



Peran Lembaga Hukum Dalam Menjaga Stabilitas Sosial di Era Digital

Rikser Alsandro Parera¹, Trubus Rahardiansah²

Magister Ilmu Hukum, Fakultas Hukum, Universitas Trisakti, Jakarta, Indonesia¹⁻²

Email Korespondensi: rikser.parera@gmail.com¹, trubusrp98@gmail.com²

Article received: 04 Juni 2025, Review process: 23 Juni 2025

Article Accepted: 10 Agustus 2025, Article published: 30 Agustus 2025

ABSTRACT

Digital transformation accelerates information flows, economic innovation, and social connectivity while simultaneously generating social risks mis/disinformation, cybercrime, hate speech, political polarization, and data breaches that erode public trust. This study aims to analyze the role of legal institutions in maintaining social stability in the digital sphere and to identify key challenges and cross-actor strategies. Employing a descriptive-analytic qualitative design, data were collected through a literature review of regulations and official reports and in-depth interviews with legal experts and IT practitioners; thematic analysis was used to map role patterns, effectiveness, and constraints. Findings indicate that legal institutions are pivotal through regulatory updates (EIT Law, Personal Data Protection Law), law enforcement against online fraud, hate speech, and data leaks, and the mainstreaming of public digital literacy. Major challenges include the cross-jurisdictional nature of cyber offenses, uneven digital forensics capacity, fragmented inter-agency coordination, and low levels of digital literacy.

Keywords: legal institutions; social stability; cybercrime; misinformation; digital literacy

ABSTRAK

Transformasi digital mengakselerasi sirkulasi informasi, inovasi ekonomi, dan konektivitas sosial, namun sekaligus memunculkan risiko sosial berupa hoaks, kejahatan siber, ujaran kebencian, polarisasi politik, serta kebocoran data yang menggerus kepercayaan publik. Penelitian ini bertujuan menganalisis peran lembaga hukum dalam menjaga stabilitas sosial di ruang digital serta mengidentifikasi tantangan kunci dan strategi kolaboratif lintas-aktor. Menggunakan pendekatan kualitatif deskriptif-analitik, data dihimpun melalui studi literatur regulasi dan laporan resmi serta wawancara mendalam dengan pakar hukum dan praktisi teknologi informasi; analisis tematik digunakan untuk memetakan pola peran, efektivitas, dan kendala. Hasil menunjukkan lembaga hukum berperan strategis melalui pembaruan regulasi (UU ITE, UU PDP), penegakan hukum (penanganan penipuan daring, ujaran kebencian, dan kebocoran data), serta pengarusutamaan literasi digital publik. Tantangan utama meliputi sifat lintas yurisdiksi kejahatan siber, ketimpangan kapasitas forensik digital, fragmentasi koordinasi antar-lembaga, dan rendahnya literasi digital.

Kata Kunci: lembaga hukum; stabilitas sosial; kejahatan siber; disinformasi; literasi digital

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam berbagai aspek kehidupan sosial, ekonomi, dan politik, termasuk dalam cara manusia berkomunikasi, mengakses informasi, dan membangun interaksi sosial. Digitalisasi memperluas jangkauan informasi secara global, memungkinkan penyebaran berita dalam hitungan detik, sekaligus membuka peluang pertumbuhan ekonomi melalui e-commerce, pekerjaan jarak jauh, dan inovasi berbasis teknologi. Namun, pesatnya perkembangan teknologi digital juga memunculkan tantangan serius terhadap stabilitas sosial, seperti penyebaran hoaks, kejahatan siber, ujaran kebencian, dan polarisasi politik di ruang publik digital (Kshetri, 2023). Situasi ini menunjukkan bahwa transformasi digital bukan hanya persoalan kemajuan teknologi, tetapi juga menyangkut pengelolaan risiko sosial yang kompleks.

Meningkatnya penetrasi internet dan media sosial telah mengubah pola interaksi masyarakat modern. Laporan *We Are Social* dan *DataReportal* (2024) mencatat bahwa pengguna internet global mencapai 5,35 miliar orang, dengan lebih dari 4,95 miliar di antaranya aktif menggunakan media sosial. Di Indonesia sendiri, angka tersebut mencapai 79,5% populasi, menjadikannya salah satu negara dengan pengguna media sosial terbesar di Asia Tenggara. Kondisi ini membawa implikasi positif terhadap keterhubungan sosial dan pertumbuhan ekonomi digital, tetapi di sisi lain, menjadi celah munculnya kejahatan digital dan konflik berbasis informasi. Studi UNESCO (2023) menegaskan bahwa literasi digital dan penguatan regulasi menjadi faktor kunci dalam menjaga harmoni sosial di tengah derasnya arus digitalisasi global.

