

Notulensi Seminar
**“Mencari Titik Tengah Demokrasi: Antara Keamanan
Nasional dan Kebebasan Sipil”**

Departemen Ilmu Hubungan Internasional, Universitas Indonesia

30 Mei 2024

Seminar ini dilaksanakan untuk merespon laporan Amnesty Internasional yang berjudul “A web of surveillance: unravelling a murky network of spyware export to Indonesia” yang mengkhawatirkan ada penggunaan peralatan sadap atau spyware terhadap para aktivis HAM dan demokrasi yang berpotensi mengganggu demokratisasi dan bahkan mengembalikan Indonesia ke periode otoriter. Seminar ini diadakan untuk mendudukkan perkara penggunaan alat sadap di Indonesia agar dapat menemukan keseimbangan antara kebutuhan keamanan nasional dan kebutuhan menjamin kebebasan sipil. Para pembicara dalam seminar ini mewakili berbagai perspektif, baik instansi keamanan, media dan lembaga swadaya masyarakat yang bergerak di bidang demokrasi dan kebebasan sipil, serta akademisi. Para pembicara dalam seminar ini adalah:

1. Dr. Sulistyono, Deputy Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia, Badan Siber dan Sandi Negara (BSSN RI).
2. Brigjen Pol. I Made Astawa, Wakil Kepala Densus 88, Polri
3. Herik Kurniawan, Ketua Ikatan Jurnalis Televisi Indonesia (IJTI)
4. Mabda H.F. Sidiq, Peneliti The Habibie Center
5. Dr. Arthur Josias Runturambi, Ketua Program Kajian Ketahanan Nasional, SKSG UI
6. Dr. Ali A. Wibisono, Lektor Kepala di Departemen Ilmu Hubungan Internasional, UI

Seminar ini dimoderatori oleh Dr. Broto Wardoyo, Ketua Program Pascasarjana Ilmu Hubungan Internasional, UI.

Seminar dibuka dengan pengantar dari Dr. Asra Virgianita, Ketua Departemen Ilmu Hubungan Internasional, UI yang menekankan pada pentingnya isu yang dibahas mengingat keamanan nasional dan kebebasan sipil merupakan dua hal yang sama pentingnya. Mencari titik temu dari keduanya merupakan hal yang krusial dan

menentukan dalam keberlanjutan demokrasi di Indonesia. Laporan Amnesty International tersebut tidak dapat dipandang remeh meski tetap harus dikritisi secara mendalam. Dan seminar ini menjadi salah satu forum untuk mendudukkan para pemangku kepentingan demokrasi dan keamanan di Indonesia.

Seminar dibuka oleh moderator yang kembali menekankan pentingnya menyikapi laporan Amnesty International secara *fair* dan kritis. Laporan tersebut harus diperlakukan sebagai pengingat atau *warning* bagi perlindungan kebebasan sipil, namun tanpa mengorbankan keamanan nasional. Karena itu, moderator menekankan sikap saling terbuka dalam mendiskusikan isu ini mengingat dua hal yang dibahas, keamanan nasional dan kebebasan sipil, merupakan dua hal yang sama pentingnya.

Pembicara kunci dalam seminar ini, Dr. Sulistyono, yang merupakan Deputy Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia, BSSN RI memaparkan beberapa hal penting terkait dengan isu penyadapan dan, lebih luas lagi, keamanan data. Menurut Dr. Sulistyono, isu penyadapan ini hanya merupakan bagian dari isu yang lebih luas yang terkait dengan keamanan data. Dalam paparannya yang berjudul "Perspektif Pemerintah dan Dinamika dalam Perlindungan Keamanan Nasional", Dr. Sulistyono menekankan beberapa poin seperti: a) perlindungan data sebagai isu nasional, b) dinamika perlindungan data nasional, dan c) kebijakan lokalisasi data.

