

BAB II

EKSTREMISME BERBASIS KEKERASAN YANG MENGARAH PADA TERORISME DAN KEAMANAN SIBER SOSIAL DI INDONESIA

2.1 Ekstremisme Berbasis Kekerasan Yang Mengarah Pada Terorisme Di Indonesia

Hingga masa modern sekarang ini, Pandemi COVID 19 dikombinasikan dengan operasi keamanan intensif dan dinamika internasional yang berubah, membuat sebagian besar organisasi teroris lokal kehilangan keseimbangan pasca tahun 2020. Di Indonesia, aksi penangkapan terduga teroris masih tinggi. Walaupun dengan tingkat kematian yang rendah. Beberapa upaya penyerangan, seperti pengeboman katedral Makassar pada Maret 2021, mengakibatkan luka-luka pada orang-orang di sekitar, tetapi tidak ada korban jiwa, selain pelaku bom bunuh diri itu sendiri (Jones, 2022). Kemudian terdapat juga penyerangan bom bunuh diri menjelang akhir tahun 2022 di Mapolsek Astanaanyar, Bandung, yang menyebabkan 1 Korban anggota polisi (Kompas.com, 2022). Selain itu, Seorang remaja Singapura yang ditangkap pada Desember 2020 tetap menjadi salah satu dari dua orang Asia Tenggara yang ditahan karena terpengaruh ideologi ekstremisme. Dia dilaporkan ingin menyerang dua masjid di Singapura pada hari peringatan penembakan Christchurch, Selandia Baru (batamnews.co.id, 2023). Memang, jika pihak berwenang Indonesia khawatir tentang pengaruh luar yang menjadi inspirasi untuk kekerasan di dalam negeri, sumbernya kemungkinan besar

adalah peristiwa-peristiwa internasional dan jaringan teroris yang mempengaruhi melalui media digital.

Yang terjadi di Indonesia saat ini adalah terus digunakannya undang-undang anti-terorisme tahun 2018 untuk “serangan pencegahan”, yang berarti bahwa saat COVID-19 melonjak pada bulan Juni dan Juli 2021 lalu, penjara di Indonesia kewalahan karena banyaknya narapidana baru. Jumlah tahanan yang bertambah banyak ini sebenarnya bukan cerminan dari peningkatan ancaman, melainkan peningkatan kekuatan polisi di bawah undang-undang anti-terorisme dan peningkatan jumlah petugas yang ditugaskan ke unit kontraterorisme. Lebih banyak kejahatan yang dapat dihukum berdasarkan undang-undang baru dan lebih banyak petugas yang melakukan penangkapan mengakibatkan meningkatnya jumlah tahanan secara langsung.

Pada November 2021, Indonesia memiliki lebih banyak tersangka dan narapidana terorisme di balik jeruji besi sejak fase terbaru terorisme global dimulai dengan serangan World Trade Center (Jones, 2022). Pada bulan Desember 2021 sendiri, lebih dari 1.000 orang berada di balik jeruji besi, dengan sekitar 370 ditangkap sejak Januari 2021 (CNN Indonesia, 2021a) dan 247 ditangkap sepanjang tahun 2022 (Rahmat & Ilham, 2023). Volume penangkapan ini sendiri sebenarnya tidak semata-mata karena undang-undang tahun 2018 tetapi juga efek dari birokrasi anti-terorisme yang bertambah. Namun meski dengan penguatan ini, masih ada masalah yang perlu diselesaikan. Seperti bagaimana Kepolisian RI telah disusupi oleh ideologi ekstremis berbasis kekerasan dan bagaimana beberapa anggotanya mendukung gerakan terorisme dengan memberikan senjata api dan amunisi

(Suradji, 2022). Sehingga perlu diamati kembali bagaimana ideologi-ideologi ini dapat dengan mudah mempengaruhi masyarakat Indonesia.

Operasi pengaruh di ruang digital pun menjadi salah satu faktor yang tidak bisa dipandang sebelah mata. Pada tahun 2022 sendiri, BNPT RI menemukan lebih dari 600 situs atau akun di berbagai platform media sosial dengan konten ekstremisme berbasis kekerasan yang juga menyebarkan lebih dari 900 konten propaganda (Detiksumut, 2022). Dengan melihat data tersebut saja, dapat dikatakan isu ini menjadi salah satu ancaman serius bagi negara.

