhadap warganet yang menyampaikan kritik terhadap pejabat publik atau institusi negara. Situasi ini mengakibatkan efek jera yang tidak sehat dalam kehidupan berdemokrasi dan mempersempit ruang kebebasan berekspresi.

Kendala lainnya datang dari sisi aparat penegak hukum yang dalam praktiknya masih belum sepenuhnya memahami karakteristik kejahatan siber yang membutuhkan penanganan khusus. Banyak penyidik yang belum memiliki keahlian forensik digital, sedangkan infrastruktur yang dimiliki lembaga penegak hukum juga belum merata dan memadai di seluruh wilayah Indonesia. Kondisi ini menjadi hambatan nyata dalam menghadapi pelaku kejahatan siber yang cenderung semakin kompleks dan canggih.Dari sisi masyarakat, rendahnya literasi digital juga menjadi tantangan tersendiri. Banyak warga yang tidak memahami batas-batas hukum dalam penggunaan media sosial dan ruang digital. Mereka kerap menyebarkan informasi tanpa verifikasi atau mengunggah konten yang melanggar hak privasi pihak lain tanpa menyadari konsekuensi hukumnya. Dalam konteks ini, perlindungan melalui UU ITE memang penting, namun pendekatan represif saja tidak cukup. Perlu ada strategi edukatif yang lebih luas dan terstruktur agar masyarakat mampu menggunakan teknologi secara bijak dan bertanggung jawab.

Menimbang dinamika tersebut, sudah saatnya UU ITE tidak hanya dilihat sebagai alat penegakan hukum yang represif, tetapi juga sebagai bagian dari regulasi yang adaptif dan edukatif (Mansur¸2007). Reformulasi beberapa pasal dalam UU ITE mutlak diperlukan agar tidak terjadi overkriminalisasi yang bisa mencederai prinsip keadilan. Pasal-pasal yang selama ini menimbulkan kontroversi perlu diperjelas unsur-unsurnya dan diberikan batasan yang tegas agar tidak disalahgunakan. Penegakan hukum terhadap kejahatan siber harus dilakukan secara terukur, proporsional, dan berbasis pada prinsip keadilan restoratif, terutama terhadap kasus-kasus ringan yang tidak menimbulkan kerugian besar. Dalam beberapa konteks, penyelesaian secara damai di luar jalur pidana dapat menjadi alternatif yang lebih manusiawi dan efisien. Pemerintah juga perlu meningkatkan kapasitas lembaga penegak hukum dengan pelatihan dan pengadaan teknologi mutakhir yang sesuai dengan perkembangan dunia digital saat ini.

Efektivitas UU ITE akan optimal apabila seluruh pemangku kepentingan, termasuk pemerintah, aparat hukum, platform digital, masyarakat sipil, dan dunia pendidikan dapat membangun sinergi dan kolaborasi dalam menciptakan ekosistem digital yang aman, sehat, dan adil. Literasi digital perlu ditanamkan sejak dini, mulai dari sekolah, kampus, hingga ruang komunitas, agar masyarakat memiliki kesadaran hukum yang baik dalam bermedia digital.

**Model Ideal Efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam Menanggulangi Kejahatan Cyber di Indonesia**

Menghadapi eskalasi kejahatan siber di era digital, keberadaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan langkah awal penting bagi negara dalam menegakkan kedaulatan hukum di ruang siber. Namun, efektivitas UU ITE dalam menanggulangi kejahatan siber di Indonesia masih menghadapi banyak tantangan struktural, kultural, dan teknis. Oleh karena itu, diperlukan suatu model ideal yang tidak hanya mengandalkan pendekatan represif, tetapi juga mengintegrasikan pendekatan preventif, edukatif, dan korektif secara menyeluruh. Model ini harus berorientasi pada perlindungan masyarakat, penegakan keadilan, dan penghormatan terhadap hak asasi manusia dalam kerangka hukum yang adaptif terhadap perubahan teknologi informasi.

Pertama, model ideal efektivitas UU ITE harus dimulai dari perbaikan substansi hukum. Beberapa ketentuan dalam UU ITE, seperti pasal tentang pencemaran nama baik, ujaran kebencian, dan informasi yang meresahkan, terbukti multitafsir dan rawan disalahgunakan. Untuk itu, perlu dilakukan reformulasi norma hukum yang lebih jelas, limitatif, dan terukur. Setiap pasal harus disusun berdasarkan prinsip lex certa (kejelasan hukum) agar tidak menimbulkan ketidakpastian hukum yang merugikan warga negara. Dengan merumuskan norma hukum yang konkret, maka aparat penegak hukum dapat menjalankan tugasnya dengan standar objektif dan profesional.

