Modernisasi Masyarakat Dan Keamanan Siber Ditinjau Dari Perspektif Hukum Perlindungan Data Pribadi

Rusdianto Sesung [1], Akhmad Anshari [2]
[1,2] Universitas Narotama Surabaya
E-mail: rusdianto@narotama.ac.id[1], anshariakhmad388@gmail.com[2]

Article History:
Received: 10 Maret 2025
Revised: 08 April 2025
Accepted: 11 April 2025

Keywords: *Modernisasi, keamanan siber, hukum perlindungan pribadi*

Abstract: *Penelitian ini bertujuan untuk mengetahui modernisasi masyarakat dan keamanan siber ditinjau dari perspektif hukum perlindungan data pribadi. Jenis data dalam penelitian ini yaitu primer dan sekunder. Tekhnik pengumpulan data primer diperoleh dari studi literatur melalui buku dan artikel jurnal dimana memiliki keterkaitan terhadap keamanan siber dan kedaulatan data. Berdasarkan hasil penelitian Modernisasi masyarakat yang ditandai dengan pesatnya perkembangan teknologi digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk cara individu, perusahaan, dan pemerintah mengelola serta memanfaatkan data pribadi. Namun, di balik kemajuan ini, muncul tantangan besar dalam hal keamanan siber, yang menjadi semakin kompleks seiring dengan meningkatnya ancaman seperti serangan peretasan, pencurian data, dan penyalahgunaan informasi pribadi. Dari perspektif hukum perlindungan data pribadi, modernisasi menuntut adanya regulasi yang kuat dan implementasi yang efektif untuk melindungi hak individu atas data mereka. Dengan pendekatan yang komprehensif dan sinergi antara berbagai pemangku kepentingan, modernisasi dapat berjalan selaras dengan keamanan siber yang optimal, sehingga hak atas perlindungan data pribadi dapat terjamin di era digital ini.*

PENDAHULUAN

Perkembangan teknologi yang sangat pesat dan kemampuan manusia untuk mendapatkan akses internet telah meningkatkan kesejahteraan hidup manusia, yang digunakan untuk keperluan berkomunikasi maupun melakukan transaksi elektronik. Perkembangan perangkat komputer yang semakin canggih dan cepat membawa manusia masuk ke dalam sebuah dunia yang sering disebut siber (Muhammad Prakoso Aji, 2023). Kemudahan dalam berkomunikasi dan bertransaksi secara daring dapat memudahkan semua pihak untuk mendapatkan dan menggunakan data pribadi seseorang untuk diproses secara baik. Seseorang dapat menunjukkan jati dirinya di dalam dunia siber, layaknya seperti di dunia nyata.

Dengan bertumbuhnya kemampuan perangkat lunak yang tersedia, masyarakat sudah dapat

melakukan hal-hal yang awalnya mustahil menjadi mungkin seperti dengan melakukan pembayaran menggunakan gadget atau gawai, melakukan pembelian makanan, membeli alat elektronik, membeli saham dan lain-lain. Salah satu kasus terbesar yang pernah terjadi di Indonesia adalah peretasan data pribadi pengguna dan penjual situs Tokopedia pada tahun 2019, dimana data atas nama lengkap, tanggal lahir, jenis kelamin, alamat email, nomor telepon genggam, dan encrypted password diperjual-beli kan melalui dark-web (Kennedy, 2024).

Pemanfaatan akan teknologi dan informasi dapat dirasakan manfaatnya baik di bidang pendidikan dan perekonomian dan lain-lain, hal-hal yang berkaitan dengan perkembanagan ilmu pengetahuan, sains dan lain sebagainya yang dengan mudah dapat di akses, sehingga milyaran bahkan triliyunan informasi dapat kita terima dengan cepat. Dalam bidang pekerjaan, pengelolaan data yang berjumlah sangat banyak dapat dikelola dengan baik, cepat, efektif dan efisien serta meminimalisir kesalahan. Dalam bidang perekonomian, promosi-promosi dan potensi-potensi dalam meningkatkan kesejahteraan masyarakat dilakukan degan cepat tanpa batasan tempat atau wilayah dan menjangkau semua lapisan masyarakat baik nasional maupun internasional. Akan tetapi perkembangan teknologi dan informasi ini tidak saja memberikan manfaat melainkan juga mengakibatkan masalah yang dapat merugikan masyarakat, seperti halnya penyalahgunaan data, pencurian data pribadi, penjualan data pribadi, penipuan dan lain-lain (Situmeang, 2021).

