KAJIAN STRATEGIS

Penguatan Keamanan Ruang Digital Indonesia Melalui Kolaborasi Strategis antara Mahasiswa dan Kepolisian

PENGURUS PUSAT

PERHIMPUNAN MAHASISWA INFORMATIKA DAN KOMPUTER

NASIONAL REPUBLIK INDONESIA

PERIODE 2024 - 2026

A. Pendahuluan

Transformasi digital merupakan salah satu agenda strategis pembangunan nasional yang telah mengubah berbagai aspek kehidupan masyarakat Indonesia. Digitalisasi telah mendorong efisiensi pelayanan publik, memperluas akses pendidikan, mempercepat pertumbuhan ekonomi digital, serta membuka peluang inovasi di berbagai sektor. Berdasarkan survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet Indonesia telah mencapai **221 juta jiwa**, menunjukkan bahwa sebagian besar aktivitas masyarakat kini bergantung pada ekosistem digital.

Di sisi lain, Badan Pusat Statistik (BPS) melalui Statistik Telekomunikasi Indonesia 2024 juga menunjukkan peningkatan pemanfaatan teknologi informasi oleh rumah tangga Indonesia, menandakan bahwa digitalisasi telah menjadi bagian dari kehidupan sehari-hari masyarakat.

Namun, pesatnya adopsi teknologi tersebut belum diimbangi dengan kesiapan keamanan digital yang memadai. Ancaman berupa penipuan daring, perjudian online, kebocoran data pribadi, pinjaman online ilegal, hingga serangan siber terus meningkat dan menimbulkan kerugian ekonomi maupun sosial yang besar.

PERMIKOMNAS memandang bahwa keamanan ruang digital merupakan bagian dari keamanan nasional yang memerlukan kolaborasi aktif antara pemerintah, aparat penegak hukum, akademisi, industri, dan masyarakat.

B. Potret Permasalahan Ruang Digital Indonesia

1. Indonesia Memiliki Populasi Digital yang Sangat Besar

• Pengguna internet Indonesia telah mencapai sekitar **221 juta orang** menurut APJII. • Digitalisasi layanan publik, transaksi ekonomi, pendidikan, dan komunikasi menjadikan ruang digital sebagai infrastruktur strategis bangsa.

Besarnya populasi digital ini juga berarti semakin luas potensi masyarakat menjadi sasaran kejahatan siber apabila tidak dibarengi dengan perlindungan yang memadai.

2. Penipuan Digital Terus Meningkat

Laporan Indonesia Anti-Scam Centre (IASC) menunjukkan lebih dari **225 ribu laporan penipuan keuangan digital** dengan total kerugian masyarakat mencapai sekitar **Rp4,6 triliun**. Fenomena ini menunjukkan bahwa masyarakat Indonesia masih menjadi target empuk berbagai modus kejahatan berbasis teknologi seperti phishing, social engineering, investasi palsu, impersonasi, hingga penyalahgunaan rekening.

3. Kejahatan Siber Menimbulkan Kerugian Ekonomi yang Besar

Kementerian Komunikasi dan Digital menyampaikan bahwa kejahatan siber telah menyebabkan kerugian hingga sekitar **Rp476 miliar**, sehingga pemanfaatan teknologi kecerdasan buatan (Artificial Intelligence/AI) dinilai penting untuk memperkuat sistem deteksi dan pencegahan

ancaman digital.

Hal ini menunjukkan bahwa penguatan teknologi keamanan siber harus menjadi prioritas nasional. 4. Tingginya Aktivitas Penegakan Hukum oleh Kepolisian

Bareskrim Polri sepanjang tahun 2025 menangani **664 perkara kejahatan siber**, menunjukkan bahwa ancaman digital bukan lagi persoalan sporadis melainkan tantangan penegakan hukum yang terus berkembang.

Peningkatan kompleksitas modus operandi juga menuntut peningkatan kapasitas digital forensik dan investigasi siber.

5. Ancaman Perjudian Online dan Kejahatan Keuangan

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dalam Catatan Capaian Strategis Tahun 2025 menegaskan pentingnya menjaga integritas ekonomi nasional dari ancaman transaksi ilegal termasuk perjudian online dan berbagai bentuk tindak pidana ekonomi berbasis digital.

