JURNAL ADHIKARI
e-ISSN 2798-9186 ; p-ISSN 2798-9178
https://www.jurnal-adhikari.id/index.php/adhikari

NEXUS PENGAWASAN SIBER SEBAGAI INSTRUMEN KEAMANAN NASIONAL DAN RELEVANSINYA DENGAN DEMOKRASI: PERBANDINGAN BEBERAPA NEGARA

Anggi Anggraeni Kusumoningtyas
Dosen Program Studi Ilmu Pemerintahan Universitas Sutomo
email : anggianggraenik27@gmail.com

Paper Accepted: 2 Januari 2023
Paper Reviewed: 3-11 Januari 2023
Paper Edited: 12-23 Januari 2023
Paper Approved: 26 Januari 2023

ABSTRAK

Beberapa tingkat pengawasan dan kerahasiaan negara diperlukan untuk melindungi dari ancaman keamanan nasional. Akan tetapi, pengawasan siber dengan transparansi minimal mengancam hak-hak politik yang melekat pada nilai-nilai demokrasi jika tidak dilakukan sesuai dengan kriteria yang ketat. Penelitian ini berfokus pada perdebatan nexus pengawasan siber sebagai instrumen keamanan nasional dan relevansinya dengan demokrasi. Untuk mendapatkan hasil yang komprehensif, peneliti menggunakan metode kualitatif yang datanya dikumpulkan melalui studi pustaka dan analisis bukti dokumen. Adapun teori yang digunakan ialah teori dan infrastruktur pengawasan siber Lawrence Lessig, serta Jack Balkin dan Sanford Levinson dengan fenomena *national surveillance state*-nya. Kemudian peneliti juga menggunakan konsep demokrasi dan konsep keamanan nasional untuk mengkaji penggunaan pengawasan siber dalam kaca mata demokrasi sehingga menghasilkan perdebatan di antara keduanya. Dari hasil penelitian ini ditemukan hal-hal sebagai berikut: *Pertama*, komponen utama dari debat pengawasan siber dan demokrasi adalah kompetisi teknologi. *Kedua*, keseimbangan dalam praktik pengawasan siber dengan memperhatikan perlindungan data pribadi sebagai bagian dari hak asasi manusia harus dihasilkan oleh demokrasi.

Kata Kunci : Pengawasan Siber, Demokrasi, Keamanan Nasional, Teknologi Siber.

PENDAHULUAN

Latar Belakang

Di balik berbagai kemudahan dan manfaat yang didapatkan dari perkembangan teknologi siber, perdebatan selalu muncul terkait resiko yang dibawanya. Pemanfaatan ruang siber yang tidak mengenal batas negara, membuat penggunaan siber oleh suatu pihak yang merugikan pihak lain dapat dilakukan oleh aktor negara (*state actor*), maupun aktor bukan negara (*non-state actor*). Siber dapat menjadi ancaman bagi negara karena membawa resiko yang destruktif yang harus diantisipasi di antaranya dalam bentuk terorisme siber, serangan siber, dan perang siber. Pada akhirnya, siber yang memiliki potensi untuk menghasilkan pengetahuan, secara bersamaan juga digunakan oleh negara untuk mengendalikan dan/atau mengambil tindakan pencegahan terhadap berbagai kemungkinan ancaman.

Negara dan praktik pengawasan siber mempunyai hubungan yang saling berkelindan. Hubungan keduanya telah mengalami perubahan dari waktu ke waktu dan berubah secara cepat pada abad ke-21. Pemahaman bahwa pengawasan siber

merupakan bagian dari alat keamanan nasional, menempatkan negara sebagai pemain kunci (*key player*). Pengerahan infrastruktur pengumpulan data untuk menganalisis dan mengelola populasi dilakukan oleh negara sebagai salah satu agen pengawasan yang paling mapan (Kristie Ball, Kevin Haggerty, dan David Lyon eds., 2012: 16). Konvergensi teknologi siber telah memperluas secara signifikan kemungkinan untuk memantau, mengumpulkan dan mengklasifikasikan data pribadi (Anggi Anggraeni K, 2020: 41).

Para realis memandang pengawasan sebagai cara pengumpulan intelijen yang digunakan oleh negara-negara untuk memiliki keunggulan informasi atas musuh di dunia di mana survival adalah tujuan utama (Jensen, McElreath dan Graves, 2013: 44). Di sisi lain, kebebasan informasi berikut akses publik akan kebijakan informasi telah dianggap sebagai ciri khas negara demokrasi. Ayse Ceyhan (2012: 38) menjelaskan bahwa pengawasan juga berfungsi sebagai alat 'dispositif keamanan', yaitu untuk mendapatkan efisiensi maksimum dengan mengamati, mengklasifikasikan dan memilah individu-individu untuk mengatasi ketidakpastian (Ceyhan, 2012: 38).

Pengawasan siber sebagai bagian dari sekuritisasi pun kemudian semakin mendapatkan momentumnya pasca peristiwa serangan teror 11 September 2001 (9/11). Semenjak itu, berbagai negara di dunia meresponnya dengan memberikan penekanan kuat pada pengamanan dan pemanfaatan kemampuan ruang siber untuk mencegah serangan di masa depan (Knake, 2010; Radu, 2014: 13). Berbagai aktivitas keamanan atas nama anti-terorisme dilakukan di hampir segala aspek kehidupan sehari-hari dan sudah dianggap sebagai hal yang wajar dilakukan oleh negara. Semakin massifnya praktik pengawasan siber, semakin menimbulkan kecemasan, mengingat pengumpulan intelijen dapat melemahkan demokrasi serta menghambat pengembangan struktur demokrasi di negara-negara demokrasi baru jika tidak dilakukan sesuai dengan kriteria yang ketat.

Berdasarkan laporan *International Network of Civil Liberties Organizations* (INCLO) yang berjudul *Surveillance and Democracy: Chilling Tales From Around The World* (2013), Argentina, Kanada, Hongaria, India, Irlandia, Israel, Kenya, Rusia, Afrika Selatan, dan Amerika Serikat telah mengalami perluasan kekuatan dan kegiatan pengawasan dalam beberapa tahun terakhir (INCLO, 2013: 112). Penggunaan teknologi pengawasan siber untuk memantau percakapan para politisi oposisi di India dan pemberdayaan Ombudsman Irlandia untuk melakukan pengawasan terhadap kepolisian nasional Irlandia adalah beberapa contoh kasus terbukanya kerentanan di mana komunikasi dan institusi bergantung pada kerahasiaan. Dalam laporan *The International Network of Civil Liberties Organizations* (INCLO), pengawasan siber di negara-negara demokrasi baru seperti Argentina, Hongaria, Kenya, dan Rusia juga memberikan ancaman terhadap privasi dan keamanan data pribadi (INCLO, 2013: 113). Kekuatan pengawasan siber di negara-negara demokrasi baik negara demokrasi lama maupun baru, menggambarkan bahwa demokrasi selalu diuji dengan urgensi pengawasan siber sebagai instrumen keamanan nasional.

Badan-badan seperti *National Security Agency* (NSA) Amerika Serikat, GCHQ Inggris, atau BND Jerman adalah bagian dari jaringan intelijen transnasional yang mengumpulkan dan bertukar data dalam skala besar-dengan dan tanpa dukungan perusahaan teknologi. Di dalam badan-badan atau agensi ini, profesional keamanan yang memahami teknologi menggunakan analitik algoritmik untuk memahami set data besar, misalnya untuk menentukan apa yang dianggap sebagai perilaku mencurigakan, dan siapa yang warga negara atau bukan warga negara. Di bawah payung keamanan nasional dan aturan "pihak ketiga", pengawasan badan intelijen dan kolaborasi mereka secara tradisional terbatas. Sejak dua dekade terakhir, penggunaan teknologi siber dan peningkatan berbagi intelijen telah memperdalam kesenjangan antara pengawasan transnasional yang kompleks

di satu sisi dan sumber daya pengawasan nasional yang buruk di sisi lain (Aradau, Bigo, Hofmann, dan Wetzling, 2019: 1).

Dalam pengawasan siber skala besar dan terhubung secara transnasional oleh badan-badan intelijen, muncul pertanyaan jika kita perlu menafsirkan kembali hubungan kategori yang mendasari demokrasi modern seperti keamanan nasional, pengawasan, dan kebebasan sipil. Kekhawatiran atas pengawasan siber yang maju secara teknologi sering kali diterjemahkan ke dalam visi *dystopia* tentang nasib demokrasi (Aradau, Bigo, Hofmann, dan Wetzling, 2019: 1). Contohnya adalah referensi ke totaliterisme seperti cara George Orwell dalam novel 1984, dengan gagasan "*post democracy*", atau peringatan terhadap "*algocracy*" yang meningkat.

