

**DINAMIKA YURISDIKSI HUKUM PIDANA DALAM
PEMBATASAN INFORMASI HOAKS TERKAIT DENGAN
KEJAHATAN CYBERCRIME****Haidar Danendra Febrian Ar Rafi¹, Sandrina Rahma Nurvita²**haidar.danendra@gmail.com¹, sandrinavita07@gmail.com²**Universitas Negeri Tidar**

Abstrak: Pada zaman milenial ini berita bohong atau hoak dewasa ini telah menjamur mengikuti informasi atau berita yang ramai dibicarakan. Berjalannya berita itu menjurus pada berita yang dikirim ke individu, kelompok, organisasi bahkan aparat pemerintahan. Ketidaksesuaian berita tersebut membuat para pembacanya sering menerima berita tersebut tanpa melihat awal muasal berita itu muncul. Berita hoak mengacu dan menunjuk pada situasi yang sekarang ini ramai dibicarakan, semakin orang terpicu maka berita itupun semakin gencar disebar. Adapun jenis-jenis berita hoak yang sering mengacu dan menuju pada penekanan perasaan seseorang, menekan dan mengancam pribadi seseorang, tokoh, serta organisasi atau perusahaan bahkan maupun instansi pemerintah. Dalam rangka mengatasi permasalahan cybercrime yang berkembang pesat di Indonesia, pemerintah membuat sebuah aturan perundang-undangan yang khusus mengatur mengenai cyberlaw yang di wujudkan pada sebuah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang. Nomor pada UUD No. 11 Tahun 2008 merupakan salah satu upaya untuk mengatasi cybercrime secara yuridis dan emperism, padahal Undang-Undang Nomor 11 Tahun 2008 tidak hanya membahas masalah situs cabul atau pornografi, akan tetapi juga mengatur mengenai aturan-aturan tentang transaksi elektronik yang merupakan payung hukum dalam aturan cyberlaw di Indonesia.

Kata Kunci: : Hoak, Cyberlaw, Cybercrime.

***Abstrak:** In this millennial era, fake news or hoaxes have mushroomed following information or news that is widely discussed. The flow of news leads to news being sent to individuals, groups, organizations and even government officials. The incongruity of the news means that readers often receive the news without seeing how the news first appeared. Hoax news refers and refers to a situation that is currently being widely discussed, the more people are triggered, the more intensively the news will be spread. There are types of hoax news that often refer to and lead to suppressing someone's feelings, suppressing and threatening the person, figure, or organization or company or even government agencies. In order to overcome the problem of cybercrime which is growing rapidly in Indonesia, the government has created legislation that specifically regulates cyberlaw which is embodied in Law Number 11 of 2008 concerning Information and Electronic Transactions. Constitution. Number in UUD no. Law No. 11 of 2008 is an effort to overcome cybercrime juridically and emperism, even though Law No. 11 of 2008 not only discusses the issue of obscene or pornographic sites, but also regulates the rules regarding electronic transactions which are the legal umbrella for cyberlaw regulations. in Indonesia.*

Keywords: Hoax, Cyberlaw, Cybercrime.

PENDAHULUAN

Dalam perkembangannya masyarakat semakin responsif dan cerdas dengan menanggapi kondisi sekarang ini yang terjadi. Baik dengan pemikiran yang positif atau bahkan pemikiran yang negatif melalui berita bohong. Perkembangan TI dalam globalisasi berdampak signifikan pada perilaku masyarakat dan bisnis di Indonesia. Internet telah menjadi bagian pola perilaku dan interaksi dengan dunia luar. Contohnya, internet memudahkan akses transaksi dengan komunitas dan bisnis mancanegara tanpa biaya tinggi. Faktanya adalah tiap orang bisa mengakses segala hal informasi dengan canggih dan cepat. Seiring kemajuan teknologi ternyata memunculkan masalah baru yaitu penyalahgunaan teknologi informasi untuk bertindak jahat atau yang sering disebut sebagai kejahatan cyber(cybercrime) yang dapat merugikan orang lain. Cybercrime merambah infrastruktur publik pemerintah berdampak pada kerugian nasional dan masyarakat. Hukum publik dan privat, seperti etika online, perlindungan konsumen, anti monopoli, persaingan sehat, perpajakan, data protection, dan cybercrime, menjadi dasar negara melawan kejahatan modern ini.

Menurut laporan Internet Security Threat Report dari Symantec, Indonesia adalah salah satu negara dengan jumlah aktivitas cybercrime terbanyak pada tahun 2011. Aktivitas online yang meningkat menjadi penyebab utama peningkatan cybercrime di Indonesia. Selain itu, Indonesia juga sering menjadi target serangan cyber oleh hacker dari berbagai negara. Untuk mengatasi hal ini, Pemerintah perlu memberikan dukungan melalui infrastruktur hukum dan pengaturan yang baik untuk menciptakan iklim aktivitas online yang aman dan mencegah ancaman dalam transaksi elektronik. Dalam penyelenggaraan sistem transaksi elektronik, ada empat elemen penting dalam keamanan informasi dan transaksi elektronik yaitu kerahasiaan, otentitas, integritas, dan nir-sangkal.