Kejahatan tersebut tidak hanya berdampak pada individu, tetapi juga berpotensi mengganggu stabilitas sistem keuangan nasional.

6. Rendahnya Literasi Digital Masyarakat

Data Indeks Literasi Digital Indonesia menunjukkan bahwa kualitas literasi digital masyarakat masih perlu terus ditingkatkan.

Sebagian masyarakat belum memiliki kemampuan memadai dalam:

- melindungi data pribadi;
- mengenali modus phishing;
- menjaga keamanan akun digital;
- melakukan verifikasi informasi;
- memahami keamanan transaksi elektronik.

Kondisi ini memperbesar peluang keberhasilan pelaku kejahatan siber.

7. Data Pribadi Menjadi Sasaran Utama

Kajian Government Technology Nasional menunjukkan bahwa informasi yang paling sering terpapar dalam insiden kebocoran data meliputi:

- nama lengkap;
- nomor telepon;
- alamat email;
- Nomor Induk Kependudukan (NIK);
- alamat;

- hingga kredensial akun.

Penyalahgunaan data tersebut dapat menjadi pintu masuk bagi penipuan digital maupun pencurian identitas.

8. Ancaman Siber Bersifat Global

Laporan statistik kejahatan siber internasional menunjukkan bahwa serangan ransomware, phishing, pencurian identitas, dan data breach terus meningkat secara global.

Hal ini menegaskan bahwa Indonesia perlu memperkuat kapasitas nasional melalui kolaborasi lintas sektor agar mampu menghadapi ancaman digital yang bersifat transnasional.

C. Analisis Kritis PERMIKOMNAS

Perkembangan teknologi digital telah menjadi salah satu pilar utama pembangunan nasional. Dengan jumlah pengguna internet Indonesia yang telah mencapai sekitar **221 juta jiwa** menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), ruang digital kini menjadi infrastruktur strategis yang menopang aktivitas ekonomi, pendidikan, pemerintahan, hingga interaksi sosial masyarakat. Kondisi tersebut juga diperkuat oleh data Badan Pusat Statistik (BPS) yang menunjukkan peningkatan pemanfaatan teknologi informasi di berbagai sektor kehidupan.

Namun demikian, di balik pesatnya transformasi digital tersebut, Indonesia masih menghadapi tantangan serius berupa meningkatnya berbagai bentuk kejahatan siber. Data Indonesia Anti-Scam Centre (IASC) mencatat lebih dari **225 ribu laporan penipuan keuangan digital** dengan total kerugian masyarakat mencapai sekitar **Rp4,6 triliun**. Sementara itu, Kementerian Komunikasi dan Digital (Komdigi) menyampaikan bahwa kejahatan siber telah mengakibatkan kerugian sekitar **Rp476 miliar**, sedangkan Bareskrim Polri menangani **664 perkara kejahatan siber sepanjang tahun 2025**.

PERMIKOMNAS memandang bahwa maraknya penipuan digital, perjudian daring, pinjaman online ilegal, pencurian data pribadi, serta berbagai bentuk kejahatan siber lainnya merupakan indikator bahwa transformasi digital Indonesia belum sepenuhnya diiringi dengan penguatan tata kelola keamanan digital yang memadai. Kemajuan teknologi yang seharusnya menjadi instrumen peningkatan kesejahteraan justru dimanfaatkan oleh pelaku kejahatan untuk mengeksploitasi rendahnya literasi digital masyarakat dan celah dalam sistem pengawasan.

Selain itu, berbagai insiden kebocoran data pribadi menunjukkan bahwa perlindungan terhadap informasi masyarakat masih menjadi tantangan besar. Kajian Government Technology Indonesia menunjukkan bahwa data seperti nama lengkap, nomor telepon, alamat email, Nomor Induk Kependudukan (NIK), hingga kredensial akun merupakan jenis data yang paling sering terpapar dalam berbagai insiden kebocoran. Situasi ini berpotensi memicu tindak pidana lanjutan seperti pencurian identitas, penipuan digital, hingga penyalahgunaan akun keuangan.