2.2 Penyebaran Ideologi Ekstremisme Berbasis Kekerasan Yang Mengarah Pada Terorisme Di Ruang Digital Indonesia

Internet memainkan peran penting dalam penyebaran ideologi ekstremis berbasis kekerasan yang mengarah pada terorisme di Indonesia walaupun sebenarnya tidak dapat ditentukan dalam perjuangan sosiopolitik. Internet secara potensial dapat mendukung individu atau kelompok yang atau menganggap diri mereka terpinggirkan. Hal ini dapat dilihat dengan bagaimana internet memungkinkan kelompok-kelompok seperti Laskar Jihad dan JI untuk mengekspresikan pendapat mereka dan memperluas pengaruh mereka. Kedua kelompok ini mengungkapkan contoh bagaimana Internet dapat digunakan oleh organisasi fundamentalis radikal untuk memperkuat identitas dan ideologinya, memperluas jaringannya, dan menyebarkan informasi dan makna (Lim, 2005).

Potensi media sosial telah mendorong pernyataan optimis tentang pemberdayaan digital dan pembaharuan ruang publik. Oleh karena itu, orang yang menggunakan media sosial dapat meningkatkan pertukaran informasi, keterlibatan, mengubah partisipasi politik mereka, dan memfasilitasi transparansi jurnalisme. Namun, sisi negatif dari penggunaan media sosial di sisi lain adalah hilangnya privasi, menurunnya kualitas informasi, berkembangnya kebohongan (hoax), dan munculnya radikal online. Ada banyak perbedaan pendapat tentang bagaimana ideologi ekstremis berbasis kekerasan dapat diintegrasikan (atau gagal diintegrasikan) ke dalam pbingkaian wacana dan berita. Di Indonesia, pola ekstremisme berbasis kekerasan yang mengarah pada terorisme sangat erat kaitannya dengan media sosial, seperti yang diungkapkan mantan Kepala Badan Nasional Penanggulangan Terorisme (BNPT) Komjen (Komjen Pol) Suhardi Alius bahwa Hampir seluruh masyarakat Indonesia memiliki akses ke media sosial namun tidak disertai dengan kemampuan untuk mem-*filter* dengan baik sehingga menyebabkan cikal bakal ekstremisme berbasis kekerasan yang mengarah pada terorisme tersebar (Kementerian Komunikasi dan Informatika Republik Indonesia, 2019).

Penyebaran ideologi ekstremisme berbasis kekerasan yang mengarah pada terorisme di Indonesia sendiri dapat dikatakan cepat beradaptasi dengan perubahan di lingkungan teknologi global. Jika kita lacak, pelopor ekstremisme kekerasan online di Indonesia adalah pelaku bom Bali, Imam Samudra. Ketika kafe internet menjadi populer pada tahun 2000, dia bergabung dengan daftar Yahoo II yang berisi berita dari medan perang jihad lokal (kebanyakan di Ambon dan Poso)

(Nuraniyah, 2019). Hal ini menginspirasinya untuk membuat serangkaian situs web untuk mengklaim kredit atas operasi JI, dibantu oleh seorang teman telah belajar dari unit media AQ di Pakistan. Pada tahun 2004, setelah dipenjara karena bom Bali, Samudra merintis kelompok pengajian online melalui relay chat (mIRC) dan bereksperimen dengan penipuan kartu kredit. Salah seorang yang bergabung dalam chatroom mIRC Samudra adalah Tuah Febriwansyah, yang lebih dikenal dengan nama Fachry. seorang mantan anggota Hizbut Tahrir yang sangat dipengaruhi oleh Al-Muhajiroun Inggris melalui ceramah daring (Paltalk) oleh pemimpinnya, Omar Bakri Muhammad (R. Hidayat, 2016). Pada tahun 2007, Fachry dipekerjakan oleh Muhammad Jibril, putra seorang veteran jihad Afghanistan senior, untuk mengembangkan Arrahmah, situs berita jihad profesional pertama di Indonesia dengan staf bergaji dan update harian (Nuraniyah, 2019). Walaupun memang sebagian besar situs web dan blog jihadis di tahun 2000-an berfokus pada penyebaran ideologis dan meningkatkan kesadaran akan jihad global daripada berfungsi sebagai panduan teroris (IPAC, 2015).

