ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

'ADALAH
Buletin Hukum & Keadilan

Hak Privasi vs Kepentingan Negara dalam Pengawasan Siber: Menemukan Keseimbangan Konstitusional di Era *Digital Panopticon*

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.51169

Abstract:
The tension between citizens' privacy rights and state cyber surveillance has become a major constitutional issue in the digital era. This article analyzes the constitutional limits of state surveillance and explores a balance between security interests and democracy. Using normative legal research with conceptual, statutory, and comparative approaches, the study finds that Indonesia's cyber surveillance framework lacks proportionality, judicial oversight, and accountability. Regulations under the ITE Law and Intelligence Law grant broad discretion without adequate due process safeguards. The article recommends stronger judicial supervision, limiting executive discretion, and establishing a special supervisory court chamber.

Keywords: *Privacy Rights, Cyber Surveillance, State Interests, Proportionality, Due Process.*

A. PENDAHULUAN

Privasi telah lama diakui sebagai salah satu pilar hak asasi manusia yang fundamental. Ia adalah perisai yang melindungi martabat dan otonomi individu dari intervensi yang tidak sah. Namun, hak ini tidak pernah bersifat absolut. Negara, dalam menjalankan fungsinya, memiliki kewajiban untuk menjaga keamanan nasional, ketertiban umum, dan penegakan hukum. Untuk itu, negara diberikan kewenangan untuk melakukan pengawasan, yang dalam konteks digital dikenal sebagai pengawasan siber (*cyber surveillance*). Ketegangan antara hak privasi dan kepentingan negara dalam pengawasan siber membentuk dilema klasik yang terus bergulir: sejauh mana negara boleh mengintip warga negaranya demi alasan keamanan tanpa menjelma menjadi negara pengawas (*surveillance state*) yang totaliter?

Kemajuan teknologi telah memperlebar kemampuan negara untuk melakukan pengawasan. Alat-alat seperti *Deep Packet Inspection* (DPI), pengenalan wajah (*facial recognition*), dan perangkat lunak mata-mata seperti Pegasus memungkinkan negara mengumpulkan data dalam jumlah masif, bahkan tanpa sepengetahuan warga yang menjadi target. Fenomena ini digambarkan oleh para pemikir hukum sebagai *Digital Panopticon*, sebuah penjara virtual di mana individu selalu merasa diawasi, meskipun mereka tidak dapat melihat atau

mengetahui siapa yang mengawasi (Zuboff, 2019). Dalam kondisi seperti ini, hak privasi tidak hanya terancam oleh korporasi, tetapi juga oleh negara yang seharusnya menjadi pelindungnya.

Di Indonesia, kewenangan pengawasan siber tersebar di berbagai instrumen hukum. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Intelijen Negara, Undang-Undang Terorisme, serta Rancangan Undang-Undang Keamanan dan Ketahanan Siber semuanya memberikan ruang bagi pemerintah untuk mengakses data pribadi. Sayangnya, kerangka hukum ini tidak disertai dengan mekanisme pengawasan yang ketat dan akuntabel. Ketiadaan batas yang jelas antara kewenangan pengawasan yang sah dan pelanggaran privasi menjadi sumber ketidakpastian hukum dan ancaman bagi hak konstitusional warga negara (Asshiddiqie, 2021). Rumusan masalah artikel ini adalah: Pertama, bagaimana pengaturan dan praktik pengawasan siber di Indonesia dalam kaitannya dengan hak privasi? Kedua, bagaimana kerangka keseimbangan ideal antara hak privasi dan kepentingan negara dapat dirumuskan dalam sistem hukum nasional? Tujuannya adalah untuk mengkritisi kerangka normatif yang ada dan menawarkan model keseimbangan yang demokratis dan konstitusional.

B. PROPORSIONALITAS DAN DOKTRIN *DUE PROCESS* DALAM PENGAWASAN

Untuk menilai legitimasi pengawasan siber, doktrin hukum HAM dan tata negara menyediakan dua instrumen analitis utama: prinsip proporsionalitas dan doktrin *due process of law.* Prinsip proporsionalitas menuntut agar setiap pembatasan terhadap hak asasi oleh negara memenuhi empat syarat kumulatif: (1) adanya tujuan yang sah (*legitimate aim*), (2) kesesuaian atau kelayakan sarana (*suitability*), (3) keharusan atau tidak adanya alternatif yang lebih ringan (*necessity*), dan (4) keseimbangan antara manfaat dan kerugian (*proportionality stricto sensu*) (Barak, 2012). Pengawasan siber yang dilakukan tanpa batas waktu, tanpa target yang spesifik, dan tanpa dasar kecurigaan yang rasional jelas akan gagal dalam uji proporsionalitas ini.

