Jurnal Transformasi Hukum dan Keadilan Sosial

https://journal.fexaria.com/j/index.php/jthks Vol. 10, No. 1, Januari 2026

TANTANGAN YURIDIS IMPLEMENTASI SMART CITY DI INDONESIA: SINKRONISASI KEWENANGAN PEMERINTAH DAERAH DALAM PERLINDUNGAN DATA PRIBADI MASYARAKAT

Ema Novitasari[1], Andin Rusmini[2]

[1,2]Universitas Merdeka Malang

e.novitagunawan@gmail.com

Abstrak

Implementasi konsep *Smart City* oleh Pemerintah Daerah di Indonesia bertujuan untuk meningkatkan efisiensi layanan publik melalui digitalisasi birokrasi. Namun, masifnya penggunaan aplikasi layanan publik di daerah menimbulkan risiko hukum terkait perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis sinkronisasi regulasi di tingkat daerah dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta mengkaji tanggung jawab hukum Pemerintah Daerah sebagai pengendali data. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Hasil penelitian menunjukkan bahwa masih terdapat kekosongan hukum dalam peraturan daerah (Perda) terkait standar keamanan data dan belum adanya integrasi pengawasan yang kuat. Pemerintah Daerah memiliki tanggung jawab hukum mutlak dalam memastikan keamanan data masyarakat guna mewujudkan tata kelola pemerintahan yang baik (*good governance*).

Kata Kunci: : Otonomi Daerah, *Smart City*, Perlindungan Data Pribadi, Digitalisasi Birokrasi

Abstract

The implementation of the Smart City concept by regional governments in Indonesia aims to improve the efficiency of public services through bureaucratic digitization. However, the widespread use of public service applications in the regions poses legal risks related to personal data protection. This study aims to analyze the synchronization of regional regulations with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and examine the legal responsibilities of regional governments as data controllers. The research method used is normative juridical with a statutory approach and a conceptual approach. The results indicate that there is still a legal gap in regional regulations (Perda) regarding data security standards and a lack of strong oversight integration. Regional governments have an absolute legal responsibility to ensure the security of public data to realize good governance.

***Keywords**: Regional Autonomy, Smart City, Personal Data Protection, Bureaucratic Digitalization*

PENDAHULUAN

Transformasi digital dalam penyelenggaraan pemerintahan daerah di Indonesia merupakan konsekuensi logis dari tuntutan reformasi birokrasi dan perkembangan teknologi informasi. Sebagaimana diamanatkan dalam Pasal 386 Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, daerah didorong untuk melakukan inovasi guna meningkatkan kinerja penyelenggaraan pemerintahan daerah.[1] Inovasi tersebut secara masif terwujud dalam konsep *Smart City* yang mengintegrasikan teknologi informasi dan komunikasi dalam tata kelola perkotaan. Secara filosofis, desentralisasi melalui *Smart City* seharusnya menjadi instrumen untuk mewujudkan kesejahteraan masyarakat melalui efektivitas layanan publik.

Namun, secara yuridis, terdapat diskoneksi antara semangat digitalisasi dengan perlindungan hak-hak konstitusional warga negara, khususnya hak atas privasi (*right to privacy*). Implementasi *Smart City* menuntut pengumpulan data masyarakat secara masif, mulai dari data kependudukan, kesehatan, hingga lokasi geografis melalui berbagai aplikasi yang dikelola oleh Perangkat Daerah. Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pengelolaan data di daerah cenderung dilakukan tanpa standar pengamanan yang seragam, sehingga menciptakan kerentanan hukum.[2]

Masalah utama muncul ketika UU PDP menetapkan standar yang sangat ketat bagi Pengendali Data Pribadi, termasuk badan publik di level daerah. Pasal 2 UU PDP menegaskan bahwa undang-undang ini berlaku untuk setiap orang, korporasi, dan badan publik.[3] Realitas di lapangan menunjukkan bahwa banyak Pemerintah Daerah belum memiliki instrumen hukum setingkat Peraturan Daerah (Perda) yang secara spesifik mengadopsi prinsip-prinsip perlindungan data pribadi sesuai mandat UU PDP. Ketidaksiapan ini berpotensi menimbulkan pelanggaran hak asasi manusia dan memunculkan tanggung jawab hukum bagi Pemerintah Daerah jika terjadi kegagalan sistem atau kebocoran data. Oleh karena itu, diperlukan analisis mendalam mengenai bagaimana sinkronisasi kewenangan daerah dijalankan agar tidak bertentangan dengan rezim hukum perlindungan data nasional.