2.2.1 Perkembangan

Dengan perkembangan tersebut disini dapat kita lihat beberapa implementasi dimana media sosial di Indonesia digunakan untuk kepentingan organisasi ekstremis berbasis kekerasan. Media sosial pada dasarnya memberikan dampak bagi ator-aktor ini untuk berkembang dengan menggunakannya untuk memobilisasi, merekrut, mempengaruhi dan melibatkan pemuda dalam jaringan terorisme. Dengan menonton film Jihad Selfie, remaja Aceh bernama Teuku Akbar Maulana (17 tahun) mengaku bahwa ISIS memiliki cara tersendiri dalam mendekati

remaja, salah satunya melalui media sosial (Kurniasih, 2019). Ia bahkan hampir bergabung sebagai anggota. ISIS sendiri menggunakan media sosial untuk menyebarkan ekstremisme dengan memanipulasi informasi. Bahkan para ahli mengatakan bahwa manipulasi informasi dipengaruhi oleh kecepatan internet atau jejaring sosial yang sebelumnya tidak ada, dan krisis kepercayaan terhadap demokrasi suatu negara (Vilmer et al., 2018). Manipulasi informasi yang dilakukan oleh ISIS diawali dengan mosi tidak percaya terhadap ISIS oleh negara-negara yang diharapkan dapat menjalankan pemerintahan sesuai dengan ajaran Al-Qur'an secara keseluruhan. Mosi ini kemudian diperhitungkan dengan membongkar kezaliman, korupsi, dan kezaliman yang dialami umat Islam. Pada gilirannya, narasi yang dimanipulasi diposting secara besar-besaran di media sosial. Internet mempercepat narasi untuk menyebar ke seluruh dunia. Akibatnya, orang mudah percaya dengan apa yang mereka baca, dan akhirnya memutuskan untuk bergabung dengan kelompok teroris atau melakukan aksi ekstremis yang berbasis kekerasan..

Dalam praktiknya sendiri, media sosial dan terorisme dapat dikatakan memiliki hubungan yang saling menguntungkan untuk mencapai tujuan politiknya masing-masing. Kelompok ISIS, misalnya, menggunakan media sosial untuk tujuan politik seperti menciptakan dan melatih teroris independen (*lone wolf*) dalam mencapai tujuan teror, yaitu menyebarkan ketakutan. Ia juga menggunakan media sosial untuk membuktikan keberadaannya dan mendapatkan pengakuan dari masyarakat internasional. Di Indonesia, media sosial sendiri cenderung riskan dalam penyebaran informasi terkait ekstremisme berbasis kekerasan yang

mengarah pada terorisme seperti insiden Bom Bali dan liputan penangkapan grup radikal yang terjadi di Sibolga (Monza, 2019).

Terkait aksi teror yang dilakukan remaja, postingan atau informasi di media sosial membuat mereka percaya akan ideologi yang mereka berikan dan akhirnya memutuskan untuk mengambil tindakan yang sama sebagai jalan pintas untuk memperjuangkan ketidakadilan yang mereka alami, seperti halnya di Indonesia. Hal ini bisa terjadi mengingat ISIS menggunakan media sosial untuk mempromosikan gerakan sosialnya dengan merepresentasikan kondisi masyarakat yang tertindas, namun tidak mendapatkan keadilan (A. Z. Huda et al., 2021).

2.2.2 Andil Pemerintah

Dengan adanya isu-isu ini, bentuk perlindungan dari pemerintah Indonesia untuk mengatasi penyebaran ekstremisme berbasis kekerasan yang mengarah pada terorisme adalah dengan menciptakan produk hukum yang sesuai. Salah satu bentuk produk hukumnya adalah dengan menerbitkan Peraturan Pemerintah Pengganti Undang-Undang (PERPU) Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme dan Perpu Nomor 2 Tahun 2002 tentang Pemberlakuan Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia. Kemudian dimutakhirkan dengan UU No. 5 Tahun 2018 tentang Perubahan atas UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang. Kemudian pada tahun 2010 pemerintah mengeluarkan Keputusan Presiden Nomor 46 Tahun 2010 tentang pembentukan Badan Nasional

