



## KEAMANAN SIBER *WEBSITE* PEMERINTAH DAERAH

Ahmad Budiman\*

Abstrak

*Kemkomdigi mencatat hingga 11 Juni 2025, telah menemukan sebanyak 60.458 konten judi online yang menyusupi situs-situs pemerintahan termasuk website pemerintah daerah. Website bermanfaat sebagai jembatan antara pemerintah daerah dan masyarakat dalam memastikan transparansi, akuntabilitas, dan keterbukaan publik. Permasalahannya, website pemerintah daerah masih sangat rentan untuk disusupi konten negatif. Tulisan ini mengkaji keamanan siber website pemerintah daerah. Keamanan data menjadi tantangan tersendiri, karena masih banyak website pemerintah daerah yang belum menerapkan standar perlindungan data yang kuat, sehingga rentan terhadap peretasan atau kebocoran informasi. Langkah strategis keamanan siber perlu dilakukan dengan menyediakan perangkat keras dan lunak yang mendukung keamanan siber. Penggunaan kecerdasan buatan mampu mendeteksi ancaman secara real-time. Komisi I DPR melalui pelaksanaan fungsi legislasi dapat memprioritaskan pembahasan RUU Keamanan dan Ketahanan Siber sebagai landasan hukum bagi pengaturan keamanan siber termasuk juga keamanan website pemerintah daerah.*

### Pendahuluan

Kementerian Komunikasi dan Digital (Kemkomdigi) memiliki fungsi yang salah satunya terkait dengan pengawasan ruang digital, termasuk kepada pemerintah daerah dalam mengelola website agar tidak mudah disusupi konten negatif. Direktur Jenderal Pengawasan Ruang Digital Kemkomdigi, Alexander Sabar, menjelaskan akan melakukan pemutusan akses terhadap *website* pemerintah daerah bila terdapat konten negatif di dalamnya (Kristianti, 2025). Data Kemkomdigi mencatat sejak 2022 hingga 11 Juni 2025, Kemkomdigi telah menemukan sebanyak 60.458 konten judi *online* yang menyusupi situs-situs pemerintahan. Sebanyak 59.447 konten telah ditangani oleh pengelola *website* terkait sehingga tidak bisa lagi diakses, dan sebanyak 1.011 konten masih dalam tahapan pemrosesan untuk ditindaklanjuti oleh pengelola (Kristianti, 2025).

Pemerintah daerah dapat meminta *Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center* (Id-SIRTII/CC) untuk memberikan bantuan pendampingan pengamanan dan keamanan jaringan termasuk website di instansinya. Hal ini

\*) Analisis Legislatif Ahli Madya Bidang Politik, Hukum, Keamanan, dan HAM pada Pusat Analisis Keparlemenan, Badan Keahlian DPR RI. Email: [lisbet@dpr.go.id](mailto:lisbet@dpr.go.id).

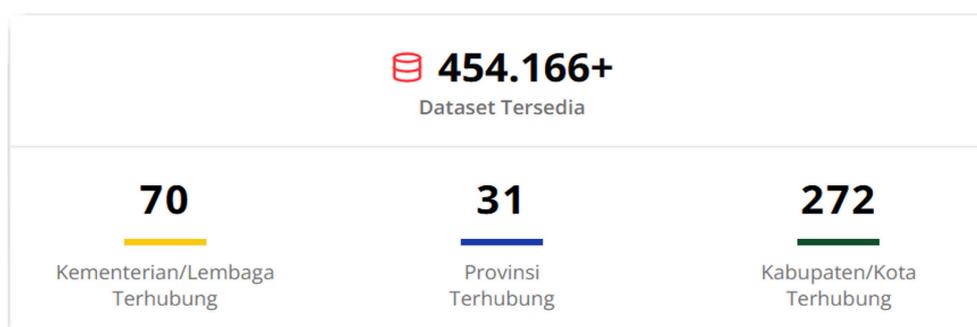
karena Id-SIRTII/CC dapat melakukan deteksi dan peringatan dini terhadap ancaman jaringan telekomunikasi (Id-SIRTII/CC, 2025).

*Website* pemerintah daerah menjadi salah satu media komunikasi untuk menyampaikan informasi kepada masyarakat. *Website* ini tidak hanya berfungsi sebagai portal informasi, tetapi juga sebagai jembatan antara pemerintah daerah dan masyarakat dalam memastikan transparansi, akuntabilitas, dan keterbukaan publik. Untuk itu keamanan siber *website* pemerintah daerah sangat diutamakan. Permasalahannya, *website* pemerintah daerah masih sangat rentan untuk disusupi konten negatif, sehingga akan mengganggu pelayanan publik secara digital. Oleh karena itu tulisan ini akan mengkaji keamanan siber *website* pemerintah daerah.