Sementara itu, doktrin due process mensyaratkan bahwa perampasan hak warga negara, termasuk privasi, harus melalui prosedur hukum yang adil dan transparan. Dalam konteks pengawasan siber, ini berarti bahwa tindakan seperti penyadapan, penggeledahan data, atau pembajakan enkripsi (*encryption backdoor*) tidak boleh dilakukan semata-mata atas perintah eksekutif, melainkan harus melalui otorisasi yudisial yang independen. Hakim harus bertindak sebagai penjaga gerbang (*gatekeeper*) yang memastikan bahwa

pengawasan benar-benar diperlukan dan sesuai dengan koridor hukum (Solove, 2021).

Di tingkat internasional, Manfred Nowak sebagai Pelapor Khusus PBB tentang Penyiksaan, dan yurisprudensi Mahkamah Eropa untuk Hak Asasi Manusia (ECtHR) dalam kasus Klass v. Germany (1978) dan Zakharov v. Russia (2015), telah menetapkan standar bahwa legislasi pengawasan harus memiliki kejelasan tentang: (1) lingkup pelanggaran yang dapat memicu pengawasan, (2) subjek yang dapat diawasi, (3) batas durasi pengawasan, (4) prosedur otorisasi, dan (5) mekanisme pengawasan serta pemulihan. Kerangka ini akan digunakan untuk menguji pengaturan pengawasan siber di Indonesia.

C. PENGAWASAN SIBER DI INDONESIA DAN DEFISIT KONSTITUSIONAL

1. Fragmentasi Regulasi dan Ketiadaan Payung Hukum yang Koheren

Pengaturan pengawasan siber di Indonesia tidak ditampung dalam satu undang-undang khusus yang terintegrasi. Sebaliknya, kewenangan ini terfragmentasi ke dalam berbagai regulasi sektoral. UU ITE memberikan kewenangan kepada penyidik untuk mengakses, meminta, dan menyita data elektronik. UU Intelijen Negara (UU 17/2011) mengizinkan penyadapan untuk

kepentingan intelijen, tetapi tidak secara rinci mengatur bagaimana, kapan, dan kepada siapa pengawasan dapat dilakukan. Lebih problematik lagi, UU Terorisme (UU 5/2018) memberikan kewenangan yang sangat luas kepada aparat untuk melakukan penyadapan dan pengumpulan data dalam rangka pencegahan terorisme, dengan pengawasan yang minimalis.

Keadaan ini menciptakan legal vacuum sekaligus legal chaos. Vakum karena tidak ada aturan umum yang menjadi pedoman bagi semua jenis pengawasan siber. Chaos karena masing-masing lembaga Kepolisian, Kejaksaan, BIN, BSSN, Kominfo memiliki aturan internal sendiri yang seringkali tidak sinkron dan bertentangan satu sama lain (Santoso, 2023). Akibatnya, sulit bagi warga negara untuk mengetahui secara pasti kapan dan mengapa data mereka diakses oleh negara.

2. Lemahnya Pengawasan Yudisial dan Dominasi Eksekutif

Masalah paling serius dalam arsitektur pengawasan siber di Indonesia adalah absennya pengawasan yudisial yang efektif. Sebagian besar kewenangan pengawasan hanya memerlukan izin dari internal lembaga eksekutif atau, paling tinggi, dari menteri. Penyadapan oleh BIN, misalnya, memerlukan izin dari Kepala BIN, tanpa harus melalui pengadilan.

Praktik ini sangat kontras dengan standar internasional yang mensyaratkan adanya judicial warrant (surat perintah dari hakim) sebelum pengawasan dilakukan.