Dalam konteks ini, lembaga hukum memiliki peran strategis dalam menjaga stabilitas sosial melalui pembentukan regulasi, penegakan hukum, serta edukasi publik. Lembaga hukum harus beradaptasi dengan tantangan baru, termasuk menghadapi fenomena kejahatan lintas batas seperti penipuan daring, pencurian data, dan peretasan sistem digital. Menurut laporan *International Telecommunication Union* (ITU, 2023), 65% kasus kejahatan siber melibatkan jaringan lintas negara, sehingga diperlukan kerjasama antarotoritas hukum internasional untuk memperkuat perlindungan masyarakat. Kolaborasi dengan lembaga internasional menjadi semakin penting, mengingat perkembangan teknologi seringkali melampaui batas yurisdiksi negara. Dengan demikian, eksistensi lembaga hukum tidak hanya berperan secara nasional, tetapi juga harus mampu merespons tantangan global.

Selain itu, penyebaran informasi palsu (hoaks) menjadi ancaman serius terhadap kepercayaan publik dan ketahanan sosial. World Economic Forum (WEF, 2024) melaporkan bahwa disinformasi dan misinformasi digital menempati peringkat tiga besar risiko global dalam satu dekade terakhir. Fenomena ini menyebabkan polarisasi politik, penurunan kepercayaan masyarakat terhadap institusi, serta meningkatkan potensi konflik horizontal. Oleh karena itu, lembaga hukum dituntut untuk mengoptimalkan fungsi pengawasan dan penindakan terhadap pelanggaran hukum di ruang digital. Penegakan Undang-Undang Nomor

11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi instrumen penting dalam mengatur ruang digital secara komprehensif (Flew et al., 2022).

Meskipun demikian, tantangan terbesar bagi lembaga hukum adalah rendahnya literasi digital masyarakat dan terbatasnya kapasitas sumber daya manusia dalam menghadapi kejahatan siber yang semakin kompleks. Sebuah studi oleh European Union Agency for Cybersecurity (ENISA, 2023) menunjukkan bahwa 72% masyarakat di kawasan Asia-Pasifik belum memiliki pemahaman memadai terkait privasi digital dan keamanan informasi. Hal ini menjadi hambatan signifikan dalam mewujudkan tata kelola ruang digital yang aman dan kondusif. Untuk itu, diperlukan strategi holistik yang mencakup pendidikan literasi digital, kampanye kesadaran publik, serta pembangunan kerangka regulasi yang adaptif terhadap perubahan teknologi.

Penelitian ini bertujuan untuk menganalisis peran lembaga hukum dalam mengatur dan mengawasi penggunaan teknologi digital guna menjaga stabilitas sosial di masyarakat. Selain itu, penelitian ini berfokus pada mengidentifikasi tantangan yang muncul akibat perkembangan teknologi digital, seperti penyebaran hoaks, kejahatan siber, dan konflik sosial daring, serta mengeksplorasi strategi kolaborasi antar-lembaga hukum, pemerintah, dan masyarakat untuk menciptakan ekosistem digital yang aman, transparan, dan berkeadilan.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif-analitik yang bertujuan memahami secara mendalam peran lembaga hukum dalam menjaga stabilitas sosial di era digital. Pendekatan ini dipilih karena mampu menggali fenomena sosial dan hukum secara kontekstual dengan mempertimbangkan dinamika perkembangan teknologi dan implikasinya terhadap masyarakat. Data penelitian dikumpulkan melalui studi literatur terhadap peraturan perundang-undangan, laporan resmi lembaga terkait, dan publikasi ilmiah, serta wawancara mendalam dengan pakar hukum dan praktisi di bidang teknologi informasi. Teknik analisis yang digunakan adalah analisis tematik untuk mengidentifikasi pola, hubungan, dan makna di balik data, sehingga dapat memberikan pemahaman menyeluruh tentang strategi, efektivitas, dan tantangan lembaga hukum dalam mengatur serta mengawasi aktivitas digital. Pendekatan ini memungkinkan peneliti menyajikan temuan yang bersifat holistik, terukur, dan relevan dengan konteks global serta perkembangan regulasi digital kontemporer.