Dalam demokrasi modern, inti dari perdebatan pengawasan siber adalah persetujuan dan pengetahuan dari pihak yang datanya sedang disurvei dan manfaat keamanan, informasi, serta intelijen yang diperoleh dari pengawasan tersebut. Beberapa berpendapat bahwa negara telah menjadi penerima manfaat utama dari metode dan alat pengawasan baru dalam menjalankan mekanisme pengawasannya (Akin Unver, 2018: 3). China misalnya, baru-baru ini meluncurkan kacamata polisi yang melakukan analisis pengenalan wajah warga negara secara *real-time* untuk tujuan penegakan hukum. Rusia memiliki undang-undang *System for Operative Investigative Activities*/Sistem untuk Kegiatan Investigasi Operatif (SORM) yang memungkinkan pengawasan penuh atas komunikasi analog dan elektronik tanpa surat perintah. Negara-negara Amerika Serikat dan Uni Eropa melakukan berbagai tingkat pemantauan jaringan, analisis data massal, pengumpulan, dan katalog waktu-nyata untuk keperluan intelijen dan keamanan.

Oleh karena itu, dapat dikatakan bahwa fenomena saat ini menggambarkan baik negara demokrasi maupun otoriter sama-sama terlibat dalam praktik pengawasan dan sering menggunakan alat yang sebanding, meskipun dengan berbagai tingkat perlindungan hukum dan legislatif. Kekuatan pengawasan siber di negara-negara demokrasi menggambarkan bahwa demokrasi selalu diuji dengan urgensi pengawasan siber bagi keamanan nasional. Demokrasi sendiri saat ini memiliki interpretasi yang berbeda dan sering bersaing dengan kebijakan "rahasia keamanan nasional", yang diperlukan untuk melindungi berbagai operasi keamanan nasional yang penting.

Rumusan Masalah

Tanpa diikuti dengan mekanisme pengawasan dan perlindungan nilai-nilai demokrasi yang kuat, pelaksanaan pengawasan siber berpotensi menimbulkan praktik pengawasan massal terhadap warga negara. Demikian kurang lebih poin dari latar belakang di atas. Namun, perhatian peneliti di sini bukan pada dampak yang mungkin dari pengawasan terhadap privasi individu, melainkan tentang seberapa besar pengawasan dalam masyarakat yang demokratis. Dengan dasar pertimbangan sebagaimana diuraikan dalam permasalahan di atas, pokok permasalahan yang diteliti dalam penelitian ini adalah:

1. Bagaimana pengawasan siber dijalankan di berbagai negara?
2. Bagaimana resistensi pengawasan siber dalam kerangka keamanan nasional terhadap nilai-nilai demokrasi?

Signifikansi Penelitian

Telah cukup banyak penelitian yang mengangkat tema tentang pengawasan siber di berbagai negara. Beberapa di antaranya spesifik mengenai praktik pengawasan siber dalam kerangka keamanan nasional dan resistensinya terhadap privasi dan pelindungan data pribadi. Namun secara keseluruhan, belum ada yang secara khusus dan komprehensif membahas mengenai nexus pengawasan siber sebagai instrument keamanan nasional berhadapan dengan demokrasi. Demokrasi yang mensyaratkan transparansi dalam pelaksanaan pengawasan siber, juga menuntut penghormatan terhadap privasi.

Oleh karena itu, penelitian ini menemukan signifikansinya dengan melihat keseimbangan di antara keduanya –demokrasi dan pengawasan siber–yang menjadi penting untuk dicarikan titik temunya dengan berbagai perdebatan keamanan nasional di dalamnya. Selain itu, urgensi lain dari penelitian ini terletak pada penggunaan perbandingan beberapa negara dengan menggunakan konsep demokrasi dan keamanan nasional sehingga terdapat perbedaan dengan penelitian-penelitian sebelumnya.

TINJAUAN PUSTAKA

Konsep Demokrasi

Dalam teori politik, telah ditulis banyak karya tentang konsep demokrasi. Held (1996) menggambarkan republikanisme, demokrasi klasik, demokrasi liberal dan demokrasi langsung sebagai salah satu di antara model demokrasi yang telah lama berakar. Model yang lebih baru termasuk antara lain demokrasi elitis kompetitif, demokrasi pembangunan dan demokrasi partisipatif. Karya Dahl (1998) menggambarkan cita-cita dan realitas demokrasi. Pekerjaan penting lainnya menekankan hak-hak yang dijamin secara konstitusional, pemilihan umum yang bebas, dan supremasi hukum sebagai 'elemen minimal demokrasi', menambahkan tiga hak tambahan yang terkait dengan hak sosial (Fuchs, 1999). Beetham (1994) merujuk pada indeks demokrasi yang meliputi kebebasan dasar, kewarganegaraan dan partisipasi, kode administrasi, pemberitahuan publik dan hak sosial. Terlepas dari teori yang ada tentang konsep demokrasi, ada juga sejumlah besar penelitian sebelumnya, yang digunakan sebagai dasar dalam proses pembuatan dan identifikasi konsep demokrasi yang digunakan dalam penelitian ini.

Kebebasan dan demokrasi sering digunakan secara bergantian, tetapi keduanya tidak identik. Demokrasi memang merupakan seperangkat gagasan dan prinsip tentang kebebasan, tetapi juga terdiri dari serangkaian praktik dan prosedur yang telah dibentuk melalui sejarah panjang. Singkatnya, demokrasi adalah pelembagaan kebebasan. Karena alasan ini, adalah mungkin untuk mengidentifikasi dasar-dasar pemerintahan konstitusional, hak asasi manusia, dan kesetaraan yang teruji oleh waktu di muka hukum yang harus dimiliki oleh setiap masyarakat untuk disebut demokratis.

Demokrasi lebih dari sekadar seperangkat institusi pemerintah tertentu; demokrasi bersandar pada kelompok nilai, sikap, dan praktik yang dipahami dengan baik-yang semuanya dapat mengambil bentuk dan ekspresi yang berbeda di antara budaya dan masyarakat yang berbeda di seluruh dunia. Berikut adalah beberapa prinsip aturan demokratis modern. Prinsip aturan demokratis modern ini kadang disebut sebagai pilar, prinsip, atau prinsip-prinsip pemerintahan demokratis. Prinsip tersebut membedakan pemerintahan demokratis dari jenis pemerintahan lainnya.

Setiap demokrasi di seluruh dunia dapat dievaluasi berdasarkan prinsip-prinsip ini, yaitu termasuk: 1) Partisipasi warga negara; 2) Kesetaraan; 3) Toleransi politik; 4) Pertanggungjawaban; 5) Transparansi; 6) Pemilihan umum yang teratur, bebas, dan adil; 7) Kebebasan ekonomi; 8) Kontrol penyalahgunaan kekuasaan; 9) Bill of Rights; 10) Budaya menerima hasil pemilihan umum; 11) Hak Asasi Manusia 12) Sistem multi-partai 13) Netralitas lembaga negara; 14) *Rule of law* (Konrad-AdeneurStiftung, 2011: 4-6).

Konsep Keamanan Nasional

Keamanan adalah konsep yang telah berkembang seiring waktu. Oleh karena itu, konsep keamanan tetap menjadi istilah yang diperdebatkan tidak hanya di bidang akademik, tetapi juga dalam hubungan internasional (Diez, Bode dan da Costa, 2011: 193). Globalisasi, sepaket dengan nilai-nilai demokrasi dan Hak Asasi Manusia (HAM) yang dibawa telah membangkitkan kesadaran universal untuk menjunjung tinggi keamanan dan keselamatan manusia. Oleh karena itu, keamanan tidak lagi hanya berorientasi pada keamanan negara untuk menghadapi

ancaman tradisional yang mengandalkan kekuatan militer semata, akan tetapi juga ditujukan untuk menghadapi ancaman non tradisional yang disebabkan oleh faktor-faktor non militer, baik yang berasal dari dalam negeri maupun luar negeri. Apalagi di era globalisasi yang kian pesat ini, situasi dan kondisi insecurity lebih banyak disebabkan oleh ancaman-ancaman non tradisional berupa ancaman politik, ekonomi, sosial, dan lingkungan.

Menurut A. Grizold, keamanan nasional didefinisikan sebagai keamanan negara dan isinya meliputi wilayah keamanan nasional, perlindungan kehidupan dan properti orang, menjaga kedaulatan nasional dan pelaksanaan fungsi-fungsi dasar negara (Grozdanoska, 2014: 304). Meskipun kebijakan keamanan terkait dengan kebijakan pertahanan, keamanan mensyaratkan aspek kebijakan luar negeri yang lebih luas seperti kerja sama melalui PBB sebagai alternatif cara militer untuk memastikan kelangsungan hidup negara (Diez, Bode dan da Costa, 2011: 193). Konsep keamanan nasional yang semula hanya berorientasi pada state centered security, kini bergeser dan semakin meluas sehingga orientasinya mencakup state centered security dan people centered security atau konsep keamanan insani (human security) (Darmono dkk., 2010: 2). Dari pendekatan *state centered security*, kini menggunakan pendekatan partisipasi warga negara dan masyarakat (*civil society*) dalam melahirkan regulasi-regulasi keamanan. Pendekatan ini kemudian dikenal dengan *Security Sector Reform* (reformasi sektor keamanan).