Meskipun Indonesia berada pada peringkat ke-24 dari 194 negara dalam Global Cyber Security Index tahun 2020, peringkat tersebut tidak serta merta mencerminkan kemampuan warga negara Indonesia untuk melindungi data pribadinya dan mendapatkan jaminan proteksi yang aman di ruang siber. Perlindungan data setiap warga negara seharusnya menjadi prioritas, namun kenyataannya berbagai insiden seperti kebocoran data BPJS dan Kementerian Kesehatan, kebocoran data E-KTP, serta peretasan situs Badan Intelijen Negara (BIN) menimbulkan pertanyaan mengenai peran dan kemampuan negara dalam melindungi data pribadi warganya (M. Prakoso Aji & Subakdi, 2024).

Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak), terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber dapat digunakan sebagai sarana melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen. Dengan demikian, keamanan siber adalah semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan pada ketersediaan (*availability*), integritas (*integrity*), dan kerahasiaan (*confidentiality*) dari sebuah informasi (Muhammad Prakoso Aji, 2023).

Perlindungan privasi dan data pribadi sangat mempengaruhi perkembangan digital di suatu negara, tanpa terkecuali Indonesia. Perlindungan tersebut merupakan faktor penentu akan adanya kepercayaan daring (*online trust*). Privasi dan data pribadi menjadi sebuah hal yang penting karena pengguna dalam jaringan tidak akan melakukan sebuah transaksi digital apabila merasa keamanan akan privasi dan data pribadinya terancam. Salah satu perlindungan privasi dan data pribadi tersebut berkenaan bagaimana data pribadi tersebut akan diproses termasuk data sensitif dari pengguna yang apabila disebarkan ke pihak yang tidak bertanggung jawab akan berpotensi menimbulkan kerugian finansial, bahkan mengancam keamanan dan keselamatan pemiliknya. Ancaman-ancaman yang timbul dari lemahnya perlindungan privasi dan data pribaditersebut memiliki korelasi garis lurus dengan pertubuhan ekonomi yang dihasilkan dari transaksi-transaksi dalam jaringan (*online*) (Hanaya, 2023).

Isu privasi dan perlindungan data pribadi perlu menjadi perhatian dalam penyelenggaraan

SPBE. Era digital saat ini justru memberikan tantangan tersendiri terhadap integritas privasi atas data pribadi. Salah satu hal yang menjadikan era digital sebagai tantangan terhadap privasi atas data pribadi adalah sifat dari informasi yang terdigitasi (*digitised information*) yang mendorong terbentuknya lingkungan yang tidak menghormati privasi atas data pribadi, mengingat data pribadi menjadi mudah dikumpulkan dan disebarkan (Rahman, 2021).

Menurut hukum positif yang ada di Indonesia perlindungan terhadap privasi telah dijamin dalam Pasal 28 G ayat 1 Undang-Undang Dasar 1945, menerangkan setiap orang memiliki hak atas perlindungan diri pribadi, keluarga, martabat, kehormatan maupun harta benda yang dimiliki, serta hak untuk memperoleh rasa aman dan perlindungan dari intimidasi untuk dapat bertindak atau tidak yang merupakan hak asasinya.

Pemerintah juga telah membuat regulasi yang mengatur tentang privasi atau data pribadi melalui berbagai regulasi yaitu Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, sebagaimana yang tertuang dalam Pasal 26 Ayat 1 menerangkan bahwa pemanfaatan informasi via elektronik yang berkaitan dengan data pribadi harus berdasarkan persetujuan orang yang bersangkutan, Pasal 1 Undang-Undang Republik Indonesia Nomor. 24 tahun 2013 yang merupakan perubahan dari Undang-Undang nomor 23 Tahun 2006 tentang Administrasi Kependudukan menyatakan data pribadi adalah data perorangan yang disimpan, dijaga, dirawat dan dilindungi kerahasiannya.

