



UNIVERSITAS INDONESIA

**TANGGUNGJAWAB NOTARIS ATAS PERLINDUNGAN
DATA PRIBADI DALAM AKSES INTEROPERABILITAS
INFORMASI DATA KEPENDUDUKAN**

TESIS

**Hartanto Budiman
1006738286**

**FAKULTAS HUKUM
PROGRAM MAGISTER KENOTARIATAN
DEPOK
JULI 2012**



UNIVERSITAS INDONESIA

**TANGGUNGJAWAB NOTARIS ATAS PERLINDUNGAN
DATA PRIBADI DALAM AKSES INTEROPERABILITAS
INFORMASI DATA KEPENDUDUKAN**

TESIS

**Diajukan sebagai salah satu syarat untuk memperoleh gelar
Magister Kenotariatan**

**Hartanto Budiman
1006738286**

**FAKULTAS HUKUM
PROGRAM MAGISTER KENOTARIATAN
DEPOK
JULI 2012**

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : Hartanto Budiman

NPM : 1006738286

Tanda Tangan : 

Tanggal : 14 Juni 2012

HALAMAN PENGESAHAN

Tesis ini diajukan oleh : Mahasiswa Fakultas Hukum Pasca Sarjana Magister
Kenotariatan
Nama : Hartanto Budiman
NPM : 1006738286
Program Studi : Magister Kenotariatan
Judul Tesis : TANGGUNGJAWAB NOTARIS ATAS
PERLINDUNGAN DATA PRIBADI DALAM
AKSES INTEROPERABILITAS INFORMASI
DATA KEPENDUDUKAN

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Kenotariatan pada Program Studi Magister Kenotariatan, Fakultas Hukum, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Dr. Edmon Makarim S.Kom., S.H., LL.M 
Penguji : Akhmad Budi Cahyono, S.H.,M.H 
Penguji : Wenny Setiawati, S.H., M.LI 

Ditetapkan di : Depok
Tanggal : 02 Juli 2012

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tesis ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Kenotariatan pada Fakultas Hukum Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tesis ini, tidak mudah bagi saya untuk menyelesaikan tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

- (1) Dr Edmon Makarim S. Kom SH LLM, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini;
- (2) Bapak Martua Batubara, Sekretaris Majelis Pengawas Pusat Notaris dan Bapak Andi Kihorman, Kepala Bidang Hubungan Masyarakat Kementrian Dalam Negeri Republik Indonesia yang membantu saya memperoleh data yang diperlukan serta bersedia menjadi narasumber;
- (3) Bapak Akhmad Budi Cahyono SH MH dan Ibu Wenny Setiawati SH MLI sebagai penguji sekaligus pihak yang banyak membantu penulis untuk memperbaiki tesis ini.
- (4) Bapak Dr Drs Widodo Suryandono SH MH, selaku Ketua Program Magister Kenotariatan Fakultas Hukum Universitas Indonesia, sekaligus pembimbing akademis penulis sejak Program Sarjana Reguler tahun 2006 hingga sekarang atas masukan dan motivasi yang diberikan selama ini.
- (5) Seluruh dosen Magister Kenotariatan Fakultas Hukum Universitas Indonesia dan Program Sarjana Reguler Fakultas Hukum Universitas Indonesia yang telah mendidik, memberikan ilmu dan berbagi pengalamannya pada penulis, khususnya Prof Dr Rosa Agustina SH MH, Bapak Abdul Salam SH MH, Prof Agus Sardjono, Ibu Darwani Sidi Bakaroesdin, Ibu Arikanti Natakusumah, Ibu Arie.S Hutagalung dan Bapak alm. Rudy Satriyo.
- (6) Petugas dan karyawan Perpustakaan Soediman Kartohadiprojo, Fakultas Hukum Universitas Indonesia yang telah melayani penulis untuk

memperoleh bahan dari perpustakaan selama menjadi Mahasiswa Notariat Fakultas Hukum Universitas Indonesia.

- (7) Orang tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral;
- (8) So Nyuh Shi Dae aka Girls Generation (Kim Taeyeon, Jung Soo Yeon, Lee Soon Kyu, Hwang Mi Young, Kim Hyo Yeon, Kwon Yuri, Choi Soo Young , Lim Yoon Ah dan Seo Joo Hyun) yang musik, daya juang dan semangatnya telah menginspirasi penulis dalam menyusun dan menyelesaikan tesis ini;
- (9) Teman – teman dari forum Indowebster yang ikut membantu penulis memperoleh ide serta bahan dan informasi juga menyemangati penulis dalam menyelesaikan tesis ini, Prima aka Kyoshiro, Yongki aka Zeroka, Bima aka love3na, Febryan aka febragon, Ezahan, callanti, phee70, dir, darkslash, Zekusion, Taishou dan Joko aka musaku;
- (10) Teman – teman saya dari berbagai forum, Soy, cedge, Angel, Cecil aka Real Chinchiu, oniontaker, trooper, youngbuck, yuldori, beyondSNSD, taenacity, linichi, pubsquash, K.N Le dan chsoshi yang selalu berbagi cerita dan informasi pada penulis; dan
- (11) Teman – teman saya Irwan Chandra, Indra Pranajaya, Bakti Simamora, Ratyan Noer Hartiko, Gibson Thomasyadi, Mohammad Thoha Hanafi, Yoshua, Gigih, Dody dan Patrick Audhie yang telah banyak membantu saya dalam menyelesaikan tesis ini serta sebagai teman yang selalu membantu ketika penulis kesulitan.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tesis ini membawa manfaat bagi pengembangan ilmu pengetahuan.

Depok, 14 Juni 2012

Penulis

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Hartanto Budiman

NPM : 1006738286

Program Studi : Magister Kenotariatan

Fakultas : Hukum

Jenis karya : TESIS

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas tesis saya yang berjudul :

Tanggungjawab Notaris Atas Perlindungan Data Pribadi Dalam Akses Interoperabilitas Informasi Data Kependudukan

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 14 Juni 2012

Yang menyatakan



(Hartanto Budiman)

ABSTRAK

Nama : Hartanto Budiman
Program Studi : Magister Kenotariatan
Judul : Tanggungjawab Notaris Atas Perlindungan Data Pribadi Dalam Akses Interoperabilitas Informasi Data Kependudukan

Saat ini tengah berkembang dua fenomena yang mempengaruhi tugas Notaris sebagai pembuat akta yang merupakan alat bukti sempurna dalam hubungan perdata antara anggota masyarakat yaitu *Cyber Notary/e-Notary* dan *e-Government*. Kedua fenomena ini menimbulkan informasi yang vital bagi Notaris yaitu terkait masalah validitas identitas penghadap dalam bentuk *Electronic Identity*. Di dalam *Electronic Identity* terdapat informasi yang merupakan data pribadi yang harus dilindungi karena terkait dengan hak seseorang atas privasi. Oleh karena itu akses atas data pribadi tersebut harus diatur dan dipertanggungjawabkan agar tidak melanggar hak atas privasi tersebut. Hingga saat ini di Indonesia belum ada peraturan khusus yang mengatur tentang perlindungan atas data pribadi . Oleh karena itu, tesis ini bertujuan untuk mengkaji bagaimana pengaturan perlindungan data pribadi di Indonesia dan bagaimana pertanggungjawaban Notaris sebagai salah satu pengakses data kependudukan yang diakses secara interoperabilitas terkait masalah perlindungan data pribadi dalam kaitannya dengan hak seseorang atas privasi. Penelitian ini adalah penelitian kualitatif dengan desain eksploratoris. Hasil penelitian ini adalah belum ada ketentuan yang secara khusus mengatur tentang perlindungan atas data pribadi di Indonesia, pengaturan yang ada saat ini terpecah – pecah di beberapa peraturan perundangan dan tanggungjawab Notaris dalam akses interoperabilitas data kependudukan adalah sebatas perolehan, penggunaan dan kerahasiaan data pribadi.