## Website Pemerintah Daerah

*Website* pemerintah daerah bukan sekadar media informasi, melainkan instrumen strategis dalam mendorong transparansi, akuntabilitas, dan keterbukaan publik. Keberadaan fitur-fitur seperti layanan publik *online*, sistem umpan balik, dan laporan keuangan terbuka juga mendorong partisipasi aktif masyarakat serta meminimalkan potensi penyimpangan birokrasi. Untuk itu, optimalisasi *website* dengan tampilan yang *user-friendly*, konten yang selalu diperbarui, aksesibilitas yang inklusif, serta jaminan keamanan data menjadi hal krusial (Diskominfo, 2024).

Jumlah pasti situs *website* pemerintah daerah di Indonesia pada tahun 2025 tidak tersedia secara spesifik. Namun, jumlahnya diperkirakan melebihi 300. Estimasi ini didasarkan pada integrasi seluruh daerah ke dalam sistem Portal Satu Data Indonesia.



Sumber: Kementerian PPN/Bapenas, 2025.

**Gambar 1.** Estimasi *Website* Pemerintah Daerah Tahun 2025

Salah satu kekurangan utama dalam pengelolaan *website* pemerintah daerah yaitu keterbatasan sumber daya manusia dan kapasitas teknis, di mana banyak ASN belum memiliki kompetensi yang memadai dalam pengelolaan teknologi informasi. Hal ini berdampak pada kualitas pengelolaan konten, pemeliharaan sistem, hingga pengolahan data publik yang tersedia di *website* tersebut (“Masalah Utama Dalam Menerapkan”, 2024).

Keamanan data menjadi tantangan tersendiri, karena belum diterapkannya standar perlindungan data yang kuat, sehingga rentan terhadap peretasan atau kebocoran informasi. Sistem tata kelola data harus memenuhi prinsip integrasi dan interoperabilitas (data dapat dibagipakaikan), seperti yang telah dilakukan di Pemerintah Daerah Gunung Kidul dalam mengagregasi data yang berasal dari pemerintah desa (“Tantangan Implementasi”, 2022).

### **Keamanan Siber Website**

Tata kelola keamanan siber sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perizinan berbasis *online*. Sepanjang tahun 2024, ancaman siber terhadap *website* pemerintah daerah di Indonesia semakin nyata dan serius, seiring dengan meningkatnya intensitas serta kompleksitas serangan yang dialami institusi pemerintah lainnya. Salah satu indikasi kerentanan *website* pemerintah daerah ditunjukkan oleh banyaknya situs mereka yang disusupi oleh konten judi *online* (Putra, 2025). Hal ini menandakan lemahnya sistem deteksi dan proteksi *website* pemerintah daerah. Ancaman ini diperburuk oleh tren global di mana serangan siber kini semakin dimotori oleh teknologi *artificial intelligence* (AI) yang memungkinkan otomatisasi serangan, pengintaian, dan eksploitasi celah sistem secara presisi dan *real-time*. AI juga dipakai untuk membuat varian *malware* baru yang sulit terdeteksi oleh sistem keamanan konvensional (Putra, 2025).

Tata kelola pengamanan siber dipentingkan dalam rangka memaksimalkan penggunaan *website* pemerintah daerah terhadap ancaman ketersediaan data dan informasi yang dimilikinya. Ancaman dimaksud akan mengarah pada tindak pidana terhadap *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) data atau sistem komputer seperti *hacking* (manipulasi data), *cracking* (merusak data), *phreaking* (menjelajahi sistem telekomunikasi), *viruses* (virus jaringan), dan lain-lain (Suseno, 2012).

Pemerintah daerah perlu mewaspadaai terjadinya anomali trafik yang dapat mengancam keamanan ketersediaan data dan informasi *website*-nya, seperti (1) *web access* (gangguan terjadi akibat adanya proses mengakses data yang tidak sah pada suatu situs untuk mencuri informasi sensitif); (2) *file transfer* (proses menyalin atau memindahkan file dari satu sistem ke sistem lain melalui jaringan atau koneksi internet); (3) *domain resolution* (proses mengakses sebuah situs web yang terindikasi terdapat konten judi *online*); dan (4) *website vulnerability exploit* (sebuah proses yang memanfaatkan celah keamanan sistem sebuah *website* untuk mengubah tampilan *website* dan mencuri data sensitif).

Langkah strategis keamanan siber pada *website* pemerintah daerah perlu dilakukan, yaitu menyediakan perangkat keras dan lunak yang mendukung keamanan, seperti *firewall*, sistem enkripsi, dan perangkat pemantauan aktivitas siber. Enkripsi dapat digunakan untuk melindungi data baik pada saat ditransmisikan maupun pada saat disimpan.

