

Legalitas Praktik Siber yang Licik: Kesiapan Hukum Siber Indonesia

Sardjana Orba Manullang 

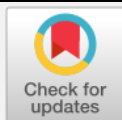
Program Studi Hukum, Fakultas Hukum, Universitas Krisnadwipayana, 13077,
Bekasi, Provinsi Jawa Barat, Indonesia

Korespondensi: somanullang@unkris.ac.id

INFO ARTIKEL

Info Publikasi:

Artikel Hasil Penelitian



Sitasi Cantuman:

Manullang, S. O. (2022). The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. *Society*, 10(2), 489-502.

DOI: [10.33019/society.v10i2.482](https://doi.org/10.33019/society.v10i2.482)

Hak Cipta © 2022. Dimiliki oleh Penulis, dipublikasi oleh Society



Artikel dengan akses terbuka.

Lisensi: Atribusi-NonKomersial-BerbagiSerupa (CC BY-NC-SA)

Dikirim: 22 September, 2022;

Diterima: 16 Desember, 2022;

Dipublikasi: 30 Desember, 2022;

ABSTRAK

Dunia maya Indonesia yang terus berkembang telah mengantarkan pertumbuhan ekonomi yang signifikan ke bisnis online dan e-commerce negara. Hal ini disebabkan oleh tingkat penetrasi internet negara yang meningkat sebesar 73% dari total populasinya, dengan sekitar 204 juta orang terhubung ke internet. Konektivitas yang tinggi ini telah menghasilkan beberapa peluang sosio-ekonomi yang positif tetapi dengan masalah pelik lainnya seperti kejahatan dunia maya, informasi yang salah, intoleransi yang dipicu oleh dunia maya, disinformasi, trolling, dan perang dunia maya. Terlepas dari intervensi pemerintah Indonesia dengan langkah-langkah untuk mengatur aktivitas dunia maya, beberapa praktik dunia maya licik yang tidak terdefinisi dalam literatur hukum terus dipraktikkan, bahkan dianggap sah, terkadang menimbulkan konsekuensi negatif. Praktik-praktik ini sering dilakukan sebagai operasi terorganisir yang menargetkan populasi untuk menciptakan ketidakpercayaan dan mempolarisasi populasi yang ditargetkan. Beberapa dibuat sebagai perang dunia maya yang dideklarasikan oleh entitas di suatu negara atau dari negara asing yang menargetkan populasi orang lain, yang merupakan ancaman bagi tatanan sosial. Penelitian ini mengeksplorasi praktik dunia maya yang licik ini dan strategi serta kemungkinan mitigasinya. Pendekatan penelitian sosiologis ditambah dengan penggunaan teori penegakan hukum diterapkan untuk mempelajari dan menganalisis kebijakan penegakan hukum keamanan dunia maya Indonesia, UU Internet dan Transaksi Elektronik (ITE), Kitab Undang-Undang Hukum Pidana, hukum Konstitusi, aktor masyarakat sipil dan sektor swasta pelaku keamanan siber. Hukum Indonesia dan hukum internasional, ditambah dengan teknologi yang tersedia, ditinjau kesiapannya untuk mengatasi

ancaman yang ditimbulkan oleh isu siber yang licik terhadap tatanan sosial. Langkah-langkah yang diambil oleh pemerintah Indonesia dalam kesiapan untuk memerangi isu-isu dunia maya ini di yurisdiksinya tetapi juga menghadirkan lebih banyak pertanyaan tentang proposal untuk meninjau undang-undang dan pengenalan sistem pemantauan konten, yang berisiko disebarkan secara tidak tepat dalam penyensoran atau penindasan terhadap kebebasan berekspresi yang sah.

Kata Kunci: Hukum Indonesia; Hukum Siber Indonesia; Kebijakan Siber; Perang Maya; Sensor

1. Pendahuluan

Dunia maya Indonesia dari Oktober 2016 hingga April 2017 dipenuhi dengan aktivitas dan materi dunia maya yang secara substansial mengarah pada unjuk rasa terbesar yang pernah ada di negara ini. Serangkaian protes di Jakarta dimulai pada pertengahan Oktober 2016 setelah sebuah video di *posting* dan dibagikan secara *online* (Lim, 2017). Peristiwa yang dihasilkan termasuk protes jalanan massal terbesar dalam sejarah Indonesia dan penangkapan dan akhirnya pemenjaraan Gubernur Jakarta yang sedang menjabat (Mietzner & Muhtadi, 2018). Kegiatan yang secara substansial mengarah pada hal ini terjadi di dunia maya terutama media sosial, aplikasi perpesanan, dan situs web. Niat dari aktivitas dunia maya ini, entah licik atau tidak, dapat memengaruhi sistem peradilan yang seharusnya independen, mengubah lanskap politik, memperkuat perpecahan sosial yang ada, dan mengganggu ketertiban umum (Nuryanti, 2020; Paterson, 2019).

Dunia maya Indonesia termasuk yang tersibuk di dunia, dengan *e-commerce* terbesar di Asia Tenggara; demikian pula, ia memiliki salah satu media sosial paling aktif. Dengan konektivitas yang tinggi tersebut, Indonesia memiliki peluang ekonomi yang luar biasa yang ditandai dengan peningkatan pertumbuhan ekonomi, dengan porsi yang cukup besar terkait langsung dengan aktivitas *online* (Manullang, 2021a; Nugraha & Putri, 2016; Paterson, 2019). Peluang yang sama disajikan dalam lanskap sosial-politik. Banyak orang Indonesia yang secara formal tidak terlibat secara politik, kebanyakan dari kelas menengah, semakin terlibat dalam percakapan sosial dan politik karena internet menghadirkan platform yang lebih baik untuk kebebasan berekspresi. Kebebasan berekspresi juga memungkinkan peningkatan aliran informasi negatif yang dibuat dan disebarluaskan dengan sengaja untuk memperkuat isu-isu yang kontroversial, mempolarisasi, dan bahkan mengintimidasi. Untuk negara dengan banyak keragaman dan sejarah politik yang memecah belah di sepanjang garis agama, suku, etnis, dan ras, internet digunakan secara aktif untuk memperkuat dan melanggengkan perpecahan ini (Lim, 2017; Toha *et al.*, 2021). Beberapa kegiatan untuk tujuan ini bahkan mengklaim legitimasi tergantung pada bagaimana, di mana dan kapan dilakukan dan atau jika mereka yang terlibat dalam praktik tersebut memiliki dukungan atau koneksi dengan yang berkuasa dan mereka yang berwenang (Gaidosch, 2018; Tyson, 2021).

Praktik dunia maya yang licik seperti itu terus menghindari hukum lokal dan internasional di banyak negara (Lubin & Townley, 2020). Pihak berwenang Indonesia menempatkan kebijakan dan langkah hukum untuk mengatur dunia maya dengan lebih banyak revisi undang-undang yang diusulkan. Pemerintah Indonesia, masyarakat sipil, akademisi, dan aktor

swasta telah memerangi praktik siber negatif (Manuhutu *et al.*, 2021; Manullang, 2020; Nugraha & Putri, 2016). Beberapa tindakan yang diterapkan dan diusulkan berada di bawah pengawasan karena kemungkinan mereka mengizinkan penyensoran, pelanggaran hak atas kebebasan berekspresi, privasi, dan bertentangan dengan nilai-nilai demokrasi (Paterson, 2019).