Seorang ahli keamanan, Barry Buzan membagi sektor keamanan ke dalam lima bidang; militer, politik, lingkungan, ekonomi dan sosial. Sistem pertahanan dan keamanan itu sendiri harus diarahkan untuk menjamin tegak dan menguatnya suatu negara bangsa (nation state) dari "external threat" dan "domestic threat" (Mukhtar, 2011: 128). Lebih jauh lagi, Burhan D. Magenda menyebutkan tentang pentingnya memikirkan "software" yaitu terutama ideologi nasional serta sistem politik, ekonomi dan sosial budaya. Untuk "hardware", yang paling penting adalah lembaga-lembaga yang fungsional yang merupakan sumber daya nasional seperti aparatur negara, masyarakat, partai politik, masyarakat ekonomi dan masyarakat sipil. Adapun dimensi lain yang diperlukan dalam memperkuat pertahanan dan keamanan nasional adalah ketahanan pangan dan masalah energi. Berikut elemen untuk mengidentifikasi keamanan (Hofreiter, 2015: 9):

Tabel 1 Elemen Pengidentifikasian Keamanan

Security paradigm	Object of reference	Object of protection	Potential threats
Traditional security	The state	Integrity of the state independence military security	Military aggression, nuclear war
Sectoral security	Individuals, groups, states, humankind, civilizations	Military, political, economical, social, societal, environmental security	Military and non-military
Human security	Human being, an individual	Human and civil rights, freedom from fear, freedom from lack	Violence, crime, poverty, repression, hunger, disease, unemployment

METODE PENELITIAN

Untuk menjawab pertanyaan-pertanyaan penelitian, peneliti menggunakan metode penelitian kualitatif agar sesuai dengan tujuan dan kebutuhan penelitian ini. Penelitian kualitatif menurut Neuman dalam bukunya yang berjudul *Social Research Methods: Qualitative and Quantitative Approachers 7th Edition* (2014), berusaha untuk menginterpretasikan data dengan cara memberi arti dan analisis terhadap hasil data yang telah diperoleh selama penelitian berlangsung. Berdasarkan jenis penelitian, Neuman menggolongkan penelitian yang dilakukan sebagai penelitian desktriptif, yaitu penelitian yang fokus pada pertanyaan *who* dan *how*. Pada penelitian ini, peneliti membuat suatu gambaran kompleks, meneliti kata-kata, laporan terinci dari pandangan responden dan melakukan studi pada situasi yang alami (Iskandar, 2009: 11).

Pendekatan kualitatif berguna untuk mengeksplorasi suatu permasalahan atau isu agar pemahaman mengenai permasalahan tersebut menjadi lebih mendalam dan lengkap (Creswell, 2015:

63-64). Data dan fakta atas suatu permasalahan yang didapat kemudian diproses secara induktif, sehingga didapat suatu generalisasi dan gambaran atas permasalahan tersebut (Creswell, 2015: 61). Dalam penelitian kualitatif, peneliti adalah instrumen kunci. Oleh karena itu, peneliti harus memiliki bekal teori dan wawasan yang luas sehingga bisa bertanya, menganalisis, dan mengkonstruksi obyek yang diteliti menjadi lebih jelas.

Penelitian kualitatif digunakan jika masalah belum jelas, untuk mengetahui makna yang tersembunyi, memahami interaksi sosial, mengembangkan teori, memastikan kebenaran data dan meneliti sejarah perkembangan. Mengingat bahwa penelitian ini bertujuan untuk memahami dan memaknai fenomena yang ada atau yang terjadi dalam kenyataan sebagai ciri khas penelitian kualitatif serta mengembangkan teori. Dalam hal ini, bagaimana fenomena pengawasan siber yang dijalankan dalam kerangka keamanan nasional dan relevansinya dengan demokrasi, maka peneliti menggunakan penelitian kualitatif deskriptif.

Bodgan dan Taylor menjelaskan bahwa metodologi penelitian kualitatif merupakan prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati (Moleong, 2000: 5). Penelitian tentang *Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara* relevan dengan menggunakan penelitian kualitatif karena memenuhi karakteristik penelitian kualitatif. Metode penelitian yang digunakan dalam penelitian ini merupakan metode penelitian kualitatif dengan pendekatan studi kasus. Studi kasus dalam penelitian kualitatif ini berupaya untuk memahami fenomena yang terjadi dalam subyek penelitian yang diangkat. Peneliti menggambarkan fenomena nexus pengawasan siber sebagai instrument keamanan nasional secaraa umum terdahulu, kemudian melihat terlebih dahulu, sebelum pada akhirnya fokus pada perbandingan beberapa negara sebagai studi kasus. Adapun teknik yang digunakan dalam penelitian kualitatif, yaitu studi pustaka dan analisis bukti dokumen.

HASIL DAN PEMBAHASAN

Pengawasan Siber sebagai Instrumen Keamanan Nasional

Demokrasi sendiri saat ini memiliki interpretasi yang berbeda dan sering bersaing dengan kebijakan "rahasia kerahasiaan", yang diperlukan untuk melindungi berbagai operasi keamanan nasional yang penting dan kepentingan di luar negeri. Ilmuwan Politik Michael Colaresi (2014) dalam bukunya yang berjudul *Democracy Declassified: The Secrecy Dilemma in National Security*, berpendapat bahwa semua penggunaan dan penyalahgunaan kerahasiaan memerlukan "biaya kerahasiaan", yang harus dikeluarkan negara untuk dapat membuat sejumlah informasi rahasia. Biaya tersebut adalah enkripsi, infrastruktur fisik untuk menyimpan rahasia dan rangkaian hubungan kekuasaan yang rumit yang menjaga set informasi dari pengawasan publik (penegakan hukum, aparat intelijen, dan lain-lain), serta dari tangan musuh. Biaya-biaya ini umumnya ditimbulkan sehubungan dengan utilitas strategis negara: baik untuk mengantisipasi tindakan musuh, menipu musuh dan menekan kemampuan saingan selama masa krisis.

Satu-satunya jenis rezim di mana biaya kerahasiaan berbenturan dengan biaya audiens di sisi lain, adalah demokrasi (Akin Unver, 2018: 4). Hanya di negara demokrasi, setiap unit biaya yang dihabiskan untuk kerahasiaan, ada kekuatan balasan lain dari publik yang menyerukan transparansi jenis informasi yang negara coba rahasiakan. Menurut ilmuwan politik Michael Desch (2002), perbedaan antara bagaimana demokrasi dan negara-negara otoriter berurusan dengan kerahasiaan dan pengawasan sangat mirip, meskipun dalam demokrasi, biaya audiensi publik dan biaya pengadilan yang menciptakan perbedaan terbesar. Dalam sebuah demokrasi, kendala tentang bagaimana para pemimpin memproses kerahasiaan dan pengawasan dilembagakan melalui serangkaian lapisan saling terkait

yang keduanya mengisolasi rahasia dari publik (dan pengawasan musuh), sementara secara bersamaan memungkinkan masyarakat untuk menekan pemerintah ketika ada keraguan tentang penanganan informasi tersebut. Sementara "biaya transparansi" di negara-negara demokrasi yang harus dibayar oleh negara-negara tersebut untuk membuat rahasia tertentu tersedia untuk pengetahuan publik. Biaya transparansi berinteraksi dengan biaya kerahasiaan, dalam arti bahwa setiap rahasia yang dibuat pemerintah untuk tujuan demokratis, juga secara otomatis dibagi dengan musuh. Untuk mengimbangi biaya transparansi dari langkah-langkah tersebut, negara kemudian harus berinvestasi lebih jauh untuk membuat rahasia informasi baru, atau hal itu akan kehilangan keunggulan komparatif utama terhadap negara-negara pesaing.

Namun, tidak semua rahasia adalah rahasia keamanan nasional dan negara sering menyembunyikan data tata kelola penting dari publik yang tidak ada hubungannya dengan kode peluncuran rudal, atau lokasi pangkalan udara lepas pantai (Akin Unver, 2018: 4). Beberapa kerahasiaan sering mengambil bentuk penggunaan kerahasiaan milik negara dan alat pengintai untuk memata-matai kelompok oposisi, partai politik, atau warga negara meskipun tidak ada ancaman keamanan nasional. Hal ini sesuai dengan contoh yang dipaparkan pada bagian pendahuluan di atas, bahwa negara-negara Eropa Tengah dan Timur melaporkan ada peretasan dalam pemilu mereka dari beberapa tahun terakhir. Serangan masif pada tahun 2007 yang menyerang infrastruktur egovernment Estonia melumpuhkan banyak infrastruktur daring negara dan publik (McGuinness dalam BBC News, 2017). Georgia mengklaim bahwa Pemilu 2008 dan 2012 diretas oleh Rusia (Watson, dkk dalam CNN, 2016). Lalu pada Pemilu 2014, situs KPU mengalami peretasan dengan teknik *Distributed Denial of Service* (DDoS) yang menyebabkan situs KPU dan situs-situs sub-domainnya lumpuh.

Dilema bagi para pemimpin dan kelompok pembuat keputusan yang memproses informasi intelijen dan rahasia berasal dari persetujuan publik. Agar setiap kebijakan berhasil, harus ada persetujuan publik dan mobilisasi yang dihasilkan untuk pelaksanaannya. Demikian pula, sistem pengambilan keputusan yang demokratis menghilangkan kesalahan perhitungan atau kesalahan persepsi, memungkinkan penemuan awal dari kesalahan yang berpotensi mahal. Kelemahannya adalah bahwa sumber daya yang dihasilkan melalui metode yang kuat biasanya lebih rendah daripada sumber daya yang dihasilkan oleh demokrasi dan kecepatan sistem yang liberal.