Cybercrime adalah kejahatan yang dilakukan di dunia maya melalui transformasi kejahatan dari dunia nyata ke dalam cyberspace. Cyberspace adalah tempat atau lokasi untuk melakukan kegiatan kriminal yang baru. Awalnya, definisi cybercrime hanya mencakup kejahatan komputer dengan berbagai istilah seperti 'computer misuse', 'computer abuse', 'computer fraud', 'computer-related crime', 'computer-assited crime', dan 'computer crime'. British Law Commission mendefinisikan 'computer crime' sebagai manipulasi komputer yang dilakukan dengan itikad buruk untuk memperoleh keuntungan material dan merugikan pihak lain. Cybercrime meliputi penggunaan komputer untuk penipuan, pencurian, penyembunyian, dan ancaman terhadap komputer seperti pencurian perangkat keras atau lunak, sabotase, dan pemerasan.

Dengan demikian, cybercrime mencakup tindak pidana yang terkait dengan sistem informasi, sistem informasi itu sendiri, dan komunikasi sebagai sarana pertukaran informasi dengan pihak lain. Cybercrime adalah bentuk kejahatan yang terkait dengan penggunaan teknologi informasi seperti komputer, jaringan internet, dan aplikasinya. Beberapa bentuk kejahatan komputer meliputi akses tidak sah ke sistem komputer, konten ilegal, pemalsuan data, mata-mata online, sabotase dan pemerasan, pelanggaran hak kekayaan intelektual, dan pelanggaran privasi. "UU ITE tahun 2016 mengubah UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Penelitian ini meninjau yurisdiksi negara dalam menangani kejahatan mayantara agar negara bisa berperan dalam penegakan hukum yang adil dan professional. Oleh karena itu penelitian ini diberi judul: "Dinamika Yurisdiksi Hukum Pidana Dalam Pembatasan Informasi Hoaks Terkait Dengan Kejahatan Cybercrime"

METODE PENELITIAN

Metode penelitian yang digunakan untuk menjawab permasalahan di atas adalah hukum normatif doctrinal penelitian, melalui pendekatan undang-undang, pendekatan konseptual, dan studi kasus. Itu pendekatan perundang-undangan dilakukan dengan menelaah peraturan perundang-undangan yang berkaitan dengan hal tersebut permasalahan yang diteliti, sedangkan pendekatan konseptual dilakukan untuk memahami permasalahan tersebut konsep yang terkait dengan

pencegahan kejahatan, kejahatan dunia maya, dan pertanggungjawaban pidana. Kasus pendekatan dilakukan untuk mengkaji kasus-kasus yang terjadi dan menyelesaikan permasalahan dalam kasus-kasus tersebut. Itu spesifikasi penelitian bersifat deskriptif. Sumber data utama adalah data sekunder yang dihasilkan dari studi literatur. Data yang telah diperoleh, kemudian dianalisis dengan menggunakan analisis deskriptif kualitatif.

HASIL DAN PEMBAHASAN

1. Internet and Cybercrime Dunia Maya dalam Perspektif Teori Teknologi

Sejak teknologi telekomunikasi dan komputer berkembang, manusia telah mulai berpikir dan bertindak di luar batas-batas tradisional. Internet telah menjadi simbol kemajuan dan peradaban, menawarkan banyak keuntungan dan peluang. Namun, internet juga menjadi sumber kejahatan cyber yang merajalela. Kejahatan dunia maya atau cybercrime adalah penggunaan teknologi komputer untuk kegiatan ilegal. Internet bisa menjadi alat untuk melakukan kejahatan tanpa hambatan. Dalam menghadapi kejahatan dunia maya, beberapa negara menggunakan undang-undang yang ada untuk mengadili pelakunya. Meski bentuk kejahatan dunia maya mirip dengan kejahatan tradisional, lingkungan di mana perilaku tersebut terjadi berbeda dan dampaknya bisa sangat besar. Internet yang terbuka dan mondial membuat pelaku sulit terlihat.

Berdasarkan teori substantif, internet tidaklah netral. Internet telah menciptakan sistem budaya baru yang mempengaruhi cara hidup dan berpikir masyarakat. Internet juga telah menjadi bagian dari hidup kita. Oleh karena itu, mengatur kejahatan dunia maya membutuhkan pendekatan yang baru. Dalam filosofi teknologi, para pelaku dunia maya dapat dikategorikan sebagai penganut determinisme teknologi. Bagi mereka, teknologi/internet adalah hal yang sangat vital dalam kehidupan mereka. Ketergantungan kita terhadap teknologi dapat dilihat dari contoh sederhana di mana pekerjaan kita tertunda atau terhenti ketika listrik padam atau baterai habis. Secara keseluruhan, internet sebagai sumber kejahatan dunia maya memerlukan regulasi yang baru. Perkembangan teknologi juga mempengaruhi cara berpikir dan bertindak kita.