Dalam studi ini, kami mengkaji kesiapan hukum siber Indonesia untuk menangani praktik-praktik yang menjadi perhatian di dunia maya dengan mengeksplorasi kebijakan Siber Indonesia, Undang-Undang Siber. Untuk lebih memahami sifat licik dari beberapa praktik dunia maya di dunia maya Indonesia, kami akan menganalisis masalah sosial-politik negara yang secara historis dibentuk oleh politik yang memecah belah dan eksploitatif, serta bagaimana dampaknya saat diperbesar oleh peningkatan konektivitas internet. Kami akan memeriksa ancaman yang ditimbulkan oleh isu-isu ini terhadap demokrasi negara yang sedang berkembang dan perubahan kebijakan pemerintah dalam menanggapi isu-isu ini.

2. Peningkatan Konektivitas, Pertumbuhan Ekonomi, dan Liberalisme

Sebagian besar pertumbuhan ekonomi Indonesia dikaitkan dengan aktivitas berbasis *online* dan *e-commerce*, sebagaimana dibuktikan dengan investasi besar di sektor ini oleh raksasa *e-commerce* seperti Alibaba, JD.com, dan Google (Jurriëns & Tapsell, 2017; Ramli, 2020). Proyeksi kurva pertumbuhan ekonomi Indonesia mengarah ke negara yang menjadi salah satu ekonomi terbesar dunia dalam hal daya beli pada tahun 2050 (Nehru, 2016; Paterson, 2019).

Pertumbuhan *e-commerce* ini didukung oleh peningkatan konektivitas, dengan lebih dari 204 juta orang terhubung ke internet, terutama melalui koneksi seluler (Chen, 2020; Manullang, 2020). Paket data yang terjangkau telah menyebabkan orang Indonesia menggunakan media sosial secara eksponensial (Manullang, 2020; Ramli, 2020). Diberi peringkat tertinggi dalam penggunaan ponsel, dengan rata-rata waktu layar hingga 180 menit setiap hari (Amin, 2014), orang Indonesia juga termasuk pengguna aktif Twitter dan Facebook dengan peringkat teratas (Paterson, 2019). Selain *e-commerce* dan media sosial, pemerintah, masyarakat sipil, dan akademisi telah mengadopsi penyampaian layanan online secara signifikan bahkan di daerah pedesaan. Alat umpan balik publik pemerintah tentang peringkat layanannya, yang disebut LAPOR, diluncurkan untuk mendorong penyelenggaraan layanan publik yang transparan dan akuntabel (Dini *et al.*, 2018; Manullang, 2021b).

Terlepas dari peningkatan konektivitas, peluang, keterlibatan sosial dan upaya pemerintah, masalah keamanan siber dan kejahatan siber, hubungan yang tidak seimbang antara daerah pedesaan dan perkotaan masih mengganggu dunia maya Indonesia (Manuhutu *et al.*, 2021; Manullang, 2021b; Setiawan & Suhartomo, 2019; Setti & Wanto, 2019). Apa yang lebih rendah dari literasi dan pengetahuan digital di antara bagian populasi tertentu yang mengecualikan mereka dari memanfaatkan peluang yang disajikan oleh konektivitas digital? Selain itu, literasi konektivitas digital yang rendah membuat banyak orang lebih rentan terhadap praktik siber yang licik, viktimisasi kejahatan siber, dan disinformasi, yang mengganggu tatanan sosial.

3. Praktik Cyber yang Licik

Banyak praktik dunia maya yang licik mengklaim legitimasi (Manning & Agnew, 2020; Payne, 2018). Pada bagian ini, kami membahas manipulasi media sosial melalui *trolling*, yang disebut secara lokal di Indonesia disebut, 'Buzzing', tetapi fokusnya adalah pada *trolling* dua sisi. Dalam penelitian lain, ini disebut sebagai *rabble-rousing*, yang telah lolos dari klasifikasi hukum (Lubin & Townley, 2020). Manipulasi media sosial di Indonesia berakar pada sejarah negara itu sendiri dan dilakukan oleh mesin propaganda negara pada masa itu sebagai alat untuk mengendalikan wacana sosial yang lebih luas, mempersenjatai keragaman untuk

menebar paranoia, dan mengatur suasana otoritarianisme (Berting, 2019; Shah & Taylor, 2021). Runtuhnya otoritarianisme di Indonesia mengantarkan pada demokratisasi, yang datang dengan kebebasan berekspresi yang dipercepat dengan hadirnya internet dan media digital. Adegan media sosial meledak dengan aktivitas dengan demokrasi yang berlaku yang mentolerir kebebasan berekspresi yang sebelumnya ditekan. Namun, kebiasaan lama memanipulasi narasi melalui media populer kini menjadi bagian dari jiwa sosial. Siapa saja bisa melaksanakannya, tidak hanya yang didominasi oleh mesin negara seperti dulu. Hal ini memunculkan pabrik *troll* media sosial dan 'pasukan siber' yang memanipulasi narasi di media sosial atas nama banyak pihak, terutama untuk tujuan politik dan sosial ekonomi (Sastramidjaja & Wijayanto, 2022).

Pemilihan gubernur Jakarta tahun 2012 memulai penggunaan 'tim siber' dalam skala besar, terutama 'buzzer' / *troll* dalam kampanye politik. Tren telah ditetapkan, dan banyak aktivitas politik berikutnya telah merekrut tim siber semacam itu untuk mendorong agenda mereka (Nuryanti, 2020; Sastramidjaja & Wijayanto, 2022). Aktivitas dunia maya yang meningkat seperti ini telah menjadi bagian dari kehidupan sehari-hari orang Indonesia, seringkali menghasilkan konsekuensi *online* dan *offline* yang nyata (Lindsey & Pausacker, 2016; Lim, 2017). Meskipun aktivitas siber semacam ini dapat bersifat konstruktif seperti peningkatan partisipasi politik dan kebebasan berekspresi, sebagian besar telah mengakibatkan perpecahan dan gangguan ketertiban, dan bahkan memengaruhi sistem peradilan seperti dalam kasus pemenjaraan Ahok, gubernur Jakarta (Lim, 2017; Berting, 2019).

Sifat licik dari *trolling* sering dirancang untuk dengan sengaja menyebarkan hal-hal negatif, yang mengarah pada konsekuensi negatif, namun penuntutan untuk *trolling* jarang terjadi atau tidak ada sama sekali. Ini bisa jadi sebagian karena koneksi para *troller* dengan entitas kuat yang berwenang. Sebuah kelompok aktivis peretas Muslim menggunakan media sosial untuk memperkuat intoleransi beragama (Tapsell, 2021). Itu mencuri informasi pribadi orang yang ditargetkan (dianggap menghina Islam) dan menerbitkannya secara *online* (Paterson, 2019; Berting, 2019). Ada indikasi hubungan antara partai politik yang kuat dan militer Indonesia (Paterson, 2019; Boyle, 2020).