Contoh dari Kanada dan Norwegia – negara-negara demokrasi teratas – mengungkapkan bagaimana penyalahgunaan kerahasiaan mengganggu semua jenis rezim. Pada tahun 1970-an, Komite Kajian Intelijen Keamanan Kanada/*Security Intelligence Review Committee* (SIRC) melaporkan pelanggaran pengawasan yang luas berupa pembobolan, pembakaran dan pencurian yang ditargetkan pada pers yang condong ke kiri dan partai-partai politik, di mana intelijen Kanada berbohong kepada Komisi Penyelidikan Menteri tentang sejauh mana program ini (Justin Ling, dalam VICE News, 2013). Melalui mekanisme penegakan, kelompok dan partai oposisi domestik secara sistematis diserang dan diganggu dengan kedok keamanan nasional. Di Norwegia, pelanggaran yang terjadi selama tahun 1970-an hanya dapat diungkapkan dalam laporan Komisi Lund pada tahun 1990-an (Hans dan Caparini, 2013: 145). Pelanggaran ini melibatkan polisi Norwegia, intelijen dan Otoritas Keamanan Nasional yang melakukan upaya bersama untuk memata-matai dan mengganggu kelompok-kelompok oposisi yang hanya memiliki sedikit pengaruh– jika ada–ancaman keamanan nasional, terbuka, atau eksplisit.

Penambangan data adalah salah satu alat yang disukai untuk melakukan pengawasan siber, yakni teknik statistik yang melibatkan pemrosesan otomatis volume data yang besar untuk mengekstraksi pola dan menghasilkan pengetahuan. Prosedur ini kemudian oleh

Gandy dikenal sebagai *Knowledge Discovery in Databases* (Gandy, 2002: 3). Penambangan aliran data menghasilkan klasifikasi yang merupakan taksonomi pengguna siber dan mengekstraksi pola yang terkait dengan kebiasaan, preferensi, dan perilaku setiap individu. Secara umum, data pada awalnya diklasifikasi berdasarkan kategori infra-individu (misalnya pengguna layanan, situs atau platform tertentu) dan tidak mengandung rincian pribadi yang akan mengidentifikasi individu yang menghasilkannya (misalnya nama, ID jumlah). Pola kemudian diekstraksi menggunakan mekanisme generasi aturan, yang paling umum adalah asosiatif (kesamaan, lingkungan dan persatuan) antara setidaknya dua elemen, yang kemudian membedakan antara jenis individu atau kelompok. Jenis ini sesuai dengan profil yang dihasilkan komputer yang diproduksi menggunakan teknik taksonomi yang dikenal sebagai profil, yang melengkapi penambangan data.

H. Akin Unver dalam jurnalnya yang berjudul *Politics of Digital Surveillance National Security and Privacy* menjelaskan bahwa pengawasan siber secara kasar dapat dibagi di seluruh domain keamanan data, pencitraan, TIK, geolokasi dan iometrik (Akin Unver, 2018: 5). Karena sebagian besar alat ini berasal dari praktik intelijen sinyal tradisional, tujuan utamanya adalah untuk mencegat komunikasi eksternal dan domestik, transfer data, dan pemantauan jaringan. Produk sampingan utama dari booming industri pengawasan dalam beberapa dekade terakhir adalah munculnya 'Kompleks Pengawasan-Industri' (Ball dan Snider, 2013). 'Kompleks Pengawasan-Industri/*Surveillance-Industrial Complex'* (SIC) berasal dari konsep kompleks militer-industri/*Military-Industrial Complex* (MIC) pasca Perang Dunia II. MIC pasca PD II menunjukkan hubungan simbiosis antara angkatan bersenjata suatu negara dan perusahaan-perusahaan produksi senjata pribadi. Argumen yang mendukung hubungan tersebut adalah peningkatan produksi militer dan keberlangsungan industri senjata besar yang responsif terhadap kebutuhan militer negara yang selalu berubah. SIC mengikuti logika yang sama, meskipun hubungan antara perusahaan teknologi dan pemerintah tidak saling menguntungkan seperti di MIC.

Sebaliknya, SIC mengacu pada badan-badan keamanan dan intelijen negara yang memasuki hubungan ekstraktif sepihak dengan perusahaan teknologi dan pengawasan sektor swasta. Negara memanfaatkan-sering kali secara ekstrayudisial - sejumlah besar data warga yang diproses oleh perusahaan swasta dan memegang kekuasaan penegakan hukum untuk "mengarahkan" perusahaan-perusahaan teknologi ini sesuai keinginan negara. Akses lembaga negara ke basis data sektor swasta menciptakan masalah hukum dan demokrasi, karena sebagian besar negara telah mengumpulkan banyak sekali data swasta warga negara sebelum diundangkannya undang-undang yang membatasi luasnya praktik pengawasan tersebut. Kecepatan berkembangnya teknologi pengawasan, membuat undangundang baru dengan cepat menjadi usang, memungkinkan lembaga untuk menghindari hukum dan undang-undang untuk menggunakan bentuk-bentuk baru dari pengawasan siber.

Dalam lingkungan teknologi saat ini, SIC memungkinkan ukuran dan granularitas data pribadi yang belum pernah terjadi sebelumnya, menjadikan pemerintah sebagai pusat jaringan informasi pribadi yang luas. Di sisi lain, bagaimanapun, SIC menciptakan dilema keamanan atas jangka panjang dengan membuat negara lebih defensif dan lebih kuat dalam membutuhkan data dan sistem lokalisasi. Sementara aliran bebas data dan informasi dianggap penting untuk perdagangan, keuangan, dan keterkaitan global, intrusi badan intelijen dunia ke dalam chokepoint transfer data (sistem cloud, kabel serat optik bawah air) telah meningkatkan permintaan lokalisasi.

Dengan melokalisasi sistem dan data, negara berusaha untuk menekankan 'nasionalisme data' dengan mencegah pengintaian oleh lembaga asing atau mengamankan data nasional mereka jika terjadi pengambilan data massal. Namun lokalisasi, menjadikan data tersebut semakin rentan terhadap serangan dunia maya dan meningkatkan biaya

perlindungan data dengan mensyaratkan pembangunan sistem penyimpanan fisik dari awal, merekrut aset manusia yang sangat terlatih, dan membangun jaringan perlindungan penyimpanan. Sementara lokalisasi data adalah langkah yang tidak diinginkan secara internasional, yang memperlambat perdagangan, transfer, dan keuangan, semakin banyak negara menganggap lokalisasi perlu mengingat pemaparan data warga negara utama ke badan intelijen asing.

Praktik Pengawasan Siber di Amerika Serikat, Cina, Rusia, Uni Eropa, dan Asia

Meskipun sejarah pengawasan sudah cukup tua, penelusuran yang berarti dari perdebatan pengawasan dan interkoneksi yang modern bisa kembali ke pengaturan keamanan pasca 9/11. Hal ini sebagian besar pasca-9/11 praktik pengawasan siber (seperti pengumpulan metadata massal, pengawasan biomedis dan intersepsi jaringan) bermula. Banyak dari program-program AS di era George W. Bush dan langkah hukum-legislatif untuk menjadikannya di bawah legitimasi telah memengaruhi negara-negara Eropa, dan memberikan contoh penting dan standar perilaku negara untuk negara-negara lain di dunia.

Di Amerika Serikat, Badan Keamanan Nasional (NSA) mulai mengumpulkan dan menyimpan panggilan telepon, email, dan aktivitas digital warga negara AS tanpa surat perintah menyusul pelonggaran perlindungan pengamanan yang sah setelah Undang-Undang Patriot Amerika Serikat tahun 2001. Praktik semacam itu –di bawah program Bushera berjudul 'Stellarwind' (L. Altheid, 2014: 1-7) –dilakukan sebagian besar tanpa sepengetahuan publik, Pada tahun 2008, Kongres membawa program tersebut di bawah yurisdiksi Undang-Undang Pengawasan Intelijen Asing/*Foreign Intelligence Surveillance Act* (FISA), yang menguraikan prosedur hukum AS untuk pemrosesan data pengawasan fisik dan elektronik yang terkait dengan aktor negara eksternal dan individu yang diduga melakukan spionase dan terorisme.

Sejak itu, Bagian 702 FISA ("memungkinkan pemerintah untuk mendapatkan komunikasi orang asing di luar Amerika Serikat, termasuk ancaman teroris asing") berada di bawah peningkatan kontroversi dan debat politik (FISA Section 702). Undang-undang tersebut melegalkan akses agen-agen AS ke perusahaanperusahaan Lembah Silikon, di samping memperluas akses yang ada ke perusahaan-perusahaan telekomunikasi, untuk keperluan 'operasi intelijen asing' yang didefinisikan secara luas. Adapun titik balik paling kritis dalam debat privasipengawasan adalah kebocoran 'Snowden' NSA 2013 (IEE Security Privacy 11, 2013: 54-63; Greenwald dan Ackerman, 2013; The Guardian, 5 Oktober 2015).