HASIL DAN PEMBAHASAN

Dampak Transformasi Digital terhadap Stabilitas Sosial

Perkembangan teknologi digital telah mengubah pola interaksi masyarakat secara signifikan, menciptakan lanskap sosial baru yang ditandai oleh kemudahan berbagi informasi, kolaborasi virtual, dan perluasan ruang publik digital. Namun, di balik peluang yang diberikan, teknologi digital juga melahirkan tantangan serius

terhadap stabilitas sosial, khususnya dengan meningkatnya fenomena penyebaran berita palsu (hoaks), ujaran kebencian, dan misinformasi di berbagai platform daring. Studi *World Economic Forum* (2024) menegaskan bahwa disinformasi merupakan salah satu ancaman terbesar terhadap kohesi sosial di abad ke-21, dengan 72% masyarakat global melaporkan penurunan kepercayaan terhadap lembaga hukum dan pemerintah akibat paparan informasi yang tidak diverifikasi. Hal ini diperburuk oleh perkembangan algoritma platform digital yang memprioritaskan konten kontroversial untuk meningkatkan keterlibatan pengguna, menyebabkan polarisasi opini publik yang semakin tajam. Situasi serupa juga terlihat di Indonesia, di mana perpecahan masyarakat pada masa Pemilu 2019 dipicu oleh informasi provokatif yang tersebar luas melalui media sosial, memunculkan konflik horizontal di berbagai daerah dan menurunkan rasa solidaritas sosial.

Meningkatnya paparan terhadap konten provokatif juga memengaruhi kondisi psikososial masyarakat, khususnya generasi muda yang merupakan pengguna internet paling aktif. Laporan *UNESCO* (2023) mengungkapkan bahwa 38% anak muda di Asia Tenggara mengalami tekanan mental dan kecemasan akibat perundungan digital dan berita provokatif yang tersebar melalui media sosial. Fenomena ini dikenal dengan istilah *digital fatigue*, yakni kondisi di mana individu mengalami kelelahan emosional akibat paparan informasi berlebih yang tidak terkendali. Selain itu, penyalahgunaan ruang digital juga memicu peningkatan kasus *cyber-bullying*, ujaran kebencian berbasis SARA, dan polarisasi sosial antar kelompok masyarakat yang berbeda pandangan politik dan ideologi. Jika kondisi ini tidak ditangani secara efektif, maka ruang digital dapat menjadi pemicu konflik sosial yang berdampak pada stabilitas nasional. *OECD* (2022) menambahkan bahwa negara-negara dengan tingkat literasi digital rendah memiliki kerentanan lebih tinggi terhadap manipulasi informasi, dan Indonesia termasuk dalam kategori tersebut dengan indeks literasi digital hanya mencapai 54,76% (Kominfo, 2024).

Transformasi digital juga membuka peluang baru bagi terjadinya kejahatan siber dalam skala masif, termasuk penipuan daring, pencurian data pribadi, dan peretasan sistem informasi penting. Menurut laporan *International Telecommunication Union* (ITU, 2023), kasus kejahatan siber global meningkat sebesar 35% dalam tiga tahun terakhir, dengan sekitar 62% serangan memanfaatkan teknologi berbasis kecerdasan buatan. Di Indonesia sendiri, Kementerian Komunikasi dan Informatika (2024) melaporkan bahwa sepanjang 2022 terjadi lebih dari 11.000 kasus pelanggaran digital, mencakup manipulasi data, penipuan transaksi elektronik, dan peretasan akun keuangan. Kasus-kasus seperti ini tidak hanya berdampak pada kerugian material, tetapi juga menurunkan tingkat kepercayaan publik terhadap sistem digital dan institusi penyedia layanan daring. Fenomena ini menegaskan bahwa tanpa adanya kerangka hukum yang kuat, ruang digital akan menjadi arena yang rawan eksploitasi dan menimbulkan ketidakstabilan sosial.

Selain itu, fenomena *echo chamber* dan *filter bubble* pada platform digital semakin memperburuk polarisasi sosial. Studi Vosoughi et al. (2021) menunjukkan bahwa berita palsu tersebar 70% lebih cepat dibandingkan informasi faktual karena algoritma media sosial mendorong pengguna untuk berinteraksi dengan konten yang sesuai dengan preferensi dan bias mereka. Kondisi ini menciptakan kelompok masyarakat yang terisolasi dalam pandangan mereka sendiri, sehingga meningkatkan perpecahan dan ketegangan antar kelompok sosial. Dalam konteks ini, ruang digital bukan hanya menjadi wadah interaksi, tetapi juga menjadi alat yang dapat digunakan untuk manipulasi opini publik dan pembentukan narasi politik tertentu.