Keuntungan menggunakan enkripsi adalah bila metode lain untuk melindungi data berhasil dirusak oleh pihak lain, maka data yang dirusak tersebut tidak lagi memiliki arti pada perusak tersebut (Purbo, 2002).

Prospek strategis penggunaan AI atau kecerdasan buatan dapat membantu mendeteksi ancaman keamanan siber *website* pemerintah daerah. Meningkatnya jumlah dan kompleksitas serangan siber, memerlukan kecerdasan buatan sebagai alat penting untuk mendeteksi ancaman secara *real-time*. Teknologi berbasis AI mampu menganalisis pola anomali dalam data untuk mengidentifikasi potensi serangan, seperti *ransomware*, *phishing*, atau *malware*, sebelum serangan tersebut menyebar lebih luas (Mirza, 2025). Langkah strategis keamanan siber pada *website* pemerintah daerah termasuk penggunaan AI dalam mengantisipasi ancaman keamanan *website*, menjadi penting untuk dimasukkan dalam pengaturan mengenai keamanan dan ketahanan siber.

## Penutup

Ancaman siber terhadap *website* pemerintah daerah di Indonesia semakin nyata dan serius. Salah satu indikasi kerentanan *website* pemerintah daerah ditunjukkan oleh banyaknya situs mereka yang disusupi oleh konten judi *online*. Tata kelola pengamanan siber dipentingkan dalam rangka memaksimalkan pelayanan publik dalam menghadapi ancaman terhadap ketersediaan data dan informasi. Prospek strategis penggunaan kecerdasan buatan dapat membantu mendeteksi ancaman keamanan siber *website* pemerintah daerah.

Untuk itu, Komisi I DPR melalui pelaksanaan fungsi legislasi dapat memprioritaskan pembahasan RUU Keamanan dan Ketahanan Siber, sebagai landasan hukum bagi pengaturan keamanan siber termasuk juga keamanan *website* pemerintah daerah. Komisi I DPR melalui pelaksanaan fungsi pengawasan dapat mengawasi koordinasi keamanan siber antara Kemkomdigi dan pemerintah daerah dalam melakukan pengamanan *website* pemerintah daerah.

## Referensi

- Dinas Komunikasi dan Informatika Kabupaten Mukomuko. (2024, Oktober 1) *Pentingnya optimalisasi website resmi pemerintah daerah untuk transparansi publik*. <https://diskominfo.mukomukokab.go.id/artikel/pentingnya-optimalisasi-website-resmi-pemerintah-daerah-untuk-transparansi-publik>
- Id-SIRTII/CC. (2025) *Sejarah Id-SIRTII/CC*, Id-SIRTII-CC. <https://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html>
- Kementerian PPN/Bappenas. (2025). *Satu data Indonesia*. <https://data.go.id/>
- Kristianti, L. (2025, Januari 22). BSSN sebut anomali trafik eeb judul turun di awal 2025 dibanding 2024, 22 Januari 2025. *Antaranews.com* <https://www.antaranews.com/berita/4601930/bssn-sebut-anomali-trafik-web-judol-turun-di-awal-2025-dibanding-2024>
- Kristianti, L. (2025, Juni 12). Langkah Kemkomdigi tangani konten judi online yang susupi web Pemda, *Antaranews.com*. <https://www.antaranews.com/berita/4895229/langkah-kemkomdigi-tangani-konten-judi-online-yang-susupi-web-pemda>
- Masalah utama dalam menerapkan Sistem Informasi Pembangunan Daerah di Daerah. (2024, Maret 15). *diklatpemerintah.id*. <https://diklatpemerintah.id/masalah-utama-dalam-menerapkan-sistem-informasi-pembangunan-daerah-di-daerah/>
- Mirza. (2025, Januari 23). Tren keamanan siber 2025: Tantangan dan peluang bagi pemerintah daerah di Indonesia. *Gentapost.com*. <https://gentapost.com/tren-keamanan-siber-2025-tantangan-dan-peluang-bagi-pemerintah-daerah-di-indonesia/>
- Purbo, O. W. & Wiharjito, T. (2002). *Keamanan Jaringan Internet*. Alex Media Komputindo.
- Putra, D. A. (2025, Januari 2). Kondisi keamanan siber 2024 dan bagaimana proyeksinya di 2025? *Tirto.id*. <https://tirto.id/kondisi-keamanan-siber-2024-bagaimana-proyeksinya-di-2025-g65P>
- Suseno, S. 2012. *Yuridiksi Tindak Pidana Siber*. PT Refika Aditama.
- Tantangan Implementasi Satu Data dari Daerah. (2022, Februari 14). *Combine.or.id*. <https://www.combine.or.id/2022/02/14/tantangan-implementasi-satu-data-dari-daerah-bag-2/>