Meskipun pemaparan rahasia negara menjadikan Snowden musuh publik di AS, di seluruh dunia, pengungkapan ini telah memulai momentum global yang signifikan untuk pembangunan norma dan hukum. Hal ini mengantarkan periode baru inisiatif privasi yang dipimpin warga, munculnya alat pengelakan baru dan tekanan signifikan pada badan legislatif untuk mendemokratisasi dan melegitimasi kegiatan mata-mata. Hal ini juga menyebabkan status quo baru ketidakpercayaan timbal balik dan dilema keamanan intelijen antara negara-negara - dan bahkan sekutu NATO - yang mengambil langkah-langkah untuk meningkatkan kemampuan pengawasan mereka baik untuk kompetisi antar negara, serta untuk pemantauan domestik kegiatan intelijen digital asing.

Saat ini AS, Rusia dan Cina memaksa perusahaan teknologi untuk membuat 'pintu belakang' (WIRED, 2018) yang akan memungkinkan badan intelijen untuk menghindari enkripsi dan kata sandi pengguna untuk mengakses informasi pada perangkat. Perusahaan-perusahaan teknologi AS juga di bawah tekanan Cina untuk membuka kode sumber mereka untuk ditinjau. Dari sudut pandang Cina, audit kode sumber ini diperlukan untuk menghindari kemungkinan 'perangkat lunak matamata' AS yang diintegrasikan ke

dalam perangkat ini (Lee, dalam BBC News, 2015). Narasi Washington di sisi lain, adalah bahwa AS tidak tertarik untuk menambahkan pintu belakang ke ekspor teknologi yang terikat Cina, tetapi khawatir tentang bagaimana proses audit semacam itu dapat menekan perusahaan teknologi untuk menginstal spyware Cina ke perangkat buatan AS (Ben Goad, dalam TheHill, 2015). Dilema spyware ini adalah alasan mengapa sebagian besar negara pengekspor teknologi telah menciptakan versi mereka sendiri dari proses backdoor atau proses audit kode sumber dalam ekspor teknologi dan impor. Demikian pula, NSA dan GCHQ telah menggunakan kapal selam untuk memanfaatkan kabel serat optik bawah laut untuk mencegat dan memanen komunikasi internet global.

Sulit untuk menarik garis yang jelas antara praktik pengawasan AS dan orang-orang dari rezim otoriter. Satu-satunya perbedaan adalah arah peraturan. Di sebagian besar negara demokrasi, kebocoran dan penemuan praktik pengawasan non-negara memicu perlunya pengawasan hukum, sedangkan di negara-negara otoriter, persyaratan intelijen menentukan tingkat pengawasan, di mana persyaratan keamanan nasional - bukan kebutuhan pengawasan - mendorong arah undangundang. Di Rusia misalnya, Sistem Operasional-Investigasi Tindakan (SORM) telah lama menjadi dasar pengawasan yang sah dari komunikasi digital dan jaringan telekomunikasi (Soldatov dan Borogan, dalam The Guardian, 2015).9 Secara hukum, SORM memungkinkan lembaga pengawasan untuk melacak dan menyimpan metadata tanpa surat perintah. Bahkan ketika lembaga memiliki surat perintah, SORM tidak memiliki tanggung jawab untuk menampilkan surat perintah kepada ISP target atau perusahaan, tetapi hanya untuk keperluan audit intraagensi.

Sebaliknya, sistem pengawasan Cina sebagian besar didorong oleh perselisihan Tibet dan Xinjiang-Uighur (Phillips dalam The Guardian, 2018). Hukum pengawasan Cina serupa dengan Rusia dalam hal arah persyaratan hukum (yaitu hukum yang didorong oleh kebutuhan keamanan). Cina juga mendorong 'pengawasan sosial', di mana warga negara diminta untuk membantu lembaga pemerintah dalam memantau pelanggaran dan aktivitas siber yang mencurigakan (Mitchell dan Diamond, dalam The Atlantic, 2018). Beberapa persyaratan hukum terbaru adalah daftar nama asli wajib untuk unggahan video online, pelaporan yang dibuat pemerintah dan aplikasi pengaduan yang memungkinkan warga Cina untuk mengambil bagian dalam pengawasan nasional, sistem kredit sosial - yang 'membuat peringkat' perilaku sosial warga negara, pengumpulan dan katalogisasi data bio-medis massal, basis data pengenalan wajah real time dan pemantauan berbasis *artificial intelligent* (AI) di negara tersebut dari 20 juta kamera CCTV (Botsman dalam WIRED UK, 2017). Pada 28 Juni 2017, Cina (sekarang Tiongkok) mengeluarkan Undang-Undang Intelijen Nasional yang baru, yang menciptakan kewenangan hukum yang luas untuk Kementerian Keamanan Nasional dan Biro Keamanan Internal dari Kementerian Keamanan Publik untuk mengumpulkan setiap dan semua data digital warga dan data perusahaan, tanpa surat perintah apa pun (Reuters, 2017).

Dibandingkan dengan AS, Cina dan Rusia, negara-negara Uni Eropa mengikuti jalur yang sedikit berbeda. Lima belas tahun setelah penandatanganan perjanjian 'Safe Harbor' 2000 (2000/520/EC), kesepakatan berbagi data yang memungkinkan transfer hukum informasi pribadi warga negara Uni Eropa dan data publik ke Amerika Serikat. Pada tahun 2015, Uni Eropa mengeluarkan keputusan di mana pengungkapan Snowden tentang pengawasan massal ekstra-yudisial membuat tidak mungkin untuk memastikan bahwa data tersebut akan cukup dilindungi ketika dibagikan dengan mitra AS. Hal ini menciptakan kesenjangan yang signifikan antara AS dan UE, di mana UE berusaha untuk melindungi yang pertama dari intrusi pengawasan yang tidak sah ke dalam arsitektur data pribadi Eropa.

Di negara-negara Asia, dunia siber adalah ranah pengawasan. Siber digunakan untuk tujuan represif dan tidak illiberal, dan pengawasan adalah norma dengan kemunculannya sebagai "media untuk komersial, manajemen, pemolisian, dan

kegiatan pemerintah" (Lyon, 2013 dalam James Gomez, 2004: 143). Pengawasan siber dilakukan baik oleh pemerintah maupun perusahaan. Pemerintah Korea Selatan, Jepang, Singapura dan Hong Kong, misalnya, mewajibkan penyedia layanan internet untuk menyimpan informasi tentang pengguna dan untuk membantu lembaga penegak hukum melacak kegiatan online mereka (James Gomez, 2004: 143). Di Jepang, UU Intersepsi Komunikasi disahkan pada Agustus 1999, yang memungkinkan aparat penegak hukum mengakses akun email pribadi pada saat menyelidiki jenis kejahatan tertentu (Williams, 2000). Secara hukum, Otoritas Komunikasi Thailand/ *Communications Authority of Thailand* (CAT) memiliki saham minimum 32 persen di semua ISP swasta. Selain itu, Komite Teknologi Informasi Nasional Thailand/ National IT Committee (NICT) telah memerintahkan ISP untuk menyimpan data koneksi tentang pelanggan mereka selama setidaknya tiga bulan. Hal ini akan memungkinkan jaksa penuntut untuk bertindak terhadap mereka yang masuk ke situs web yang tidak diinginkan dan hal tersebut akan mendorong otoritas pemerintah untuk memblokir situs tersebut (Reporters Without Borders, 2002, dalam James Gomez, 2004: 144).

Demikian pula, perangkat genggam seperti ponsel juga harus diawasi. Di Singapura, pelaku tipuan bom yang tidak disengaja melalui sistem pesan singkat ponsel (SMS) dilacak dalam waktu dua minggu setelah kejadian. Hal ini dilakukan oleh polisi dengan kerjasama dari ketiga perusahaan telekomunikasi - Tarhub, M1 dan SingTel. Semuanya menyimpan pesan SMS di server atau database mereka, untuk jangka waktu mulai dari dua hari hingga beberapa minggu, sebelum dihapus (The New Paper, 2002, 2004 dalam James Gomez, 2004: 144). Polisi memiliki kekuatan untuk memaksa perusahaan telekomunikasi untuk menyerahkan informasi dalam database mereka (The New Paper, 2002, dalam James Gomez, 2004: 144). Di bawah Undang-Undang Telekomunikasi, warga negara yang bersalah karena mengirimkan tipuan bom dapat didenda hingga $ 50.000, dipenjara hingga tujuh tahun, atau keduanya (Soh dan Dawson, 2002). Pemerintah otoriter mengutip 'keamanan nasional' atau 'ketertiban internal', dan perusahaan membenarkan tindakan pemerintahan tersebut dalam hal 'pelumas mekanisme pasar' (James Gomez, 2004: 144). Karenanya, pengawasan siber dipromosikan sebagai 'perlu' untuk 'mempertahankan negara kuat dan mengembangkan pasar'. Akuntabilitas dan perlindungan privasi, bagaimanapun, tidak memadai (Lyon, 2003).