Kedua, model ideal harus melibatkan rekonstruksi kelembagaan. Dalam konteks penegakan UU ITE, terdapat banyak lembaga yang memiliki kewenangan, seperti Kepolisian, Kejaksaan, Kementerian Kominfo, Badan Siber dan Sandi Negara (BSSN), dan Otoritas Jasa Keuangan (OJK) dalam hal transaksi digital. Namun, koordinasi antar lembaga ini sering kali tidak optimal karena ego sektoral dan tumpang tindih kewenangan. Oleh karena itu, model ideal yang diusulkan adalah pembentukan Satuan Tugas Nasional Kejahatan Siber, yang bersifat lintas sektor dan bertanggung jawab langsung kepada Presiden. Satgas ini akan berfungsi sebagai pusat komando penanganan kasus *cyber crime* secara terintegrasi, mulai dari pemantauan, investigasi, hingga pelaporan dan evaluasi. Selain pembentukan lembaga khusus, penting juga untuk meningkatkan kompetensi dan kapasitas sumber daya manusia. Banyak kasus kejahatan siber tidak tertangani karena keterbatasan kemampuan penyidik, jaksa, maupun hakim dalam memahami teknologi informasi dan komunikasi. Oleh karena itu, harus ada kebijakan nasional tentang peningkatan kapasitas SDM penegak hukum melalui pelatihan khusus di bidang forensik digital, keamanan jaringan, hingga hukum internasional terkait *cyber crime*. Dalam model ideal ini, pengembangan SDM bukan hanya sekadar pelatihan teknis, tetapi juga mencakup pembentukan kultur profesionalitas dan integritas dalam penegakan hukum.

Ketiga, model ideal efektivitas UU ITE perlu mengedepankan penguatan infrastruktur teknologi hukum. Penegakan hukum di dunia digital tidak dapat berjalan efektif tanpa dukungan teknologi yang mutakhir. Pemerintah harus berinvestasi dalam sistem pemantauan konten otomatis (*automated content monitoring system), big data analytics, artificial intelligence* (AI) untuk pelacakan pelaku siber, serta pengembangan digital forensik yang terdesentralisasi hingga ke tingkat kepolisian daerah. Infrastruktur ini harus dibangun dengan prinsip keamanan siber nasional, transparansi, dan perlindungan data pribadi yang ketat (Maskun,2020).

Keempat, untuk membangun model penegakan hukum UU ITE yang ideal, perlu pendekatan berbasis masyarakat atau *community-based cyber law enforcement.* Artinya, masyarakat tidak lagi diposisikan hanya sebagai objek hukum, tetapi juga sebagai subjek aktif yang turut menjaga ruang digital. Ini dapat diwujudkan melalui pelibatan organisasi masyarakat sipil, komunitas digital, akademisi, dan media massa dalam program literasi digital, kampanye anti-hoaks, pelaporan konten ilegal, dan pengawasan terhadap implementasi hukum. Masyarakat perlu diberi akses terhadap mekanisme pelaporan cepat dan perlindungan hukum yang adil jika menjadi korban kejahatan digital. Dengan pendekatan partisipatif ini, penegakan hukum tidak menjadi alat represi, tetapi justru menjadi instrumen perlindungan kolektif di masyarakat digital.

Selanjutnya, aspek penguatan literasi hukum dan digital juga menjadi komponen utama dalam model ideal ini. Tingkat kesadaran hukum masyarakat Indonesia dalam bermedia sosial masih relatif rendah. Banyak pengguna internet yang belum memahami batasan antara kebebasan berekspresi dengan pelanggaran hukum. Dalam hal ini, pemerintah melalui kementerian pendidikan, kominfo, dan dinas terkait harus mengintegrasikan kurikulum literasi digital sejak tingkat pendidikan dasar hingga perguruan tinggi. Modul literasi digital tidak hanya mengajarkan teknis penggunaan media,

tetapi juga nilai-nilai etika digital, hukum siber, dan hak digital warga negara.