Kata kunci : *Electronic Identity* , *cyber-notary*, data pribadi, data kependudukan, interoperabilitas.

ABSTRACT

Name : Hartanto Budiman
Study Program : Notary Magistrate
Title : Notary Responsibility Regarding Personal Data Protection in Interoperability Access of Demographic Information

Now, there are two developing phenomenon's that have impact to Notary duty as authentic official documents maker as the strongest evidence of society member relation which are *Cyber Notary/e-Notary* and *e-Government*. Both of them create vital information for notary regarding validity matter in Electronic Identity. Electronic Identity contains of information related to personal data which must be protected regarding a person privacy right. Because of that access of personal data must be regulated and justify so the right of privacy not violated. Until now Indonesia still doesn't have specific regulations that regulated protection of personal data. Because of that situation, this thesis aims to explore personal data protection in Indonesia and notary responsibility as one that access demographic information that being accessed interoperable in relation with personal data protection regarding a person's privacy right. This research is qualitative with explorative typology. The result of this research is there is still no regulation that specifically regulated about personal data protection in Indonesia, the regulation that exist now is split into some regulations and notary responsibility regarding interoperability access of demographic information is limited to acquisition, using and confidentiality of personal data.

Key words: *Electronic Identity* , *cyber-notary*, personal data, demographic data, interoperability

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PERNYATAAN ORISINALITAS.....	ii
LEMBAR PENGESAHAN.....	iii
KATA PENGANTAR.....	iv
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH.....	vi
ABSTRAK.....	vii
DAFTAR ISI.....	ix
DAFTAR LAMPIRAN.....	xi
1. PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Pokok Masalah.....	5
1.3. Metode Penelitian	5
1.4. Sistematika Penulisan	6
2. KONSEP UMUM PRIVASI, <i>e-GOVERNMENT</i> dan NOTARIS.....	9
2.1. Privasi, Data Pribadi dan Perlindungan Data Pribadi	9
2.1.1. Pengertian Privasi	9
2.1.2. Data dan Data Pribadi.....	13
2.1.3. Perlindungan Data Pribadi.....	13
2.2. Electronic Government (E-Government), Pelayanan Publik, Electronic Identity dan Identity Management System	20
2.2.1. <i>Government</i> (Pemerintah) dan <i>Governance</i> (Pemerintahan).....	20
2.2.2. Pelayanan Publik.....	22
2.2.3. <i>E-Government</i>	24
2.2.4. Sistem Administrasi Kependudukan sebagai bentuk pelaksanaan <i>E-Government</i> di Indonesia.....	25
2.2.5. <i>Electronic Identity</i>	26
2.2.6. Pengamanan <i>Electronic Identity</i>	27
2.2.7. Identity Management System.....	31
2.2.8. Interoperabilitas dalam <i>Identity Management System</i>	31
2.3. Notaris Sebagai Pejabat Umum yang Berwenang membuat Akta Otentik.....	32
2.3.1. Notaris	32
2.3.2. Notaris Sebagai Pejabat Umum Dalam Kaitan Dengan Pasal 1868 KUHPerdara.....	33
2.3.3. Akta dan Akta Otentik.....	34
2.3.4. Syarat Otentisitas Akta Notaris	35
2.3.5. Pengawasan Terhadap Notaris.....	44
3. PERLINDUNGAN DATA PRIBADI DI INDONESIA DAN TANGGUNG JAWAB NOTARIS DALAM AKSES INTEROPERABILITAS DATA KEPENDUDUKAN.....	48
3.1. Perlindungan Data Pribadi di Indonesia	48

3.2. Urgensi Akses Data Kependudukan Oleh Notaris.....	53
3.3. Hak dan Kewajiban Notaris Sebagai Pengakses Data Kependudukan.....	58
3.4. Tanggung Jawab Notaris Sebagai Pengakses Data Kependudukan	59
4. PENUTUP.....	66
4.1. Kesimpulan	66
4.2. Saran	67
DAFTAR REFERENSI.....	68



DAFTAR LAMPIRAN

- Lampiran 1: Tampilan Sistem Administrasi Kependudukan
- Lampiran 2: Skema Prediksi Hubungan Antara Para Pihak Dalam Sistem Administrasi Kependudukan (SIAK)
- Lampiran 3: Sistem INI-SAN Adminstrasi Notaris Secara Elektronik
- Lampiran 4: Diagram Flow dan Fitur INI-SAN



BAB I

PENDAHULUAN

1.1. Latar Belakang

Tanggungjawab Notaris atas perlindungan data pribadi dalam akses interoperabilitas informasi data kependudukan merupakan hal yang penting terkait penerapan Sistem Administrasi Kependudukan (SIAK)¹ yang digunakan di Indonesia sebagai salah satu bentuk penerapan *electronic government (e-government)*.

Perkembangan teknologi khususnya teknologi informasi yang sangat pesat mengakibatkan perubahan di berbagai sektor kehidupan manusia, termasuk perubahan transaksi/perjanjian yang semula menggunakan kertas menjadi menggunakan sistem elektronik (transaksi elektronik). Hal ini telah diakomodasi oleh forum internasional yaitu UNCITRAL² yang telah lama memberikan rekomendasi tentang perlunya pengakuan terhadap nilai hukum pada sutau informasi dan/atau dokumen elektronik. UNCITRAL telah menggulirkan *Model Law on E-Commerce (1996)*³ dan *Model Law on E-Signatures (2001)*⁴ yang dapat digunakan oleh semua negara dalam mengembangkan sistem hukum nasionalnya untuk mengakomodir dinamika perniagaan secara elektronik dan pengaturan tentang tandatangan elektronik.

Terkait dengan tandatangan elektronik yang merupakan instrumen autentifikasi dan penandatanganan secara elektronik disinggung peranan notaris publik untuk mendukung *E-Commerce* (perjanjian elektronik) dan memperlihatkan pentingnya perhatian terhadap perkembangan Hague Agreement 1961 tentang *The Convention Abolishing the Requirement of*

¹ Sistem Informasi Administrasi Kependudukan, selanjutnya disingkat SIAK, adalah sistem informasi yang memanfaatkan teknologi informasi dan komunikasi untuk memfasilitasi pengelolaan informasi administrasi kependudukan di tingkat Penyelenggara dan Instansi Pelaksana sebagai satu kesatuan, lihat Indonesia (a), *Undang-Undang Administrasi Kependudukan*, UU No.23 tahun 2006, LN No.124 Tahun 2006, TLN No. 4674, Ps. 1 angka 21..

² UNCITRAL adalah singkatan dari *United Nations Commission on International Trade Law*.

³ UCITRAL (1), *Model Law on E-Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*, New York, 1999.

⁴ UCITRAL (1), *Model Law on E-Signatures with Guide to Enactment 2001*, New York, 2002.

Legislation for Foreign Public Documents, yang mengarahkan setiap otoritas publik yang berkompoten (termasuk notaris) untuk melakukan simplifikasi dan format standar (“*Apostille*”) dalam mensertifikasi keotentikan sesuatu dokumen publik menjadi bentuk yang elektronik (*electronic apostille*).