Dr. Sulistyono menjelaskan bahwa pada dasarnya data dapat diklasifikasikan menjadi dua, yaitu data publik dan data strategis. Sifat keduanya berbeda dan ketersediaannya untuk masyarakat juga berbeda. Meski demikian, kedua data tersebut harus mendapatkan jaminan keamanan atau perlindungan. Penyimpanan atau *data center* dari data publik dan data strategis, menurut Dr. Sulistyono, sebaiknya tetap berada di dalam wilayah Indonesia. Selain itu, kedua jenis data tersebut harus dapat diakses oleh pemerintah atau institusi terkait, terutama institusi keamanan, jika dibutuhkan. Poin ini penting mengingat tidak tertutup kemungkinan data-data tersebut, terutama data strategis memiliki sensitivitas keamanan nasional.

BSSN RI sendiri, papar Dr. Sulistyono, memiliki standarisasi dalam penyimpanan data, dan hal ini sudah dikomunikasikan dengan seluruh pemangku kepentingan, namun sayangnya hingga saat ini belum ada sanksi atau unsur paksaan bagi

lembaga, negara maupun privat, yang tidak mengikuti standarisasi tersebut. Ada beberapa kasus yang pernah terjadi di Indonesia dimana kebocoran data terjadi di beberapa lembaga pemerintahan maupun privat akibat dari ketidakmampuan mereka mengikuti standar yang telah ditentukan. Dalam bahasa setengah becanda yang menohok, Dr. Sulistyو mengatakan “kita harus berterima kasih kepada para *hacker* karena mereka menunjukkan kelemahan dalam sistem pengamanan kita”.

Dr. Sulistyو juga memaparkan prediksi ancaman siber tahun 2024 yang dapat berupa banyak hal, termasuk *ransomware*, yang dilakukan dengan berbagai perangkat dan media (*tools*) yang ada, seperti pemanfaatan *artificial intelligence* (AI) dimana data diambil oleh penyerang untuk dimanfaatkan ataupun penggunaan *internet of things* (IoT) yang pada dasarnya memang sangat rentan oleh serangan *hacker*. Serangan tersebut dapat ditujukan pada perangkat dalam berbagai tingkat, baik rumah tangga maupun industri.

Poin menarik lain yang dipaparkan Dr. Sulistyو adalah tiga bentuk ancaman yang dapat terjadi di tiga level yang berbeda. Pertama, di level individu, ada ancaman “data dicari”. Ancaman ini dilakukan oleh individu yang tanpa sengaja sering memasukkan data pribadi ke media sosial. Hal-hal sederhana mengucapkan selamat ulang tahun di Facebook yang akan dengan mudah dimanfaatkan oleh pihak-pihak yang tidak bertanggungjawab untuk aktivitas ilegal. Dr. Sulistyو menekankan bahwa saat ini sangat mudah bagi seseorang untuk mendapatkan informasi pribadi, bahkan yang sifatnya sebenarnya rahasia sekalipun, di internet. Informasi-informasi seperti Nomor Induk Kependudukan, tanggal lahir, dan lain sebagainya bisa dengan mudah dicari di internet.

Kedua, “data diberi” yang biasanya dilakukan oleh perusahaan atau swasta. Para pembuat platform, biasanya perusahaan developer atau pengembang apps, mengumpulkan data-data dari para pengguna untuk diperdagangkan ke pihak lain. Dr. Sulistyو memberikan contoh sederhana tentang kebiasaan pengguna mengkonsumsi konten tertentu, misalnya memancing, di internet atau media sosial yang kemudian memunculkan tawaran-tawaran terkait aktivitas memancing. Problem dengan ancaman ini, menurut Dr. Sulistyو, adalah ketiadaan mekanisme memaksa yang kuat oleh negara ke perusahaan-perusahaan swasta tersebut.

Ketiga, “data dicuri” yang dilakukan oleh para kriminal dunia siber (cyber criminal). Dalam konteks inilah penggunaan spyware atau alat sadap muncul. Namun, hal ini membutuhkan usaha (*efforts*) khusus sehingga target biasanya adalah seseorang atau lembaga yang memiliki nilai strategis tertentu. Dari penjelasan tersebut, nampak bahwa sebenarnya dalam konteks keamanan data, problem terbesarnya ada pada dua jenis data pertama, “data dicari” dan “data diberi”. Karena itu, Dr. Sulistyو lebih menekankan pada literasi digital untuk mencegah kebocoran data akibat “data dicari” dan “data diberi” tersebut.