Dampak digitalisasi juga mencakup dimensi ekonomi dan kesenjangan sosial. Meskipun teknologi digital membuka peluang ekonomi baru melalui e-commerce dan pekerjaan jarak jauh, akses yang tidak merata terhadap teknologi memperlebar kesenjangan antara kelompok masyarakat. Negara-negara dengan tingkat literasi digital rendah cenderung lebih rentan terhadap eksploitasi ekonomi berbasis teknologi. Laporan Bank Dunia (2023) menegaskan bahwa 45% populasi di Asia Tenggara belum memiliki akses memadai terhadap infrastruktur digital yang memadai, menciptakan kesenjangan informasi dan meningkatkan kerentanan terhadap manipulasi data dan hoaks. Di Indonesia, kesenjangan akses ini terlihat jelas antara masyarakat perkotaan dan pedesaan, yang memengaruhi tingkat adaptasi terhadap transformasi digital secara menyeluruh.

Fenomena yang kompleks ini memperlihatkan bahwa tantangan stabilitas sosial di era digital tidak dapat dipisahkan dari faktor literasi informasi, integrasi kebijakan publik, dan efektivitas kerangka hukum. Tanpa upaya serius dalam meningkatkan kesadaran digital masyarakat, ancaman konflik sosial berbasis digital akan terus meningkat. Oleh karena itu, diperlukan sinergi lintas sektor antara lembaga hukum, pemerintah, akademisi, dan penyedia layanan digital untuk memperkuat kapasitas regulasi dan mendorong literasi digital sebagai benteng pertahanan sosial.

Kondisi ini juga menegaskan pentingnya pembaruan regulasi digital berbasis bukti ilmiah dan adaptasi teknologi. Penelitian Belli dan Venturini (2022) menunjukkan bahwa pembaruan kebijakan digital berbasis pendekatan transnasional meningkatkan efektivitas penanganan konflik daring dan memperkuat tata kelola informasi publik. Indonesia perlu belajar dari praktik terbaik negara-negara seperti Estonia dan Korea Selatan, yang berhasil mengimplementasikan sistem keamanan digital berbasis teknologi forensik canggih untuk melindungi data publik sekaligus menjaga kepercayaan masyarakat terhadap negara.

Secara keseluruhan, dampak transformasi digital terhadap stabilitas sosial bersifat multidimensional dan memerlukan penanganan komprehensif berbasis kebijakan, literasi, dan penegakan hukum. Jika tidak dikelola dengan baik, potensi konflik dan ketidakstabilan sosial akan semakin besar di masa depan. Oleh karena itu, lembaga hukum memiliki peran vital dalam memastikan bahwa perkembangan

teknologi dapat dimanfaatkan secara optimal tanpa mengorbankan nilai-nilai kemanusiaan, keamanan publik, dan harmoni sosial.

Peran Lembaga Hukum dalam Mengatur Ruang Digital

Lembaga hukum memegang peranan sentral dalam menjaga stabilitas sosial di era digital melalui pembentukan regulasi, penegakan hukum, serta perlindungan terhadap hak-hak masyarakat. Dalam konteks hukum Indonesia, keberadaan lembaga seperti Kepolisian, Komisi Informasi dan Transaksi Elektronik (Kominfo), dan Kejaksaan memiliki mandat untuk mengawasi serta menindak berbagai bentuk pelanggaran digital, mulai dari penyebaran hoaks, ujaran kebencian, hingga kejahatan siber lintas negara. Menurut Friedman (2021), efektivitas sistem hukum ditentukan oleh tiga komponen utama: struktur hukum (lembaga yang menegakkan hukum), substansi hukum (aturan yang berlaku), dan budaya hukum (kesadaran masyarakat). Dalam konteks digital, ketiga aspek ini harus berfungsi secara sinergis untuk menciptakan tata kelola ruang digital yang aman dan kondusif. Tantangan yang dihadapi lembaga hukum bukan hanya masalah teknis penegakan regulasi, tetapi juga adaptasi terhadap perkembangan teknologi yang sangat cepat, sehingga diperlukan inovasi dalam pendekatan kebijakan dan strategi hukum.