Sehubungan dengan hal tersebut, urgensi fungsi dan peran notaris secara elektronik telah mengemuka pada International Congress XXIV Notaris Latin tahun 2004 yang sempat dibahas dalam *Working Group* untuk *Theme II* (“*The Notary and Electronic Contracts*”) yang intinya meyakini untuk membuka diri dengan mengakomodir semua perkembangan tersebut dengan baik dan tidak mengurangi ketentuan sebagaimana mestinya. Pada intinya kongres ini telah menyadari adanya kemungkinan pembuatan akta secara elektronik. Pengakomodasian perkembangan ini kemudian melahirkan konsep *cyber-notary* ataupun *e-notary*⁵. di mana untuk pelaksanaan konsep tersebut Notaris sebagai pejabat umum⁶ untuk memenuhi persyaratan dalam pembuatan akta otentik⁷ sebagai alat bukti yang sempurna atas suatu perbuatan hukum sebagaimana ditentukan dalam pasal 39 ayat (2) Undang Undang Jabatan Notaris⁸ yaitu mengenal penghadap yang membuat akta⁹. Selama ini untuk

⁵ Istilah *Cyber Notary* pertama kali dikemukakan oleh Information Security Committee of the American Bar Association, Section of Science and Technology yaitu bahwa Notaris tidak hanya terlibat dengan dokumen tertulis tetapi juga dengan dokumen elektronik dengan kata lain Notaris membuat dokumen secara elektronik. Lihat Kristel Kreek, “Electronic Signatures and E-invoicing; legislative approaches to electronic authentication and integrity of data” <http://www.virtuallawjournal.net/?nodeid=39&lang=en>, diakses 23 Mei 2011, lihat juga Laurence Leff, ed, “*Notaries and Electronic Notarization, Western Illinois University*” <http://www.oasis-open.org/committees/download.php/4541/enotarization.pdf>, hlm 6, diunduh 25 Maret 2012.

⁶ Notaris adalah pejabat umum sebagaimana dinyatakan dalam pasal 1 angka 1 Undang Undang Jabatan Notaris “Notaris adalah pejabat umum yang berwenang membuat akta otentik dan kewenangan lainnya sebagaimana dimaksud dalam Undang-Undang ini”. Lihat Indonesia (b), *Undang-Undang Tentang Jabatan Notaris*, UU No. 30, LN No. 117 tahun 2004, TLN. No. 4432, pasal 1 angka 1.

⁷ Akta otentik adalah suatu akta yang didalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau dihadapan pegawai-pegawai umum yang berkuasa untuk itu ditempat dimana akta dibuatnya, lihat Kitab Undang Undang Hukum Perdata (*Burgerlijk Wetboek*) diterjemahkan oleh R. Subekti dan R. Tjitrosudibio, cet.32, (Jakarta : Pradnya Paramita, 2004), ps, 1868.

⁸ Lihat Indonesia (b), *loc.cit*, pasal 39 ayat (2).

⁹ Pengertian kenal dalam akta ini tidaklah sama dengan kenal secara pribadi, melainkan kenal secara hukum/yuridis, yaitu kenal berdasarkan identitas yang sah, yang memuat secara benar nama, alamat, tempat dan tanggal lahir yang dikenal oleh umum/masyarakat sebagai benar bahwa itu adalah orang yang bersangkutan, selain itu bahwa penghadap mempunyai wewenang untuk melakukan suatu tindakan hukum yang disebutkan dalam akta, lihat Tan Thong Kie, *Studi Notariat & Serba – Serbi Praktek Notaris*, Cet 1 (Jakarta : Ichtiar Baru Van Hoeve,2007), hlm 499 dan G.H.R Lumban Tobing, *Peraturan Jabatan Notaris*, cet 4 (Jakarta : Erlangga, 1996), hlm 172.

mengenal penghadap, Notaris menggunakan identitas yaitu KTP, SIM dan paspor. Dengan adanya konsep *Cyber Notary* maka media yang digunakan oleh Notaris untuk mengenal penghadap adalah *Electronic Identity (e-ID)*.

e-ID tersebut merupakan salah satu bentuk penerapan konsep *e-government* dalam pelayanan publik oleh pemerintah. *E-government* adalah pemanfaatan teknologi informasi (internet dan *World Wide Web*) oleh pemerintah dalam pemberian informasi dan pelayanan publik. Salah satu bentuk layanan pemerintah kepada publik tersebut adalah terkait administrasi kependudukan¹⁰, saat ini beberapa Negara seperti Belgia dan Perancis telah menerapkan teknologi informasi dalam administrasi kependudukan, melalui penerapan *digital identity (digital ID/e-ID)* tersebut.

Di Indonesia konsep *E-ID* tersebut mulai digulirkan dengan ditetapkannya Peraturan Presiden Republik Indonesia Nomor 26 Tahun 2009 yang kemudian diubah dengan Peraturan Presiden Republik Indonesia Nomor 35 Tahun 2010 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (“Perpres KTP berbasis NIK/Perpres e-KTP”), di mana dalam penerapan tersebut digunakan perangkat lunak, perangkat keras dan blangko berbasis Nomor Induk Kependudukan yang dilengkapi kode keamanan dan rekaman elektronik¹¹ dengan kata lain menggunakan teknologi informasi. Kemudian di dalam pasal 6 ayat (1) revisi Peraturan Presiden tersebut (Peraturan Presiden Nomor 35 Tahun 2010) menyatakan bahwa KTP berbasis NIK memuat kode keamanan dan rekaman elektronik sebagai alat verifikasi dan validasi jati diri penduduk, kemudian pada ayat (2) nya dinyatakan bahwa rekaman elektronik tersebut berisi biodata, tandatangan, pas foto, dan sidik jari tangan penduduk yang bersangkutan.

¹⁰ Administrasi Kependudukan adalah rangkaian kegiatan penataan dan penertiban dalam penerbitan dokumen dan Data Kependudukan melalui Pendaftaran Penduduk, Pencatatan Sipil, pengelolaan informasi Administrasi Kependudukan serta pendayagunaan hasilnya untuk pelayanan publik dan pembangunan sektor lain, lihat Indonesia (a), *loc.cit*, Ps. 1 angka 1.

¹¹ Indonesia (c), *Peraturan Presiden Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional*, Perpres No.26 tahun 2009, Ps. 2 ayat 1.

Ketentuan pada 6 ayat (1) dan (2) revisi Perpres *e-KTP* tersebut menunjukkan bahwa Tanda Tangan Elektronik¹² yang digunakan adalah berbasis biometrik (sidik jari, photo dan tanda tangan) yang merupakan data yang bersifat statis (tidak berubah)¹³. Oleh karena itu sangat berbahaya apabila data tersebut diakses oleh pihak yang tidak berwenang maka pemilik data tersebut yang sah harus menarik data tersebut. Oleh karena itu perlindungan atas rekaman biometrik tersebut sangat penting, hal ini mengingat dalam Undang Undang Administrasi Kependudukan pada pasal 87 ayat (1) ditentukan bahwa pengguna data pribadi penduduk dapat memperoleh dan menggunakan data pribadi dari petugas pada penyelenggara dan Instansi Pelaksana yang memiliki hak akses dimana data pribadi tersebut mencakup juga data kependudukan yang memuat rekaman biometrik tersebut. Hal ini berarti pengguna data pribadi penduduk yang bisa merupakan perorangan atau badan bisa memperoleh data tersebut dengan mengajukan permohonan. Oleh karena itu hak akses tersebut haruslah diatur dengan ketat agar tidak terjadi kebocoran informasi data pribadi penduduk.