4. *Trolling/Buzzing*

Pengguna jejaring sosial online akhir-akhir ini harus bergulat dengan *trolling*. Sebanyak *trolling* memiliki klasifikasi negatif dan positif, penelitian ini berfokus pada *troller* negatif yang secara khusus diidentifikasi oleh praktisi sebagai Pembenci (*Hater*) (Hodge & Hallgrimsdottir, 2020; Horse et al., 2021). Dalam hal ini, istilah tersebut telah digunakan dengan sengaja memposting pesan yang provokatif, ofensif, atau mengancam melalui jaringan komunikasi. Definisi ini dengan jelas menggambarkan sifat licik dari *trolling*, namun ini merupakan aktivitas yang dilakukan oleh banyak orang, termasuk mereka yang berwenang. *Trolling* terus menghindari hukum, bahkan dalam beberapa kasus mengklaim legalitas dan meneruskannya sebagai 'kebebasan berbicara' atau 'seni' seperti dalam kasus Elonis Vs. Amerika Serikat (Reichel, 2019; Roark, 2015).

Contoh umum *trolling* di Indonesia adalah 'pasukan dunia maya' yang secara lokal disebut sebagai 'buzzers' (Sastramidjaja dan Wijayanto, 2022). Literatur yang tersedia tentang subjek tersebut menyatakan bahwa *buzzer* memperkuat pendapat sudut pandang tertentu tentang isu atau merek tertentu untuk menjangkau audiens yang lebih luas (Lim, 2017; Sastramidjaja & Wijayanto, 2022). Fenomena *buzz* di Indonesia menjadi populer pada tahun 2009, dengan *influencer* utama dibayar untuk mempromosikan produk dan merek, dan meledak selama pemilihan gubernur 2012 di Jakarta (Neyasyah, 2020; Syahputra, 2019). Kandidat politik di

semua sisi merekrut dan membayar tim buzzer untuk mendorong agenda politik mereka. Tentu saja, cara kerja *buzzer* tergantung pada kreativitas *buzzer*. Kreativitas dalam trolling sering melibatkan mengeluarkan materi yang paling menarik perhatian. Politik Indonesia berarti memperkuat pendapat yang memecah belah di sepanjang garis agama, budaya, etnis, ras dan ekonomi. Setelah tuduhan penistaan terhadap Ahok, Gubernur Jakarta, pada tahun 2016 dan demonstrasi berikutnya yang menyebabkan penangkapan dan pemenjarannya, aktivitas dunia maya dibanjiri dengan materi yang memecah belah yang tersebar di internet dan diperkuat oleh troll. Materi anti-Ahok yang beredar, misalnya, mengkritisi etnis Tionghoa yang dianggap sebagai orang asing dan komunis; iman Kristennya disebut-sebut melalui nada Islam radikal sebagai seorang kafir (Lim, 2017; Ong & Tapsell, 2021). Pihak lain juga mendorong fakta yang diputarbalikkan tentang lawan Ahok; Anies menuduhnya terkait dengan beberapa kasus korupsi dan melontarkan tuduhan absurd bahwa dia berniat memberlakukan hukum syariah dan disanjung kelompok Syiah Iran. Materi semacam itu menenggelamkan opini alternatif dan menciptakan suasana terpolarisasi yang sangat kuat yang menyebar dari dunia maya ke komunitas dan rumah, membuat orang saling bertentangan.

5. *Trolling Dua Sisi (rabble-rousing)*

Menghindari sorotan analisis ilmiah yang luas adalah cara licik yang sangat kejam dan berbahaya untuk menanamkan ketidakharmonisan di antara masyarakat adalah kebiasaan "bermain di kedua sisi" di internet (Fichman & McClelland, 2021). Praktisi yang telah mempelajari praktik ini menyebutnya sebagai *rabble-rousing* (Lubin & Townley, 2020). Untuk studi ini, kami akan menyebutnya sebagai 'trolling dua sisi', yang melibatkan pengorganisasian dan koordinasi operasi untuk memperkuat masalah yang memecah belah dengan mendukung kedua belah pihak. Untuk memahami praktik ini dengan lebih baik, kami akan mengambil dari contoh-contoh baik dari lingkungan lokal maupun internasional.

Secara lokal, *trolling* dua sisi lebih terwujud dalam isu-isu yang memecah belah dan berorientasi politik. Kembali ke kampanye gubernur Ahok-Anies Jakarta dan insiden penistaan agama, *trolling* dua sisi dipraktikkan oleh kelompok-kelompok yang mengoperasikan situs web berbeda, yang memperkuat materi perpecahan yang bertentangan satu sama lain karena beroperasi serupa di media sosial. Misalnya, arrahmah.com memposting materi anti-Ahok, sementara spoofnya arrahmahnews.com memposting materi pro-Ahok. Hal yang sama terjadi pada VOA-islamnews.com, tiruan dari VOA-islam.com, dan pkspuyengan.com, tiruan dari pkspiyungan.com yang saat ini sudah tidak berfungsi (Lim, 2017). Mengesampingkan niat ideologis dari praktik trolling dua sisi ini, tindakan mereka bertujuan untuk menanamkan ketidakharmonisan dalam demokrasi muda Indonesia (Lubin & Townley, 2020). Para *troller* bermain di kedua sisi dalam kasus seperti itu, membuat korban rakyat Indonesia.

Secara internasional, contoh *trolling* dua sisi yang paling terkenal terjadi di dunia maya Amerika Serikat. *Troll* memainkan kedua belah pihak dengan memperkuat isu-isu yang memecah belah, seperti dalam pemilihan presiden 2016 antara Trump dan Hillary Clinton dan debat mandat Vaksinasi AS pada tahun 2020, yang disalahkan pada trolling dua sisi Rusia untuk menabur ketidakharmonisan dan melemahkan demokrasi AS (Broniatowski *et al.*, 2018). Di Jerman, *troll* dua sisi Rusia dikatakan telah bermain baik di sisi 'sayap kanan' dan secara aktif di sisi 'anti-fasis sayap kiri', menegaskan kembali sikap analis yang menyatakan bahwa Rusia bermaksud untuk ketidakharmonisan tanaman di negara-negara demokrasi barat. Demikian pula, para analis telah menunjukkan bahwa China memiliki ribuan agen berbayar, alias '50-cent army', yang tugasnya memanipulasi kepercayaan umum melalui praktik dunia maya yang licik seperti interaksi media sosial (Lubin & Townley, 2020).

6. Ancaman Dijeda oleh Trolling Dua Sisi

Inti masalah dalam *trolling* dua sisi adalah kemampuannya untuk secara bersamaan memperkuat masalah yang bertentangan. Sifat dua sisi dari jenis *trolling* ini, ditambah dengan produksi massal dan penyebarannya, yang terkadang melibatkan *bot* sambil menyembunyikan niat sebenarnya mereka menimbulkan serangan nyata terhadap keharmonisan sosial, menyamakannya sebagai ekspresi yang sah. Niat licik dari praktik-praktik ini tidak memberikan manfaat apa pun bagi masyarakat.

Praktik ini dapat mengguncang komunitas yang lebih luas, dan oleh karena itu perlu diperhatikan daya rusaknya. Ini secara diam-diam mengganggu wacana publik dan mencemari pandangan dan opini asli, sehingga memalsukan domain fundamental yang memungkinkan proses demokrasi berfungsi dengan baik (McGonagle *et al.*, 2019). *Trolling* dua sisi mengeksploitasi elemen polarisasi dalam suatu komunitas, mendorong orang untuk mengambil sikap yang lebih memecah belah dan ekstrim (Clark & Aufderheide, 2011). Studi telah menunjukkan bahwa algoritma media sosial dikonfigurasi untuk mempercepat polarisasi sosial (Paterson, 2019).

