SISTEM IDENTITAS DIGITAL DI INDONESIA

RINGKASAN

Sistem identitas di Indonesia saat ini berfungsi sebagai versi digital dari sistem identitas utama yang dikelola pemerintah, yaitu sistem pendaftaran penduduk dan pencatatan sipil. Kartu Tanda Penduduk Elektronik (sistem KTP elektronik atau KTP nasional elektronik) berfungsi sebagai aplikasi digital yang menggunakan data kependudukan. Meskipun saat ini upaya-upaya transisi dari e-KTP fisik ke KTP Digital sedang dilakukan, KTP digital nasional belum bisa diterapkan di seluruh negeri. KTP Digital akan melibatkan pemindahan e-KTP ke ponsel.

Sistem tanda pengenal nasional yang ada saat ini mengundang kekhawatiran mengenai potensi pengawasan yang luas dan risiko keamanan dari pengumpulan data dalam jumlah sangat besar. Untuk mengatasi tantangan-tantangan ini, perlu langkah-langkah ketat dalam UU Pelindungan Data Pribadi, seperti membatasi jenis dan durasi data, mengontrol akses oleh publik dan pihak swasta, dan menetapkan keadaan pengungkapan. Perlu juga kebijakan keamanan siber dan mitigasi insiden yang kuat.

Selain itu, hanya mengandalkan satu dokumen identitas tertentu, seperti e-KTP, menimbulkan risiko pengucilan dan marginalisasi terhadap segmen masyarakat tertentu. Sebab, dokumen ini sangat penting untuk syarat mengakses layanan-layanan publik bagi warga. Undang-undang dan kebijakan nasional e-KTP harus diubah agar dapat menerima bentuk bukti identitas lain saat pendaftaran. Perubahan-perubahan ini akan menghadirkan inklusivitas ke dalam sistem identitas dan menghilangkan hambatan yang dihadapi komunitas marginal selama proses pendaftaran.

Materi ini diambil dari hasil riset *State of Digital Identification System in South and Southeast Asia* yang diterbitkan EngageMedia dengan dukungan USAID dan Internews pada Agustus 2023. SAFEnet berpartisipasi dalam riset yang dilakukan sebagai bagian dari program Greater Internet Freedom (GIF) Tahun Ketiga pada 2023 ini. Materi disesuaikan dengan konteks untuk organisasi masyarakat sipil di Indonesia.

Konteks Sejarah

Sistem pencatatan sipil di Indonesia saat ini berawal dari sejarah kolonial. Sistem itu kemudian berkembang menjadi dua versi berbeda yang dibentuk pada masa penjajahan Belanda dan Jepang. Kartu Nasional Indonesia, atau Kartu Tanda Penduduk, diwajibkan sebagai bukti identitas bagi warga negara dan penduduk berusia 17 tahun ke atas (atau setelah menikah, bagi mereka yang berusia di bawah 17 tahun). Sistem ini dibangun berdasarkan tradisi panjang pencatatan sipil – pencatatan kelahiran, kematian, dan perkawinan – yang diperkenalkan pada tahun 1945.

Pada tahun 2011, pemerintah Indonesia meluncurkan KTP elektronik (e-KTP) yang dikelola secara nasional oleh Kementerian Dalam Negeri melalui Direktorat Kependudukan dan Pencatatan Sipil. E-KTP berisi sebuah mikrocip, biometrik (sidik jari, iris mata dan pengenalan wajah), dan nomor seri unik. E-KTP dapat digunakan untuk menggunakan beberapa aplikasi layanan pemerintah. Sistem biometrik diperkenalkan untuk menghapus duplikat dalam basis data dan mengaktifkan verifikasi identitas untuk orang Indonesia.

E-KTP kini menjadi dasar penerbitan paspor Indonesia, Surat Izin Mengemudi (SIM), kartu SIM, Nomor Pokok Wajib Pajak (NPWP), polis asuransi, kepemilikan tanah sertifikat, dan beberapa dokumen identitas lainnya. Menurut Survei Bank Dunia pada tahun 2017, 96 persen penduduk Indonesia berusia 16 tahun ke atas sudah memiliki KTP atau e-KTP.