Sejumlah model berbeda telah digunakan untuk "mengatur" teknologi dan praktik pengawasan, termasuk regulasi oleh pemerintah nasional (eksekutif, legislatif, dan yudikatif); organisasi ekstra pemerintah; perjanjian internasional; dan pengaturan sendiri oleh industri. Dua model yang muncul selama ini: beberapa negara mengadopsi pendekatan perlindungan data dan yang lainnya pendekatan kebebasan sipil (Flaherty 1989; Bennett 1992; Regan 1995). Pendekatan perlindungan data memandang masalah sebagai salah satu pertanggungjawaban dan tanggung jawab pihak organisasi yang mengumpulkan dan menggunakan informasi yang dapat diidentifikasi secara pribadi. Solusinya kemudian dibingkai dalam hal menempatkan persyaratan prosedural untuk dan mekanisme pengawasan pada organisasi-organisasi ini. Pendekatan kebebasan sipil memandang masalah tersebut sebagai salah satu kemungkinan pelanggaran hak-hak individu dalam konteks pengungkapan informasi kepada organisasi dan penggunaan selanjutnya dari informasi tersebut oleh organisasi. Solusi dalam model ini dibingkai dalam hal memberikan individu hak-hak hukum yang dengannya mereka dapat menemukan informasi yang dapat diidentifikasi secara pribadi yang dikumpulkan dan penggunaan serta pertukaran informasi tersebut, serta mekanisme pengaduan yang dengannya mereka dapat menantang praktik dan kualitas informasi organisasi. Inti dari kedua pendekatan ini adalah kerangka kerja "prinsip informasi yang adil"; kedua pendekatan tersebut berbeda terutama dalam hal apakah prinsip-prinsip ini akan

ditegakkan oleh pengawasan pemerintah atau oleh masing-masing penanganan keluhan (Regan dalam Kirstie Ball, Kevin D. Haggerty dan David Lyon ed., 2012: 398).

Nexus Pengawasan Siber sebagai Instrumen Keamanan Nasional dan Relevansinya dengan Demokrasi

Nexus pengawasan siber sebagai instrumen keamanan nasional dan relevansinya dengan demokrasi dapat dilihat baik dari tingkat nasional, maupun internasional. Di tingkat nasional, sisi negara dari debat mendukung penggunaan pengawasan siber sebagai bagian dari strategi keamanan nasional dan komponen-komponennya seperti kontraterorisme, kontranarkotika, profil kriminal dan sebagainya (Cole dan Lederman, 2006: 1355-1426). Terutama dengan meningkatnya ancaman terorisme, radikalisasi sayap kanan dan kelompok-kelompok ekstremis yang muncul di masyarakat barat, pengawasan siber tidak hanya dipandang perlu secara politis, tetapi juga populer secara elektoral (Baum dan Groeling, 2009: 157-186).

Sisi masyarakat dari perdebatan tersebut, terutama berkaitan dengan tingkat dan cakupan pengawasan (seberapa banyak pengawasan terlalu banyak) dan mekanisme pengawasan hukum dan legislatif apa yang digunakan untuk mencegah penyalahgunaan dan mendapatkan persetujuan publik. Di sisi lain, meskipun ada legitimasi yang lebih besar dari mekanisme perlindungan gaya 'kunci ganda' di Inggris, model-model seperti itu menunda pemrosesan intelijen dan menyebabkan badan-badan kehilangan kecerdasan kritis. Pemerintah biasanya percaya bahwa keterlambatan pemrosesan intelijen yang menghasilkan serangan aktual menciptakan biaya publik/audiens yang jauh lebih besar, dibandingkan dengan praktik pengawasan kejam yang tidak populer, tetapi perlu (Monaghan dan Walby, 2012: 133-151).

Namun, dilema ini tidak semudah yang dibahas dalam arus utama, karena perdebatan tidak terbatas pada ranah hubungan negara-masyarakat. Pemangku kepentingan lain dalam debat tersebut adalah agen intelijen asing yang bersaing untuk mendapatkan informasi dan akses, serta mengancam aktor non-negara dari kelompok militan hingga peretas (Richards, 2012: 761-780). Pengawasan siber menjadi praktik global, tidak hanya karena memberikan keuntungan terhadap kelompok-kelompok teroris dan jaringan kriminal, tetapi juga mencegah lembaga intelijen tunggal mana pun untuk memiliki akses yang tidak proporsional ke data pengawasan dan membangun 'monopoli intelijen siber global'. Artinya, jika sebuah agen intelijen tunggal memiliki kemampuan untuk memproses dan menyimpan volume data yang sangat besar dibandingkan dengan agen-agen lain, hal ini memungkinkan agen monopoli untuk mempersenjatai data tersebut dalam bentuk spionase siber atau diplomasi yang kuat terhadap negara lain. Oleh karena itu, lembaga lain memperluas kemampuan pengawasan mereka secara eksponensial untuk melakukan hal yang sama, menciptakan 'dilema keamanan' yang khas di ruang siber dengan implikasi pada transparansi dan kerahasiaan. Sudut persaingan intelijen internasional inilah yang mencegah sebagian besar pemerintah terlibat dalam diskusi publik mengenai pengawasan siber.

Di samping itu, ada biaya yang melekat dari pengawasan siber, terutama untuk rezim demokratis. Demokrasi bekerja berdasarkan premis transparansi informasi, di mana masyarakat memiliki hak untuk memantau, mengevaluasi, dan memberikan suara untuk kebijakan pemerintah (Ronald J dan Rafal, 2010: 15-32). Logika demokrasi adalah bahwa proses pembuatan kebijakan yang lebih transparan dan terencana dengan baik memiliki kemungkinan kegagalan yang lebih rendah karena kesalahan perhitungan dan kesalahan persepsi, karena dimasukkannya beragam pandangan dalam proses tersebut. Selain itu, karena publik dan perwakilan publik memiliki pengetahuan dan pengawasan yang lebih besar atas praktik pemerintah, pemerintah yang demokratis juga cenderung tidak mampu menutupi korupsi, kesalahan dan memanipulasi statistik, secara signifikan mengurangi limbah pemerintah (Bennett dan Lyon, 2008). Sistem otoriter, karena

pemerintah mengecualikan dan mencegah sebagian besar pandangan dari proses pembuatan kebijakan berdasarkan ideologi atau identitas, masuk ke dalam perang yang lebih mahal, mengeluarkan biaya hangus yang lebih besar dan memiliki kemungkinan lebih besar untuk terjebak dalam perselisihan jangka panjang dengan negara tetangga. Lebih jauh, karena pemerintahan otoriter dapat secara andal menahan kebijakan utama, pengeluaran dan informasi penunjukan dari publik dengan alasan 'keamanan nasional'. Pemerintahan otoriter cenderung lebih boros dalam hal mengelola kemampuan manusia dan material.

Baik negara demokrasi maupun otoriter tidak dapat sepenuhnya mengabaikan pengawasan atau privasi yang melekat pada prinsip-prinsip demokrasi. Bahkan pemerintah yang paling transparan terlibat dalam praktik pengawasan luas yang tidak selalu tercakup sepenuhnya di bawah pengawasan hukum atau mekanisme perlindungan (Matthew C. dan James A., 2013: 941-955). Demikian pula, bahkan negara yang paling otoriter harus menjaga kemiripan kebebasan berekspresi dan privasi sehingga represi tidak mengarah pada pemberontakan habis-habisan. Apa yang benarbenar memisahkan doktrin pengawasan demokrasi dan rezim otoriter di sisi lain, adalah masalah persetujuan publik. Di negara-negara demokrasi, publik dapat menyingkirkan pemimpin yang menyalahgunakan kekuasaan pengawasan dan menyalahgunakan aparat kerahasiaan negara melalui pemilihan umum yang bebas dan adil; sebuah kemewahan yang tidak dimiliki warga rezim otoriter. Lebih jauh, negara demokrasi memiliki undang-undang kebebasan informasi yang memungkinkan warga negara untuk mengawasi pemerintahan mereka dalam jangka panjang. Negara demokrasi juga memiliki komite legislatif yang berfungsi sebagai jembatan antara warga dan mekanisme kerahasiaan politik dan pers bebas yang dilindungi yang dapat membangun jaringan di dalam dan di sekitar negara untuk pemantauan publik berkelanjutan.

Dengan demikian, mekanisme pengawasan merupakan batu pengunci mendasar dari perdebatan demokrasi-pengawasan. Lembaga-lembaga semacam itu dirancang untuk membangun dan memantau perlindungan dengan pemerintah dan bertindak sebagai jembatan persetujuan publik untuk kebijakan pengawasan/kerahasiaan (Gorman, 2017). Mekanisme pengawasan juga memastikan bahwa penyalahgunaan monopoli kerahasiaan pemerintah dapat dihukum oleh publik melalui biaya publik atau perilaku pemilihan umum. Namun gagasan membangun perlindungan terhadap praktik pengawasan di negara-negara demokrasi dapat menjadi masalah pelik, terutama ketika negara-negara demokrasi tersebut menghadapi krisis keamanan nasional yang akut. Kanada, Swedia, Norwegia, dan Belanda misalnya, telah membentuk pengamanan yang sangat kuat yang membatasi sejauh mana kekuatan pengawasan pemerintah mereka. Adapun Amerika Serikat, Prancis, Yunani, Italia, dan Irlandia belum dikarenakan sebagian besar sedang menghadapi masalah keamanan yang luas. Di Prancis, tidak adanya perlindungan telah menyebabkan skeptisisme yang luas terhadap hukum pengawasan pasca Bataclan dan menghasilkan perlawanan terhadap persyaratan layanan militer. Dalam kasus Amerika Serikat dan Inggris misalnya, ekses agen pengawasan dan kemampuan mereka untuk menyembunyikannya dari mata publik telah menyebabkan banyak kebocoran yang menyatakan perbedaan pendapat internal terhadap kekuatan-kekuatan luas ini.