Penanggulangan Terorisme (BNPT) sebagai pengembangan dari Desk Koordinasi Penanggulangan Terorisme (DKPT) yang dibentuk pada tahun 2002 (Sitinjak, 2021). Undang-undang anti terorisme ini diperlukan karena termasuk kejahatan luar biasa, maka penegakan hukum di Indonesia memerlukan tindakan luar biasa. UU Antiterorisme telah mengatur aspek materil dan formil, artinya merupakan *lex specialis* dari KUHP dan KUHPA.

Masyarakat sebenarnya diharapkan akan mendapatkan kenyamanan dalam berselancar di internet yang telah terpelihara dengan baik. Faktanya, kebebasan berekspresi dijamin oleh konstitusi dan undang-undang. Namun, penting untuk bijak dalam menggunakan media sosial dan menjalankan kebenaran atau informasi valid yang akan dibagikan kepada orang lain sebelum menjadi konsumsi publik yang masif. Selama tidak melanggar hak orang lain, berperilaku buruk, atau menyerang orang lain dengan fitnah, media sosial dapat digunakan dengan nyaman. Sisi negatif kebebasan ini menciptakan momentum atau peluang bagi para penganut ideologi radikal atau ekstrimis yang menggunakan haknya untuk menyampaikan pendapatnya di media sosial dengan menyebarkan informasi yang dapat mempengaruhi publik, hingga merekrut orang untuk mengikuti keyakinannya.

2.3 Perkembangan Ruang Digital di Indonesia

Dari berbagai contoh kasus dan kejadian-kejadian yang sudah dijelaskan, dapat dikatakan ekspansi dunia maya yang terjadi di Indonesia pasca pandemi Covid-19 dan pertumbuhan e-commerce yang sepadan telah menghadirkan banyak peluang, tetapi juga menimbulkan efek samping yang negatif. Semakin banyak

orang Indonesia yang mengakses teknologi smartphone murah dan terhubung ke internet, tantangan seputar privasi data pribadi, masalah kejahatan dunia maya, dan masalah disinformasi pun semakin bermunculan. Di lingkungan legislatif yang kerdil yaitu dunia maya Indonesia, oknum-oknum telah belajar bagaimana memanipulasi perangkat dunia maya untuk kepentingan mereka sendiri. Teknologi ini telah memungkinkan kelompok-kelompok Islam ekstremis untuk mengakses audiens yang jauh lebih besar daripada yang mungkin sampai sekarang, dan dengan demikian memproyeksikan Ekstremisme berbasis kekerasan yang mengarah pada terorisme dengan cara yang jauh lebih luas. Sementara pemerintah Indonesia telah mengambil langkah-langkah positif untuk memerangi masalah di dunia maya, ia juga mencoba memperkenalkan undang-undang baru yang kejam dan terlibat dalam sensor politik. Langkah-langkah ini sayangnya telah digunakan untuk menekan kebebasan berbicara dan lawan politik, serta menimbulkan ancaman besar bagi kesehatan dan reputasi demokrasi Indonesia. Ketika semua persoalan ini dipandang dalam bayang-bayang meningkatnya konservatisme Islam dan kecenderungan otoriter dalam politik Indonesia, muncul gambaran yang memprihatinkan. Oleh karena itulah suatu upaya konkret melalui perlindungan dunia maya itu sendiri, memerlukan perhatian lebih untuk mengikuti perkembangan Indonesia saat ini.

2.4 Keamanan Siber Sosial di Indonesia

Pada laporan terbaru dari National Cyber Security Index (NCSI), indeks keamanan siber Indonesia berada di peringkat ke-47 dengan 63.64 poin (National Cyber Security Index, 2023). NCSI menggunakan 12 indikator dalam laporan ini,