Berdasarkan latar belakang tersebut di atas, maka terdapat diskoneksi yuridis antara inovasi digital daerah dengan standar perlindungan data nasional yang menuntut adanya kejelasan tanggung jawab pengendali data. Oleh karena itu, permasalahan dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana sinkronisasi regulasi *Smart City* di tingkat daerah dalam kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi?
2. Bagaimana tanggung jawab hukum Pemerintah Daerah sebagai Pengendali Data Pribadi dalam penyelenggaraan birokrasi digital?

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*doctrinal research*), yaitu penelitian yang mengkaji hukum tertulis dari berbagai aspek teoretis maupun substansi.[4] Fokus penelitian ini adalah sinkronisasi vertikal antara regulasi otonomi daerah dengan regulasi perlindungan data pribadi.

---

[1] Indonesia, *Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah*, Pasal 386 ayat (1)
[2] Shita Laksmi dan Dyah Arum, *Privasi dan Tata Kelola Data di Indonesia* (Jakarta: ELSAM, 2023), hlm. 45.
[3] Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Pasal 2.
[4] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2015), hlm. 13.

1) Pendekatan Penelitian

Penelitian ini menggunakan tiga pendekatan utama:

1. **Pendekatan Perundang-undangan (*Statute Approach*):** Dilakukan dengan menelaah UU No. 23 Tahun 2014 tentang Pemerintahan Daerah, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta berbagai peraturan pelaksana terkait *Smart City*.
2. **Pendekatan Konseptual (*Conceptual Approach*):** Merujuk pada prinsip-prinsip otonomi daerah, konsep *good governance*, dan teori perlindungan hukum untuk membangun argumentasi hukum.
3. **Pendekatan Analitis (*Analytical Approach*):** Digunakan untuk mengetahui makna yang terkandung dalam istilah-istilah hukum dan menguji sinkronisasi antar peraturan.[5]

2) Sumber Bahan Hukum

Bahan hukum yang digunakan meliputi:

a. **Bahan Hukum Primer:** Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, UU Pemerintahan Daerah, UU PDP, UU ITE (UU No. 1 Tahun 2024), dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).
b. **Bahan Hukum Sekunder:** Buku-buku teks hukum, jurnal ilmiah bereputasi, hasil penelitian hukum, dan makalah yang relevan dengan topik otonomi daerah dan keamanan siber.

3) Teknik Pengumpulan dan Analisis Bahan Hukum

Bahan hukum dikumpulkan melalui studi kepustakaan (*library research*) dengan teknik dokumentasi. Selanjutnya, bahan hukum diolah secara deduktif, yaitu menarik kesimpulan dari permasalahan yang bersifat umum menuju permasalahan konkret yang dihadapi dalam implementasi *Smart City* di daerah. Analisis dilakukan secara kualitatif-deskriptif untuk menghasilkan argumen preskriptif mengenai langkah hukum yang harus diambil oleh Pemerintah Daerah.

HASIL DAN PEMBAHASAN

A. Sinkronisasi Regulasi Smart City di Tingkat Daerah dalam Kerangka UU Perlindungan Data Pribadi

Implementasi *Smart City* oleh Pemerintah Daerah secara yuridis berpijak pada kewenangan atributif dalam urusan pemerintahan wajib yang berkaitan dengan pelayanan dasar serta urusan pemerintahan pilihan di bidang komunikasi dan informatika.[6] Namun, dalam praktiknya, terdapat ambiguitas norma ketika daerah menyusun regulasi teknis setingkat Peraturan Daerah (Perda) atau Peraturan Kepala Daerah (Perkada) mengenai tata kelola data digital.

