Polri di Era Siber: Tantangan dan Peluang Transformasi Digital

Oleh: Tim CSP – Center for Strategic Policing

A. Pendahuluan

Perkembangan teknologi digital dalam dua dekade terakhir telah mengubah hampir seluruh aspek kehidupan manusia. Di Indonesia, percepatan transformasi digital makin nyata sejak pandemi Covid-19, ketika layanan publik, aktivitas ekonomi, hingga interaksi sosial beralih ke ruang daring. Fenomena ini melahirkan lanskap baru yang tidak hanya menghadirkan peluang, tetapi juga tantangan serius bagi institusi penegak hukum.

Polri sebagai garda terdepan dalam menjaga keamanan dan ketertiban masyarakat tidak bisa menghindar dari arus perubahan ini. Jika dahulu fokus utama adalah penanganan kejahatan konvensional seperti pencurian, narkotika, dan tindak kekerasan, kini Polri dihadapkan pada spektrum ancaman yang jauh lebih kompleks: serangan siber, penipuan online lintas negara, peredaran informasi palsu yang

memicu keresahan publik, hingga risiko pelanggaran privasi akibat pengawasan digital.

Di satu sisi, teknologi digital menyediakan instrumen baru bagi Polri untuk meningkatkan efektivitas kerja—mulai dari pemantauan berbasis CCTV cerdas, penggunaan artificial intelligence untuk prediksi kriminalitas, hingga pemanfaatan aplikasi digital untuk laporan masyarakat. Namun di sisi lain, pemanfaatan teknologi tanpa regulasi dan etika yang jelas berpotensi menimbulkan masalah baru: penyalahgunaan kewenangan, pengawasan massal yang menggerus hak privasi, dan menurunnya kepercayaan publik.

Karena itu, pembahasan mengenai Polri di era siber tidak hanya berhenti pada aspek teknis atau modernisasi peralatan. Lebih dari itu, terdapat sejumlah persoalan fundamental yang perlu dicermati.

Pertama, keterbatasan kapasitas sumber daya manusia Polri dalam menghadapi kejahatan berbasis teknologi tinggi, di mana para pelaku sering kali lebih cepat beradaptasi dibanding aparat penegak hukum.

Kedua, persoalan regulasi dan koordinasi lintas lembaga: belum adanya payung hukum yang komprehensif terkait keamanan siber sering menimbulkan tumpang tindih kewenangan antara Polri, BSSN, dan lembaga lain.

Ketiga, risiko penyalahgunaan kewenangan dalam pemanfaatan teknologi digital, misalnya praktik pengawasan massal tanpa mekanisme akuntabilitas

yang jelas, yang berpotensi menggerus hak privasi dan kebebasan sipil warga.

Keempat, kesenjangan teknologi dan infrastruktur: masih ada daerah yang minim akses digital, sementara Polri dituntut untuk melayani masyarakat secara setara di seluruh wilayah Indonesia.

Persoalan-persoalan ini menunjukkan bahwa transformasi digital Polri tidak cukup hanya berorientasi pada modernisasi alat, melainkan harus ditempatkan dalam kerangka tata kelola demokratis, transparan, dan berbasis hak asasi manusia.

B. Lanskap Tantangan Polri di Era Siber

Transformasi digital membuka peluang besar bagi Polri dalam memperkuat pelayanan publik sekaligus meningkatkan efektivitas penegakan hukum. Namun, di balik peluang itu, terbentang pula tantangan yang kompleks. Era siber melahirkan bentuk-bentuk kejahatan baru yang melintasi batas negara, menyebar dalam hitungan detik, dan sering kali melibatkan teknologi yang jauh lebih canggih dibandingkan perangkat yang dimiliki aparat. Kondisi ini menuntut Polri tidak hanya mengejar ketertinggalan dari sisi teknologi, tetapi juga beradaptasi secara kelembagaan, regulatif, dan etis.