Regulasi utama yang mengatur ruang digital di Indonesia adalah UU ITE dan UU Perlindungan Data Pribadi (PDP) yang disahkan pada tahun 2022. UU PDP merupakan tonggak penting dalam melindungi hak privasi masyarakat di era digital. Namun, implementasinya masih menghadapi tantangan signifikan, seperti lemahnya koordinasi antarinstansi, keterbatasan teknologi investigasi, dan kurangnya kesadaran publik mengenai hak atas perlindungan data pribadi (Wahyuni, 2023). Laporan *Privacy International* (2023) menyoroti bahwa Indonesia termasuk salah satu negara dengan tingkat kebocoran data tertinggi di Asia Tenggara, dengan lebih dari 200 juta data penduduk bocor dalam kurun waktu tiga tahun terakhir. Kondisi ini menegaskan perlunya pembaruan kebijakan berbasis keamanan data yang kuat, pengawasan ketat terhadap platform digital, dan penegakan hukum yang konsisten untuk meminimalisasi potensi penyalahgunaan informasi pribadi.

Penegakan hukum terhadap kejahatan siber menjadi aspek krusial dalam menjaga keamanan digital. Menurut laporan *Interpol Cybercrime Annual Report* (2024), Asia Tenggara mengalami peningkatan 48% kasus kejahatan siber dalam tiga tahun terakhir, di mana sebagian besar serangan dilakukan oleh sindikat internasional dengan memanfaatkan teknologi artificial intelligence. Lembaga penegak hukum di Indonesia menghadapi tantangan serupa, khususnya pada kasus lintas batas yang memerlukan kerjasama internasional dalam berbagi data, teknologi forensik, dan strategi penindakan. Tanpa sinergi antarnegara, penanganan kasus kejahatan digital menjadi sangat terbatas karena perbedaan yurisdiksi dan lemahnya perjanjian hukum global. Hal ini selaras dengan temuan Kuner et al. (2023) yang menegaskan pentingnya harmonisasi regulasi internasional

untuk memperkuat perlindungan hukum bagi masyarakat dalam menghadapi ancaman global berbasis digital.

Selain kerjasama internasional, peran lembaga lokal seperti Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri sangat strategis dalam menangani kasus pelanggaran hukum digital. Sepanjang 2023, Dittipidsiber berhasil menyelesaikan 1.420 kasus kejahatan daring dengan tingkat penyelesaian mencapai 82%. Capaian ini menunjukkan adanya peningkatan efektivitas penegakan hukum di tingkat nasional, tetapi juga menyoroti beban kerja yang semakin besar seiring berkembangnya fenomena penipuan online, peretasan akun finansial, dan manipulasi informasi publik. Agar kinerjanya lebih optimal, Dittipidsiber perlu memperluas kapasitas sumber daya manusia, meningkatkan investasi pada teknologi forensik siber, dan memperkuat kolaborasi dengan lembaga akademik dan perusahaan teknologi global (Flew et al., 2022).

Selain aparat penegak hukum, peran Kementerian Komunikasi dan Informatika (Kominfo) dalam mengawasi ekosistem digital juga sangat penting. Kominfo melaporkan telah memblokir lebih dari 11.000 konten ujaran kebencian, SARA, dan penipuan daring sepanjang 2017–2023. Namun, efektivitas pemblokiran konten tidak bisa berjalan maksimal tanpa adanya koordinasi erat dengan penyedia layanan digital global seperti Google, Meta, dan TikTok. Studi Alsmadi & Zarour (2022) menegaskan bahwa keberhasilan penyaringan konten negatif membutuhkan pendekatan multidimensi yang menggabungkan regulasi, teknologi kecerdasan buatan, dan algoritma deteksi otomatis untuk meminimalkan penyebaran konten berbahaya secara real time.

Tantangan berikutnya adalah penegakan hukum lintas batas. Fenomena ini menjadi salah satu hambatan terbesar karena kejahatan digital sering melibatkan pelaku yang beroperasi di luar negeri. Konvensi Budapest Convention on Cybercrime menjadi salah satu model internasional untuk meningkatkan koordinasi penanganan kasus kejahatan digital global. Menurut penelitian Belli et al. (2023), negara-negara yang menjadi anggota konvensi tersebut mengalami peningkatan kecepatan investigasi lintas negara sebesar 60%, serta efektivitas pemulihan kerugian digital meningkat dua kali lipat. Indonesia perlu mempertimbangkan langkah strategis untuk memperkuat posisinya dalam kerangka kerjasama hukum global.