PERMIKOMNAS juga menilai bahwa ancaman terhadap ruang digital tidak lagi bersifat lokal,

melainkan telah berkembang menjadi ancaman lintas negara (transnasional). Berbagai laporan internasional menunjukkan peningkatan serangan ransomware, phishing, dan pencurian data secara global, sehingga Indonesia memerlukan strategi keamanan siber yang adaptif, kolaboratif, dan berbasis teknologi.

Di sisi lain, upaya penegakan hukum dan pemblokiran platform bermasalah perlu terus diperkuat. Namun, pendekatan yang hanya bersifat represif tidak akan mampu menyelesaikan akar persoalan. Negara perlu mengedepankan strategi yang lebih komprehensif melalui peningkatan literasi digital masyarakat, penguatan implementasi perlindungan data pribadi, percepatan koordinasi lintas kementerian dan lembaga, optimalisasi pemanfaatan teknologi kecerdasan buatan (Artificial Intelligence) untuk deteksi dini ancaman, serta pembangunan sistem respons insiden yang lebih terintegrasi.

PERMIKOMNAS berpandangan bahwa pembagian peran antarinstansi harus semakin diperjelas dan diperkuat. Kementerian Komunikasi dan Digital memiliki fungsi strategis dalam tata kelola ruang digital dan pengawasan platform, Kepolisian Negara Republik Indonesia berperan sebagai ujung tombak penegakan hukum terhadap tindak pidana siber, Badan Siber dan Sandi Negara berperan dalam penguatan keamanan siber nasional, sementara PPATK memiliki peran penting dalam pelacakan transaksi keuangan mencurigakan yang berkaitan dengan tindak pidana digital. Sinergi yang kuat di antara seluruh lembaga tersebut menjadi syarat mutlak untuk menciptakan ekosistem digital yang aman dan terpercaya.

PERMIKOMNAS juga menilai bahwa perguruan tinggi dan mahasiswa bidang informatika memiliki posisi strategis sebagai mitra pemerintah dan aparat penegak hukum dalam membangun ekosistem digital yang sehat melalui riset, inovasi teknologi, edukasi masyarakat, serta pengembangan talenta keamanan siber. Potensi sumber daya manusia muda Indonesia perlu diberdayakan secara optimal agar tidak hanya menjadi pengguna teknologi, tetapi juga menjadi pelindung dan pengembang teknologi yang aman dan berkelanjutan.

Oleh karena itu, PERMIKOMNAS mendorong lahirnya kebijakan keamanan digital nasional yang tidak hanya berorientasi pada penindakan, tetapi juga menempatkan aspek pencegahan, edukasi, inovasi, dan pemberdayaan masyarakat sebagai pilar utama. Keamanan ruang digital harus dipandang sebagai investasi jangka panjang untuk menjaga kedaulatan negara, melindungi masyarakat, serta memastikan bahwa transformasi digital benar-benar memberikan manfaat yang sebesar-besarnya bagi kemajuan bangsa Indonesia.

D. Pandangan Sikap PERMIKOMNAS

PERMIKOMNAS berpandangan bahwa:

1. Keamanan ruang digital merupakan bagian integral dari keamanan nasional dan perlindungan hak warga negara.
2. Kepolisian Republik Indonesia memiliki peran strategis dalam penegakan hukum terhadap tindak pidana siber melalui investigasi, digital forensik, patroli siber, dan perlindungan masyarakat.

3. Penegakan hukum harus berjalan beriringan dengan penguatan literasi digital agar masyarakat tidak hanya menjadi objek perlindungan, tetapi juga subjek yang memiliki kemampuan menjaga keamanan dirinya di ruang digital.

4. Pengembangan talenta keamanan siber nasional harus menjadi investasi jangka panjang untuk menghadapi tantangan transformasi digital dan perkembangan kecerdasan buatan.

5. Kolaborasi antara pemerintah, Polri, perguruan tinggi, organisasi kemahasiswaan, dan sektor swasta perlu diperkuat sebagai fondasi ekosistem keamanan digital Indonesia.