Dr. Sulistyو mengakhiri paparannya dengan menekankan bahwa problem utama terkait data sebenarnya adalah pada upaya pengumpulan data untuk keuntungan komersial, atau istilah yang digunakan adalah merekam *tracking* untuk menampilkan algoritma. Hal ini kemudian menjadi dilema antara potensi ekonomi dengan hak pribadi terkait data. Data-data yang dikumpulkan kemudian diproses sehingga hasil dari analisis data, dapat berupa apapun seperti *sexual orientation, ethnic, culture, political value*, atau *believe*, yang kemudian dapat dimanfaatkan. Hal ini secara konsetual disebut sebagai *surveillance capitalism* dan diperkenalkan oleh Shoshana Zuboff.

Lebih lanjut, Dr. Sulistyو menekankan bahwa perlindungan data adalah isu nasional karena melibatkan banyak aktor. Data sensitif dan pribadi, menurut Dr. Sulistyو, harus dilindungi dan pemerintah hadir untuk melindungi data nasional meski saat ini kapasitas negara, dalam hal ini BSSN RI, masih terbatas karena berbagai alasan.

Mengingat Dr. Sulistyو harus meninggalkan ruang seminar lebih awal karena ada kegiatan lain, moderator mempersilakan para peserta untuk mengajukan pertanyaan kepada beliau. Feline dari Program Pascasarjana Ilmu Hubungan Internasional menanyakan apakah aturan, terutama UU keamanan siber yang ada sudah cukup untuk menjamin keamanan nasional dan kebebasan sipil atau sebenarnya Indonesia butuh aturan baru? Dr. Sulistyو tegas menyatakan bahwa pengaturan yang ada saat ini belum cukup, khususnya dalam isu pengelolaan data. Mekanisme compliance yang ada saat ini bentuknya *voluntary*, sehingga tidak bisa diberikan sanksi terhadap pelanggaran tersebut.

Pembicara kedua, Brigjen. Pol. I Made Astawa, yang menjabat Wakadensus 88 AT, Polri memaparkan tentang "Penggunaan Teknologi Intelijen dalam Penanganan Terorisme". Brigjen Made memulai penjelasan dengan memaparkan perkembangan terorisme di Indonesia juga terkait dengan terorisme global. Brigjen Made yang merupakan anggota Satgas Bom Bali I dan banyak berkarir di penanggulangan terorisme menjelaskan evolusi dari Jamaah Islamiyah (JI) ke Jamaah Anshorut Daulat (JAD) dan keterkaitannya dengan Al-Qaeda (AQ) dan Islamic State (ISIS). Kemudian, Brigjen Made menjelaskan sifat-sifat terorisme yang membuatnya berbeda dari ancaman keamanan lain, seperti a) karakternya sebagai *extraordinary crime*; b) sifatnya yang transnational; c) karakternya sebagai *crime against humanity*; d) pelaksanaannya oleh kelompok terorganisir (*organized crime*).

Berbagai karakter terorisme dan juga evolusi perkembangan terorisme tersebut membuat cara penanggulangan masalah terorisme harus memiliki kecepatan dan sifatnya yang tidak boleh pasif. Dalam kebutuhan tersebut maka aparat hukum yang menangani masalah terorisme diizinkan untuk melakukan penyadapan serta lebih intoleran kepada para pelaku. Densus 88 sendiri diberikan kewenangan untuk melakukan penyadapan. Namun, secara prinsip Densus 88 tetap menghormati hak masyarakat dan hukum yang ada. Densus 88 bukan satu-satunya lembaga hukum yang diberi kewenangan penyadapan. Dalam penanganan isu narkoba atau tindakan pelanggaran hukum yang memiliki hukuman lebih dari lima tahun juga diizinkan menggunakan penyadapan.