1. Konflik Norma dan Asas *Lex Superior Derogat Legi Inferiori*

Banyak regulasi *Smart City* di berbagai daerah di Indonesia lahir sebelum disahkannya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Secara teoretis,

[5] Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Jakarta: Kencana, 2017), hlm. 129.

[6] Indonesia, *Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah*, Lampiran Huruf L (Urusan Pemerintahan Bidang Komunikasi dan Informatika).

berdasarkan asas *lex superior derogat legi inferiori*, maka seluruh ketentuan dalam Perda yang mengatur mengenai pengelolaan data masyarakat harus tunduk dan menyesuaikan diri dengan UU PDP sebagai norma yang lebih tinggi.[7] Namun, sinkronisasi ini tidak berjalan otomatis.

Masalah utama terletak pada definisi "Pengendali Data Pribadi". Dalam UU PDP, badan publik (termasuk Dinas-Dinas di Pemda) ditetapkan sebagai Pengendali Data yang memikul kewajiban berat, seperti melakukan *Data Protection Impact Assessment* (DPIA).[8] Di sisi lain, mayoritas Perda *Smart City* yang ada saat ini hanya berfokus pada aspek teknis efisiensi layanan (seperti kecepatan akses dan integrasi aplikasi) tanpa memberikan jaminan perlindungan terhadap hak-hak subjek data sebagaimana diatur dalam Pasal 4 sampai Pasal 15 UU PDP.

2. Kewenangan Daerah vs Standardisasi Nasional

Berdasarkan UU No. 23 Tahun 2014, daerah memiliki otonomi untuk mengatur rumah tangganya sendiri. Namun, dalam hal perlindungan data pribadi, otonomi ini dibatasi oleh kepentingan nasional. Terjadi tarikan menarik kepentingan: daerah ingin memiliki basis data sendiri guna kepentingan PAD (Pendapatan Asli Daerah) atau profil warga, sementara UU PDP menuntut adanya standardisasi keamanan yang tinggi yang seringkali belum mampu dipenuhi secara finansial maupun SDM oleh daerah.

Ketidaksinkronan ini menciptakan celah hukum. Jika terjadi kebocoran data pada aplikasi milik Pemda, terdapat ketidakjelasan apakah yang digunakan adalah instrumen sanksi administrasi yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), UU PDP, atau mekanisme pertanggungjawaban pejabat dalam UU Administrasi Pemerintahan. Sinkronisasi regulasi di daerah bukan hanya sekadar memindahkan pasal-pasal UU PDP ke dalam Perda, melainkan melakukan kontekstualisasi terhadap bagaimana data warga di tingkat lokal dikelola secara transparan dan akuntabel.[9]

B. Tanggung Jawab Hukum Pemerintah Daerah sebagai Pengendali Data Pribadi dalam Penyelenggaraan Birokrasi Digital

Penetapan Pemerintah Daerah sebagai "Pengendali Data Pribadi" membawa konsekuensi yuridis yang signifikan. Dalam teori hukum administrasi, setiap kewenangan selalu diikuti oleh pertanggungjawaban (*kewenangan melahirkan tanggung jawab*).[10] Ketika Pemerintah Daerah mengumpulkan data biometrik, NIK, hingga data kesehatan warga melalui platform *Smart City*, Pemda telah mengambil alih risiko hukum atas keamanan data tersebut.

1. Tanggung Jawab Administrasi dan Perdata

Berdasarkan Pasal 57 UU PDP, kegagalan dalam melindungi data pribadi dapat berujung pada sanksi administratif berupa penghentian sementara kegiatan pemrosesan data hingga denda administratif.[11] Bagi Pemerintah Daerah, sanksi ini tidak hanya bersifat finansial, tetapi juga mencederai legitimasi politik kepala daerah. Secara perdata, masyarakat sebagai subjek data yang dirugikan memiliki hak untuk menggugat Pemerintah Daerah melalui mekanisme Perbuatan Melawan Hukum oleh Penguasa (*Onrechtmatige Overheidsdaad*).