E. Gagasan Strategis PERMIKOMNAS

PERMIKOMNAS menawarkan beberapa gagasan strategis:

• Gerakan Nasional Literasi Keamanan Digital berbasis kampus.
• Program Cyber Awareness bersama Kepolisian Republik Indonesia.
• Penguatan pelatihan digital forensik dan keamanan siber bagi mahasiswa. • Pembentukan pusat kajian keamanan ruang digital berbasis perguruan tinggi. • Kolaborasi riset dan penyusunan rekomendasi kebijakan mengenai pemberantasan penipuan digital, perjudian online, perlindungan data pribadi, dan peningkatan kapasitas sumber daya manusia digital.

F. Rekomendasi Kebijakan PERMIKOMNAS kepada Kepolisian Republik Indonesia

Penguatan Keamanan dan Perlindungan Masyarakat di Ruang Digital

Sebagai organisasi mahasiswa nasional yang bergerak di bidang informatika, komputer, dan teknologi informasi, PERMIKOMNAS menyampaikan beberapa rekomendasi kebijakan kepada Kepolisian Negara Republik Indonesia dalam rangka memperkuat keamanan ruang digital dan perlindungan masyarakat Indonesia sebagai berikut:

1. Memperkuat Pendekatan Preventif melalui Literasi Keamanan Digital

Polri perlu memperluas program edukasi dan kampanye nasional terkait keamanan digital, khususnya mengenai penipuan online, phishing, pencurian identitas, investasi ilegal, perjudian daring, serta perlindungan data pribadi. Edukasi harus menyasar pelajar, mahasiswa, masyarakat umum, dan kelompok rentan melalui pendekatan yang mudah dipahami dan berkelanjutan.

2. Membentuk Sistem Peringatan Dini Ancaman Digital kepada Masyarakat

Polri dapat mengembangkan mekanisme Early Warning System yang memberikan informasi cepat kepada masyarakat mengenai modus-modus kejahatan digital terbaru melalui media sosial, aplikasi pesan, situs resmi, dan kerja sama dengan operator telekomunikasi.

3. Memperkuat Sinergi Antar-Lembaga dalam Penanganan Kejahatan Siber

Penanganan kejahatan digital memerlukan koordinasi yang lebih erat antara Polri, Kementerian Komunikasi dan Digital Republik Indonesia, Badan Siber dan Sandi Negara, sektor perbankan, penyelenggara sistem elektronik, serta platform digital untuk mempercepat proses penindakan dan perlindungan korban.

4. Meningkatkan Kapasitas dan Ketersediaan SDM Siber

Polri perlu terus memperkuat kapasitas personel di bidang forensik digital, investigasi siber, kecerdasan siber, dan analisis data melalui pelatihan berkelanjutan serta kolaborasi dengan perguruan tinggi dan komunitas teknologi.

5. Membangun Mekanisme Pelaporan yang Lebih Cepat dan Terintegrasi

Diperlukan sistem pelaporan kejahatan siber yang mudah diakses, responsif, dan terintegrasi secara nasional sehingga masyarakat dapat segera melaporkan kasus penipuan digital, pencurian data pribadi, maupun kejahatan siber lainnya tanpa hambatan birokrasi yang panjang.

6. Mengoptimalkan Pemanfaatan Teknologi dan Kecerdasan Buatan untuk Deteksi Kejahatan Siber

Polri dapat memperkuat penggunaan teknologi analitik, big data, dan kecerdasan buatan (AI) untuk mendeteksi pola kejahatan digital, memetakan jaringan pelaku, serta meningkatkan efektivitas pencegahan dan penegakan hukum.

7. Membentuk Forum Kolaborasi Keamanan Digital Nasional

PERMIKOMNAS merekomendasikan pembentukan forum kolaboratif yang melibatkan pemerintah, aparat penegak hukum, akademisi, industri teknologi, organisasi mahasiswa, dan masyarakat sipil untuk merumuskan solusi bersama terhadap tantangan keamanan digital nasional.

8. Mendorong Program Nasional Relawan Keamanan Digital

Polri dapat berkolaborasi dengan perguruan tinggi dan organisasi kemahasiswaan untuk membentuk relawan keamanan digital yang berperan dalam edukasi masyarakat, kampanye anti penipuan digital, serta peningkatan kesadaran keamanan siber di berbagai daerah.