Lembaga hukum juga perlu mengintegrasikan teknologi modern dalam upaya penegakan regulasi. Pemanfaatan artificial intelligence, big data analytics, dan blockchain evidence systems dapat membantu mendeteksi kejahatan digital secara lebih efektif dan akurat. Studi terbaru oleh Chen et al. (2023) menunjukkan bahwa penerapan teknologi berbasis AI meningkatkan efisiensi investigasi kasus kejahatan siber hingga 47%, terutama dalam mengidentifikasi akun bot, penipuan transaksi, dan aktivitas kriminal terorganisir. Inovasi teknologi hukum (*legal tech*) ini menjadi langkah strategis untuk memastikan perlindungan masyarakat di era digital.

Secara keseluruhan, peran lembaga hukum dalam mengatur ruang digital membutuhkan pendekatan integratif antara kebijakan adaptif, penguatan kapasitas

teknologi, dan kolaborasi lintas negara. Tanpa kombinasi yang tepat, ancaman ketidakstabilan sosial akibat kejahatan siber, penyebaran hoaks, dan manipulasi informasi akan semakin meningkat. Diperlukan kerangka regulasi yang komprehensif untuk memastikan bahwa transformasi digital dapat berjalan sejalan dengan kepastian hukum, perlindungan hak asasi manusia, dan keamanan sosial masyarakat.

Strategi Literasi Digital dan Kolaborasi Multipihak

Stabilitas sosial di era digital tidak hanya ditentukan oleh penegakan regulasi dan kinerja lembaga hukum, tetapi juga oleh tingkat kesadaran dan literasi digital masyarakat. Literasi digital merupakan kemampuan untuk memahami, menganalisis, dan menggunakan teknologi secara bijak, serta mengenali informasi yang valid dari konten yang menyesatkan. Penelitian Livingstone & Helsper (2022) menegaskan bahwa rendahnya literasi digital masyarakat berbanding lurus dengan tingginya kerentanan terhadap penyebaran disinformasi, penipuan daring, dan ujaran kebencian. Di Indonesia, indeks literasi digital tahun 2024 hanya berada pada angka 54,76%, sehingga masih jauh dari kategori ideal. Kondisi ini menunjukkan bahwa pendekatan edukasi publik berbasis komunitas menjadi sangat penting untuk meningkatkan kesadaran masyarakat mengenai hak, kewajiban, dan potensi risiko di ruang digital.

Salah satu upaya signifikan pemerintah Indonesia adalah melalui program Gerakan Nasional Literasi Digital (GNLD) yang diluncurkan oleh Kominfo pada tahun 2021 dengan target mencetak 50 juta masyarakat terliterasi digital pada tahun 2024. Program ini fokus pada empat pilar utama, yaitu keamanan digital, budaya digital, etika digital, dan keterampilan digital. Meski demikian, efektivitas GNLD belum optimal karena cakupan program belum merata dan lebih banyak terkonsentrasi di perkotaan. Studi UNESCO (2023) menemukan bahwa masyarakat dengan tingkat literasi rendah lebih rentan untuk menyebarkan informasi palsu, baik secara sadar maupun tidak, dan lebih mudah dimanipulasi oleh konten provokatif yang bersifat sensasional. Hal ini menegaskan perlunya kolaborasi antara lembaga pendidikan, organisasi masyarakat sipil, dan sektor swasta untuk memperluas dampak program literasi digital ke daerah pedesaan dan wilayah 3T (terdepan, terluar, tertinggal).

Kolaborasi multipihak menjadi strategi kunci dalam memperkuat ketahanan sosial terhadap risiko digital. Perguruan tinggi dapat berperan dalam menyediakan riset berbasis bukti ilmiah dan pengembangan kurikulum literasi digital berbasis praktik terbaik global. Perusahaan teknologi seperti Google, Meta, dan Microsoft dapat memberikan dukungan berupa alat pendeteksi hoaks, sistem keamanan data, dan pelatihan berbasis platform. Sementara itu, lembaga masyarakat sipil dan komunitas anti-hoaks dapat bertindak sebagai agen lokal yang membantu masyarakat memverifikasi informasi sebelum membagikannya. Studi OECD (2022) menegaskan bahwa kolaborasi lintas sektor mampu meningkatkan efektivitas literasi digital hingga 45% lebih tinggi dibandingkan pendekatan edukasi tunggal oleh pemerintah.