Oleh karena itu, untuk dapat menjalankan tugasnya sebagai pejabat publik dalam membuat akta dalam era teknologi informasi saat ini, maka Notaris memerlukan akses terhadap data *e-ID (e-KTP)* untuk memastikan identitas penghadap yang merupakan data kependudukan yang berisi data pribadi yang perlu untuk dilindungi dari akses orang yang tidak berwenang, karena terkait dengan hak setiap orang atas privasi.

Akses terhadap data kependudukan tersebut tidak hanya dilakukan oleh pejabat pelaksana administrasi kependudukan dan Notaris tetapi juga oleh

¹² Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentifikasi, lihat Indonesia (d), *Undang-Undang Informasi dan Transaksi Elektronik*, UU No.11 tahun 2008, LN No.58 Tahun 2008, TLN No. 4843, Ps. 1 angka 12.

¹³ *Biometrik* adalah metode pengukuran yang digunakan untuk mengidentifikasi kejelasan individu melalui ciri – ciri intrinsiknya secara fisik atau perilaku yang dapat berupa DNA, sidik jari, iris, retina, tangan atau geometri wajah, bentuk telinga, suara, bau badan, pola pembuluh darah, tulisan tangan dan pola menulis ataupun mengetik, lihat United Nations Commission on International Trade Law (UNCITRAL), *Promoting Confidence in E-Commerce Legal Issues on International Use of Electronic Authentication and Signature Methods* (Vienna : United Nations Publication, 2009), hlm 27, lihat juga Kai Ronnenberg, Dennis Royer, André Deuker, ed, *The Future of Identity in the Information Society Challenges and Opportunities* (Berlin Heidelberg : Springer – Verlag, 2009), hlm. 138.

lembaga pemerintah lainnya seperti Kementerian Hukum dan Hak Asasi Manusia dan Kementerian Komunikasi dan Informasi (KOMINFO) selain itu juga pihak swasta yang berkepentingan atas data identitas tersebut misalnya bank dan lembaga keuangan lainnya, oleh karena itu akses terhadap data pribadi tersebut dilakukan oleh banyak pihak dan juga melibatkan banyak pihak di mulai dari perancangan sistem database oleh developer, pengelolaan database (*database maintenance*), hingga pada penggunaannya sebagai sumber data kependudukan oleh pihak – pihak yang memerlukannya termasuk Notaris.

Oleh karena itu penting untuk dikaji mengenai aspek perlindungan data pribadi yang perlu dilindungi terhadap akses interoperabilitas yang dilakukan oleh berbagai pihak dan ketentuan hukum yang mengatur perlindungan tersebut dan bagaimana tanggungjawab Notaris atas akses interoperabilitas tersebut sebagai salah satu pihak yang melakukan akses tersebut.

1.2. Pokok Masalah

1. Bagaimanakah ketentuan hukum yang mengatur tentang perlindungan data pribadi dan kewenangan akses data kependudukan ?
2. Bagaimanakah tanggungjawab Notaris atas perlindungan data pribadi terkait akses interoperabilitas data kependudukan yang dilakukan dalam pembuatan akta otentik ?

1.3. Metode Penelitian

Dalam tesis ini metode penelitian yang digunakan adalah penelitian hukum normatif¹⁴. Sehingga data yang dipergunakan adalah data sekunder, yaitu data – data yang diperoleh dari studi kepustakaan¹⁵, berupa buku – buku, artikel dan jurnal yang terkait dengan masalah yang sedang diteliti. Tipologi penelitian yang digunakan adalah penelitian yang bersifat eksploratoris¹⁶ untuk mengeksplorasi perlindungan data pribadi dalam akses interoperabilitas informasi data kependudukan. Dari sudut penerapannya penelitian ini adalah

¹⁴ Penelitian hukum normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka, lihat Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, (Jakarta : Rajawali Pers, 2007), hal 13.

¹⁵ Sri Mamudji et al, *Metode Penelitian Dan Penulisan Hukum*, (Jakarta : Badan Penerbit Fakultas Hukum Universitas Indonesia, 2005), hal 28.

¹⁶ Penelitian eksploratoris adalah penelitian yang bertujuan untuk mencari data awal tentang suatu gejala, lihat *ibid*, hal. 4.

penelitian murni¹⁷ yang bertujuan untuk pengembangan ilmu pengetahuan atau teori dalam hal ini adalah tanggungjawab Notaris atas perlindungan data pribadi dalam akses interoperabilitas informasi data kependudukan.

Penelitian ini menggunakan bahan – bahan hukum yaitu bahan hukum primer¹⁸ berupa peraturan perundang – undangan, bahan hukum sekunder¹⁹ berupa buku – buku mengenai *e-Id*, Notaris, *e-Government*, artikel – artikel baik dari Koran maupun internet, jurnal hukum, tesis yang terkait dengan penelitian.

Di dalam penelitian, pada umumnya dikenal tiga jenis pengumpulan data, yaitu studi dokumen atau bahan pustaka, pengamatan atau observasi dan wawancara atau interview.²⁰ Alat pengumpulan data yang digunakan dalam penelitian tesis ini adalah studi dokumen/pustaka, karena data yang diperlukan adalah data sekunder (data yang diperoleh dari bahan kepustakaan). Sedangkan untuk analisis data, metode yang digunakan adalah pendekatan kualitatif, yang menyajikan data secara deskriptif. Hasil dari penelitian ini adalah data – data awal mengenai perlindungan data pribadi dalam akses interoperabilitas data kependudukan dan pertanggungjawaban notaris atas hal tersebut sebagai salah satu pihak yang melakukan akses interoperabilitas tersebut sesuai dengan tipe penelitian yang bersifat eksploratoris (menjelajah)

1.4 Sistematika Penulisan

Sistematika penulisan tesis ini bertujuan untuk memudahkan penulis dalam menguraikan isi dari tesis ini yang secara keseluruhan terbagi dalam 4 (empat) bab. Pada tiap-tiap bab terbagi dalam beberapa sub-sub bab yang saling terkait satu sama lain sehingga menjadi satu kesatuan utuh dalam

¹⁷ Penelitian muni atau penelitian dasar adalah penelitian yang bertujuan untuk pengembangan ilmu dan teori, lihat *ibid*, hal. 5.

¹⁸ Bahan primer adalah bahan-bahan hukum yang mengikat seperti norma dasar, peraturan dasar, ketetapan MPR, undang-undang, perturan pemerintah, keputusan presiden, peraturan daerah, bahan hukum yang tidak dikodifikasikan, yurisprudensi, traktat, peraturan dari zaman kolonial penjajahan yang kini masih berlaku, lihat *ibid*, hal. 30.

¹⁹ Bahan sekunder adalah bahan-bahan yang memberikan informasi atau hal-hal yang berkaitan dengan isi bahan primer serta implementasinya, contoh: buku, makalah dan artikel ilmiah, lihat *ibid*, hal. 31.

²⁰ Soerjono Soekanto, *Pengantar Penelitian Hukum*, cet. 3, (Jakarta: UI – Press, 1986), hal. 21.

pemahaman permasalahan. Pada bagian akhir tesis ini dilengkapi pula dengan daftar pustaka dan lampiran-lampiran. Adapun susunan sistematika yang dimaksud adalah sebagai berikut:

BAB 1 PENDAHULUAN

Dalam bab ini berisikan gambaran umum mengenai latar belakang masalah yang menjadi dasar penulisan, pokok permasalahan, metode penelitian dan sistematika penulisan.