Praktik *trolling* dua sisi yang memperkuat perpecahan secara serius mengancam demokrasi muda dengan beragam keragaman seperti Indonesia, karena hal itu merusak isu-isu rentan dalam mempromosikan masyarakat terbuka dengan kebebasan arus informasi, kebebasan berekspresi, dan diskusi tentang isu dan identitas yang saling bertentangan (Fichman & McClelland, 2021).

Dari perspektif pengaturan hukum internasional, inti dari hukum internasional adalah menghubungkan negara-negara dalam suatu kesatuan di sekitar nilai-nilai bersama, kolaborasi dan perdamaian. Oleh karena itu, praktik-praktik yang didasarkan pada niat *absurd* untuk mendorong kelompok, komunitas, dan individu semakin jauh bertentangan dengan gagasan '*peace with one another*' sebagaimana dinyatakan dalam Piagam PBB (Lubin & Townley, 2020).

7. Legalitas Beberapa Praktik Siber yang Licik

Sebagian besar praktik dunia maya yang licik dapat ditempatkan dalam kategorisasi kejahatan dunia maya yang jelas seperti disinformasi, berita palsu, peretasan, dan sejenisnya. Namun, *trolling* terus menghindari segala bentuk kategorisasi hukum meskipun memiliki konsekuensi yang merusak. Sebagai praktik yang dilakukan di dunia maya, tantangan untuk menemukan pelaku atau membuktikan ketidakabsahan praktik tersebut sangat besar.

Eksplorasi unsur-unsur hukum Indonesia dan hukum internasional pada persoalan *trolling* dua sisi yang bermasalah ini terbatas pada beberapa prinsip yang sebagian besar merupakan domain hukum internasional. Domain ini termasuk intervensi koersif yang dilarang, kedaulatan, dan penentuan nasib sendiri. Domain hukum nasional dan internasional meliputi hak asasi manusia, kebebasan berekspresi dan kegiatan subversif. Ilegalitas praktik dunia maya yang licik ini dapat dikonseptualisasikan melalui domain hukum ini. Langkah-langkah yang diterapkan dan disarankan untuk tinjauan kebijakan siber dan hukum siber di Indonesia bermasalah dalam kasus-kasus tertentu, ironisnya bermanifestasi sebagai tindakan kejam yang berisiko mengorbankan populasi yang dilindunginya (Ong & Tapsell, 2021).

8. Paradigma Internasional

8.1. Prinsip Non-intervensi

Biasanya, prinsip non-intervensi secara intuitif berkonotasi dengan implikasi bahwa praktik siber yang licik "mengintervensi" urusan orang lain. Melalui lensa larangan yang melekat pada intervensi dalam urusan orang lain, *trolling* dua sisi adalah tindakan campur tangan. Praktisi

menunjukkan bahwa paksaan harus dibuktikan untuk menunjuk non-intervensi sebagai ilegal (Lubin & Townley, 2020). Pemaksaan sebagai unsur dalam hukum merupakan determinan dalam asas hukum non-intervensi. Tapi sekali lagi, *trolling* mengeksploitasi wacana dan sistem teknologi yang ada untuk mengganggu dan atau secara kalkulasi mencemari wacana *online*. Selicik apa pun praktik ini, biasanya tidak bermanifestasi sebagai pemaksaan atau mengambil alih fungsi apa pun.

8.2. Subversi

Orang berhak menentukan nasibnya sendiri. Hukum lokal dan internasional mengakui hak orang untuk memutuskan hal-hal yang mempengaruhi nasib mereka dan memiliki kebebasan untuk terlibat dalam kegiatan politik, ekonomi, budaya dan sosial tanpa campur tangan (Castellino, 2021). Kegiatan subversif mengganggu kebebasan ini; propaganda subversif digambarkan sebagai informasi yang dimaksudkan untuk merusak fungsi institusi dengan memengaruhi populasi menuju pemberontakan atau pemberontakan (Breitenbauch & Byrjalsen, 2019). Sifat destabilisasi dari *trolling* dua sisi dapat masuk ke dalam aktivitas subversif. Selain itu, menyebarkan propaganda subversif merupakan larangan hukum dalam hukum lokal dan internasional. Namun, ini mungkin tidak terjadi jika *trolling* hanya memperkuat masalah yang sudah ada, tetapi sekali lagi penguatan ini membantu menjaga aktivitas tetap hidup dan memenuhi tujuan yang dimaksudkan.

8.3. Hak Asasi Manusia

Sifat luas dari mendefinisikan hak atas kebebasan berekspresi menghadirkan tantangan dalam menetapkan *trolling* sebagai legal atau ilegal. Definisi luas badan-badan internasional tentang hukum hak asasi manusia telah menempatkan kebebasan berekspresi termasuk hak untuk mencari, menerima dan berbagi informasi dan ide apapun tanpa memandang batas (Farsi et al., 2018). Semua jenis batasan diuraikan lebih lanjut untuk merujuk pada semua jenis ide dan opini yang dapat ditularkan kepada orang lain melalui semua jenis media dan metode ekspresi (Howie, 2018; Lubin & Townley, 2020). Banyak praktik dunia maya licik yang mampu menyamar sebagai kebebasan berekspresi asli berhasil mendapatkan perlindungan hukum dan bahkan mengklaim legitimasi sebagai kebebasan berekspresi. *Trolling* dua sisi dan praktik dunia maya licik lainnya menerima lebih sedikit regulasi kebijakan karena perlindungan hukum yang kuat yang diberikan pada kebebasan berekspresi. Dalam hal ini, praktisi dunia maya, akademisi, dan masyarakat sipil di Indonesia memiliki pandangan yang sama bahwa tindakan pemerintah untuk memerangi masalah di dunia maya memiliki tinjauan legislatif yang bermasalah, dan moderasi konten otomatis dapat menjadi alat untuk menyensor dan menekan kebebasan berekspresi (Paterson, 2019; Ong & Tapsell, 2021).

9. Kesiapan Kebijakan dan Hukum Siber Indonesia

Manfaat internet yang sangat besar bagi penduduk Indonesia tidak dapat disangkal, begitu pula kerugian dan ancamannya. Undang-undang nasional dan internasional dalam bentuknya saat ini tidak memberikan solusi hukum yang memuaskan untuk masalah praktik siber yang licik seperti *trolling* dua sisi. Fenomena tersebut menghindari penangkapan bahkan di bawah prinsip non-intervensi dan penentuan nasib sendiri. Hal yang sama berlaku untuk larangan propaganda subversif, yang mungkin tidak menawarkan tindakan substantif yang dapat diterapkan untuk mengatasi masalah seperti *trolling*. Ketidacukupan solusi hukum memerlukan pertimbangan tindakan non-hukum untuk mengatasi praktik dunia maya tersebut. Pemerintah Indonesia, masyarakat sipil, akademisi, dan sektor swasta merupakan

pemain dalam upaya mengatasi aktivitas siber negatif di dunia maya Indonesia.