9. Memperkuat Perlindungan Kelompok Rentan di Ruang Digital

Polri perlu memberikan perhatian khusus terhadap perlindungan anak, perempuan, lansia, dan masyarakat dengan tingkat literasi digital rendah yang sering menjadi sasaran utama kejahatan

siber dan eksploitasi digital.

10. Membangun Kemitraan Strategis dengan PERMIKOMNAS

PERMIKOMNAS siap menjadi mitra strategis Polri dalam pengembangan talenta digital, edukasi keamanan siber, riset teknologi, kampanye literasi digital, serta pelaksanaan program-program penguatan keamanan ruang digital yang melibatkan mahasiswa di seluruh Indonesia.

G. Posisi Strategis PERMIKOMNAS

Sebagai organisasi nasional yang menghimpun mahasiswa informatika, komputer, dan teknologi informasi dari berbagai perguruan tinggi di Indonesia, PERMIKOMNAS memiliki tanggung jawab moral dan akademik untuk berkontribusi dalam penguatan keamanan ruang digital nasional. Mahasiswa tidak hanya diposisikan sebagai pengguna teknologi, tetapi juga sebagai calon inovator, peneliti, dan agen perubahan yang mampu mendukung pembangunan ekosistem digital Indonesia

H. Penutup

PERMIKOMNAS meyakini bahwa keberhasilan transformasi digital Indonesia tidak hanya diukur dari tingginya tingkat adopsi teknologi, tetapi juga dari kemampuan negara dalam melindungi masyarakat dari berbagai ancaman di ruang digital. Oleh karena itu, diperlukan kolaborasi yang erat antara pemerintah, Kepolisian Republik Indonesia, perguruan tinggi, dunia usaha, dan masyarakat untuk mewujudkan ruang digital Indonesia yang aman, produktif, inklusif, dan berkeadilan.

Daftar sumber

1. PPATK – *Catatan Capaian Strategis PPATK Tahun 2025: Menjaga Kedaulatan dan Integritas Ekonomi Bangsa*
   https://www.ppatk.go.id/siaran_pers/read/1594/catatan-capaian-strategis-ppatk-tahun 2025-menjaga-kedaulatan-dan-integritas-ekonomi-bangsa-jakarta-28-januari-2026-b001hm0531i2026-.html
2. Hukumonline – *Penipuan Keuangan Melonjak, 225 Ribu Laporan dan Rp4,6 Triliun Kerugian*
   https://www.hukumonline.com/berita/a/penipuan-keuangan-melonjak--225-ribu-laporan dan-rp4-6-triliun-kerugian-lt68a6959902069/
3. Komdigi – *Kejahatan Siber Capai Kerugian Rp476 M, AI Diperkuat untuk Cegah Ancaman di Ruang Digital*
   https://www.komdigi.go.id/berita/siaran-pers/detail/kejahatan-siber-capai-kerugian-rp 476-m-ai-diperkuat-untuk-cegah-ancaman-di-ruang-digital
4. Tempo – *Bareskrim Tangani 664 Kasus Kejahatan Siber Sepanjang 2025*
   https://www.tempo.co/hukum/bareskrim-tangani-664-kasus-kejahatan-siber-sepanjang 2025-2105460

5. Open Data Jawa Barat – *Indeks Literasi Digital Berdasarkan Provinsi di Indonesia*
https://opendata.jabarprov.go.id/en/dataset/indeks-literasi-digital-berdasarkan-provinsi-di-indonesia
6. Indonesia Baik – *Seberapa Digital Masyarakat Indonesia*
https://indonesiabaik.id/infografis/seberapa-digital-masyarakat-imd-indonesia 7. Government Technology Indonesia – *Data Pribadi yang Paling Sering Terpapar dalam Kebocoran Data*
https://govtech.ksp.go.id/data-pribadi-yang-paling-sering-terpapar-dalam-kebocoran-data-seriesamankandatapribadi.html
8. AAG IT – *The Latest Cyber Crime Statistics*
https://aag-it.com/the-latest-cyber-crime-statistics/
9. APJII – *Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*
https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang
10. BPS – *Statistik Telekomunikasi Indonesia 2024*
https://www.bps.go.id/id/publication/2025/08/29/beaa2be400eda6ce6c636ef8/statistik-telekomunikasi-indonesia-2024.html