Kekhawatiran terhadap potensi pengawasan yang luas dan risiko keamanan pun muncul. Dilihat dari pengumpulan data dalam jumlah yang sangat besar dan kaitan erat antara pencatatan sipil dan digitalisasi identitas nasional. Untuk mengatasi tantangan-tantangan ini, perlu langkah-langkah ketat untuk membatasi jenis dan durasi data, mengontrol akses oleh publik dan pihak swasta, dan menetapkan keadaan pengungkapan. Kebijakan keamanan siber dan mitigasi bencana yang kuat juga sangat diperlukan.

Menurut pemantauan SAFEnet, selama dua tahun terakhir terjadi kebocoran data pribadi setidaknya 113 kali, yaitu 36 kali pada 2022[2] dan 77 kali pada 2023[3]. Jumlah itu jauh lebih sedikit dibandingkan temuan lembaga keamanan siber Surfshak yang menemukan lebih dari 143 juta akun di Indonesia menjadi korban kebocoran data hanya sepanjang tahun 2023[4]. Jumlah tersebut membuat Indonesia berada

[2]Laporan Situasi Hak-hak Digital Indonesia 2022
[3]Laporan Situasi Hak-hak Digital Indonesia 2023
[4]https://surfshark.com/research/data-breach-monitoring

di urutan ke-13 secara global sebagai negara yang paling banyak mengalami kebocoran data.

Ironisnya, sebagian besar insiden kebocoran data pribadi justru terjadi pada lembaga pemerintah. Salah satu contohnya adalah kebocoran data pribadi sekitar 204 juta pemilih yang diduga diambil dari data Komisi Pemilihan Umum (KPU) pada November 2023. Data pribadi pemilih yang ditawarkan melalui forum jual beli data itu mencakup nama lengkap, tanggal lahir, jenis kelamin, nomor induk kependudukan (NIK), dan alamat lengkap.

Selain itu, hanya mengandalkan satu dokumen identitas tertentu, seperti e-KTP, menimbulkan risiko pengucilan dan marginalisasi terhadap segmen masyarakat tertentu, mengingat pentingnya dokumen ini untuk mengakses layanan-layanan penting. Undang-undang dan kebijakan nasional e-KTP harus diubah agar dapat menerima berbagai bentuk bukti identitas yang berbeda pada saat pendaftaran. Perubahan-perubahan ini dapat memperkenalkan inklusivitas ke dalam sistem identitas, dan menghilangkan hambatan yang dihadapi oleh komunitas marginal selama proses pendaftaran.

Pinjaman Bank Dunia

Menjelang akhir tahun 2022, pemerintah Indonesia memulai negosiasi dengan Bank Dunia untuk mendapatkan pinjaman sebesar USD 250 juta atau hampir Rp 4 triliun. Pinjaman ini digunakan untuk ‘memperkuat sistem pencatatan sipil negara dan meningkatkan penggunaan identifikasi digital biometrik untuk mengakses

layanan sektor publik dan swasta.' Upaya ini akan dilaksanakan melalui proyek yang dikenal sebagai 'ID untuk Pemberian Layanan Inklusif dan Transformasi Digital di Indonesia'. Proyek ini bertujuan untuk mengubah sistem tanda pengenal digital dasar di Indonesia menjadi sistem tanda pengenal digital lengkap, sehingga memberikan akses kepada layanan pemerintah dan swasta terhadap sistem tersebut. Rincian sistem ini dan kerangka ID digital yang diusulkan masih belum terlaksana.

Meskipun sistem tanda pengenal dasar di Indonesia sudah beralih ke digital serta mencakup pengumpulan dan penggunaan informasi biometrik, negara ini belum memiliki sistem tanda pengenal digital dan kerangka kerja untuk autentikasi digital atau daring. Saat ini, pemegang KTP Indonesia diminta untuk memverifikasi diri melalui mekanisme verifikasi demografi atau dengan mengambil foto selfie sambil memegang e-KTP. Oleh karena itu, sebagian besar proyek Bank Dunia berfokus pada penggunaan sistem pendaftaran penduduk dan pencatatan sipil yang ada sebagai platform bagi layanan tanda pengenal digital nasional dan verifikasi identitas.