Model ideal ini juga harus menyelaraskan hukum nasional dengan norma dan standar internasional. Mengingat kejahatan siber bersifat lintas negara, maka kerja sama internasional sangat penting dalam menegakkan hukum. Indonesia perlu aktif menjalin kerja sama dengan negara lain dalam rangka mutual legal assistance (MLA), ekstradisi pelaku cyber crime, pertukaran data intelijen, serta harmonisasi regulasi. Partisipasi dalam konvensi internasional seperti Budapest Convention on Cybercrime, meski belum diratifikasi, dapat menjadi kerangka referensi normatif dalam pengembangan hukum siber nasional yang sejalan dengan prinsip-prinsip global. Sebagai bagian dari upaya perlindungan hak asasi manusia (Raharjo, 2006), model ideal juga harus menempatkan prinsip *checks and balances* dalam implementasi UU ITE. Untuk mencegah penyalahgunaan wewenang dan kriminalisasi terhadap kebebasan berekspresi, diperlukan lembaga pengawas independen seperti Komisi Etik Siber atau Ombudsman Digital yang bertugas memantau pelaksanaan UU ITE, menampung pengaduan publik, dan memberikan rekomendasi perbaikan kebijakan. Dengan cara ini, masyarakat memiliki jalur pengawasan terhadap penyalahgunaan hukum, sehingga kepercayaan publik terhadap sistem penegakan hukum dapat meningkat.

Penting juga untuk dicatat bahwa model ideal ini tidak dapat berjalan efektif jika hanya bergantung pada upaya negara. Dunia usaha, khususnya penyedia platform digital seperti media sosial, marketplace, dan aplikasi pesan instan, harus memiliki tanggung jawab sosial dan hukum dalam mencegah penyebaran konten ilegal. Pemerintah harus mewajibkan platform-platform ini untuk memiliki mekanisme moderasi konten berbasis algoritma yang transparan, sistem pelaporan pengguna yang responsif, serta kerja sama aktif dengan aparat hukum dalam penanganan kejahatan siber. Penyedia platform yang beroperasi di Indonesia wajib tunduk pada ketentuan perundang-undangan nasional dan dapat dikenai sanksi administratif jika terbukti lalai atau membiarkan platformnya menjadi sarang kejahatan digital.

Model ideal efektivitas UU ITE dalam menanggulangi kejahatan siber di Indonesia harus memiliki dimensi reformasi hukum berkelanjutan. UU ITE tidak boleh bersifat statis, tetapi harus terus dievaluasi dan disesuaikan dengan perkembangan teknologi, dinamika sosial, dan kebutuhan hukum masyarakat. Pemerintah bersama DPR RI harus memiliki mekanisme monitoring dan evaluasi berkala terhadap pelaksanaan UU ITE, termasuk melalui riset akademik, konsultasi publik, serta forum-forum dialog terbuka yang inklusif (Rosadi, 2022). Hukum yang hidup adalah hukum yang senantiasa mampu menjawab tantangan zaman. Selain pilar-pilar utama yang telah diuraikan, terdapat beberapa aspek strategis tambahan yang perlu menjadi bagian dari model ideal efektivitas UU ITE. Salah satunya adalah pendekatan restoratif (*restorative justice*) dalam penyelesaian kasus-kasus tertentu. Tidak semua pelanggaran UU ITE harus berujung pada pemidanaan yang kaku. Dalam praktiknya, banyak kasus pelanggaran di ruang digitalseperti ujaran kebencian, pencemaran nama baik, atau penyebaran informasi yang merugikan yang sesungguhnya dapat diselesaikan melalui pendekatan non-litigasi dengan mengedepankan permintaan maaf, rehabilitasi reputasi, dan rekonsiliasi antar pihak.

Model pendekatan restoratif ini dapat diterapkan secara selektif, terutama pada kasus-kasus yang tidak menimbulkan kerugian publik yang besar, serta melibatkan individu atau kelompok rentan seperti anak-anak, pelajar, atau masyarakat yang belum memiliki pemahaman digital yang cukup. Dengan penerapan keadilan restoratif, sistem peradilan pidana tidak menjadi beban berlebih, dan masyarakat digital didorong untuk menyelesaikan konflik secara bermartabat dan produktif. Tidak kalah penting dalam model ideal ini adalah perlindungan terhadap korban kejahatan siber, yang hingga kini masih menjadi aspek yang terabaikan. Banyak korban kejahatan digital seperti doxing, penipuan

online, peretasan akun, pemerasan seksual digital (*sextortion*), hingga penyebaran konten pribadi, yang tidak mendapatkan dukungan hukum dan psikologis yang memadai. Negara harus menyediakan layanan bantuan hukum siber dan layanan pemulihan psikososial secara gratis bagi para korban, serta memastikan adanya jalur pelaporan yang aman, cepat, dan ramah korban (Sugeng, 2020).