Penyadapan itu sendiri dalam dilakukan dengan berbagai perangkat. Brigjen Made kemudian menceritakan pengalaman beliau melakukan penyadapan di masa lalu dengan menggunakan perangkat *recorder* yang ditempelkan pada alat komunikasi di penyedia platform telco. Namun, saat ini penyadapan sudah dilakukan dengan peralatan yang canggih.

Hal penting lain yang dipaparkan oleh Brigjen Made adalah adanya prinsip-prinsip khusus dalam melakukan penyadapan. Ada prosedur dan juga ada aturan hukum, termasuk UU, yang mengatur penyadapan tersebut. Beberapa hal yang harus diperhatikan dalam melakukan penyadapan adalah: a) kepatuhan pada hukum dan HAM; b) pendekatan komprehensif; dan c) keberlanjutan dan efektivitas. Brigjen Made menekankan bahwa penyadapan hanya boleh dilakukan oleh penyidik dan hasil penyadapan tidak dapat sembarangan dipublikasikan (hanya boleh digunakan

untuk kepentingan penyidikan dan pembuktian hukum). Target penyadapan pun sifatnya khusus, yaitu mereka yang memang terkait dengan kejahatan, baik terorisme maupun kejahatan lain yang diatur dalam UU.

Contoh kasus yang dijelaskan oleh Brigjen Made adalah target yang diawasi karena mengunggah (*upload*) konten terorisme. Hal ini pun masih melalui proses, seperti pengumpulan informasi berupa log data dan alamat IP dan hanya bisa dilakukan oleh institusi yang bertanggungjawab atas kejahatan tersebut, misalnya Bareskrim Siber. Problem yang kadang dihadapi adalah sifat dari dunia maya yang tidak memiliki batas. Hal ini membuat Polri beberapa kali perlu berkordinasi dengan Interpol untuk mengetahui alamat IP dimaksud terkait dengan perangkat yang mana di negara asing tersebut.

Brigjen Made memaparkan beberapa dasar hukum dalam penanganan teror, seperti: a) UU no. 5 tahun 2018; b) Peraturan Pemerintah Pengganti Undang-Undang (Perppu) Nomor 1 Tahun 2002; c) Undang-Undang Nomor 19 Tahun 2016; Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Pasal 83 ayat 1 dan 2 huruf m yang menjadi pijakan dalam melakukan penyadapan.

Mengakhiri paparannya, Brigjen Made memaparkan isu-isu yang kerap muncul terkait penyadapan, seperti: a) privasi dan HAM; b) penyalahgunaan wewenang; c) kerahasiaan data; dan d) teknologi dan kapasitas. Dari paparan Brigjen Made, nampak bahwa penyadapan merupakan proses yang membutuhkan kehati-hatian terkait dengan target dan pelaksanaan penyadapan itu sendiri. Dan dalam pelaksanaannya, ada banyak perangkat yang membatasi aktivitas penyadapan tersebut, baik alasannya harus jelas maupun prosedurnya yang juga harus jelas.

Pembicara selanjutnya, Herik Kurniawan, yang merupakan Pemimpin Redaksi GTV dan Ketua Ikatan Jurnalis Televisi Indonesia (IJTI), memaparkan penjelasan tentang "Pers, Demokrasi, Hak Sipil, dan Keamanan Nasional". Herik menegaskan bahwa media merupakan pilar keempat demokrasi yang harus berhadapan dengan tiga pilar lain yang sangat kuat. Herik menekankan pada adanya upaya melemahkan media secara struktural dengan revisi UU Penyiaran dan UU Pers yang saat ini sedang terjadi.

Terlepas dari pelemahan tersebut, Herik menegaskan bahwa media sepenuhnya memahami bahwa tugas mereka dalam isu penanganan terorisme adalah memberitakan dan menayangkan berita dengan tujuan untuk meredam serangan terorisme itu terjadi lagi di masa depan. Hal ini penting mengingat terkadang media disalahpahami melakukan pemberitaan yang mendukung (*encouraging*) terorisme karena menelusuri cerita-cerita personal yang terkait dengan terorisme. Terkadang media memang memberikan pemberitaan tentang para pelaku namun hal ini tetap dilakukan dengan hati-hati dan dengan mengikuti kaidah etika jurnalistik yang ketat.