Selain dimensi teknis, era digital juga membawa problem serius bagi demokrasi dan hak asasi manusia. Teknologi siber berpotensi menjadi pedang bermata dua: di satu sisi dapat melindungi masyarakat, tetapi

di sisi lain dapat digunakan secara represif jika tidak diawasi dengan baik. Polri ditantang untuk membangun keseimbangan yang sulit antara menjaga keamanan siber nasional, memberantas kejahatan digital, dan tetap menghormati hak-hak sipil. Dalam konteks inilah, beberapa tantangan utama perlu dicermati lebih jauh.

Beberapa statistik terbaru menunjukkan bahwa kejahatan siber dan isu keamanan digital di Indonesia bukan cuma potensi — tapi sudah nyata dan terus meningkat dalam berbagai bentuk. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2023 Indonesia menjadi sasaran serangan digital dalam skala yang sangat masif. Tercatat sekitar **403 juta trafik anomali atau serangan siber** masuk ke sistem dan jaringan di Indonesia, dengan intensitas serangan paling tinggi terjadi pada bulan Agustus. Angka ini menunjukkan betapa luasnya kerentanan ruang digital nasional terhadap berbagai upaya peretasan maupun serangan siber lintas negara.

Kerentanan tersebut semakin terasa dalam kehidupan sehari-hari masyarakat. Riset yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2024 mengungkap bahwa **lebih dari sepertiga pengguna internet di Indonesia, yakni sekitar 32,50 persen, pernah menjadi korban penipuan online**. Angka ini melonjak tajam dibandingkan tahun sebelumnya. Tidak hanya itu, **20,97 persen responden** mengaku mengalami kebocoran data pribadi, menandakan lemahnya

perlindungan informasi digital dan tingginya risiko penyalahgunaan identitas di ruang maya.

Dampak finansial dari kejahatan digital juga tidak bisa dipandang sebelah mata. Otoritas Jasa Keuangan (OJK) melaporkan bahwa hingga 9 Februari 2025, lembaga ini telah menerima **42.257 laporan kasus penipuan transaksi keuangan** yang ditangani melalui Indonesia Anti-Scam Centre (IASC). Total kerugian yang diderita masyarakat akibat penipuan ini mencapai **Rp700,2 miliar**, sebuah angka yang memperlihatkan skala kerusakan ekonomi akibat maraknya kejahatan digital, sekaligus tantangan besar bagi aparat penegak hukum untuk melakukan pencegahan dan penindakan yang lebih efektif.

Data dari laporan penipuan keuangan melalui IASC maupun survei APJII menunjukkan bahwa persoalan keamanan digital bukan sekadar urusan teknis. Masalah ini sudah menyentuh hal yang lebih mendasar, yaitu kepercayaan publik terhadap sistem digital, kerentanan sosial masyarakat terhadap kejahatan online, serta hak setiap warga negara untuk mendapatkan perlindungan atas data pribadi dan keamanan digitalnya.

Melihat tingginya angka serangan siber, penipuan online, hingga kebocoran data pribadi, jelas bahwa Polri menghadapi tantangan serius dalam menjaga ruang digital Indonesia. Masalah-masalah ini tidak berdiri sendiri, tetapi saling terkait dan membentuk lanskap ancaman yang kompleks. Untuk itu, penting dipetakan secara lebih rinci beberapa tantangan utama yang dihadapi Polri di era siber.

Pertama, Kejahatan Siber yang Meluas. Dalam lima tahun terakhir, Indonesia menghadapi lonjakan signifikan kasus kejahatan siber, mulai dari penipuan online, peretasan data pribadi, hingga serangan ransomware terhadap institusi vital. Kasus kebocoran data besar-besaran yang melibatkan jutaan pengguna platform digital menegaskan rapuhnya sistem keamanan siber nasional. Di sisi lain, perdagangan ilegal di dark web juga kian marak, mulai dari jual beli narkoba, senjata, hingga data pribadi warga negara. Polri memang telah membentuk Direktorat Tindak Pidana Siber, namun kapasitas penanganannya masih tertinggal dibandingkan kecepatan inovasi para pelaku. Modus operandi pelaku semakin kompleks—menggunakan server lintas negara, sistem enkripsi berlapis, dan teknik manipulasi digital—sehingga banyak kasus yang sulit diungkap tuntas.