[7] Jimly Asshiddiqie, *Perihal Undang-Undang* (Jakarta: Rajawali Pers, 2010), hlm. 182.
[8] Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Pasal 34.
[9] Bagir Manan, *Menyongsong Fajar Otonomi Daerah* (Yogyakarta: Pusat Studi Hukum FH UII, 2004), hlm. 55.
[10] Ridwan HR, *Hukum Administrasi Negara* (Jakarta: RajaGrafindo Persada, 2016), hlm. 245.
[11] Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Pasal 57 ayat (2).

Gugatan ini dapat diajukan jika Pemda terbukti lalai dalam menyediakan sistem pengamanan yang layak (standar *cyber security*), sehingga menyebabkan kerugian materiil maupun immateriil bagi warga. Dalam konteks otonomi daerah, tanggung jawab ini bersifat melekat pada jabatan (*ambtelijk*), di mana daerah harus mengalokasikan anggaran khusus untuk mitigasi risiko siber sebagai bagian dari biaya pelayanan publik.[12]

2. Doktrin *Strict Liability* dalam Kegagalan Sistem

Dalam diskursus hukum siber yang berkaitan dengan pelayanan publik, mulai berkembang pemikiran mengenai penerapan prinsip *strict liability* (tanggung jawab mutlak). Artinya, Pemerintah Daerah tidak dapat berdalih bahwa kebocoran data terjadi karena serangan pihak ketiga (hacker) jika terbukti infrastruktur digital yang dibangun tidak memenuhi standar minimum nasional. Sebagai penyelenggara negara, Pemda memiliki kewajiban untuk memberikan perlindungan hukum yang setara dengan kemajuan teknologi yang mereka adopsi.[13] Kegagalan dalam melindungi data pribadi warga adalah bentuk pengabaian terhadap hak privasi yang merupakan bagian dari hak asasi manusia.

Kewajiban Pemerintah Daerah dalam konteks ini tidak lagi sekadar *obligation of conduct* (kewajiban berperilaku), melainkan telah bergeser menjadi *obligation of result* (kewajiban hasil). Dalam diskursus hukum administrasi modern, kegagalan sistem elektronik yang dikelola negara tidak bisa lagi berlindung di balik dalih *force majeure* digital atau serangan siber pihak ketiga semata. Hal ini dikarenakan Pemerintah Daerah memiliki posisi tawar dan sumber daya yang jauh lebih besar dibandingkan subjek data (warga) yang bersifat pasif.[14]

Lebih lanjut, penerapan *strict liability* di sini sejalan dengan prinsip *precautionary principle* (prinsip kehati-hatian). Mengingat data pribadi adalah aset yang bersifat *irreplaceable* (tidak dapat diganti) jika telah bocor ke ruang publik, maka standar kelalaian biasa (*ordinary negligence*) tidak lagi cukup untuk memberikan keadilan bagi korban. Pemerintah Daerah, melalui perangkat dinasnya, memegang kendali penuh atas arsitektur sistem informasi. Oleh karena itu, beban pembuktian seharusnya berada di tangan Pemerintah Daerah (*shifting burden of proof*) untuk membuktikan bahwa mereka telah melakukan upaya keamanan maksimal sesuai standar ISO/IEC 27001 atau standar yang ditetapkan oleh Badan Siber dan Sandi Negara (BSSN).[15]

Tanpa adanya penerapan tanggung jawab yang ketat, inovasi *Smart City* hanya akan menjadi proyek teknokratis yang mengabaikan aspek perlindungan hak asasi manusia. Penegasan tanggung jawab mutlak ini berfungsi sebagai fungsi pencegahan (*deterrence effect*) agar Pemerintah Daerah tidak sembarangan dalam memilih pihak ketiga (*vendor*) pengembang aplikasi tanpa kualifikasi keamanan yang mumpuni."

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, maka dapat disimpulkan sebagai berikut:

[12] Sjachran Basah, *Eksistensi dan Tolok Ukur Badan Peradilan Administrasi di Indonesia* (Bandung: Alumni, 2005), hlm. 151.

[13] Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2010), hlm. 312.