BAB 2 KONSEP UMUM PRIVASI, *e-GOVERNMENT* dan NOTARIS

Bab ini berisi kajian yang lebih mendalam mengenai teori – teori mengenai perlindungan data pribadi dan kewenangan akses data kependudukan serta ketentuan hukum positif yang ada terkait perlindungan data pribadi, *Electronic Government*, Pelayanan Publik, *Electronic Identity* serta *Identity Management System* dan pembahasan mengenai Notaris sebagai Pejabat Umum yang berwenang membuat akta otentik. Penulisannya dibagi ke dalam beberapa sub-sub bab sebagai berikut :

2.1 Privasi, Data Pribadi dan Perlindungan Data Pribadi

2.1.1. Pengertian Privasi

2.1.2. Data dan Data Pribadi

2.1.3. Perlindungan Data Pribadi

2.2. Electronic Government (*E-Government*), Pelayanan Publik, *Electronic Identity* dan *Identity Management System*

2.2.1. *Government* (Pemerintah) dan *Governance* (Pemerintahan)

2.2.2. Pelayanan Publik

2.2.3. *E-Government*

2.2.4. Sistem Administrasi Kependudukan (SIAK) Sebagai Bentuk Penerapan *e-Government* di Indonesia.

2.2.5. *Electronic Identity*

2.2.6. Pengamanan *Electronic Identity*

2.2.6.1. Biometrik

2.2.6.2. *Digital Signature* (Tanda Tangan Digital)

2.2.7. *Identity Management System*

- 2.2.8. Interoperabilitas dalam *Identity Management System*
- 2.3. Notaris Sebagai Pejabat Umum yang Berwenang membuat Akta Otentik
 - 2.3.1. Notaris
 - 2.3.2. Notaris Sebagai Pejabat Umum Dalam Kaitan Dengan Pasal 1868 KUHPperdata
 - 2.3.3. Akta dan Akta Otentik
 - 2.3.4. Syarat Otentisitas Akta Notaris
 - 2.3.5. Pengawasan Terhadap Notaris

BAB 3 PERLINDUNGAN DATA DAN TANGGUNGJAWAB NOTARIS DALAM AKSES INTEROPERABILITAS DATA KEPENDUDUKAN

Bab ini berisi kajian mengenai tanggungjawab Notaris atas perlindungan data pribadi dalam akses interoperabilitas data sebagai salah satu pihak yang melakukan akses secara interoperabilitas. Penuliskannya dibagi ke dalam beberapa sub-sub bab sebagai berikut :

- 3.1 Perlindungan Data Pribadi di Indonesia
- 3.2 Urgensi Akses Data Kependudukan Oleh Notaris
- 3.3 Hak dan Kewajiban Notaris Sebagai pengakses Data Kependudukan
- 3.4 Tanggungjawab Notaris Sebagai Pengakses Data Kependudukan

Bab 4 PENUTUP

Bab ini merupakan bagian terakhir dari penulisan tesis. Di dalamnya memuat tentang simpulan atas pembahasan terhadap pokok-pokok permasalahan disertai dengan saran dari penulis.

Bab II

KONSEP UMUM PRIVASI, *e-GOVERNMENT* DAN NOTARIS

2.1 Privasi, Data Pribadi dan Perlindungan Data Pribadi

2.1.1 Pengertian Privasi

Dalam survei mengenai sejarah pengaturan privasi di Amerika Serikat, Ken Gormley mengidentifikasi dalam literturnya, empat pengertian dari privasi, yaitu :

1. *“an expression of one’s personality or personality or personhood, focusing on the right of the individual to define his or her essence as a human being” (Roscoe Pound dan Paul Freund);*
2. *“autonomy-the moral freedom of the individual to engage his or her own thoughts, actions and decisions” (Louis Henkin);*
3. *“citizen’ ability to regulate information about themselves , and thus control their relationship with other human beings” (Alan Westin dan Charles Fried); dan*
4. *“the essential components approach, in which scholars identify certain essential components, such as secrecy, anonymity and solitude” (Ruch Gavinson)²¹*

Dari keempat pengertian privasi tersebut dapat ditarik kesimpulan bahwa pengertian – pengertian tersebut saling berhubungan satu dengan yang lainnya. Informasi yang oleh seseorang ditentukan boleh dipublikasikan berarti bahwa seseorang mempunyai kontrol/kendali atas informasi yang merefleksikan identitasnya sebagai manusia yang menunjukkan keterkaitan antara pengertian privasi yang ketiga dengan yang pertama. Kebebasan seseorang melakukan tindakan tertentu secara bebas berdasarkan pikiran dan keputusannya dalam pengertian kedua berhubungan dengan pengertian ketiga mengenai kontrol atas informasi tentang dirinya yang juga menunjukkan esensinya sebagai manusia dan terkait dengan keputusannya untuk merahasiakan sesuatu tentang dirinya yang terkait dengan pengertian

²¹ Ken Gormley, “One hundred Years of Privacy”, *Winsconsin Law Review* (September-October 1992), hlm. 1337-1338.

keempat. Jika digabungkan maka keempat pengertian di atas menjadi kebebasan seseorang untuk bertindak dan memutuskan secara bebas informasi mengenai dirinya yang akan ia publikasikan maupun rahasiakan yang merefleksikan dirinya sebagai manusia.

Terkait dengan kebebasan untuk bertindak dan memutuskan tersebut Francis Chalapowski menyatakan privasi adalah ‘harta milik’ (property) “*personality information is not only an aspect of personality, it is also an object of personality*” dengan mengutip pendapat John Locke bahwa “setiap orang mempunyai harta milik dalam dirinya” sehingga “menikmati hak untuk mengontrol dan mendominasi hasil dari dirinya tersebut”.²²

Dalam artikelnya ‘*Privacy, privacies and basic needs*’ Hayden Ramsay (2010) mengidentifikasi lima bentuk pengertian privasi secara filosofis dan menganalisisnya, yaitu :

1. Mengontrol arus informasi yang menurutnya sangat kabur, karena kebebasan dan kepribadian bukan hal terpenting dalam kehidupan seseorang, karena masih ada hal lain yang penting yaitu kebijaksanaan (*wisdom*) dan kejujuran (*truthfulness*). Walaupun kehilangan kontrol atas informasi mengenai dirinya mengurangi kebebasan dan kepribadian tidak berarti pelanggaran atas privasi hanya masalah moral, selain itu privasi berarti lebih dari sekedar kontrol atas informasi jika seseorang percaya dia sedang dimata – matai, maka itu juga merupakan pelanggaran atas privasi yang menurutnya tidak hanya ketakutan atas kehilangan data tetapi juga kemarahan karena diawasi dan diganggu dan marah karena tidak dihargai dan tidak dibiarkan menyendiri.
2. Bebas dari gangguan dan pengawasan, yang menjadi perdebatan apakah bentuk gangguan dan pengawasan tersebut karena pada keadaan tertentu pengawasan sangat diperlukan misalnya orang yang diduga melakukan tindak pidana dan teroris. Terhadap mereka tentunya pengawasan dan pengintaian atas gerak – gerik sangat diperlukan untuk mencegah terjadinya tindak pidana ataupun aksi terorisme.