2. Kebijakan dan Hukum Siber di Indonesia dalam Menaggulangnya

Hukum Cyber atau Cyber Law diperlukan untuk menangani kejahatan Cyber. Itu adalah aspek hukum yang terkait dengan penggunaan teknologi internet/elektronik oleh individu atau subyek hukum sejak mereka online. Negara-negara maju yang menggunakan internet/elektronik secara luas telah mengembangkan hukum Cyber yang canggih. Dalam penegakan hukum terhadap kejahatan transnasional, termasuk kejahatan siber, masalah yurisdiksi menjadi kendala. Pakar hukum mengakui ketidakjelasan penentuan yurisdiksi di dalam ruang siber. Komunikasi dan informasi multimedia bersifat internasional, multi yurisdiksi, dan tanpa batas geografis. Oleh karena itu, belum ada kepastian bagaimana suatu negara dapat menghukum komunikasi multimedia dalam era teknologi informasi saat ini.

Penentuan yurisdiksi adalah diskursus penting dalam penegakan hukum cyber, terutama dalam konteks penegakan hukum terhadap kejahatan transnasional. Pasal 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur masalah yurisdiksi, yang berlaku untuk semua orang yang melakukan perbuatan hukum, baik di dalam maupun di luar wilayah hukum Indonesia, dengan akibat hukum di Indonesia dan/atau merugikan kepentingan Indonesia. Pasal 1 angka 21 juga merinci bahwa "orang" mencakup individu, warga negara Indonesia, warga negara asing, dan badan hukum.

Penentuan yurisdiksi kejahatan cyber dapat dilihat dari asas-asas hukum internasional. Ada dua pandangan dari negara tentang hukum pidana yang berlaku, yaitu asas teritorial yang berlaku bagi semua tindakan pidana di dalam wilayah negara, dan asas personal yang berlaku bagi semua tindakan pidana dilakukan oleh warga negara di mana saja, juga di luar wilayah negara. Ada juga asas melindungi kepentingan nasional dan internasional dalam hukum pidana di luar negara.

KESIMPULAN

Dari penjelasan dan uraian diatas mengenai dinamika yurisdiksi hukum pidana dalam pembatasan informasi hoaks terkait dengan kejahatan cybercrime. Kejahatan dunia maya, atau cybercrime, seringkali sulit ditangani karena tidak terbatas oleh batasan negara dan bukti yang mudah diubah. Hal ini menjadi ancaman serius bagi individu, kelompok, badan usaha, hingga pertahanan nasional. Untuk mengatasi masalah ini, perlu dilakukan kriminalisasi kejahatan internet dan penerapan model pencegahan serta pengendalian yang beragam. Dalam hal ini, perlu mempertimbangkan filosofi dan teori teknologi, individualisasi pidana, fleksibilitas dalam pemilihan sanksi, modifikasi pidana, dan kekuasaan hakim dalam membuat undang-undang. Dengan demikian, Indonesia dapat menjadi negara yang bebas dari kejahatan dunia maya. Terkadang cybercrime cukup menyulitkan yurisdiksi hukum tapi bukan berarti tidak bisa ditangani ketika bukti itu ada. Alasan sulitnya adalah; pertama, kegiatan dunia cyber tidak dibatasi oleh teritorial Negara, Kedua, Kegiatan dunia cyber relatif tidak berwujud hingga secara hukum tradisional kadang sulit untuk menemukan bukti yang dapat disebut pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik.

DAFTAR PUSTAKA

- Hafidz, Jawade. 2014. "Kajian Yuridis Dalam Antisipasi Kejahatan Cyber." *Jurnal Pembaharuan Hukum* Vol. I(No.1):32–40.
- Lailiyah, Kusroh. 2022. "RISTEK : Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang." *RISTEK : Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang* 7(1):20–30.
- Masitoh Indriani, Adhy Riadhy Arafah, Fitri Nuril Islamy. 2018. "IMPLEMENTASI PERATURAN PEMERINTAH NOMOR 82 TAHUN 2012 SEBAGAI UPAYA NEGARA MENCEGAH CYBERCRIME DALAM SISTEM TRANSAKSI ELEKTRONIK." (82):53–54.
- Sudjati,;, Xaviera Qatrunnada Djana; Dewi Cahyandari. 2021. "Jurnal Dinamika Hukum." *Journal of Dinamika Hukum* 21(3):432–45. doi: 10.20884/1.jdh.2021.21.3.3256.This.