Kedua, Disinformasi dan Hoaks. Selain kejahatan siber konvensional, penyebaran disinformasi dan hoaks di media sosial menjadi tantangan besar. Gelombang informasi palsu yang menyebar cepat melalui WhatsApp, Twitter/X, atau Facebook kerap memicu instabilitas sosial-politik. Kasus hoaks seputar pandemi COVID-19, misalnya, memperlihatkan bagaimana kabar bohong dapat memengaruhi perilaku masyarakat secara masif. Demikian pula menjelang pemilu, maraknya disinformasi politik dapat menggerus kepercayaan publik terhadap institusi demokrasi. Polri dituntut tidak hanya melakukan penindakan hukum, tetapi

juga membangun strategi literasi digital bersama masyarakat sipil untuk mencegah dampak lebih luas.

Ketiga, Kesenjangan Kapasitas SDM. Sumber daya manusia menjadi salah satu persoalan mendasar. Banyak personel Polri masih memiliki keterbatasan dalam literasi digital, terutama terkait investigasi forensik siber, cyber intelligence, hingga penggunaan artificial intelligence untuk mendeteksi pola kejahatan digital. Pelatihan yang ada sering kali berfokus pada prosedur umum, bukan penguasaan teknis mendalam. Kondisi ini menyebabkan kasus-kasus besar seperti peretasan server pemerintah atau penipuan lintas negara kerap membutuhkan waktu lama untuk ditangani, bahkan tak jarang melibatkan bantuan pihak luar negeri. Tanpa penguatan kapasitas SDM yang sistematis, Polri akan terus tertinggal dalam menghadapi perkembangan kejahatan digital yang semakin canggih.

Keempat, Risiko Etis dan Hak Asasi. Transformasi digital juga membuka potensi problem etis yang serius. Teknologi digital yang seharusnya dipakai untuk melindungi masyarakat bisa berubah menjadi instrumen represi apabila digunakan tanpa mekanisme akuntabilitas. Dugaan praktik pengawasan digital massal, pemantauan percakapan pribadi, atau pemblokiran akun tanpa dasar hukum yang jelas sering menimbulkan kecurigaan publik. Hal ini menyinggung isu fundamental tentang privasi dan kebebasan berekspresi. Tanpa regulasi yang transparan serta mekanisme pengawasan independen, risiko penyalahgunaan teknologi oleh

aparat justru akan merusak kepercayaan publik terhadap institusi Polri.

Kelima, Kesenjangan Infrastruktur dan Akses Digital. Di luar persoalan teknis dan etis, transformasi digital Polri juga menghadapi kendala struktural berupa kesenjangan infrastruktur. Aplikasi layanan kepolisian berbasis daring seperti e-Tilang atau SPKT online relatif mudah diakses masyarakat perkotaan, tetapi di daerah pedalaman atau wilayah 3T (terdepan, terluar, tertinggal), akses internet masih menjadi persoalan besar. Keterbatasan infrastruktur ini membuat sebagian warga tetap bergantung pada mekanisme manual, sehingga reformasi digital Polri berjalan tidak merata. Alih-alih memperkuat pelayanan publik, hal ini justru berpotensi memperlebar jurang kepercayaan antara masyarakat di pusat dan pinggiran.

C. Peluang Transformasi Digital Polri

Jika tantangan di ruang siber begitu kompleks, maka peluang yang terbuka melalui transformasi digital juga tidak kalah besar. Polri memiliki kesempatan untuk memanfaatkan teknologi bukan hanya sebagai alat pendukung, tetapi juga sebagai fondasi utama dalam memperkuat legitimasi dan kinerja institusi.