Sistem Identifikasi dan Kebijakan

Pengumpulan dan pengelolaan data pribadi melalui sistem e-KTP di Indonesia diatur dalam Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan dan Pencatatan Sipil (UU Administrasi Kependudukan), yang kemudian diperbaharui dengan UU Nomor 24 Tahun 2013 (UU Perubahan). Komponen utama sistem identitas dasar Indonesia yang ditetapkan oleh undang-undang ini meliputi:

- Database Sistem Informasi Administrasi Kependudukan ("SIAK")
- Nomor Identitas Kependudukan ("NIK") unik yang diterbitkan pada saat pencatatan kelahiran
- e-KTP tersedia mulai usia 17 tahun. Penduduk diwajibkan untuk memiliki e-KTP ketika mereka mencapai usia 17 tahun atau jika mereka menikah. Yang dimaksud dengan penduduk adalah warga negara Indonesia dan orang asing yang bertempat tinggal di Indonesia
- Kartu Keluarga (KK), dan
- Berbagai akta kelahiran, kematian, perkawinan, dan peristiwa penting lain.

Data yang dikumpulkan melalui sistem pendaftaran penduduk dan pencatatan sipil, termasuk e-KTP berjumlah sangat besar. E-KTP berisi data pribadi dan data pribadi sensitif, termasuk NIK, nama lengkap, foto wajah, jenis kelamin, alamat tempat tinggal, tempat dan tanggal lahir, agama, pekerjaan, golongan darah,

kewarganegaraan, status perkawinan, tanda tangan pemegang, tanggal habis masa berlaku e-KTP, dan sidik jari biometrik. Berdasarkan Pasal 13 UU Nomor 23 Tahun 2006, semua penduduk wajib memiliki NIK, dan ini harus disertakan pada setiap dokumen administrasi penduduk. Pendaftaran dan pemutakhiran data, termasuk perubahannya, dilakukan oleh Dinas Kependudukan dan Pencatatan Sipil (Dinas Dukcapil) yang dilaporan kepada pemerintah daerah.

Baik Dinas Dukcapil maupun Ditjen Dukcapil menyediakan data kependudukan untuk pengguna institusi. Pada tingkat agregat, hal ini memungkinkan terjadinya produksi statistik, dan pada tingkat individu, hal ini memungkinkan penyedia layanan, seperti lembaga pemerintah, atau bank untuk memverifikasi identitas nasabah.

Implikasi terhadap Sistem ID di Indonesia

Eksklusi dan Diskriminasi

KTP dan versi elektroniknya sangat diperlukan untuk hidup di Indonesia. Warga memerlukan ID untuk mengakses layanan dasar publik, seperti kesehatan dan pendidikan; berpartisipasi dalam pemilu; mencatat kelahiran, kematian, pernikahan; mengajukan SIM, pekerjaan dan rekening bank. UU Administrasi Kependudukan bahkan mengamanatkan pemerintah menyediakan segala pelayanan publik berdasarkan nomor NIK. Hal ini mengakibatkan pengucilan dan diskriminasi terhadap kelompok dan komunitas minoritas, berdasarkan agama dan identitas gender mereka. Akibatnya, komunitas orang-orang rentan dan terpinggirkan dalam kehidupan masyarakat Indonesia tidak dapat mengakses sebagian besar layanan publik atau swasta.

Agama

Pencantuman keterangan keagamaan pada kartu e-KTP telah menjadi sumber permasalahan bagi masyarakat Indonesia. UU Perubahan menetapkan bahwa penduduk yang agamanya tidak diakui secara resmi oleh hukum di Indonesia harus diperlakukan sama dengan masyarakat lainnya dan terdaftar di sistem.

Pada tahun 2017, perwakilan komunitas Ahmadiyah mengajukan permohonan pengaduan resmi terhadap pemerintah daerah di kabupaten Jawa Barat. Ada dugaan bahwa mereka tidak akan diberikan kartu identitas kecuali mereka melepaskannya keyakinannya. Hal ini tidak semata-mata karena fakta bahwa Ahmadiyah tidak termasuk di antara enam agama yang resmi diakui di Indonesia.

Dalam keluhannya, kelompok Ahmadiyah mengatakan bahwa hidup mereka sangat terkena dampak karena tidak adanya tanda pengenal nasional. Mereka tidak dapat mengakses sebagian besar layanan pemerintah, termasuk pendaftaran rumah sakit dan pernikahan.