Dalam konteks tersebut, Herik kembali menekankan betapa revisi UU Penyiaran dan UU Pers yang memunculkan pasal atau regulasi yang membuat jurnalis tidak bisa bekerja secara maksimal akibat berbagai pembatasan. Padahal, menurut Herik, saat jurnalis tidak bisa memaksimalkan tugasnya maka kepercayaan terhadap jurnalis menjadi terbatas. Hal ini memberikan ruang bagi media yang tidak bertanggung jawab untuk beroperasi dan biasanya pemberitaan mereka lebih diminati karena memberikan apa yang “diinginkan” publik sedangkan media yang benar memberikan apa yang “dibutuhkan” publik.

Herik mengakhiri paparannya dengan menegaskan bahwa dalam jurnalistik ada investigasi untuk menelusuri suatu kasus. Ada kaidah dan etika yang harus dijaga dalam melakukan hal tersebut. Dan pers selalu berkontribusi pada menjaga keamanan nasional dalam melakukan aktivitas pemberitaan.

Mabda H.F. Sidiq, peneliti The Habibie Center (THC), memaparkan pandangannya tentang “Keamanan Siber, Teknologi Intelijen, dan Demokrasi di Indonesia”. THC sendiri banyak menyuarakan tentang isu keamanan siber dan ancaman demokrasi di Indonesia. Mabda memulai paparannya dengan menjelaskan keberadaan teknologi intelijen di ruang siber. Secara sederhana, menurut Mabda, ada beberapa implikasi dari teknologi intelijen di ruang siber yang memang berkontribusi pada gangguan kebebasan sipil.

Namun, yang pasti, menurut Mabda, ada beberapa masalah dalam transisi keamanan siber secara global, terutama dalam politisasi dan sekuritisasi isu siber saat ini semakin kuat. Dalam konteks tersebut, visibilitas penggunaan siber dimana siber dijadikan alat *surveillance* menjadi semakin kuat. Mabda menilai bahwa alasan

mengapa siber digunakan untuk militer dan intelijen terkait dengan karakter ruang siber yang *non-physical, stealth, functional, dan pervasive*. Mabda mempertanyakan apakah saat siber masuk ke dalam ranah keamanan dia mampu meningkatkan keamanan nasional. Lalu apakah siber kemudian mengurangi akses teknologi masyarakat.

Terkait dengan sekuritisasi siber, Mabda menilai adanya pengadopsian lensa keamanan komprehensif dalam diskusi mengenai ruang siber. Pendekatan keamanan komprehensif tersebut tidak hanya terfokus pada negara namun juga individu, dalam hal ini jaminan pada kebebasan sipil. Kondisi intelijen siber di Indonesia saat ini, menurut Mabda, ditandai dengan adanya inflow teknologi intelijen siber dari luar. Salah satu yang dikritisi oleh Mabda adalah adanya *software* intelijen dengan kemampuan akses data dengan *zero clicks*. Pada saat yang sama, ada ambiguitas regulasi. Indonesia, menurut Mabda, membutuhkan penguatan regulasi, dan pembahasan mengenai siber yang diperkuat. Peran *civil society* masih sangat pasif dan masih sangat dibatasi.

Mabda menutup paparannya dengan mempertanyakan takaran keseimbangan antara keamanan nasional dan kebebasan sipil terkait teknologi siber dalam aspek intelijen. Selain itu, Mabda juga mempertanyakan adanya landasan hukum yang memastikan transparansi dan akuntabilitas.

Setelah paparan dari sisi pemerintah, media, dan lembaga swadaya masyarakat tersebut, dua pembicara yang memiliki latar belakang akademik, Dr. Arthur Josias Runturambi dan Dr. Ali A. Wibisono, memberikan paparan mereka.