²² Francis S. Chalapowski, “The Constitutional Protection of Information Privacy”, *Boston University Law Review*, vol.71 (Januari 1991), hlm. 133.

3. Penghargaan atas diri seseorang yang mempunyai kesadaran dan kepentingan yang memiliki sikap dalam hubungan/interaksi dengan sesama seperti pengakuan, penghargaan, penghormatan dan meminta maaf. Dengan kata lain privasi sangat terkait dengan moralitas.
4. Keperluan seseorang untuk sendiri/menyendiri
5. Perlindungan dari pengawasan dan gangguan, hal ini terkait dengan pengertian kedua yaitu bebas dari gangguan dan pengawasan²³

Adapun terkait dengan gangguan dan pengawasan, gangguan bersifat acak sedangkan pengawasan karena adanya suatu tujuan yang ingin dicapai/diperoleh dari tindakan pengawasan tersebut.

Terkait pengertian privasi dalam informasi digital, pengertian tentang privasi diungkapkan oleh Alan F. Westin dalam studinya “Privacy and Freedom” di mana ia mendefinisikan “*Privacy is claims of individuals, groups or institution to determine for themselves when, how and to what extent information about them is communicated to others.*”²⁴. Pengertian ini berfokus pada kontrol/kendali atas informasi jadi privasi dalam informasi digital adalah kebebasan seseorang, kelompok atau lembaga untuk menentukan informasi mengenai/terkait mereka yang akan diberitahukan/diinformasikan kepada orang lain.

Menurut Thomas J.Smedinghoff ada tiga aspek dari privasi yaitu privasi mengenai pribadi seseorang (*Privacy of a Person's Persona*), privasi dari data tentang seseorang (*Privacy of Data About a Person*) dan privasi atas komunikasi seseorang (*Privacy of a Person's Communications*).²⁵

1. *Privacy of a Person's Persona*

Hak atas privasi ini didasarkan pada prinsip umum bahwa setiap orang mempunyai hak untuk dibiarkan sendiri (*the right to be let alone*). Pada umumnya ada empat jenis pelanggaran terhadap privasi atas pribadi seseorang yaitu:

²³ Hayden Ramsay. “Privacy, Privacies and Basic Needs”, *The Heythrop Journal*, vol.51 (Februari 2010), hlm. 288-297.

²⁴ Alan F. Westin, *Privacy and Freedom*, (Atheneum, 1967), hlm.7.

²⁵ Thomas J. Smedinghoff, ed., *Online Law – The SPA's Legal Guide to Doing Business on The Internet* (Canada : Addison-Wesley Developers Press, 1996), hlm. 269.

1. Publikasi yang menempatkan seseorang pada tempat yang salah. Misalnya dengan menggunakan foto seorang perempuan sebagai ilustrasi artikel tentang seorang ibu yang menelantarkan anaknya;
2. Penggunaan yang tidak tepat nama atau kesukaan seseorang untuk tujuan komersial;
3. Pembukaan fakta – fakta pribadi yang memalukan kepada publik;
4. Mengganggu kesunyian dan kesendirian seseorang.²⁶

2. *Privacy of Data About a Person*

Hak privasi dapat juga mengikat pada informasi mengenai seseorang yang dikumpulkan dan digunakan oleh orang lain. Termasuk di dalamnya, seperti informasi mengenai kebiasaan seseorang, catatan medis, agama, keanggotaan dalam suatu partai politik, catatan pajak, data – data karyawan, catatan asuransi, catatan tindak pidana, dan lain sebagainya. Penyalahgunaan informasi – informasi yang dikumpulkan atas anggota – anggota suatu organisasi/lembaga atau atas pelanggaran – pelanggaran dari suatu perusahaan termasuk dalam pelanggaran hak privasi seseorang.²⁷

3. *Privacy of a Person's Communications*

Dalam kondisi/keadaan tertentu, hak atas privasi dapat juga mencakup komunikasi secara online. Dalam kondisi/keadaan tertentu, pengawasan dan penyingkapan isi dari komunikasi elektronik oleh orang lain bukan oleh pengirim ataupun penerima dapat merupakan pelanggaran atas privasi seseorang.²⁸

Terkait luasnya pengertian tentang privasi ini Ulrike Hugl dalam artikelnya '*Approaching the value of Privacy: Review of theoretical privacy concepts and aspects of privacy management*' menyimpulkan bahwa privasi adalah hak manusia yang terkait dengan moralitas (termasuk kontrol, tidak

²⁶ *Ibid.*, hlm. 270.

²⁷ *Ibid.*, hlm. 273.

²⁸ *Ibid.*, hlm. 269.

dilanggar, hak untuk menyendiri dan kebebasan) yang diperlukan agar seseorang dapat hidup dengan baik sebagai manusia.²⁹

2.1.2 Data dan Data Pribadi

Dalam United Kingdom Data Protection Act 1988, data didefinisikan sebagai setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi – instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses sedangkan data pribadi didefinisikan sebagai data yang berhubungan dengan seorang individu yang hidup yang dapat diidentifikasi dari data atau dari data – data atau informasi yang dimiliki oleh *data controller*.³⁰

Dalam *Directive 45/2001/EC of The Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, data pribadi didefinisikan sebagai segala informasi yang terkait untuk mengidentifikasi atau dapat mendefinisikan seseorang³¹

Jadi pada dasarnya data pribadi adalah informasi yang berhubungan dengan seorang individu yang dapat digunakan untuk mengenali seseorang individu di dalam suatu kelompok masyarakat.

2.1.3 Perlindungan Data Pribadi

Data pribadi merupakan informasi yang berhubungan dengan seseorang yang dapat mengidentifikasi orang tersebut oleh karena itu data pribadi sangat terkait dengan privasi karena merupakan informasi tentang diri seseorang oleh karena itu data pribadi perlu dilindungi.

Adapun perlindungan atas data pribadi di beberapa negara :

1. Uni Eropa

Perlindungan terhadap data pribadi di Uni Eropa terdapat dalam *Directive 95/46/EC of The Parliament and of the Council on The*

²⁹ Urike Hugi, “Approaching the value of Privacy: Review of theoretical privacy concepts and aspects of privacy management”, (disampaikan dalam *Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru*, 15 Desember 2010), hlm.3.

³⁰ United Kingdom, *Data Protection Act 1998, Article 1 (1)*. *Data controller* adalah orang perorangan atau beberapa orang yang menentukan ditujukan untuk apa dan dalam bentuk apa data pribadi akan diproses, lihat *Data Protection Act 1998, Article 1 (1)*.

³¹ The European Parliament And Council, EU Directive on The Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies

Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data yang dilengkapi dengan *Directive 45/2001/EC of The Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* yang ditujukan untuk melindungi hak – hak dasar dan kebebasan dari setiap orang khususnya hak atas privasi dalam kaitannya dengan pemrosesan data pribadi.

Dalam ketentuan tersebut perlindungan atas data pribadi tidak dapat dilakukan terkait dengan masalah keamanan nasional dan peraturan terkait tindak pidana dan mengenai pengelolaan data pribadi yang dilakukan oleh orang (pribadi kodrati) dalam kegiatan murni untuk kepentingan pribadi.