Identitas Gender
Pada tahun 2019, seorang transpuan yang diusir dari keluarganya sehingga tidak memiliki e-KTP tidak dapat mengakses layanan kesehatan. Dia meninggal karena komplikasi HIV AIDS. Digitalisasi sistem ini hanya menambah ketidaktampakan mereka, karena orang-orang trans seolah tidak hadir atau salah diidentifikasi pada semua pangkalan data. Dengan kebijakan pemerintah yang kini ditetapkan berdasarkan basis data ini, marjinalisasi orang-orang dengan identitas gender berbeda sudah pasti terjadi.

Kesehatan
Selama pandemi COVID-19, vaksinasi diberikan berdasarkan e-KTP, sehingga pelayanan kesehatan yang esensial tidak mencakup sebagian besar kelompok penduduk marginal.

Privasi dan Perlindungan Data

Pada 17 Oktober 2022, pemerintah Indonesia mengesahkan UU Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Ini adalah upaya pertama dari undang-undang perlindungan data yang komprehensif di Indonesia. Penerapan UU PDP pada e-KTP tersebut tidak ditetapkan dengan tepat. Namun, UU mewajibkan pengendali data, termasuk administrator sistem dasar ID Indonesia, untuk melakukan penilaian dampak perlindungan data untuk pemrosesan data pribadi yang berisiko tinggi.

Sebelum disahkannya UU PDP sejak 2022, peraturan sektor khusus mengatur pengumpulan dan penggunaan data pribadi dalam sistem e-KTP, jika relevan, dan mencakup:

- Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)
- Peraturan Pemerintah tentang Penyelenggaraan Sistem Elektronik (PSE)
- Peraturan Menteri Komunikasi dan Informatika tentang Pelindungan Data Pribadi dalam Sistem Elektronik.

Kebocoran data pribadi vaksin warga Indonesia pada Juli 2023 yang dijual di forum dark web. Meskipun kebocoran data pribadi terus terjadi, tidak cukup ada tanggung jawab pemerintah terhadap kebocoran tersebut.

Secara khusus, hukum yang mengatur sistem e-KTP adalah UU Administrasi Kependudukan yang secara tegas mengatur perlindungan data pribadi penduduk. Pasal 85 dan 86 menugaskan otoritas pelaksana untuk menyimpan dan melindungi data pribadi ini. Sebelum ada Amandemen UU, Pasal 84 UU Administrasi Kependudukan mendefinisikan data pribadi sebagai 'nomor KK, NIK, rincian kelahiran, informasi tentang seseorang cacat fisik atau mental,'.

Menyusul penerapan UU Perubahan, Pasal 21 (perubahan Pasal 84 UU Administrasi Kependudukan), definisi data pribadi diubah menjadi data biometrik (pemindaian mata, sidik jari), cacat fisik/mental, tanda tangan, dan elemen data lainnya "merupakan kekurangan seseorang." Pada dasarnya, perubahan ini berarti bahwa data pribadi, seperti NIK dan nomor e-KTP, tidak dilindungi sebagai data pribadi berdasarkan UU ini.

Juga tidak jelas berapa banyak badan yang memiliki akses terhadap data dalam sistem e-KTP. Pada tahun 2021, Kementerian Dalam Negeri mengungkapkan bahwa 3.904 badan publik, yang terdiri dari 2.178 kementerian/lembaga pusat dan 1.726 lembaga pemerintah daerah, diberikan akses terhadap database tersebut.

Selama ini, terjadi beberapa kasus kebocoran data pribadi dan penyalahgunaan informasi pada sistem e-KTP, termasuk:

- Pada tahun 2017, mantan menteri Tjahjo Kumolo dilaporkan membagikan data e-KTP seorang pembela hak asasi manusia, Veronica Koman, yang secara terbuka mengkritik pemerintah Indonesia.
- Pada Mei 2020, terdapat pemberitaan yang merinci kebocoran informasi terkait jutaan penduduk Indonesia dari Daftar Pemilih Tetap Pemilu 2014. Data tersebut mencakup informasi sensitif seperti nama penduduk, nomor kartu keluarga, NIK, tempat dan tanggal lahir, alamat rumah, dan data pribadi lainnya.
- Kebocoran data tersebut juga berdampak pada badan-badan pemerintah, yaitu:
    - Pada tahun 2021, empat lembaga pemerintah yang memiliki akses terhadap pangkalan data pribadi warga telah mengalami kebocoran data pribadi
    - Pada tahun 2022, setidaknya terjadi 40 insiden kebocoran data terhadap 60 lembaga publik di Indonesia.