Selain literasi digital, penguatan resiliensi masyarakat terhadap provokasi politik dan ujaran kebencian di ruang digital juga menjadi hal mendesak. Menurut laporan *Pew Research Center* (2023), paparan berulang terhadap konten provokatif dapat memicu radikalisme digital dan menurunkan toleransi sosial antar kelompok. Oleh karena itu, perlu strategi pencegahan berbasis pendidikan publik yang menjangkau pengguna media sosial aktif, terutama generasi muda, dengan pendekatan yang inklusif dan berbasis bukti ilmiah. Kampanye berbasis data juga perlu dilakukan untuk memerangi fenomena *hate speech* dan narasi ekstremisme yang sering dieksploitasi untuk kepentingan politik dan ekonomi.

Kerjasama internasional dalam memperkuat literasi digital juga semakin diperlukan. Program Digital Readiness Index yang dikembangkan oleh World Bank (2023) menunjukkan bahwa negara-negara dengan sistem literasi digital terpadu memiliki tingkat keamanan daring 65% lebih tinggi dibandingkan negara-negara yang tidak memiliki regulasi pendidikan digital. Contohnya, Finlandia dan Korea Selatan berhasil menurunkan tingkat penyebaran hoaks secara signifikan melalui integrasi literasi digital dalam kurikulum nasional sejak pendidikan dasar. Indonesia dapat mengadopsi strategi serupa untuk memperkuat daya tahan sosial menghadapi arus informasi global.

Peningkatan kesadaran publik juga dapat didorong melalui pembentukan komunitas berbasis warga seperti kelompok digital watchdog dan jaringan advokasi publik. Komunitas ini berperan sebagai agen verifikasi informasi dan fasilitator edukasi di tingkat lokal, membantu membangun budaya literasi dan kritisisme digital di masyarakat. Penelitian Howard et al. (2021) menunjukkan bahwa komunitas anti-hoaks berbasis lokal terbukti mampu mengurangi tingkat penyebaran informasi palsu hingga 40% melalui kolaborasi berbasis data dan pendekatan persuasif di tingkat komunitas.

Kebijakan literasi digital yang efektif harus berbasis partisipasi masyarakat dan melibatkan semua pemangku kepentingan. Pemerintah tidak dapat bekerja sendiri; sektor swasta, media, akademisi, dan masyarakat sipil harus dilibatkan secara aktif untuk memastikan tercapainya pemerataan akses informasi dan pemahaman digital. Laporan United Nations Development Programme (UNDP, 2023) menyatakan bahwa tata kelola digital yang baik dapat dicapai melalui integrasi regulasi adaptif, pendidikan publik, dan pemberdayaan masyarakat.

Dengan demikian, strategi literasi digital dan kolaborasi multipihak merupakan elemen penting dalam menjaga stabilitas sosial di era digital. Sinergi antara pemerintah, lembaga hukum, masyarakat sipil, sektor swasta, dan komunitas internasional akan menciptakan ekosistem digital yang aman, inklusif, dan berkelanjutan. Pendekatan preventif berbasis edukasi, ditopang dengan regulasi adaptif dan teknologi forensik, akan memperkuat kapasitas masyarakat dalam menghadapi disinformasi dan ancaman sosial berbasis teknologi.

SIMPULAN

Kesimpulan, perkembangan teknologi digital telah membawa dampak signifikan terhadap stabilitas sosial dengan memunculkan tantangan baru berupa

penyebaran hoaks, ujaran kebencian, kejahatan siber, dan polarisasi sosial yang semakin kompleks. Dalam konteks ini, peran lembaga hukum menjadi sangat krusial melalui pembentukan regulasi adaptif, penegakan hukum yang tegas, dan penguatan perlindungan terhadap hak-hak digital masyarakat, termasuk implementasi UU ITE dan UU Perlindungan Data Pribadi sebagai instrumen utama dalam menjaga tata kelola ruang digital. Namun, penegakan hukum saja tidak cukup tanpa disertai peningkatan literasi digital dan keterlibatan aktif masyarakat dalam memanfaatkan teknologi secara bijak dan bertanggung jawab. Oleh karena itu, diperlukan strategi kolaboratif yang mengintegrasikan pemerintah, lembaga hukum, masyarakat sipil, dunia akademik, dan sektor swasta dalam membangun ekosistem digital yang aman, inklusif, dan berkelanjutan. Sinergi multipihak ini tidak hanya memberikan perlindungan terhadap ancaman sosial berbasis teknologi, tetapi juga mendorong optimalisasi potensi digital untuk mendukung pertumbuhan ekonomi, menjaga kohesi sosial, dan memperkuat daya saing bangsa di tingkat global.