Pengawasan adalah persaingan antara pembuat keputusan (atau kelompok pengambil keputusan) yang berusaha untuk membuat keputusan yang cepat dan hasil maksimal yang akan meningkatkan popularitas, status dan otoritas, dan masyarakat sipil yang lebih luas yang bertujuan untuk mencegah penyalahgunaan, jangkauan dan ekstra-yudisial perilaku selama pembuatan kebijakan. Untuk itu, eksekutif selalu melihat pengawasan sebagai beban yang tidak perlu yang memperlambat proses

pengambilan keputusan, terutama yang berkaitan dengan risiko tinggi dan kejadian yang dibatasi waktu seperti perang, protes atau serangan teroris.

Kemajuan teknologi modern membuat perlombaan antara lembaga pengawasan dan mekanisme pengawasan menjadi tidak adil, dengan keunggulan jelas dimiliki oleh lembaga pengawasan. Dengan kapabilitas teknologi yang ditingkatkan, agensi jauh lebih mampu menyembunyikan detail rumit dari praktik pengawasan mereka dan jumlah rahasia yang mereka simpan, menyebabkan mekanisme pengawasan untuk mundur dan tumbuh lebih lambat dari waktu ke waktu. Bahkan di negara demokrasi seperti Inggris, mekanisme pengawasan yang lambat mencegah publik dan Komite Intelijen dan Keamanan Parlemen Inggris/*The Intelligence and Security Committee of Parliament* (ISC) untuk memahami dengan baik ruang lingkup dan kedalaman praktik pengawasan GCHQ - masalah yang ada dalam proporsi yang lebih besar di AS (Evans, 2018).

Dalam beberapa tahun terakhir, Kanada, Belgia, Kroasia, Norwegia, Swedia, dan Belanda telah membuat kemajuan signifikan dalam menciptakan pakar, badan pengawas yang dipimpin oleh warga sipil yang ada di samping komite keamanan formal nasional (Goldman dan Rascoff, 2016). Sementara sebagian besar contoh Eropa, Swedia dan Kanada menciptakan komite independen hibrid, di mana para ahli teknis sipil duduk bersama legislator. Kegunaan badan-badan independen ini adalah penyampaian detail teknis yang lebih cepat kepada legislator itu sendiri, daripada semua komite legislatif yang secara teknis tidak cakap. Suatu standar yang ditetapkan oleh Komite Tinjauan Intelijen Belgia, yang menerjemahkan semua laporan pengawasannya ke dalam Bahasa Inggris dan menerbitkan semua data pengawasannya secara online untuk penggunaan negara-negara lain dan warga negara Belgia (Boring, 2016). Data tersebut dibuat untuk umum dan dalam bahasa Inggris, karena komite percaya bahwa pengawasan adalah masalah transnasional yang hanya dapat diselesaikan melalui mekanisme kerjasama internasional, antar-legislatif.

Namun seperti halnya pemilihan yang bebas dan adil dianggap bermakna karena adanya pengawasan dan kebebasan informasi, kebalikannya juga berlaku: mekanisme pengawasan dapat bekerja, hanya ketika pemilu benar-benar kompetitif dan bebas. Tren global baru-baru ini menghasilkan pandangan pemilih yang bermasalah di mana demokrasi yang menghasilkan kecenderungan tidak liberal semakin bergantung pada kecurangan, persekongkolan atau penggunaan ancaman tersirat. Agar segala bentuk pengawasan bekerja, termasuk pengawasan siber, negara-negara harus memiliki pemilihan yang berarti dan mekanisme informasi sehingga publik dapat secara andal memantau dan menghukum pemerintah (baik secara elektoral atau melalui biaya audiensi) dalam kasus penyalahgunaan.

KESIMPULAN DAN SARAN

Kesimpulan

Pengawasan siber berkembang dan berubah seiring dengan kemajuan teknologi siber; semakin cepat kemajuan teknologi, semakin mudah untuk melakukan pengawasan dan menggunakan alat pengelakan terhadapnya. Kecanggihan alat pengelakan pengawasan siber sebagian karena pembaharuan teknologi, tetapi sebagian besar karena tidak adanya kontrak sosial dan hukum politik yang kuat antara negara, perusahaan teknologi dan warga negara atas tingkat dan kedalaman praktik pengawasan. Defisit demokratis dan hukum telah memaksa warga untuk menjaga pertahanan mereka sendiri ketika menyangkut prinsip-prinsip demokrasi. Menghadapi pengawasan kontemporer memerlukan pengakuan bahwa tindakan negara terkait erat dengan tindakan pribadi, dan sebaliknya. Fokus berlebihan pada negara sebagai ancaman utama terhadap demokrasi juga mengabaikan potensi "tirani sosial".

Kekuatan pengawasan siber di negara-negara demokrasi menggambarkan bahwa demokrasi selalu diuji dengan urgensi pengawasan siber bagi keamanan

nasional. Demokrasi sendiri saat ini memiliki interpretasi yang berbeda dan sering bersaing dengan kebijakan "rahasia keamanan nasional", yang diperlukan untuk melindungi berbagai operasi keamanan nasional yang penting. Satu-satunya jenis rezim di mana biaya kerahasiaan berbenturan dengan biaya audiens (transparansi) di sisi lain, adalah demokrasi. Hanya di negara demokrasi, setiap unit biaya yang dihabiskan untuk kerahasiaan, ada kekuatan balasan lain dari publik yang menyerukan transparansi. Dilema bagi para pemimpin dan kelompok pembuat keputusan yang memproses informasi intelijen berasal dari persetujuan publik. Agar setiap kebijakan berhasil, harus ada persetujuan publik dan mobilisasi yang dihasilkan untuk pelaksanaannya.

Pengawasan siber dengan transparansi minimal mengancam hak-hak politik yang melekat pada nilai-nilai demokrasi, jika tidak dilakukan sesuai dengan kriteria yang ketat. Dalam *zeitgeist* ketidaktenangan karena terus-menerus dipantau, negara, warga negara dan perusahaan teknologi sama-sama rentan terhadap berbagai aspek pengawasan. Hal ini menghasilkan simpul dari tata kelola siber, yang memiliki implikasi global, regional dan nasional dari politik, ekonomi dan sosial, serta memaksa semua pihak untuk melakukan sensor diri dan membatasi kebebasan bereskpresi. Pelanggaran kepercayaan atau kerahasiaan dapat dikenakan kompensasi setelah fakta dalam konteks di mana pengawasan dan pendistribusian data terkait telah terjadi secara tidak sah. Kekhawatiran atas pengawasan siber yang maju secara teknologi sering kali diterjemahkan ke dalam visi d*ystopia* tentang nasib demokrasi kita.

Dengan demikian, peneliti menyimpulkan bahwa peran hukum dalam regulasi pengawasan negara dan pengembangan struktur regulasi yang secara efektif melindungi prinsip-prinsip demokrasi berupa privasi individu dan kolektif. Hukum memiliki peran sentral dalam menentukan batasan privasi individu dan menetapkan standar yang harus dipenuhi baik oleh sektor publik yang dijalankan oleh negara maupun sektor swasta ketika keduanya terlibat dalam segala bentuk pengawasan siber. Namun, tidak bisa juga hanya menaruh terlalu banyak kepercayaan pada kapasitas hukum dalam mengawasi negara, karena sebagian disebabkan oleh masalah yang ditimbulkan oleh pengaturan teknologi baru. Bahkan undang-undang yang paling maju dan berwawasan ke depan dapat dengan cepat menjadi usang dalam menghadapi perubahan teknologi yang sangat cepat. Sebagai akibatnya, kontrol yang efektif terhadap pengawasan siber negara memerlukan pendekatan yang beranekaragam untuk regulasi yang tidak hanya mengacu pada aturan substantif dan ancaman sanksi, akan tetapi juga memberikan peran penting pada solusi teknologi.

Pada akhirnya, demokrasi harus menghasilkan keseimbangan demokrasi-pengawasan yang sesuai dengan budaya politik negara, juga dengan hak asasi manusia universal. Tugas pengawasan dalam konteks ini berat. Pengawasan siber harus terus mengejar komunitas eksekutif dan intelijen dalam mendeteksi penyalahgunaan dan kelebihan kewenangan, sambil tetap mahir secara teknologi pada saat yang sama. Mekanisme pengawasan warga negara akan gagal untuk menyeimbangkan jika warga negara tertinggal di belakang perkembangan teknologi. Oleh karena itu, evaluasi perluasan lebih lanjut dalam aparatus pengawasan dan penilaian mendasar atas penggunaan teknologi pengawasan siber negara menjadi penting bagi tiap-tiap negara demokrasi.

Saran

Melindungi demokrasi di era siber ini memerlukan tindakan di beberapa bidang: penyebaran luas dan tanpa batasan enkripsi kuat dan alat anonimitas; reformasi hukum dan kebijakan dalam negeri; menghormati standar internasional; dan perlindungan pelapor yang mengungkap informasi kepentingan publik seperti bukti pelanggaran hak asasi manusia.

DAFTAR PUSTAKA

Altheide, David L. "The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 4, no. 1 (January 1, 2014): 1–7. https://doi.org/10.4018/ijcwt.2014010101.