Secara singkat, *Directive* ini mensyaratkan bahwa pengguna (*user*) harus dapat mengontrol/mengatur pengumpulan dan pemrosesan data pribadi termasuk informasi yang langsung maupun tidak langsung berhubungan dengannya, termasuk pengumpulan data harus spesifik, eksplisit dan untuk tujuan yang legal (*specified, explicit and legitimate purposes*), pengumpulan data harus sesuai dengan tujuannya (*adequate, relevant, not excessive*), pengumpulan data harus akurat dan bila perlu selalu *up to date* (diperbaharui), pihak yang menjadi subyek (pihak yang terkait dengan data) harus memberikan persetujuan tegas untuk pemrosesan data dan penggunaan data lebih lanjut untuk hal yang tidak sesuai dengan tujuan tidak diperbolehkan.³²

Adapun perlindungan privasi di beberapa Negara di Eropa :

1. Inggris

Perlindungan terhadap data pribadi di Inggris terdapat dalam *Data Protection Act 1998* yang mengatur mengenai *Data Protection Comissioner*, Subyek Data, *Data Controller* (pengguna data) dan

³² Kai Ronnenberg, Dennis Royer dan André Deuker, *op.cit*, hlm. 351-352 lihat juga The European Parliament, *DIRECTIVE 2002/58/EC Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, Article 4.

Data Processor yaitu pihak selain data controller yang memproses data atas nama *data controller*.³³

Adapun prinsip perlindungan data yang ditentukan oleh *Data Protection Act* ini adalah :

1. Data Pribadi harus diperoleh secara jujur dan sah.
2. Data pribadi harus dimiliki hanya untuk satu tujuan atau lebih yang spesifik dan sah. Dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan-tujuan tersebut.
3. Data pribadi harus layak, relevan, dan tidak terlalu luas dalam hubungannya dengan tujuan atau tujuan-tujuan pengolahannya.
4. Data pribadi harus akurat dan jika perlu selalu *up-to-date*.
5. Data pribadi harus diproses sesuai dengan tujuannya dan tidak boleh dikuasai lebih lama dari waktu yang diperlukan untuk kepentingan tujuan atau tujuan-tujuan tersebut.
6. Data pribadi harus diproses sesuai dengan hak-hak dari subyek data sebagaimana yang diatur dlm undang-undang ini.
7. Tindakan-tindakan pengamanan yang memadai harus diambil untuk menghadapi kegiatan pemrosesan data pribadi yang tidak sah serta atas kerugian yang tidak terduga atau kerusakan dari data pribadi.
8. Data pribadi tidak boleh dikirim ke negara atau wilayah lain di luar Wilayah Ekonomi Eropa kecuali jika negara atau wilayah tersebut menjamin dengan suatu tingkat perlindungan terhadap hak-hak dan kebebasan-kebebasan subyek data sehubungan dengan pemrosesan data pribadi.³⁴

Selain itu ditentukan bahwa setiap individu yang menjadi subyek data sehubungan dengan data pribadi mengenai mereka yang dimiliki oleh orang/pihak lain mempunyai hak untuk mengakses informasi, mencegah pemrosesan yang dapat menyebabkan kerusakan atau keadaan yang membahayakan, hak untuk meminta

³³ Edmon Makarim (a), *Pengantar Hukum Telematika Suatu Kompilasi Kajian* (Jakarta : Rajawali Press, 2005), hlm. 171.

³⁴ *Ibid*, hlm.172.

kompensasi, hak untuk mengambil tindakan untuk membatasi, menghalang – halangi, menghapus atau menghancurkan data yang tidak akurat serta mempunyai hak meminta commissioner untuk membuat penyelesaian terhadap tindakan – tindakan yang melanggar ketentuan – ketentuan dalam *Data Protection Act* ini.³⁵

Adapun ketentuan atas data pribadi dalam *Data protection Act* ini dikecualikan dari masalah keamanan nasional, kejahatan, perpajakan, kesehatan, pendidikan dan kerja sosial.

2. Jerman

Di dalam konstitusi di Jerman (*Grundgesetz*) , tidak terdapat ketentuan khusus yang mengatur mengenai perlindungan atas data pribadi akan tetapi terdapat beberapa ketentuan yang terkait dengan perlindungan atas data pribadi yaitu hak atas kebebasan untuk mengembangkan diri pada *Article 2 Paragraph 1* yang di dalamnya mencakup hak untuk menentukan informasi atas diri sendiri (*right of informational self – determination*), hak istimewa terhadap pengkriminalisasian diri (*privilege against self-incrimination*) dan juga privasi, perlindungan atas penggeledahan atas rumah/tempat tinggal termasuk penyadapan baik secara manual maupun menggunakan media elektronik dalam *Article 13 Paragraph 1*³⁶, perlindungan terkait penggeledahan badan dalam *Article 2 Paragraph 2* dan ketentuan mengenai kerahasiaan atas komunikasi dalam *Article 10 Paragraph 1*³⁷.

³⁵ *Ibid*, hlm.173.

³⁶ Terkait dengan hal ini, di Jerman di kenal dua ruang lingkup yaitu lingkup yang sangat pribadi (*Inner Circle*) dan lingkup pribadi (*private life*), untuk lingkup yang sangat pribadi sama sekali tidak boleh diganggu/disentuh, misalnya percakapan antara anggota keluarga, percakapan dengan diri sendiri (*soliloquy*) ataupun hubungan seksual. Apabila informasi terkait lingkup sangat pribadi tersebut terekam maka harus segera di hapus. Penyadapan secara elektronik hanya dapat dilakukan jika ada indikasi yang jelas bahwa tempat tersebut harus diawasi dan ada hubungan dengan orang yang akan diawasi, lihat Ronald Leenes, Bert Joop Koops dan Paul De Hert, ed., *Information and Technology & Law Series Constitutional Rights and New Technologies A Comparative Study* (Hague Netherlands : TMC Asser Press, 2008), hlm.147-148.

³⁷ Kerahasiaan atas komunikasi yang diatur adalah komunikasi individual sedangkan media massa seperti radio dan televisi tidak. Ketentuan ini tidak spesifik menyebutkan bentuk komunikasi tertentu, semua gelombang elektromagnetik dan bentuk transmisi yang lainnya dilindungi tidak masalah apakah analog ataupun digital sehingga bentuk komunikasi dengan media elektronik pun dilindungi oleh ketentuan ini, lihat *Ibid*, hlm. 150-152.

3. Belanda

Di Belanda perlindungan atas data pribadi terdapat dalam beberapa Article dalam konstitusi (*Grondwet*) yaitu *Article 10 Paragraph 1* mengenai hak umum atas privasi, *Article 10 Paragraph 2-3* mengenai empat hak terkait privasi dan data proteksi, *inviolability of the home (Article 12)* dan kerahasiaan atas komunikasi (*Article 13*). Walau demikian ketentuan mengenai privasi di dalam konstitusi tidak dinyatakan secara eksplisit tetapi implisit dalam pasal – pasal konstitusi.