Undang-undang RI No. 24 Tahun 2013 perubahaan atas Undang - Undang RI No. 23 Tahun 2006 Pasal 1 Angka 22 tentang Administrasi Kependudukan dinyatakan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dijaga kebenarannya, serta dilindungi kerahasiannya, Pasal 17 huruf h Undang-Undang Nomor 14 Tahun 2008 tentang Informasi Publik menyebutkan informasi publik apabila dibuka dapat membahayakan riwayat, kondisi anggota keluarga, perawatan, pengobatan Kesehatan fisik maupun psikis,kondisi keuangan, aset, pendapat dan rekening bank seseorang yang menyangkut kegiatan Pendidikan formal maupun non formal, Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Berdasarkan latar belakang diatas Penulis tertarik meneliti tentang Modernisasi Masyarakat Dan Keamanan Siber Ditinjau Dari Perspektif Hukum Perlindungan Data Pribadi.

METODE PENELITIAN

Penelitian ini menggunakan bentuk analisis deskriptif dengan metodologi kualitatif guna menjelaskan sesuatu secara intuitif dan sistematis. Penelitian ini bersifat kualitatif, dimana peneliti kualitatif berusaha mencari arti, pemahaman, definisi tentang suatu fenomena, kejadian melalui keterlibatan langsung maupun tidak langsung dalam obyek yang diteliti. Penelitian kualitatif adalah cara yang memfokuskan untuk mendapatkan makna, definisi, konsep, karakteristik, dan sebagainya termasuk deskripsi mengenai fenomena tertentu yang memiliki sifat alami dan menyeluruh yang disajikan secara narratif. Penelitian kualitatif merupakan mekanisme pencarian dan pengumpulan, termasuk analisis dan interpretasi secara komprehensif untuk menghasilkan pemahaman mengenai permasalahan yang menarik (Marzuki, 2005) . Penekanan analisis dekskriptif digunakan dalam penelitian ini untuk menganalisis dan memberikan pemahaman.

Jenis data dalam penelitian ini yaitu primer dan sekunder. Tekhnik pengumpulan data primer diperoleh dari studi literatur melalui buku dan artikel jurnal dimana memiliki keterkaitan

terhadap keamanan siber dan kedaulatan data. Di sisi lain, data sekunder dalam penelitian ini didapatkan melalui media online dan sumber-sumber lainnya, serta digunakan sebagai data pendukung yang memiliki keterkaitan terhadap masalah penelitian. Dengan penggunaan studi pustaka, peneliti akan menjabarkan dan menganalisis sesuai dengan data dan informasi yang dikumpulkan.

HASIL DAN PEMBAHASAN

Perlindungan Data Pribadi

Dalam UU ITE belum memuat aturan tentang perlindungan data pribadi secara khusus. Perlindungan data pribadi dalam sebuah sistem elektronik dalam UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal. Sistem elektronik sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Jadi yang termasuk ke dalam sistem elektronik adalah jaringan internet, layanan e-banking, e-government, jejaring sosial, media elektronik, website, dan lain sebagainya.

Subyek hukum lainnya adalah “Pemroses Data Pribadi” yaitu orang badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang melakukan pemrosesan data pribadi atas nama pengelola data. Pemroses Data Pribadi melakukan kegiatan pemrosesan data pribadi yang berupapengumpulan, perekaman, pencatatan dan atau penyimpanan data pribadi, atau pelaksanaan penyusunan, penyesuaian, perubahan data pribadi, pemulihan kembali data pribadi yang telah dimusnahkan, pengungkapan data pribadi, penggabungan, pembetulan, penghapusan atau penghancuran data pribadi. Ketentuan mengenai perlindungan privasi dan data pribadimerupakan amanah Pasal 28 G Undang-Undang Dasar Republik Indonesia Tahun 1945yang mengatur hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya. Untuk dapat melihat ketentuan tersebut sebagai ketentuan mengenai privasi dan data pribadi, pendapat Warren dan Brandeis dalam karyanya yang berjudul “The Right to Privacy”menyatakan bahwa privasi adalah hak untuk menikmati kehidupan dan hak untukdihargai perasaan dan pikirannya (Hanaya, 2023).