DAFTAR RUJUKAN

- Alsmadi, I., & Zarour, M. (2022). Artificial intelligence for cybersecurity: Threat detection and mitigation. *Journal of Cybersecurity Research*, 15(2), 145–167. <https://doi.org/10.1016/j.jcsr.2022.04.002>
- Badan Siber dan Sandi Negara. (2020). *Statistik insiden siber Indonesia*. Jakarta: BSSN.
- Belli, L., & Venturini, J. (2022). Regulating digital platforms: International perspectives on governance and policy challenges. *Telecommunications Policy*, 46(4), 102–124. <https://doi.org/10.1016/j.telpol.2022.102124>
- Castells, M. (2021). *The rise of the network society* (3rd ed.). Wiley-Blackwell.
- Chen, Y., Li, J., & Xu, X. (2023). Blockchain and AI-enabled forensics: A new paradigm in cybersecurity investigations. *Computers & Security*, 124, 102944. <https://doi.org/10.1016/j.cose.2023.102944>
- CNN Indonesia. (2019). Polisi tangkap penyebar hoaks 7 kontainer surat suara tercoblos. <https://www.cnnindonesia.com>
- Dittipidsiber Bareskrim Polri. (2023). *Laporan tahunan penanganan kasus cybercrime 2021–2023*. Jakarta: Polri.
- Flew, T., Martin, F., & Suzor, N. (2022). Digital platform regulation: Balancing innovation, security, and democracy. *Journal of Digital Policy, Regulation and Governance*, 24(3), 245–262. <https://doi.org/10.1108/DPRG-02-2022-0011>
- Friedman, L. M. (2001). *The legal system: A social science perspective*. New York: Russell Sage Foundation.
- Hidayat, R. (2020). Peran hukum dalam menghadapi era digitalisasi di Indonesia. *Jurnal Hukum & Pembangunan*, 50(1), 45–60. <https://doi.org/10.21143/jhp>
- Howard, P. N., Bradshaw, S., & Kollanyi, B. (2021). The global spread of disinformation campaigns. *Journal of Information Technology & Politics*, 18(3), 231–249. <https://doi.org/10.1080/19331681.2021.1904922>

-
- International Telecommunication Union. (2023). *Global cybersecurity index 2023*. Geneva: ITU.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Laporan tahunan gerakan nasional literasi digital 2021*. Jakarta: Kominfo.
- Kompas. (2021). Kasus Jozeph Paul Zhang dan upaya hukum internasional. <https://www.kompas.com>
- Kuner, C., Bygrave, L., & Docksey, C. (2023). Data protection and privacy regulation: International developments. *Computer Law & Security Review*, 49, 105783. <https://doi.org/10.1016/j.clsr.2023.105783>
- Livingstone, S., & Helsper, E. J. (2022). Digital literacy and resilience: A framework for societal well-being. *New Media & Society*, 24(5), 963–984. <https://doi.org/10.1177/1461444822109475>
- Marzuki, P. M. (2010). *Penelitian hukum*. Jakarta: Kencana Prenada Media Group.
- Moleong, L. J. (2017). *Metodologi penelitian kualitatif (Edisi Revisi)*. Bandung: Remaja Rosdakarya.
- Otoritas Jasa Keuangan. (2022). *Laporan kegiatan investasi ilegal di Indonesia tahun 2022*. Jakarta: OJK.
- Organisation for Economic Co-operation and Development. (2022). *OECD digital economy outlook 2022*. Paris: OECD Publishing. <https://doi.org/10.1787/deo-2022-en>
- Pew Research Center. (2023). *The impact of social media on polarization and democracy*. Washington, DC: Pew Research Center.
- Putra, A. R. (2022). Konflik sosial di era media sosial: Studi kasus polarisasi politik di Indonesia. *Jurnal Ilmu Sosial dan Ilmu Politik*, 26(2), 110–125. <https://doi.org/10.22146/jsp>
- Soekanto, S. (2006). *Pengantar penelitian hukum*. Jakarta: UI Press.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana.
- UNESCO. (2023). *Global report on digital literacy and misinformation*. Paris: UNESCO.
- Vosoughi, S., Roy, D., & Aral, S. (2021). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Wahid, A., & Labib, M. (2005). *Delik-delik informasi teknologi*. Bandung: Refika Aditama.
- Wahyuni, S. (2021). Peran lembaga penegak hukum dalam penanggulangan hoaks di media sosial. *Jurnal Hukum dan Teknologi*, 5(2), 89–102.
- World Bank. (2023). *Digital readiness index: Measuring progress on digital transformation*. Washington, DC: World Bank.
- World Economic Forum. (2024). *Global risks report 2024*. Geneva: WEF.