Mahkamah Konstitusi dalam Putusan Nomor 5/PUU-VIII/2010 pernah menegaskan bahwa penyadapan harus diatur dengan undang-undang yang jelas dan melibatkan pengadilan. Namun, putusan ini tidak kunjung ditindaklanjuti dengan legislasi yang komprehensif. Dominasi eksekutif dalam pengawasan siber menciptakan situasi di mana negara dapat mengawasi tanpa check and balance yang berarti. Ini adalah defisit konstitusional yang serius karena melanggar prinsip due process dan membahayakan hak privasi (Setiawan, 2023). Bahkan, RUU Keamanan dan Ketahanan Siber yang sempat dibahas justru memperkuat otoritas eksekutif dalam hal ini BSSN untuk melakukan tindakan pengamanan siber yang bisa mencakup pengawasan konten tanpa batasan yang memadai.

3. Prinsip Proporsionalitas yang Terabaikan

Pengujian terhadap pengawasan siber di Indonesia dari perspektif proporsionalitas memperlihatkan gambaran yang suram. Pertama, pada asas tujuan yang sah, memang keamanan nasional dan pemberantasan kejahatan adalah tujuan yang sah.

Namun, kedua, pada asas kelayakan, banyak instrumen pengawasan yang terlalu luas dan tidak spesifik, sehingga tidak betul-betul cocok untuk mencapai tujuan. Pengawasan massal terhadap metadata komunikasi, misalnya, tidak selalu relevan untuk menangkal terorisme.

Ketiga, pada asas keharusan, pemerintah Indonesia tidak pernah membuktikan bahwa pengawasan massal atau penembusan enkripsi adalah cara yang benar-benar esensial dan tidak ada alternatif yang lebih ringan. Padahal, banyak studi menunjukkan bahwa investigasi berbasis target spesifik jauh lebih efektif daripada pengawasan massal. Keempat, pada asas keseimbangan, pengawasan yang dilakukan secara luas tanpa sepengetahuan subjek jelas menimbulkan kerugian besar bagi privasi, padahal hasilnya seringkali tidak sebanding (Deibert, 2019). Singkatnya, praktik pengawasan siber di Indonesia gagal memenuhi uji proporsionalitas secara holistik.

D. KONTROVERSI AKSES DATA DAN PENYADAPAN OLEH APARAT

Salah satu isu yang sempat mengemuka adalah dugaan penggunaan alat sadap canggih oleh lembaga penegak hukum Indonesia untuk mengakses komunikasi tersangka dan aktivis. Meskipun sulit diverifikasi karena

sifatnya yang tertutup, berbagai laporan masyarakat sipil mengindikasikan adanya praktik penyadapan di luar koridor hukum. Pada tahun 2022, terungkap bahwa aplikasi pesan instan yang diunduh melalui tautan tidak resmi digunakan sebagai pintu masuk untuk menyadap komunikasi personal. Kasus ini memperlihatkan betapa rentannya warga negara terhadap pengawasan yang tidak sah.

Lebih memprihatinkan lagi, tidak ada mekanisme yang memungkinkan korban penyadapan ilegal untuk mengetahui, apalagi menggugat. Mereka tidak memiliki akses terhadap informasi apakah data mereka telah diakses oleh aparat. Ketiadaan *notification requirement* (kewajiban memberitahu) pasca-pengawasan adalah bentuk pengingkaran terhadap hak privasi. Subjek data tidak dapat menuntut akuntabilitas karena tidak pernah tahu bahwa haknya telah dilanggar. Ini sangat kontradiktif dengan asas negara hukum yang menuntut adanya akses terhadap keadilan dan pemulihan (Prasetyo, 2024).

E. MERUMUSKAN KESEIMBANGAN: PRIVASI YANG AMAN, NEGARA YANG BERTANGGUNG JAWAB

Keseimbangan antara privasi dan pengawasan bukanlah rumus matematis yang kaku, melainkan

merupakan proses konstitusional yang dinamis. Ada beberapa prasyarat untuk mencapai keseimbangan tersebut. Pertama, Indonesia harus segera memiliki Undang-Undang Pengawasan (*Surveillance Law*) yang terpadu. Undang-undang ini harus mengkodifikasi semua jenis pengawasan siber, mengatur tentang dasar hukum, batas durasi, otorisasi, pengawasan, dan pemulihan secara terpadu. Semua lembaga negara yang memiliki kewenangan pengawasan harus tunduk pada undang-undang yang sama, sehingga tidak ada lagi fragmentasi dan kompetisi antarlembaga yang merugikan privasi.