Dr. Runturambi, Ketua Program Kajian Ketahanan Nasional, SKSG UI, memaparkan keseimbangan antara keamanan nasional dan kebebasan sipil dalam penggunaan teknologi intelijen di Indonesia. Dr. Runturambi memulai dengan menjelaskan aturan perundang-undangan yang mengatur sistem keamanan siber, yaitu UU 17/2011 pasal 2-3. Meski telah ada aturan tersebut, Dr. Runturambi menilai bahwa dalam praktik seringkali penyalahgunaan dan melanggar kebebasan sipil. Karena itu, Dr. Runturambi menekankan pada pentingnya prinsip tata kelola intelijen.

Problem dengan tata kelola intelijen tersebut ada banyak. Intelijen merupakan fungsi yang dijalankan di berbagai lembaga. Dengan demikian, kadang tanpa kita sadari kita bersinggungan dengan aktivitas intelijen dan secara *voluntary* memberikan data. Ketika kita ada di Imigrasi, misalnya, dan kita memberikan data-data untuk registrasi, misalnya di bandara, apakah hal tersebut dapat dikatakan melanggar kebebasan sipil.

Tata kelola intelijen, menurut Dr. Runturambi, juga mencakup atribut dan aturan berkaitan dengan kepemimpinan. Dan dalam banyak kasus, harus ada trade off dalam demokrasi dan keamanan. Untuk dapat menemukan titik temu, menurut Dr. Runturambi, perlu ada keseriusan dalam melanjutkan reformasi intelijen yang menekankan terkait penguasaan dan batasan kewenangan sehingga ada akomodasi kebebasan sipil tapi tetap tidak mengganggu kewenangan sehingga lebih efektif. Selain itu, perlu ada pengawasan legislatif terhadap aktivitas dan lembaga intelijen untuk menjamin keamanan negara dan kebebasan sipil.

Dr. Runturambi menekankan, dan sekaligus menutup paparannya, pada kebutuhan untuk menciptakan *intelligence oversight* untuk mencegah penyimpangan. Apalagi, pro dan kontra penilaian ancaman oleh pada intelijen pada dasarnya dapat menyebabkan perbedaan definisi keamanan.

Pembicara terakhir, Dr. Ali A. Wibisono dari Departemen Ilmu Hubungan Internasional, UI, menekankan pergeseran landscape keamanan, termasuk keamanan siber, yang berkembang sejak pasca berakhirnya Perang Dingin. Jika membahas tentang siber, teknologi siber, dan keamanan siber maka, menurut Dr. Wibisono, pertanyaan yang harus dijawab terlebih dahulu adalah keamanan nasional itu lokusnya ada dimana. Dengan kata lain, keamanan itu untuk siapa: apakah kita bicara *security for gadgets*, *security for software*, atau *security for users*.

Dr. Wibisono juga menjelaskan bahwa keamanan siber saat ini ada dalam keseharian kita. Istilah akademik yang digunakan adalah *it's an everyday security*. Dalam konteks Indonesia, Dr. Wibisono menekankan bahwa kondisi Indonesia saat ini ada pada *unfinished nation building* sehingga aspek siber terpengaruh oleh kondisi ini dan perlu dilihat juga bagaimana Indonesia menghadapi *unfinished nation building*. Kita, menurut Dr. Wibisono, belum bisa membedakan mana keamanan *nation*, *state*, dan *regime*. Ada banyak isu non-tradisional yang menyengol

keamanan nasional. Saat ini, seperti yang juga dipaparkan oleh Dr. Sulisty, *information is weaponize* yang menyebabkan ancaman siber seperti penyadapan dilakukan untuk mendapatkan informasi.

Bicara mengenai keberadaan aturan, Dr. Wibisono menyoroti bahwa UU ITE yang seharusnya melindungi data pribadi justru melindungi kepentingan rezim. Contoh nyatanya adalah adanya kasus penyadapan 14 jurnalis oleh pejabat. Bicara teknologi, Dr. Wibisono juga menyoroti bahwa bentuk penyadapan juga sudah sangat beragam, salah satunya adalah bentuk penyadapan "*end-to-end encrypted chat*" yang dapat diakses oleh apps seperti Pegasus. Problem lain yang muncul adalah, dalam *cyberspace*, aktor yang banyak terlibat adalah swasta. Swasta dapat memainkan posisi sebagai penyedia jasa dan atau broker perdagangan antara pemerintah/instansi/aktor yang membeli apps penyadapan dari aktor lain.