Penyalahgunaan data pribadi tanpa disadari dapat terjadi karena merupakan kelalaian dari calon korban (masyarakat) itu sendiri dalam melaksanakan aktifitasnya sehari-hari. Misalnya tanpa kita sadari pada saat membeli kartu perdana dan kemudian meminta agar petugas konter untuk melakukan pendaftarannya, pada saat mendownload aplikasi, melampirkan data-data pribadi dalam platform atau formulir dan lain sebagainya yang tanpa disadari dapat disalahgunakan oleh petugas konter tersebut dan berpotensi dapat menimbulkan kerugian bagi pemilik data. Selain itu, sebagai akibat lajunya perkembangan ilmu dan teknologi dewasa ini yang populer digunakan adalah terkait big data. Big data yang dianggap sebagai suatu solusi yang menjanjikan dalam mengolah data karena mampu mengolah data yang besar dan bervariatif serta dapat membuat lampiran yang akurat, sehingga membuat big data tidak saja hanya digunakan oleh pihak pemerintah namun digunakan juga oleh pihak swasta. Perusahaan-perusahaan besar yang memanfaatkannya sebagai upaya mempelajari tingkah laku konsumen, seperti loyalitas, pola kunjungan, histori pembelian dan lain-lain, sehingga efektif dalam memasarkan produk atau jasanya. Akan tetapi di sisi lain penyalahgunaan big data tidak dapat dipungkiri dapat juga mengancam privasi seseorang. Misalnya saja gejolak yang muncul ketika harus melakukan regisrasi data pribadi seperti kartu tanda penduduk (KTP) serta kartu keluarga (KK), contoh lain misalnya history pada aplikasi ojeg online, dimana hal tersebut terdapat peluang terjadinya

penyalahgunaan data yang menimbulkan kerugian. Selain itu, saat ini yang sedang marak yaitu dark website yang diduga dapat mengambil data-data pengguna aplikasi zoom.

Peran Negara dalam Ruang Siber

Memaknai perkembangan teknologi dalam suatu negara tidak mungkin tanpa mengkaitkannya dengan peranan negara di dalamnya. Untuk itu, perlu memaknai negara sebagai salah satu bagian dari elemen yang terdapat di dalam politik, selain kekuasaan, pengambilan keputusan, kebijakan, dan pembagian alokasi sumber daya. Representasi kekuasaan yang terdapat dalam suatu negara demokrasi dipegang oleh pemerintah berdaulat yang mendapatkan mandat dari rakyat yang memiliki pokok tujuannya, yaitu untuk meningkatkan kesejahteraan rakyat. Adanya perkembangan teknologi berdampak besar terhadap cara-cara pemerintah menjalankan roda pemerintahan, memberikan pelayanan publik, dan memberikan kepastian hukum yang lebih baik kepada rakyatnya dengan memanfaatkan segala bentuk teknologi baru dalam ruang siber (Muhammad Prakoso Aji, 2023).

Hukum Perlindungan Data Pribadi di Indonesia

Seiring meningkatnya ancaman terhadap data pribadi, pemerintah Indonesia mengesahkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengatur tata kelola data pribadi oleh individu, organisasi, dan perusahaan. Beberapa poin penting dalam UU PDP adalah:

1. Hak Subjek Data
   a. Hak untuk mengetahui bagaimana data pribadinya digunakan
   b. Hak untuk memperbaiki atau menghapus data yang tidak akurat
   c. Hak untuk menarik persetujuan pengolahan data
2. Kewajiban Pengendali Data
   a. Memastikan keamanan data pribadi yang dikelola
   b. Memperoleh persetujuan sah sebelum mengolah data
   c. Melaporkan insiden kebocoran data dalam waktu 72 jam
3. Sanksi bagi Pelanggar
   a. Denda administratif hingga 2% dari pendapatan tahunan
   b. Pidana penjara bagi pelaku penyalahgunaan data
   c. Tuntutan hukum oleh subjek data yang dirugikan

UU PDP ini sejalan dengan regulasi global seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang menjadi standar internasional dalam perlindungan data pribadi.