Pemerintah juga perlu mendorong pembentukan pusat krisis kejahatan digital (*cybercrime crisis center*) di berbagai wilayah sebagai tempat konsultasi, pelaporan, dan penanganan cepat kasus-kasus siber. Ini akan memperkuat kehadiran negara dalam melindungi warga negaranya secara langsung dan konkret di dunia digital.Dalam kerangka ekonomi digital yang berkembang pesat, model ideal UU ITE juga harus menjamin kepastian hukum dalam transaksi elektronik, perlindungan data pribadi, dan keamanan digital bagi pelaku usaha dan konsumen. Tanpa jaminan hukum yang kuat, masyarakat akan enggan bertransaksi secara daring, yang pada akhirnya menghambat pertumbuhan ekonomi digital nasional. Maka dari itu, perlu integrasi yang lebih solid antara UU ITE dengan regulasi lainnya, seperti UU Perlindungan Data Pribadi, UU Perdagangan Elektronik, dan UU Tindak Pidana Pencucian Uang.

## D. Penutup

UU ITE sejatinya merupakan perangkat hukum yang penting dan dibutuhkan dalam menghadapi kejahatan siber. Namun agar efektivitasnya semakin maksimal, diperlukan langkah-langkah korektif berupa revisi, penguatan sumber daya, pembaruan infrastruktur hukum, serta strategi edukatif jangka panjang yang melibatkan seluruh elemen bangsa. Ke depan, UU ITE diharapkan tidak hanya menjadi instrumen pemidanaan, tetapi juga menjadi katalisator dalam mewujudkan tata kelola dunia digital yang demokratis, berkeadilan, dan menjunjung tinggi hak asasi manusia. Model ideal efektivitas UU ITE dalam menanggulangi kejahatan siber bukan hanya berbicara soal ketegasan hukum, tetapi lebih jauh tentang keseimbangan antara kepastian hukum, keadilan, perlindungan hak asasi manusia, dan kemajuan teknologi. Negara harus hadir bukan untuk menakut-nakuti warga digital, melainkan untuk melindungi mereka dari ancaman yang nyata di ruang siber. Dalam kerangka besar pembangunan nasional, keberadaan model hukum siber yang ideal menjadi fondasi penting menuju Indonesia digital yang berdaulat, adil, dan manusiawi.

## Daftar Pustaka

Didik M. Arief Mansur, *Cyber Crime Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, 2007.

Didik M. Arief Mansur, *Cyber Crime Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, 2007.

Dikdik dan Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2009.

Galuh Kartiko, *Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional*, Politeknis Negeri Malang Press, Malang, 2023.

Hidayat Chusnul Chotimah, *Membangun Pertahanan dan Keamanan Nasional dari Ancaman Cyber di Indonesia*, Jurnal Diplomasi, Volume 7, Nomor 4, 2025.

Jerry Kang, *Information Privacy in Cyberspace Transactions*, Stanford Law Review, Volume 50, Nomor 4, 2018.

Judhariksawan, et all, *Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes*, Fiat Justisia, Volume 13, Nomor 4, 2019.

Kurniawan, *Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasiona*l, Disertasi, Fakultas Hukum Universitas Brawjaya, Malang, 2014.

Marisa Amalina Shari Harahap, *Analisis Penerapan Undang- Undang No.11 tahun 2008 tentang Informasi dan Tranksaksi elektronik Dalam ,Tindak Pidana Siber*, Fakultas Hukum Universitas Indonesia, Jakarta, 2012.

Maskun, et all, *Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer*, Jurnal Hukum Kontemporer, Volume 42, Nomor 4, 2013.

Maskun, et.all, *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional,* CV. Nas Media Pustaka, Makassar, 2020.

Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Volume 4, Nomor 2, 2020.

Satjipto Raharjo, Ilmu Hukum, PT. Citra Aditya Bakti, Bandung, 2006.

Sinaga, *Penanggulangan Kejahatan International Cyber Crime Di Indonesia*, Makalah, Fakultas Universitas Padjajaran, Bandung, 2020.

Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika Aditama, Bandung, 2022.

Sugeng, *Hukum Telematika Indonesia*, Prenadamedia Group, Jakarta, 2020.