9.1. Lanskap Hukum Isu Siber di Dunia Maya Indonesia

Undang-undang utama tentang isu siber di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik (ITE) (2008) (Nugraha & Putri, 2016). Undang-undang ini ditinjau ulang pada tahun 2006 untuk melayani kejahatan dunia maya dan juga memberdayakan pejabat dengan kekuatan untuk memblokir apa yang dianggap sebagai materi terlarang. Pasal 27 sampai dengan 36 UU ITE mengatur ketentuan mengenai perbuatan yang berkaitan dengan dunia maya yang dilarang (Siregar & Lubis, 2021).

9.1.1. Elemen Hukum Isu Cyber

Pembuktian: Pasal 42 UU ITE juga mengatur tentang penyidikan yang sejalan dengan Pasal 183 KUHAP (Fernando *et al.*, 2022). Dengan demikian, sistem penentuan bukti yang diadopsi mengikuti teori bukti di mana putusan mengikuti bentuk penalaran silogistik, yang dikritik oleh para ahli karena tidak berkontribusi pada pengetahuan tentang kebenaran (Sommer, 1997). Mengingat bahwa pembuktian harus berdasarkan ketentuan undang-undang, maka wajib dicatat dan diajukan sebagai alat bukti di sidang pengadilan mengikuti ketentuan Pasal 184 KUHAP yang mensyaratkan sebagai berikut:

Kesaksian Saksi: Hal ini diharapkan dapat disampaikan mengikuti ketentuan acara Penuntutan Pidana dan dilaksanakan di bawah sumpah serta memenuhi persyaratan sebagai berikut (Arimuladi, 2022).

- Bebas dari rekayasa, pendapat dan pandangan ahli.
- Selaras dengan asas '*unus testis nullus testis*' adanya saksi lebih dari satu.
- Kesaksian saksi tidak bergantung pada kabar angin.
- Konsistensi informasi di antara para saksi.

Sifat dari praktik siber, yang terjadi seluruhnya di dunia maya, membuat sulit atau tidak mungkin memperoleh keterangan saksi yang dapat digunakan dalam suatu masalah hukum. Kesaksian saksi di sini hanya dapat berupa kabar angin, yang hanya dapat diambil dengan syarat '*testimonium di auditu*'. Walaupun tidak secara langsung dianggap sebagai bukti, hal ini dapat berperan penting dalam upaya memperkuat pendirian kasus tersebut (Amin & Huda, 2021; Pujoyono, 2020).

Pendapat ahli: Melibatkan ahli di bidang yang diperiksa, yang mampu mengelaborasi secara gamblang persoalan tentang kasus/permasalahan. Harus dapat memberikan pernyataan yang meyakinkan yang mencerminkan pendapat yang tidak memihak pada aspek-aspek tertentu dalam keahliannya yang dipersengketakan (Harahap *et al.*, 2019).

Dokumentasi sebagai bukti: Banyak jenis dokumen diakui sebagai bukti jika diautentikasi. Ketentuan tentang dokumentasi sebagai alat bukti diatur dalam Pasal 184 ayat C dan pasal 187 KUHAP (Asmara *et al.*, 2019).

Pernyataan terdakwa: Hal ini diatur dalam Pasal 189 dan 184 KUHAP, di mana para terdakwa membuat pernyataan dan narasi tentang tindakan mereka dan apa yang mereka alami (Balo *et al.*, 2020).

9.2. Penegakan Hukum pada Isu Siber

Menyusul munculnya isu-isu dunia maya, strategi kebijakan yang ditujukan untuk mencegah, menghilangkan, dan memitigasi isu-isu terkait dunia maya diterapkan di masing-masing negara dan di kancah internasional. Hukum siber adalah salah satu elemen penting

untuk menerapkan strategi kebijakan siber, yang tidak dapat bekerja sendiri tetapi bersama-sama dengan elemen kebijakan strategis lainnya untuk mengatasi kejahatan siber (Amin & Huda, 2021). Hal ini sejalan dengan musyawarah Kongres Perserikatan Bangsa-Bangsa, yang mengeksplorasi kemungkinan penggunaan kebijakan yang diarahkan untuk mengatur aktivitas dan praktik dunia maya untuk mengatasi kejahatan dunia maya sehubungan dengan hukum pidana masing-masing negara (Rajput, 2018).

9.2.1. Pendekatan Punitif

Pendekatan pidana terhadap kejahatan dunia maya dan praktik dunia maya lainnya di Indonesia sedang diterapkan. Ada beberapa penuntutan yang terkait dengan aktivitas dunia maya. Sebagian besar kasus terkait dengan aktivitas kriminal langsung, seperti penipuan dan pencurian melalui peretasan; yang lain dituntut sebagai kasus pencemaran nama baik. Namun, hukum pidana seringkali tidak dianggap sebagai instrumen kebijakan yang ideal untuk mengatasi praktik siber yang licik, melainkan sebagai alat yang memiliki kepentingan strategis dalam upaya tersebut. Para praktisi telah mengemukakan gagasan pembahasan isu siber dengan harmonisasi hukum siber yang ada dengan fokus mengkriminalkan kegiatan tertentu di dunia maya, memperhatikan pendekatan dan pertimbangan prosedural dalam hukum tata negara (Schallbruch & Skierka, 2018; Amin & Huda, 2021).

9.2.2. Pendekatan Non-Punitif

Gagasan untuk mencegah praktik siber yang licik tanpa pendekatan hukuman di Indonesia harus melibatkan lebih banyak tindakan pencegahan. Langkah-langkah tersebut dapat mengatasi kombinasi faktor-faktor yang dapat mengarah pada praktik siber yang licik dengan berbicara tentang fenomena sosio-hukum yang dapat mengarah pada praktik semacam itu (Paterson, 2019; Tapsell, 2021). Upaya literasi digital masyarakat berguna pada saat ini. Dalam harmonisasi hukum siber dan hukum tata negara, dapat dilakukan upaya untuk meminimalisir praktik siber negatif dengan mengidentifikasi faktor-faktor yang memberatkan praktik tersebut (Lim, 2017). Namun, efektivitas upaya non-punitif dalam menangani maraknya praktik siber negatif masih belum pasti, tetapi yang pasti adalah bahwa isu yang dilakukan di dunia maya memerlukan kewaspadaan global karena melampaui batas teritorial dan dapat memiliki konsekuensi di negara mana pun (Lubin & Townley, 2020).

10. Teknologi dan Pemerintah dalam Membatasi Praktik Siber yang Liar

Setidaknya dalam versinya saat ini, hukum Indonesia dan internasional tidak cukup menangani masalah praktik *online* yang licik. Di ranah internasional, prinsip non-intervensi dalam urusan negara lain atau hak bangsa untuk menentukan nasib sendiri dan menjaga kedaulatan teritorial tidak menghalangi praktik *online* negatif. Larangan tentang bahaya lintas batas, misalnya, lebih bersifat simbolis daripada praktis dalam kemampuan mereka untuk mengurangi risiko yang terkait dengan praktik licik daring lintas wilayah. Tanpa upaya hukum yang tepat, negara-negara dapat mempertimbangkan untuk menggunakan metode ekstra-hukum untuk melindungi masyarakat mereka dan secara agresif memerangi efek destabilisasi dari tindakan *online* seperti *buzzing/trolling* dua sisi. Banyak metode teknologi yang dapat digunakan untuk melawan praktik *online* yang licik akan dibahas di bagian ini.