Tantangan dalam Implementasi Hukum Perlindungan Data Pribadi

Meskipun regulasi sudah ada, implementasinya masih menghadapi beberapa tantangan:

1. **Kurangnya Kesadaran Publik**
   Banyak individu yang masih kurang memahami pentingnya perlindungan data pribadi dan bagaimana data mereka digunakan.
2. **Kepatuhan Perusahaan yang Rendah**
   Beberapa perusahaan belum menerapkan langkah-langkah keamanan yang memadai atau belum menyesuaikan sistem dengan regulasi yang berlaku.
3. **Serangan Siber yang Semakin Canggih**
   Peretas menggunakan teknologi yang semakin maju, sehingga sistem keamanan juga harus selalu diperbarui.

4. **Kurangnya Penegakan Hukum yang Tegas**
   Belum ada banyak kasus pelanggaran data pribadi yang ditindak dengan tegas, sehingga ada celah bagi pelaku untuk lolos dari sanksi.

KESIMPULAN

Modernisasi masyarakat yang ditandai dengan pesatnya perkembangan teknologi digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk cara individu, perusahaan, dan pemerintah mengelola serta memanfaatkan data pribadi. Namun, di balik kemajuan ini, muncul tantangan besar dalam hal keamanan siber, yang menjadi semakin kompleks seiring dengan meningkatnya ancaman seperti serangan peretasan, pencurian data, dan penyalahgunaan informasi pribadi.

Dari perspektif hukum perlindungan data pribadi, modernisasi menuntut adanya regulasi yang kuat dan implementasi yang efektif untuk melindungi hak individu atas data mereka. Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 di Indonesia telah menjadi landasan hukum penting dalam memastikan bahwa setiap entitas yang mengelola data pribadi bertanggung jawab atas keamanan dan penggunaannya. Regulasi ini sejalan dengan standar global seperti General Data Protection Regulation (GDPR), yang memberikan hak kepada individu atas data mereka serta menetapkan sanksi bagi pelanggar.

Meskipun demikian, tantangan dalam implementasi regulasi masih cukup besar, termasuk rendahnya kesadaran masyarakat akan pentingnya perlindungan data pribadi, kurangnya kepatuhan dari perusahaan, serta meningkatnya serangan siber yang semakin canggih. Oleh karena itu, diperlukan langkah-langkah konkret, seperti penguatan regulasi, peningkatan kesadaran publik, adopsi teknologi keamanan yang lebih baik, serta kolaborasi antara pemerintah, sektor swasta, dan akademisi untuk menciptakan ekosistem keamanan siber yang lebih kuat.

Dengan pendekatan yang komprehensif dan sinergi antara berbagai pemangku kepentingan, modernisasi dapat berjalan selaras dengan keamanan siber yang optimal, sehingga hak atas perlindungan data pribadi dapat terjamin di era digital ini.

DAFTAR REFERENSI

Aji, M. Prakoso, & Subakdi, Subakdi. (2024). Sosialisasi Kesadaran Keamanan Siber dan Perlindungan Data Pribadi Bagi Warga di Kelurahan Pangkalan Jati, Kota Depok. *Jurnal Syntax Admiration*, *5*(8), 2928–2937. https://doi.org/10.46799/jsa.v5i8.1494

Aji, Muhammad Prakoso. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Hanaya, Esther. (2023). Perlindungan Data Pribadi di Era Digital Dalam Perspektif Perbandingan Hukum. *Jurnal Bevinding*, *1*(9), 11–22.

Kennedy, Alexander. (2024). Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. *Hukum Dinamika Ekselensia*, *6*(2), 82–98. Retrieved from https://journalpedia.com/1/index.php/hde/article/view/1559

Rahman, Faiz. (2021). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia. *Jurnal Legislasi Indonesia*, *18*(1), 81. https://doi.org/10.54629/jli.v18i1.736

Situmeang, Sahat Maruli Tua. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394