Aradau, Claudia, Luis Lobo-Guerrero, dan Rens Van Munster. "Security, Technologies of Risk, and the Political: Guest Editors' Introduction." *Security Dialogue* 39, no. 2–3 (April 1, 2008): 147–54. doi:10.1177/0967010608089159.

Ball, Kirstie and Laureen Snider, eds. (2013). *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. Abingdon, UK: Routledge.

Baum, Matthew A., dan Tim Groeling. "Shot by the Messenger: Partisan Cues and Public Opinion Regarding National Security and War." *Political Behavior* 31, no. 2 (June 1, 2009): 157–86. https://doi.org/10.1007/s11109-008-90749.

BBC/Panorama, Source: "Edward Snowden: GCHQ Wants to Own Your Phone – Video." The Guardian, October 5, 2015, sec. US news. http://www.theguardian.com/us-news/video/2015/oct/05/edward-snowdengchq-wants-own-your-phone-video, diakses pada 9 Desember 2022 pukul 21.03 WIB.

Bennett, Colin J., Kevin D. Haggerty, David Lyon dan Valerie Steeves, eds. (2014). *Transparent Lives: Surveillance in Canada*. Edmonton, AB: Athabasca University Press.

Bennett, Colin J., dan David Lyon, eds. (2008). *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. 1 edition. London, New York: Routledge.

Boring, Nicolas. "Foreign Intelligence Gathering Laws: Belguim." Web page, June 2016. https://www.loc.gov/law/help/intelligence-activities/belguim.php, diakses pada 8 Januari 2023, pukul 19.00 WIB.

Born, Dr Hans, dan Ms Marina Caparini. (2013). *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Ashgate Publishing, Ltd.

Botsman, Rachel. "Big Data Meets Big Brother as China Moves to Rate Its Citizens." WIRED UK, October 2017. http://www.wired.co.uk/article/chinese-government-social-credit-scoreprivacy-invasion, diakses pada 9 Desember 2022, pukul 19.00 WIBCeyhan, Ayse. (2012). *"Surveillance as Biopower." Dalam Routledge Handbook of Surveillance Studies*, disunting oleh Kirstie Ball, Kevin D. Haggerty, dan David Lyon, 38–45. New York: Routledge.

Cole, David, dan Martin S. Lederman. "The National Security Agency's Domestic Spying Program: Framing the Debate Document." *Indiana Law Journal* 81 (2006): 1355–1426.

Creswell, John W. (2015). *Penelitian Kualitatif dan Desain Riset: Memilih di antara Lima Pendekatan*, terj. Ahmad Lintang Lazuardi. Yogyakarta: Pustaka Pelajar.

Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News. 27 April 2017. https://www.bbc.com/news/39655415, diakses pada 9 Desember 2022 pukul 09.00 WIB.

Darmono, Bambang. (2010). *Konsep*. Jakarta: Jurnal Ketahanan Nasional XV (1).

Deibert Ronald J., dan Rohozinski Rafal. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (March 7, 2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Diez, Thomas, Ingvild Bode, dan Aleksandra Fernandes da Costa. (2011). *Key Concepts in International Relations*. Los Angeles, London: SAGE Publications Ltd.

Evans, Hayley. "Summary: U.K. Intelligence and Security

Committee Annual Report." *Lawfare*, January 4, 2018. https://www.lawfareblog.com/summary-uk-intelligence-and-securitycommittee-annual-report, diakses pada 8 Januari 2023 pukul 09.00 WIB.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, dan Marisol Sandoval, eds. 2011. Internet and Surveillance: The Challenges of Web 2.0 and Social Media. New York: Routledge, 2011.

Fuchs, Christian. "New Media, Web 2.0 and Surveillance." Sociology Compass 5, No. 2 (2011): 134–47.

Goad, Ben. "New Pressure on US Tech to Comply with China's Access Demands." Text. TheHill, October 16, 2015. http://thehill.com/policy/cybersecurity/257194-new-pressure-on-us-techto-comply-with-chinas-access-demands.

Goldman, Zachary K., dan Samuel J. Rascoff. (2016). *Global Intelligence Oversight: Governing Security in the Twenty-First Century*. Oxford: Oxford University Press Gomez, James. (2004). "Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia", Monash Asia Institute, Monash University, *Pacific Journalism Review* 10 (2) 2004.

Gorman, Siobhan. "Reengineering Surveillance Oversight." *Lawfare*, September 6, 2017. https://www.lawfareblog.com/reengineering-surveillance-oversight, diakses pada 8 Januari 2023 pukul 12.30 WIB.

Greenwald, Glenn, dan Spencer Ackerman. "How the NSA Is Still Harvesting Your Online Data." the Guardian, June 27, 2013. http://www.theguardian.com/world/2013/jun/27/nsa-online-metadatacollection, diakses pada 9 Desember 2022 pukul 11.00 WIB.

Grozdanoska, Natasha. (2014). National Defence and Security. *European Scientific Journal* February 2014/SPECIAL/edition vol.1 ISS: 1857.

Heywood, Andrew. (1997). *Politics*. Macmillan: England.

Iskandar. (2009). *Metodologi Penelitian Kualitatif*. Jakarta: Gaung Persada.

Ivan Watson, Antonia Mortensen, & Victoria Butenko, "Ex-Soviet states tell US 'I told you so' over Russia hacking allegations," CNN. 16 Desember 2016. https://edition.cnn.com/2016/12/16/politics/russia-hackingallegations-mikheil-saakashvili/index.html, diakses pada 9 Desember 2022.

Jensen, Carl J., David H. McElreath, dan Melissa Graves. (2013). *Introduction to Intelligence Studies*. Boca Raton: CRC Press.

Kristie Ball, Kevin Haggerty, dan David Lyon (Eds.). (2012). *Routledge Handbook of Surveillance Studies*. New York: Routledge.

Knake, Robert K. (2010). *Internet Governance in an Age of Cyber Insecurity*. New York: Council on Foreign Relations.

Ladislav Hofreiter. (2015). *About Security in Contemporary World*. Slovakia: Securitologia No. 1/2015.

Lee, Dave. "China and US Clash over Backdoors." BBC News, March 4, 2015, sec. Technology. http://www.bbc.com/news/technology-31729305, diakses pada 9 Desember 2022 pukul 16.00 WIB

Ling, Justin. "The Story of How Canadian Police Committed Arson to Stop a Black Panther Meeting." VICE News, June 2017. https://news.vice.com/en_ca/article/eva8da/story-of-how-canadianpolicecommitted-arson-to-stop-a-black-panther-meeting, diakses pada 9 Desember 2022 pukul 19.00 WIB.

Mitchell, Anna, and Larry Diamond. "China's Surveillance State Should Scare Everyone." The Atlantic, February 2, 2018. https://www.theatlantic.com/international/archive/2018/02/chinasurveillance/552203/, diakses pada 9 Desember 2022 pukul 22.00 WIB.

Monaghan, Jeffrey, dan Kevin Walby. "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression." Policing and Society 22, no. 2 (June 1, 2012): 133–51. https://doi.org/10.1080/10439463.2011.605131.

Moleong, Lexy J. (2000). *Metodologi Penelitian Kualitatif*. Bandung: Remaja Rosdakarya.

Phillips, Tom. "China Testing Facial-Recognition Surveillance System in Xinjiang – Report." the Guardian, January 18, 2018. http://www.theguardian.com/world/2018/jan/18/china-testing-facialrecognitionsurveillance-system-in-xinjiang-report, diakses pada 9 Desember 2022 pukul 12.23 WIB.

Reuters, China Passes Tough New Intelligence Law." Reuters, June 28, 2017. https://www.reuters.com/article/us-china-securitylawmaking/china-passes-tough-new-intelligence-lawidUSKBN19I1FW, diakses apda 9 Desember 2022 pukul 17.07 WIB.

Richards, Julian. "Intelligence Dilemma? Contemporary Counter-Terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (October 1, 2012): 761–80. https://doi.org/10.1080/02684527.2012.708528.

Soldatov, Andrei, and Irina Borogan. "Inside the Red Web: Russia's Back Door onto the Internet–Extract. "the Guardian, September 8, 2015. http://www.theguardian.com/world/2015/sep/08/red-web-book-russiainternet, diakses pada 9 Desember 2022 pukul 10.30 WIB.

Unver, H. Akin. "Politics of Digital Surveillance, National Security and Privacy, Oxford CTGA & Kadir Has University", *Centre for Economics and Foreign Policy Studies* (edam), Cyber Governance and Digital Democracy 2018/2. dan Sistem Keamanan Nasional Indonesia

Williams, M. J. "(In) Security Studies, Reflexive Modernization and the Risk Society." Cooperation and Conflict 43, no. 1 (March 1, 2008): 57–79. doi:10.1177/0010836707086737.

Williams, Nik. "The Cost of Silence: Mass Surveillance & SelfCensorship." openDemocracy, April 6, 2015. https://www.opendemocracy.net/nik-williams/cost-of-silence-masssurveillance-selfcensorship, diakses pada 8 Januari 2023 pukul 11.00 WIB.

Wilson Matthew C., and Piazza James A. "Autocracies and Terrorism: Conditioning Effects of Authoritarian Regime Type on Terrorist Attacks." American Journal of Political Science 57, no. 4 (June 3, 2013): 941–55. https://doi.org/10.1111/ajps.12028.