Memahami perubahan teknologi tertentu pada informasi kita sangat penting sebelum mempertimbangkan solusi apa yang mungkin bermanfaat. Tanpa bantuan lanskap teknologi informasi, fenomena seperti *trolling/buzzing* tidak mungkin muncul. Dominasi internet dan media sosial dalam lanskap informasi dan komunikasi yang berubah secara signifikan saat ini

secara langsung berkontribusi pada praktik *online* yang licik (Lubin & Townley, 2020). Beberapa dekade yang lalu, memiliki mesin cetak adalah satu-satunya metode komunikasi massa yang realistis, dan diskusi publik dilakukan dengan sangat berbeda. Praktik negatif *online* yang umum adalah fenomena yang tidak dapat terjadi dalam kondisi tersebut.

Tindakan dan debat publik pengguna Internet di seluruh dunia saat ini dapat diakses, memudahkan para aktor untuk memeriksa perbedaan budaya dan sosial-ekonomi yang siap untuk tindakan negatif seperti *trolling* dua sisi. Siapa pun sekarang dapat secara instan mengakses khalayak nasional karena hambatan komunikasi yang terkait dengan komunikasi berbasis kertas *offline* dan media massa telah sangat berkurang. Pemain yang ditentukan dan didanai dengan baik dapat membanjiri forum diskusi publik dengan data untuk mempengaruhi diskusi demi keuntungan mereka. Selain itu, kami memiliki akses langsung ke orang-orang karena teknik penargetan yang dibuat untuk periklanan. Akibatnya, beberapa aktor diperlengkapi dengan baik untuk mempengaruhi segmen demografis yang berbeda dari komunitas yang ditargetkan, seringkali dengan hasil yang menghancurkan komunitas.

Agen siber yang licik dilindungi oleh anonimitas. Banyak *platform* populer telah menyerah untuk menggunakan nama asli seseorang sebagai alat identifikasi resmi. Pengguna tidak diharuskan untuk mengungkapkan informasi apa pun tentang identitas fisik mereka saat menggunakan berbagai *platform online* untuk komunikasi, termasuk memposting reaksi di situs web berita dengan kemampuan komentar umpan balik. Identitas *online* yang kabur mempersulit penegak hukum untuk membuat identifikasi formal dan memungkinkan praktik *online* yang licik untuk menipu pengguna internet biasa agar berpikir bahwa telah terjadi peningkatan opini publik yang tidak direncanakan.

Materi sensitif, kontroversial, menyesatkan, dan predator telah terbukti menyebar. Namun, umpan berita dan algoritme kurasi digunakan (Tenove *et al.*, 2018), yang diperlukan untuk mengatur sejumlah besar konten internet *online* yang dapat diakses pengguna dengan lebih cepat. Menurut para ahli, rekomendasi konten dapat mengarahkan pengguna ke konten yang lebih kontroversial atau radikal daripada yang mereka cari. Yang lain telah menunjukkan bahwa, meskipun sebagian besar pengguna media sosial moderat, kecil, tetapi sangat aktif, komunitas memposting dan membagikan tautan ke situs web manipulatif dan eksploitatif dan bertanggung jawab atas konten *online* yang paling banyak dilihat.

Sebagian besar platform populer dirancang untuk meningkatkan partisipasi dan menghasilkan pendapatan, membuat mereka rentan terhadap troll daripada menyediakan forum yang terstruktur dan produktif. Hal ini memungkinkan aktor jahat membingkai masalah sensitif dengan cara kontroversial yang mungkin menjadi viral, memberi mereka kekuasaan atas masalah yang sering diperdebatkan di depan umum.

Solusi realistis untuk kerentanan ini sangat sulit dipraktikkan. Pendapat yang berbeda ada pada materi pelajaran literasi digital. Menurut penelitian, mereka yang kurang melek digital lebih rentan terhadap manipulasi karena kurang mampu mengevaluasi validitas atau asal muasal komunikasi digital. Praktisi menegaskan bahwa menyalahkan individu daripada pemerintah, perusahaan teknologi, dan penyedia layanan Internet tidak pantas. Yang lain berpendapat bahwa satu-satunya cara untuk mengurangi kejadian dan efek negatif *online* seperti kampanye pelecehan adalah melalui penyedia teknologi; mengingat kedekatan mereka dengan masalah dan pesatnya kemajuan teknologi, mereka dapat mengembangkan cara untuk mendeteksi pengguna yang licik dan memperingatkan pengguna yang rentan.

Jika tidak ada, atau sebagai tambahan, solusi jangka panjang yang efektif, negara mungkin diwajibkan untuk merespons dengan membentuk organisasi proaktif yang didedikasikan untuk memerangi kampanye informasi yang menyesatkan. Lembaga-lembaga ini mungkin, jika

diterapkan dengan buruk, hanya berfungsi untuk meningkatkan kemarahan publik terhadap sistem yang sudah tidak memadai untuk memerangi disinformasi. Inisiatif pemantauan internet pemerintah Indonesia, yang dibentuk untuk mengurangi perilaku *online* yang licik, telah menuai kritik karena kecenderungan mereka untuk melanggar kebebasan berekspresi sementara gagal menghentikan ujaran kebencian dari kelompok tertentu di masyarakat. Kebijakan-kebijakan ini dipandang sebagai alat efektif yang mendukung negara-negara dalam pertempuran sengit mereka melawan informasi yang salah dan mendorong para pelaksananya ke arah kediktatoran.

Beberapa negara mengandalkan upaya literasi digital dan kampanye kesadaran publik untuk meningkatkan kesadaran akan dampak internet yang berbahaya. Para ahli setuju bahwa mengembangkan dan mempertahankan percakapan yang konstruktif adalah tanggapan terbaik daripada membantah fakta dengan penuh semangat. Selain itu, banyak negara telah mendirikan institusi untuk secara preventif mengatasi aktivitas online yang negatif.

11. Kesimpulan

Mengingat sifat sulit dipahami yang khas dan kontradiktif dari praktik *online* yang licik, opsi yang layak untuk mengatasinya adalah dengan penggunaan teknologi dan hukum, mengingat pentingnya inisiatif kolaboratif multi-segi internasional yang sama. Sulit untuk mengidentifikasi kerangka hukum internasional yang dapat diterapkan yang akan memungkinkan karakteristik korosif dari praktik online yang licik, seperti *trolling* dua sisi, untuk dianggap ilegal, seperti halnya dengan aktivitas amplifikasi secara lebih luas. Meskipun mungkin sulit untuk melakukannya secara legal, ada alasan untuk merasa bahwa praktik online yang licik seperti *trolling* dua sisi dan *buzzing* tidak boleh terus ada tanpa ditangani oleh kerangka hukum lokal dan internasional. Sifat kontradiktif dari *trolling* dua sisi dalam konteks hak asasi manusia untuk kebebasan berbicara membuat orang percaya bahwa itu tidak memiliki banyak manfaat ekspresif yang pantas dilindungi. *Trolling* dua sisi dimungkinkan oleh banyak perubahan signifikan dalam lingkungan informasi kita yang disebabkan oleh kemajuan teknologi. Mengingat tidak adanya pemulihan hukum, negara yang berusaha menggagalkan praktik tersebut dan mengurangi dampak negatifnya mungkin perlu mempertimbangkan alternatif teknologi. Penelitian ini menciptakan peluang untuk lebih banyak upaya di beberapa bidang. Ini menyoroti pentingnya tinjauan hukum dan kolaborasi internasional pada isu-isu konseptual yang membahas karakteristik destruktif yang khas dari praktik dan operasi licik *online* dari jenis yang sama di era digital, seperti *trolling* dua sisi dan dengungan. Pentingnya melakukan penelitian terkonsentrasi ke dalam keefektifan berbagai taktik teknologi untuk menangkis praktik *online* yang licik dan operasi informasi *online* yang memecah belah harus disorot. Ahli teori dan teknolog harus berkolaborasi untuk memajukan kedua tujuan ini karena keduanya harus dikejar secara bersamaan.

12. Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah bersedia membantu selama penelitian ini dilakukan.

13. Pernyataan *Conflicts of Interest*

Penulis menyatakan tidak ada potensi konflik kepentingan sehubungan dengan penelitian, kepengarangan, dan/atau publikasi dari artikel ini.

Daftar Pustaka

- Amin, K. (2014). Indonesians Spend most Time on Smartphones in the World. The Jakarta Post, June 5. Retrieved from <https://www.thejakartapost.com/news/2014/06/05/indonesians-spend-most-time-smartphones-world.html>
- Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology*, 15(1), 79-94.
- Arimuladi, S. U. (2022). Access to Justice Based on Expert Testimony in Tax Crimes: An Integrated Criminal Justice System Perspective in Indonesia. *Pandecta Research Law Journal*, 17(1), 29-36. Retrieved from <https://journal.unnes.ac.id/nju/index.php/pandecta/article/view/32622>
- Asmara, T. T. P., Ikhwanasyah, I., & Afriana, A. (2019). Ease of Doing Business: Gagasan Pembaruan Hukum Penyelesaian Sengketa Investasi di Indonesia. *University of Bengkulu Law Journal*, 4(2), 118-136. <https://doi.org/10.33369/ubelaj.4.2.125-143>
- Balo, H. H. R., Wantu, F. M., & Tijow, L. M. (2020). System for Evidence of Corruption Criminal Act in Indonesia. *Asian Journal of Education and Social Studies*, 8(2), 46-55. Retrieved from <https://doi.org/10.9734/ajess/2020/v8i230222>
- Berting, N. (2019). *On the shrinking spaces of social media, in Indonesia and elsewhere* (Graduation Thesis). Willem de Kooning Academy (WDKA), The Netherlands. Retrieved from https://pzwiki.wdka.nl/mw-mediadesign/images/c/cf/Tash_1902.2_Thesis.pdf
- Boyle, P. (2020). *Indonesia's cyber war on West Papua solidarity*. Green Left Weekly, (1251), 13. <https://search.informit.org/doi/abs/10.3316/informit.934561010777204>
- Breitenbauch, H., & Byrjalsen, N. (2019). Subversion, statecraft and liberal democracy. *Survival*, 61(4), 31-41. <https://doi.org/10.1080/00396338.2019.1637118>
- Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., ... & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American journal of public health*, 108(10), 1378-1384. <https://ajph.aphapublications.org/doi/abs/10.2105/AJPH.2018.304567>
- Castellino, J. (2021). *International law and self-determination: the interplay of the politics of territorial possession with formulations of post-colonial 'national' identity*. BRILL.
- Chen, L. (2020). *Improving digital connectivity for e-commerce: A policy framework and empirical note for ASEAN*. Economic Research Institute for ASEAN and East Asia. <https://www.think-asia.org/handle/11540/11681>
- Clark, J., & Aufderheide, P. (2011). *A New Vision for Public Media*. In *Media and Social Justice* (pp. 55-67). Palgrave Macmillan, New York. https://doi.org/10.1057/9780230119796_5
- Dini, A. A., Sæbo, Ø., & Wahid, F. (2018). Affordances and effects of introducing social media within eParticipation—Findings from government-initiated Indonesian project. *The Electronic Journal of Information Systems in Developing Countries*, 84(4), e12035. <https://doi.org/10.1002/isd2.12035>
- Farsi, M., Daneshkhah, A., Far, A. H., Chatrabgoun, O., & Montasari, R. (2018). Crime data mining, threat analysis and prediction. In *Cyber Criminology* (pp. 183-202). Springer, Cham. https://doi.org/10.1007/978-3-319-97181-0_9
- Fernando, J. Z., Pujiyono, P., Rozah, U., & Rochaeti, N. (2022). The freedom of expression in Indonesia. *Cogent Social Sciences*, 8(1), 2103944. <https://doi.org/10.1080/23311886.2022.2103944>

- Fichman, P., & McClelland, M. W. (2021). The impact of gender and political affiliation on trolling. *First Monday*, 26(1). <https://doi.org/10.5210/fm.v26i1.11061>
- Gaidosch, T. (2018). The Industrialization of Cybercrime: Lone-wolf hackers yield to mature businesses. *Finance & Development*, 55(2), 22-26.
- Harahap, R. R. M., Munawir, Z., & Hidayani, S. (2019). Tinjauan Yuridis Penyelesaian Sengketa Atas Pemakai Kartu Kredit Tipe Gold Dengan Bank Penerbit Kartu Kredit (Studi Putusan No. 161/Pdt-G/2017/PN. Mdn). *JUNCTO: Jurnal Ilmiah Hukum*, 1(2), 136-142. <https://doi.org/10.31289/juncto.v1i2.210>
- Hodge, E., & Hallgrimsdottir, H. (2020). Networks of hate: the alt-right, "troll culture", and the cultural geography of social movement spaces online. *Journal of Borderlands Studies*, 35(4), 563-580. <https://doi.org/10.1080/08865655.2019.1571935>
- Horse, A. J. Y., Jeung, R., Lim, R., Tang, B., Im, M., Higashiyama, L., ... & Chen, M. (2021). *Stop AAPI hate national report*. Stop AAPI Hate: San Francisco, CA, USA. <https://stopaapihate.org/wp-content/uploads/2021/11/21-SAH-NationalReport2-v2.pdf>
- Howie, E. (2018). Protecting the human right to freedom of expression in international law. *International Journal of Speech-language Pathology*, 20(1), 12-15. <https://doi.org/10.1080/17549507.2018.1392612>
- Jurriëns, E., & Tapsell, R. (Eds.). (2017). *Digital Indonesia: connectivity and divergence*. ISEAS-Yusof Ishak Institute. <https://doi.org/10.1355/9789814786003>
- Lim, M. (2017). Freedom to hate: social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies*, 49(3), 411-427. <https://doi.org/10.1080/14672715.2017.1341188>
- Lindsey, T., & Pausacker, H. (Eds.). (2016). *Religion, law, and intolerance in Indonesia*. Routledge, Taylor & Francis Group. <https://doi.org/10.4324/9781315657356>
- Lubin, A., & Townley, H. (2020). The International Law of Rabble Rousing. 45 *Yale Journal of International Law Online* 1 (March 2020). <https://www.repository.law.indiana.edu/facpub/2907/>
- Manning, M., & Agnew, S. (2020). Policing in the era of AI and smart societies: austerity; legitimacy and blurring the line of consent. In *Policing in the Era of AI and Smart Societies* (pp. 59-82). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_2
- Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., ... & Karim, A. (2021). *Pengantar Forensik Teknologi Informasi*. Medan: Yayasan Kita Menulis.
- Manullang, S. O. (2020). The Declaration Content in Law of Electronic Transaction Information on Online Prostitution: In the Review of the Legal Sociology View. *International Journal of Social Sciences*, 3(1), 62– 70. <https://doi.org/10.31295/ijss.v3n1.151>
- Manullang, S. O. (2021a). Perubahan Sosial Masyarakat Pedesaan Di Era Teknologi. *Cross-border*, 4(1), 83-88.
- Manullang, S. O. (2021b). Kesadaran Masyarakat Dalam Memahami Undang Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik Dalam Media Sosial. *International Journal of Community Service and Development (INCOMMENT)*, 1(1), 10–20. Retrieved from <http://incomment.org/index.php/INCOMMENT/article/view/2>
- McGonagle, T., Bednarski, M., Francese Coutinho, M., & Zimin, A. (2019). *Elections and media in digital times*. UNESCO Publishing. <https://hdl.handle.net/11245.1/fa304e04-40bb-4519-b0db-f272de79b83f>