Ketidakmampuan untuk menjaga keamanan siber di Indonesia juga masih rendah. Berdasarkan penjelasan Dr. Sulisty sebelumnya dari jumlah peringatan dan rekomendasi yang dikeluarkan BSSN maka hanya sekitar 6% yang melakukan follow up kembali notifikasi BSSN tersebut sehingga Dr. Wibisono tidak heran jika kebocoran data dapat terjadi. Meski Dr. Wibisono menilai bahwa penyadapan bisa menjadi refleksi bagi instansi, namun dia menekankan bahwa problem dengan keamanan data tidak hanya di situ namun lebih pada data tersebut juga diberikan langsung.

Menutup paparannya, Dr. Wibisono menekankan bahwa dalam aktivitas penyadapan yang menjadi kondisi melanggar hak individu terkait privasi maka diperlukannya pertimbangan-pertimbangan khusus, seperti: a) apa yang ingin dicapai dari pelanggaran hak privasi tersebut; b) apakah ada bahaya dari individu tersebut; dan c) lembaga mana yang berwenang dalam menentukan hal tersebut. Hal tersebut akan membuat keputusan untuk melakukan penyadapan dapat dikatakan memiliki *ethical decision making* dan akuntabel.

Dalam sesi tanya jawab, pertanyaan diajukan oleh Chris Wibisono, mahasiswa Program Sarjana Ilmu Hubungan Internasional UI. Chris menilai bahwa keamanan nasional dan keamanan sipil merupakan dua lokus berbeda. Namun, seberapa jauh kemudian ekspresi kebebasan sipil dinilai mengancam keamanan nasional dan siapa yang dianggap ancaman keamanan nasional oleh negara ini. Chris

menggunakan kasus penyadapan terhadap tiga Ketua BEM UI terakhir. Brigjen Made menekankan bahwa yang pasti bukan Densus yang menyadap mereka, jika memang mereka disadap. Namun, beliau juga menekankan bahwa belum tentu itu sebenarnya penyadapan namun hacking. Sementara itu, Herik menilai bahwa negara bisa melakukan apa saja untuk keamanan negara, salah satunya penyadapan. Namun, karena teknologi penyadapan telah berkembang pesat maka kita tidak bisa memastikan siapa pelaku penyadapan tersebut. Mabda juga menilai bahwa masih belum jelas siapa pelaku penyadapan tersebut namun dia menekankan pentingnya membangun kepercayaan pada BSSN dan pemangku kepentingan lain dengan catatan ada mekanisme pembatasan yang juga kuat. Dr. Runturambi menilai bahwa penyadapan yang dilakukan di luar kewenangan adalah sebuah pelanggaran. Dia menegaskan bahwa penyadapan tidak sesederhana yang dibayangkan. Dr. Wibisono juga meragukan apakah penyadapan tersebut dilakukan oleh negara mengingat aktor swasta juga dapat melakukan penyadapan.

Menutup diskusi, moderator, Dr. Wardoyo, menekankan bahwa penggunaan alat sadap pada dasarnya dibutuhkan dalam menjamin keamanan nasional, terutama dalam kasus-kasus yang sifatnya *extraordinary* seperti terorisme. Meski demikian, ada landasan hukum dan prosedur yang ketat dalam melaksanakan aktivitas penyadapan. Bahwa langkah tersebut akan mengurangi kebebasan sipil bisa jadi memang demikian. Namun, mengingat yang disasar adalah mereka yang menjadi agen ancaman keamanan nasional maka sebenarnya ada sifat khusus dalam penyadapan. Terakhir, Dr. Wardoyo menekankan bahwa hak privasi sebenarnya tidaklah absolut. Dia dapat dikecualikan jika memang ada kondisi bahaya yang sifatnya khusus dan dapat didefinisikan dengan tegas.