Pertama, pemanfaatan *digital tools* dapat menjadi langkah konkret untuk meningkatkan akuntabilitas dan efektivitas. Penggunaan *body-worn camera*

misalnya, terbukti di banyak negara mampu mengurangi potensi penyalahgunaan wewenang dan sekaligus menjadi bukti obyektif dalam penanganan kasus. Di sisi lain, sistem *e-reporting* memungkinkan masyarakat melaporkan tindak kejahatan secara lebih cepat, transparan, dan mudah diakses, tanpa harus melalui jalur birokratis yang panjang. Sementara itu, *big data analytics* dapat membantu Polri dalam menganalisis pola kriminalitas, memprediksi potensi kejahatan, dan merancang strategi pencegahan yang lebih presisi.

Kedua, konsep *smart policing* memberi ruang bagi Polri untuk melangkah lebih jauh. Integrasi ribuan kamera CCTV di ruang publik dengan *command center* berbasis kecerdasan buatan (AI) akan memperkuat sistem pencegahan kejahatan. Teknologi ini memungkinkan pengawasan yang lebih luas, identifikasi dini terhadap ancaman, hingga respons cepat terhadap insiden di lapangan. Model ini juga sejalan dengan praktik kepolisian modern di berbagai negara yang mengedepankan efisiensi dan efektivitas penanganan kasus.

Ketiga, di era kejahatan siber yang melintasi batas negara, kerja sama internasional menjadi peluang strategis. Polri dapat memperkuat sinergi dengan Interpol, ASEANAPOL, maupun forum regional lainnya untuk menghadapi kejahatan lintas negara seperti *ransomware*, *phishing*, atau perdagangan ilegal di *dark web*. Kolaborasi ini penting, sebab kejahatan digital tidak mengenal batas yurisdiksi, dan hanya bisa dihadapi melalui koordinasi global.

Keempat, transformasi digital juga membuka jalan bagi peningkatan transparansi layanan publik. Aplikasi resmi, portal digital, hingga dashboard keterbukaan data dapat menjadi sarana bagi masyarakat untuk mengakses informasi layanan kepolisian secara cepat dan akuntabel. Langkah ini tidak hanya meningkatkan kualitas pelayanan publik, tetapi juga memperkuat kepercayaan masyarakat terhadap Polri sebagai institusi yang terbuka dan modern.

Dengan mengoptimalkan peluang ini, Polri bukan hanya mampu menjawab tantangan era siber, tetapi juga menempatkan diri sebagai institusi yang adaptif, transparan, dan sejalan dengan kebutuhan masyarakat di era digital.

D. Konsep, Kebijakan, dan Strategi Transformasi Digital Polri

Transformasi digital di tubuh Polri tidak bisa berjalan spontan atau parsial; ia membutuhkan fondasi konseptual yang jelas, arah kebijakan yang konsisten, serta strategi implementasi yang terukur. Tanpa itu, penggunaan teknologi hanya akan menjadi simbol modernitas tanpa menghasilkan perubahan nyata.

Pertama, aspek konsep. Transformasi digital Polri harus berpijak pada paradigma *policing by consent*—bahwa legitimasi kepolisian bukan sekadar berasal dari kewenangan hukum, tetapi dari penerimaan

masyarakat. Artinya, setiap teknologi yang diadopsi, baik berupa *AI surveillance*, *big data analytics*, maupun aplikasi layanan publik, harus dirancang dengan prinsip *human-centered policing*. Prinsip ini memastikan bahwa teknologi mendukung pelayanan dan perlindungan masyarakat, bukan menjadi instrumen kontrol yang menimbulkan ketakutan.