Kedua, pemberlakuan judicial warrant secara mutlak. Setiap tindakan pengawasan yang bersifat intrusif, seperti penyadapan, penggeledahan data, atau penembusan enkripsi, harus mendapatkan izin dari pengadilan. Pengadilan harus membentuk panel khusus atau weeskamer yang bertugas menilai permohonan izin pengawasan secara rahasia dan independen. Model ini diterapkan di Belanda, di mana hakim komisaris menangani permintaan penyadapan dengan standar yang ketat. Ketiga, transparansi yang bertanggung jawab. Warga negara yang menjadi target pengawasan berhak untuk diberitahu setelah pengawasan berakhir dan tidak lagi membahayakan penyidikan. Jika pengawasan tidak menghasilkan bukti, subjek harus

memiliki hak untuk menggugat dan meminta pemusnahan data (Greenleaf, 2022).

Terakhir, kepentingan negara tidak boleh dikonstruksi secara monolitik. Negara dibentuk untuk melindungi warga, termasuk privasinya. Oleh karena itu, kepentingan negara yang sesungguhnya adalah melindungi privasi secara maksimal. Pengawasan hanya boleh dilakukan sebagai pengecualian yang terbatas dan terukur, bukan sebagai aturan umum.

F. KESIMPULAN

Ketegangan antara hak privasi dan kepentingan negara dalam pengawasan siber di Indonesia masih belum menemukan titik keseimbangan yang sehat. Kerangka hukum yang ada masih sangat fragmentaris, minim pengawasan yudisial, dan tidak memenuhi standar proporsionalitas. Akibatnya, hak privasi warga negara berada dalam posisi yang sangat rentan terhadap diskresi eksekutif yang tidak terbatasi. Menjawab rumusan masalah, pengaturan pengawasan siber di Indonesia saat ini lebih condong membela kepentingan negara secara sempit dengan mengorbankan privasi, sementara keseimbangan ideal hanya dapat diwujudkan melalui reformasi legislasi yang meletakkan prinsip judicial warrant, proporsionalitas, dan transparansi sebagai pilar utama.

Sebagai rekomendasi, pemerintah bersama DPR harus segera merumuskan RUU Pengawasan yang komprehensif, yang menundukkan semua kewenangan pengawasan di bawah pengawasan hakim. Selain itu, Mahkamah Agung perlu mempersiapkan pembentukan kamar pengawas khusus serta pedoman teknis bagi hakim dalam memutus izin penyadapan. Hanya dengan kerangka hukum yang akuntabel, Indonesia dapat menjadi negara yang aman tanpa berubah menjadi negara yang mengawasi setiap langkah warganya.

REFERENCE:

Asshiddiqie, J. (2021). Hukum dan Teknologi: Pergulatan Konstitusi dalam Masyarakat Digital. Rajawali Pers.

Barak, A. (2012). Proportionality: Constitutional Rights and their Limitations. Cambridge University Press.

Deibert, R. J. (2019). The Road to Digital Unfreedom: Three Painful Truths about Social Media. Journal of Democracy, 30(1), 25–39. https://doi.org/10.1353/jod.2019.0002

Greenleaf, G. (2022). Global Convergence of Data Privacy Standards and Asia: The Unfinished Agenda.

International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Prasetyo, B. (2024). Pengawasan Tanpa Pemberitahuan: Tantangan Akuntabilitas dalam Hukum Intelijen Indonesia. Jurnal Hukum dan Keamanan, 16(1), 45–65.

Santoso, L. (2023). Fragmentasi Regulasi Penyadapan dan Implikasinya terhadap Hak Privasi. Jurnal Yudisial, 16(2), 201–220.

Setiawan, R. (2023). Pengawasan Digital dan Batas-Batas Privasi di Indonesia. Jurnal Konstitusi, 20(4), 801–822. https://doi.org/10.31078/jk2045

Solove, D. J. (2021). The Digital Person: Technology and Privacy in the Information Age. New York University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara (Lembaran Negara Tahun 2011 Nomor 105, Tambahan Lembaran Negara Nomor 5249).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).