[14] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia* (Surabaya: Bina Ilmu, 1987), hlm. 72.

[15] Shinta Dewi, *Cyber Law: Perlindungan Privasi atas Data Pribadi dalam Sistem Elektronik* (Bandung: Refika Aditama, 2020), hlm. 118.

1. **Sinkronisasi regulasi *Smart City* di tingkat daerah dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) saat ini masih belum optimal.** Ditemukan adanya ketidaksinkronan (antinommi) dan kekosongan norma dalam berbagai Peraturan Daerah yang mengatur mengenai tata kelola digital. Banyak regulasi daerah yang hanya berfokus pada aspek teknis pelayanan publik namun mengabaikan standar perlindungan data pribadi sebagaimana diatur dalam UU PDP. Oleh karena itu, diperlukan rekonsiliasi hukum melalui harmonisasi Perda agar selaras dengan standar keamanan data nasional.
2. **Tanggung jawab hukum Pemerintah Daerah sebagai Pengendali Data Pribadi bersifat mutlak dalam penyelenggaraan birokrasi digital.** Pemerintah Daerah tidak hanya bertanggung jawab secara administratif dalam pengelolaan sistem, tetapi juga memiliki tanggung jawab hukum perdata maupun publik apabila terjadi kegagalan perlindungan data (kebocoran data). Dalam kerangka *Good Governance*, Pemerintah Daerah wajib menyediakan infrastruktur keamanan yang memadai dan mekanisme pengawasan yang terintegrasi sebagai bentuk perlindungan hukum terhadap hak privasi masyarakat selaku subjek data.

Saran

1. Pemerintah Daerah perlu segera melakukan revisi terhadap Peraturan Daerah mengenai *Smart City* atau Penyelenggaraan Sistem Elektronik dengan menyisipkan klausul perlindungan data pribadi yang merujuk pada UU PDP.
2. Perlu dibentuk otoritas pengawas data pribadi di tingkat daerah atau penguatan peran Dinas Komunikasi dan Informatika (Diskominfo) sebagai unit yang bertanggung jawab penuh atas keamanan data masyarakat.
3. Pemerintah Daerah disarankan untuk segera melakukan integrasi sistem informasi daerah ke dalam platform Satu Data Indonesia. Langkah ini krusial untuk meminimalisir praktik replikasi aplikasi layanan publik yang berlebihan di tingkat Perangkat Daerah. Replikasi aplikasi yang tidak terstandarisasi secara nasional cenderung memperluas permukaan serangan siber dan memperbesar risiko kebocoran data masyarakat. Dengan melakukan konsolidasi data melalui portal nasional, Pemerintah Daerah dapat memastikan bahwa setiap pemrosesan data pribadi telah memenuhi standar keamanan yang diawasi secara terpusat, sekaligus mewujudkan efisiensi anggaran dan akuntabilitas birokrasi digital.

DAFTAR PUSTAKA

Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

Indonesia. *Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah*. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587.

Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 7, Tambahan Lembaran Negara Republik Indonesia Nomor 6931.

Indonesia. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

Asshiddiqie, Jimly. *Perihal Undang-Undang*. Jakarta: Rajawali Pers, 2010.

Basah, Sjachran. *Eksistensi dan Tolok Ukur Badan Peradilan Administrasi di Indonesia*. Bandung: Alumni, 2005.

Dewi, Shinta. *Cyber Law: Perlindungan Privasi atas Data Pribadi dalam Sistem Elektronik*. Bandung: Refika Aditama, 2020.

Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: Bina Ilmu, 1987.

HR, Ridwan. *Hukum Administrasi Negara*. Jakarta: RajaGrafindo Persada, 2016.

Laksmi, Shita dan Dyah Arum. *Privasi dan Tata Kelola Data di Indonesia*. Jakarta: ELSAM, 2023.

Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Rajawali Pers, 2010.

Manan, Bagir. *Menyongsong Fajar Otonomi Daerah*. Yogyakarta: Pusat Studi Hukum FH UII, 2004.

Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana, 2017.

Soekanto, Soerjono dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2015