Kedua, arah kebijakan. Polri sebenarnya sudah merumuskan kerangka *Polri Presisi* (Prediktif, Responsibilitas, Transparansi Berkeadilan) sejak 2021, yang salah satu pilar utamanya adalah digitalisasi pelayanan publik dan manajemen internal. Program seperti *E-Tilang*, *SPKT Online*, *SIM Online*, hingga *SKCK Digital* menunjukkan upaya Polri mengurangi birokrasi manual dan membuka akses layanan berbasis daring. Selain itu, terdapat pengembangan *Command Center* di beberapa Polda dengan integrasi CCTV dan sistem *face recognition* untuk menunjang *predictive policing*. Namun, kebijakan ini masih menghadapi tantangan konsistensi, terutama dalam hal perlindungan data pribadi, transparansi algoritma, dan pengawasan eksternal. Oleh karena itu, sinkronisasi dengan UU Perlindungan Data Pribadi (PDP) 2022, strategi keamanan siber BSSN, serta kerangka transformasi digital nasional menjadi mutlak.

Ketiga, strategi implementasi. Pada tahap ini, ada beberapa hal krusial. Pertama, penguatan kapasitas SDM digital di internal Polri. Tanpa literasi digital yang merata, teknologi secanggih apapun akan sia-sia. Kedua, pembangunan infrastruktur digital yang andal, termasuk jaringan komunikasi aman,

pusat data terintegrasi, dan *command center* modern di tiap wilayah. Ketiga, mendorong kerja sama multipihak—baik dengan sektor swasta, akademisi, maupun lembaga internasional—untuk mempercepat adopsi teknologi dan alih pengetahuan. Keempat, menerapkan mekanisme *check and balance* dengan melibatkan pengawasan eksternal agar setiap strategi digital Polri tetap selaras dengan prinsip akuntabilitas publik.

Dengan konsep yang berpihak pada warga, kebijakan yang konsisten, serta strategi implementasi yang inklusif, transformasi digital Polri dapat diarahkan bukan hanya untuk meningkatkan keamanan, tetapi juga untuk memperkuat demokrasi dan hak-hak sipil di Indonesia.

E. Penutup

Memasuki era digital yang ditandai dengan percepatan teknologi informasi, Polri berada pada persimpangan penting. Di satu sisi, ancaman kejahatan siber, disinformasi, dan penyalahgunaan data semakin kompleks dan menuntut respons yang adaptif. Di sisi lain, peluang untuk memanfaatkan teknologi digital sebagai sarana meningkatkan pelayanan publik, memperkuat transparansi, serta mengembangkan *predictive policing* terbuka sangat luas.

Tantangan terbesar bukan sekadar ketersediaan teknologi, melainkan bagaimana Polri mampu

mengelola transformasi ini dengan tetap berpegang pada prinsip demokrasi, penghormatan hak asasi manusia, serta akuntabilitas publik. Data yang menunjukkan ratusan juta serangan siber, puluhan ribu laporan penipuan digital, hingga kebocoran data pribadi yang dialami jutaan warga, memperlihatkan bahwa keamanan digital tidak lagi bisa dipandang sebagai isu teknis semata. Ia telah menjadi bagian integral dari kepercayaan publik terhadap negara dan aparat penegaknya.

Oleh karena itu, keberhasilan transformasi digital Polri akan sangat ditentukan oleh tiga hal: orientasi kebijakan yang konsisten, kemampuan membangun kapasitas SDM digital yang mumpuni, serta keterbukaan dalam melibatkan publik dan lembaga pengawas independen. Tanpa itu, modernisasi digital Polri berisiko terjebak menjadi proyek teknologi semata—canggih di permukaan, tetapi gagal menjawab kebutuhan masyarakat.

Dengan strategi yang tepat, Polri tidak hanya dapat menegakkan hukum di ruang siber, tetapi juga tampil sebagai institusi yang adaptif, transparan, dan dipercaya. Transformasi digital bukanlah tujuan akhir, melainkan jalan untuk membangun kepolisian yang relevan dengan tantangan zaman sekaligus teguh pada mandat demokratisnya: melindungi, mengayomi, dan melayani seluruh warga negara. []