- Mietzner, M., & Muhtadi, B. (2018). Explaining the 2016 Islamist mobilisation in Indonesia: Religious intolerance, militant groups and the politics of accommodation. *Asian Studies Review*, 42(3), 479-497. <https://doi.org/10.1080/10357823.2018.1473335>
- Nehru, V. (2016). *Indonesia: The Reluctant Giant*. The National Interest, February 11. <https://carnegieendowment.org/2016/02/11/indonesia-reluctant-giant-pub-62745>
- Neyasyah, M. S. (2020, March). Legal Resilience in the Phenomenon of Social Media Political Buzzer in Indonesia. In *3rd International Conference on Law and Governance (ICLAVE 2019)* (pp. 338-344). Atlantis Press. <https://dx.doi.org/10.2991/aebmr.k.200321.044>
- Nugraha, L. K., & Putri, D. A. (2016). *Mapping the Cyber Policy Landscape: Indonesia*. London: Global Partners Digital.
- Nuryanti, S. (2020). Populism in Indonesia: Learning from the 212 Movement in Response to the Blasphemy Case against Ahok in Jakarta. In *Populism in Asian Democracies* (pp. 165-175). Brill. https://doi.org/10.1163/9789004444461_011
- Ong, J. C., & Tapsell, R. (2021). Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines. *Asian Journal of Communication*, 1-17. <https://doi.org/10.1080/01292986.2021.1971270>
- Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy*, 4(2), 216-234. <https://doi.org/10.1080/23738871.2019.1627476>
- Payne, B. (2018). White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?. *Criminology, Criminal Justice, Law & Society*, 19(3), 16-32. <https://www.proquest.com/scholarly-journals/white-collar-cybercrime-crime-both/docview/2164138515/se-2>
- Pujoyono, N. W. (2020). Penal Policy dalam Upaya Preventif Kejahatan Carding di Indonesia. *Jurnal Panji Keadilan: Jurnal Ilmiah Nasional Mahasiswa Hukum*, 3(1), 86-98. <https://doi.org/10.36085/jpk.v3i1.1183>
- Rajput, B. (2018). Identifying the challenges of criminal justice system while responding to cyber economic crime. *International Journal of Creative Research Thoughts*, 6(1), 146-155.
- Ramli, K. (2020). *Indonesia on the Move: Improving Connectivity to Support E-commerce*. E-commerce Connectivity in ASEAN, 31.
- Reichel, P. L. (Ed.). (2019). *Global Crime: An Encyclopedia of Cyber Theft, Weapons Sales, and Other Illegal Activities* [2 volumes]. ABC-CLIO.
- Roark, M. M. (2015) *Elonis v. United States: The Doctrine of True Threats: Protecting Our Ever-Shrinking First Amendment Rights in the New Era of Communication*. *Pittsburgh Journal of Technology Law & Policy*, 15. <https://doi.org/10.5195/tlp.2015.162>
- Sastramidjaja Y. & Wijayanto (2022). Cyber Troops, Online Manipulation of Public Opinion and Co-Optation of Indonesia's Cybersphere. *ISEAS - Yusof Ishak Institute. Issue 7*. <https://doi.org/10.1355/9789815011500>
- Schallbruch, M., & Skierka, I. (2018). Current Priorities and Gaps in German National Cybersecurity, Future Trends. In *Cybersecurity in Germany* (pp. 49-64). Springer, Cham. https://doi.org/10.1007/978-3-319-90014-8_5
- Setiawan, T., & Suhartomo, A. (2019, August). The relation between internet use and societal development in Indonesia. In *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)* (pp. 133-137). IEEE. <https://doi.org/10.1109/ICSECC.2019.8907127>
- Setti, S., & Wanto, A. (2019). Analysis of Backpropagation Algorithm in Predicting the Most Number of Internet Users in the World. *Jurnal Online Informatika*, 3(2), 110-115.

- Shah, T. S., & Taylor, C. H. (2021). The "Ashoka Approach" and Indonesian Leadership in the Movement for Pluralist Re-Awakening in South and Southeast Asia. *The Review of Faith & International Affairs*, 19(2), 56-71. <https://doi.org/10.1080/15570274.2021.1917149>
- Siregar, G., & Lubis, M. R. (2021). Juridical Analysis of Religious Blasphemy Crimes Through Smartphone Application Based On The Information and Electronic Transaction. *Journal of Contemporary Issues in Business and Government*, 27(2), 1006-1012. <http://dx.doi.org/10.47750/cibg.2021.27.02.120>
- Sommer, P. (1997). Downloads, Logs and Captures: Evidence from Cyberspace. *Journal of Financial Crime*, 5(2), 138-151. <https://doi.org/10.1108/eb025826>
- Syahputra, I. (2019). Expressions of hatred and the formation of spiral of anxiety on social media in Indonesia. *SEARCH Journal of Media and Communication Research*, 11(1), 95-112. <http://search.taylors.edu.my/>
- Tapsell, R. (2021). Social media and elections in Southeast Asia: The emergence of subversive, underground campaigning. *Asian Studies Review*, 45(1), 117-134. <https://doi.org/10.1080/10357823.2020.1841093>
- Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). *Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy*.
- Toha, R. J., Gueorguiev, D. D., & Sinpeng, A. (2021). The normalization of intolerance: The 2019 presidential election in Indonesia. *Electoral Studies*, 74, 102391. <https://doi.org/10.1016/j.electstud.2021.102391>
- Tyson, A. (2021). Blasphemy and judicial legitimacy in Indonesia. *Politics and Religion*, 14(1), 182-205. <https://doi.org/10.1017/S1755048319000427>

Tentang Penulis

Sardjana Orba Manullang memperoleh gelar Doktor Ilmu Hukum dari Universitas Parahyangan, Indonesia, pada tahun 2011. Penulis adalah dosen pada Program Studi Hukum, Fakultas Hukum, Universitas Krisnadwipayana, Indonesia.

Email: somanullang@unkris.ac.id