antara lain pengembangan kebijakan keamanan siber, perlindungan data pribadi, dan pemberantasan kejahatan dunia maya. Laporan tersebut menunjukkan bahwa masih terdapat beberapa hal yang harus dibenahi dari keamanan siber di Indonesia apabila dibandingkan negara lain. Di antara negara-negara anggota G20, Indonesia menduduki peringkat ketiga terbawah, hanya lebih tinggi dari Meksiko dan Afrika Selatan (Annur, 2022). Laporan NCSI dapat dibenarkan jika kita mempertimbangkan beberapa fakta tertentu di Indonesia. Seperti bagaimana pada tahun 2022 sendiri, terdapat 148 situs yang diretas oleh peretas. Website yang mereka retas beragam mulai dari situs pemerintah, aparat hukum, hingga situs pendidikan. Kasus peretasan website yang paling banyak terjadi adalah situs pemda sebanyak 62 kasus, disusul situs pendidikan sebanyak 54 kasus, lalu situs aparat hukum sebanyak 19 kasus, dan situs lainnya (Putra, 2023). Anomali lalu lintas yang tinggi, phishing email, dan peretasan situs web yang dijelaskan di atas menunjukkan kepada kita bahwa sistem keamanan siber Indonesia masih belum memadai untuk menghadapi serangan dunia maya yang merugikan orang dan keamanan nasional.

Salah satu contoh besar yang juga terjadi tahun ini adalah kampanye *doxing* dan kebocoran data secara besar-besaran yang dilakukan oleh peretas anonim atau tim peretas yang menggunakan alias “Bjorka” (Putri, 2023). Dimana data sensitif dari badan intelijen, badan usaha milik negara, bisnis, dan jutaan warga negara biasa terungkap. Kebocoran tersebut juga menyoroti masalah yang sedang berlangsung dengan dasar kelembagaan tata kelola keamanan siber. Hal ini terlihat dari kegagalan Badan Siber dan Sandi Negara (BSSN) Indonesia dalam mewujudkan visi dan mandatnya. Memang isu keamanan siber di Indonesia sangat

kompleks dan dapat dikaitkan dengan sejumlah faktor, termasuk kurangnya kemauan politik, persaingan antar lembaga, dan politik patronase. Variabel-variabel ini menghambat kemajuan landasan strategis, hukum, dan kebijakan keamanan siber Indonesia. Mereka juga dapat dikatakan mengikis profesionalisme birokrasi.

Walaupun begitu, masalah kejahatan siber dan disinformasi justru telah memaksa pemerintah Indonesia untuk lebih aktif dalam isu keamanan siber. Dimana hal ini juga meningkatkan kesadaran atas keamanan siber dari sisi sosial yang sebelumnya mungkin belum terjamah. Salah satu contohnya adalah Program CekFakta, sebuah proyek pengecekan fakta dan verifikasi yang diluncurkan oleh dua puluh dua perusahaan media dengan tujuan melatih jurnalis untuk memerangi misinformasi dan disinformasi (Sasmito, 2018). Dimana isu misinformasi dan disinformasi ini sendiri merupakan suatu bagian dari studi keamanan siber sosial. Inisiatif ini sendiri merupakan hasil kerjasama antara Google News, Asosiasi Media Siber Indonesia (AMCI), Masyarakat Anti Fitnah Indonesia (Mafindo), Aliansi Jurnalis Independen (AJI) dan Internews (Sasmito, 2018). Mafindo sendiri memiliki ratusan relawan, yang memantau internet dalam upaya untuk menemukan dan menyanggah tipuan sebelum mereka dapat memperoleh daya tarik (Clarissa, 2023). Dimana relawan-relawan tadi berupaya untuk mengidentifikasi peningkatan yang signifikan dari hoaks yang tersebar di ruang digital Indonesia. Walaupun upaya mereka tetap dipersulit oleh *buzzers* atau *cyber troll* yang dibayar untuk berbagi dan memperkuat hoaks menggunakan akun media sosial palsu. Dapat dikatakan beberapa dari prakarsa untuk memerangi disinformasi dan kejahatan dunia maya ini merupakan langkah positif yang dirancang untuk meningkatkan

transparansi dan literasi digital, ada banyak tindakan sewenang-wenang lainnya yang dilakukan yang tidak transparan dan bahkan mengancam supremasi hukum. Dimana contoh lainnya adalah operasi pengaruh di ruang digital. Dimana upaya Indonesia dalam menanggulangi hal ini akan dibahas pada bab selanjutnya melalui teori sekuritisasi.