Rekomendasi

Berdasarkan situasi tersebut, riset ini merekomendasikan beberapa hal, khususnya untuk pemerintah Indonesia.

Pertama, pemerintah Indonesia perlu untuk:

- Mengeluarkan arahan yang mengklarifikasi bahwa Undang-Undang Perlindungan Data Pribadi (2022) berlaku untuk semua data pribadi dan data sensitif yang dikumpulkan dan diproses berdasarkan undang-undang identitas nasional, Undang-Undang Administrasi Kependudukan.
- Mengubah undang-undang e-KTP, serta undang-undang dan kebijakan lain yang berlaku, untuk menerima berbagai bentuk bukti identitas yang berbeda pada saat pendaftaran.
- Selama penerapan KTP Digital, berikan perhatian khusus pada penyebab eksklusi saat ini (misalnya keyakinan agama atau identitas), dan terapkan verifikasi identitas yang inklusif untuk semua.

Kedua, Ditjen Dukcapil perlu:

- Menetapkan kebijakan keamanan siber dan mitigasi bencana yang komprehensif untuk memitigasi pelanggaran data pada sistem atau kegagalan sistem.
- Menerapkan langkah-langkah untuk membatasi:
    - jenis dan durasi data yang disimpan,
    - akses yang dimiliki oleh sektor publik dan swasta, dan
    - keadaan di mana pengungkapan informasi dari sistem ini dapat dilakukan.

Khusus untuk organisasi masyarakat sipil ada beberapa hal yang bisa dilakukan sebagaimana disarankan dalam Modul Pelindungan Data Pribadi bagi Organisasi Masyarakat Sipil yang diterbitkan Yayasan Tifa dan Combine Resources Institution (2023), termasuk:

- Hanya menyimpan data yang dibutuhkan untuk meminimalisir risiko jika terjadi kebocoran data pribadi. Selalu sesuaikan data yang dikumpulkan dengan tujuan pemrosesan.
- Membuat klasifikasi data sehingga data-data sensitif tidak diperlakukan sama dengan data lain yang tidak sensitif.
- Menyusun manajemen akses terutama untuk data sensitif. Selain mempertimbangkan siapa saja yang berhak mengakses, hal penting lainnya adalah mengenai media transfer dan penyimpanannya.
- Menyusun manajemen risiko untuk memetakan kerentanan dan potensi risiko dari ancaman yang ada. Respons atas kerentanan tersebut dapat ditentukan

berdasarkan skala prioritas dengan mempertimbangkan dampak dan keparahannya.

- Menyusun manajemen insiden. Ini tidak hanya untuk merespons insiden yang mungkin terjadi, tetapi juga sebagai masukan untuk menyusun ulang standar keamanan yang ditetapkan melalui manajemen risiko.
- Menyusun standar keamanan yang ketat untuk *Bring Your Own Devices* (BYOD). Istilah ini merujuk pada penggunaan perangkat pribadi dalam pekerjaan kantor.
- Menyusun aturan khusus mengenai keamanan data untuk menciptakan standar keamanan bersama yang harus dipatuhi semua anggota organisasi. Misalnya menghapus atau memusnahkan data-data pribadi yang sudah tidak terpakai, baik berupa data digital maupun fisik.
- Meningkatkan kapasitas anggota, sebab faktor manusia sangat dominan dalam insiden kebocoran data.
- Memilih lokasi penyimpanan data yang aman dengan mempertimbangkan kekurangan dan kelebihan dari penyimpanan tersebut. Baik yang bersifat lokal (*local storage*) maupun awan (*cloud storage*). Pastikan mereka memiliki sistem keamanan berlapis.

SAFEnet

Jalan Gita Sura III Nomor 55 Peguyangan Kaja
Denpasar, Bali 80115

safenet.or.id
info@safenet.or.id
@safenetvoice
@safenetvoice