Dalam ketentuan mengenai hak umum atas privasi dinyatakan bahwa setiap orang mempunyai hak atas privasi tanpa pembatasan. Sama seperti di Jerman terdapat lingkup personal dan lingkup yang sangat pribadi, perlindungan atas privasi dan data pribadi tersebut diberikan pada lingkup yang sangat pribadi. Di luar lingkup yang sangat pribadi ini tidak banyak yang dipertimbangkan terkait dengan privasi hanya saja interaksi di ruang publik yang terkait dengan lingkup yang sangat pribadi. Terkait dengan perlindungan data pribadi *Article 10 Paragraph 2* dan *3* memberikan instruksi kepada parlemen untuk membuat peraturan terkait dengan perekaman dan penyebaran data pribadi serta ketentuan terkait kewajiban agar setiap orang diberitahu terkait perekaman data pribadinya serta penggunaannya dan pengkoreksiannya.³⁸

Terkait mengenai tidak bolehnya dilakukan penggeledahan/pengawasan atas properti seseorang (*inviolability at home*) ditentukan bahwa memasuki rumah/kediaman seseorang tanpa izin dari pemiliknya hanya dapat dilakukan seizin parlemen, lebih lanjut apabila pejabat pemerintah akan memasuki kediaman/rumah seseorang berdasarkan ketentuan tersebut maka mereka harus memperkenalkan diri dan memberitahu tujuan mereka dan juga dipersyaratkan adanya pemberitahuan tertulis kepada pemiliknya

³⁸ *Ibid*, hlm.165-166.

kecuali terkait keamanan Negara (*Article 12 Paragraph 2-3 Grondwet*)

Sementara itu mengenai kerahasiaan komunikasi berdasarkan ketentuan pada *Article 13 Paragraph 1 dan 2* maka yang dilindungi kerahasiaannya adalah korespondensi dan percakapan telepon secara telegraf. Berbeda dengan ketentuan di Jerman yang menyatakan bahwa semua bentuk komunikasi baik analog maupun digital dilindungi maka di Belanda tidak ada ketentuan tersebut sehingga ada usulan perubahan dengan memasukan media komunikasi lainnya yang muncul sesuai perkembangan zaman namun hingga saat ini belum dilakukan perubahan.

2. Amerika Serikat

Berbeda dengan Uni Eropa, Amerika Serikat tidak memiliki undang-undang yang mengatur mengenai perlindungan data dan/atau informasi secara keseluruhan. Selain itu pengaturan yang ada dibatasi hanya untuk suatu pihak tertentu, misalnya perbankan, asuransi dan lain – lain. Oleh karena itu, pengaturan mengenai pengumpulan secara online dan pengomunikasian dari data pribadi harus dievaluasi dari aturan hukum yang telah ada.

Misalnya dalam *Privacy Act 1974* ditentukan pembatasan pengumpulan dan penggunaan informasi pribadi oleh agen – agen pemerintah federal, namun ketentuan dalam *Privacy Act* ini tidak berlaku bagi pengumpulan data pribadi oleh lembaga – lembaga swasta.

Meskipun demikian ada beberapa ketentuan dalam hukum Amerika Serikat yang memberikan perlindungan terkait data pribadi yaitu ketentuan terkait penggeledahan atas rumah/properti seseorang tanpa alasan yang jelas dan penyadapan (*wiretapping*)³⁹, perlindungan atas

³⁹ Ketentuan ini terdapat dalam *Fourth Amendment of US Constitution*, pada mulanya hanya terbatas pada perlindungan atas pencarian/penggeledahan tanpa alasan atas properti (khususnya rumah). Namun perkembangan yang terjadi selanjutnya merubah ketentuan ini salah satunya adalah kasus *Olmstead Vs. United States* di mana digunakan alat penyadap pada kabel telepon yang berada di luar rumah untuk menyadap pembicaraan Olmstead dan tiga rekannya sehingga konsep perlindungan dirubah karena yang dilindungi adalah orang bukan tempatnya. Kemudian berkembang menjadi teori Katz bahwa ada dua syarat keberlakuan *Fourth Amendment* yaitu seseorang menunjukkan harapan akan privasi (*Subjective Expectation of Privacy*) dan harapan

diri seseorang dari penggeledahan atas tubuhnya termasuk pemaksaan atas tindakan operasi/pembedahan atas dirinya⁴⁰ dan ketentuan – ketentuan yang menyatakan bahwa komunikasi seseorang haruslah rahasia dengan ketentuan hanya berlaku terkait tindakan pejabat pemerintah sedangkan bila dilakukan oleh pihak swasta maka menjadi gugatan hukum biasa⁴¹.

Dari uraian mengenai privasi dan perlindungan data pribadi di Uni Eropa dan Amerika Serikat terdapat perbedaan mendasar, di mana di Eropa, pengaturan privasi diatur secara ketat melalui European Directive yang memberikan batasan yang sangat jelas mengenai perlindungan atas data pribadi terkait dengan hak atas privasi seperti ketentuan mengenai perolehan dan penggunaan data pribadi yang harus spesifik ditujukan untuk apa. Sementara itu di Amerika, pengaturan terhadap privasi hanya sebatas terkait hal – hal yang mengarah pada tindak kriminal seperti penyadapan, penggeledahan itupun dengan mensyaratkan bahwa orang tersebut memang mengharapkan adanya perlindungan atas privasi yang dapat dilihat dengan adanya usaha agar informasi tentang dirinya tidak diketahui oleh orang lain (*Subjective Expectation of Privacy*) dan bahwa hal tersebut oleh publik dianggap wajar (*Reasonable to public*).

Dapat dikatakan bahwa Uni Eropa menganut asas *option in*, di mana ketentuan mengenai privasi dan data pribadi sudah diatur secara ketat tanpa

tersebut dianggap masuk akal oleh masyarakat/public (*Reasonable to public*). Lihat *Ibid*, hlm. 234-235. Perkembangan selanjutnya dari teori Katz ini juga mensyaratkan analisa atas asumsi resiko (*Assumption of Risk*) yang mensyaratkan adanya tindakan dari seseorang untuk memastikan komunikasi mereka rahasia, misalnya dengan penggunaan teknologi enkripsi/pengacakan atas pesan/komunikasi mereka sehingga komunikasi tersebut tidak dengan mudah dapat dibaca oleh orang lain.

⁴⁰Hal ini juga diatur dalam *Fourth Amendment*, di mana terkait dengan pemeriksaan/pembedahan terkait upaya penegakan hukum maka harus dilakukan pertimbangan antara perlunya alat bukti dan keselamatan nyawa seseorang, antara lain dalam kasus *Rochin vs California* dan *Winston vs. Lee*, lihat *Ibid*, hlm. 243-244.

⁴¹ Terkait dengan kerahasiaan atas komunikasi ini ada beberapa ketentuan yang terkait yaitu ketentuan *First Amendment* of US Constitution yang mengatur mengenai hak atas kebebasan berbicara dan kebebasan pers serta kebebasan berserikat. Selain itu juga hak atas anonimitas, hanya saja terkait anonimitas ini bila ada pernyataan yang tidak benar untuk tujuan komersial, maka tidak dilindungi, lihat *Ibid*, hlm. 247-251. Selain itu juga terdapat perlindungan atas paksaan untuk membuat kesaksian yang mengkriminalisasi seseorang yang terdapat pada *Fifth Amendment*, namun tidak termasuk pada pemberian contoh tulisan tangan, rambut, darah atau alat bukti fisik lainnya dan juga harus terdapat unsur paksaan dari pemerintah dan bahwa kesaksian tersebut tidak diberikan secara sukarela (*voluntary testimony*), lihat *Ibid*, hlm.251-253.

harus ada tindakan dari seseorang apakah dia mengharapkan perlindungan atas privasi sedangkan di Amerika menganut *option out* di mana, perlindungan atas data pribadi terkait privasi baru timbul jika memang orang tersebut mengharapkan adanya perlindungan atas privasinya.

2.2 Electronic Government (*E-Government*), Pelayanan Publik, *Electronic Identity* dan *Identity Management System*

2.2.1 *Government* (Pemerintah) dan *Governance* (Pemerintahan)

Sebelum membahas mengenai pemerintah dan pemerintahan, perlu dipahami lebih dulu mengenai konsep negara dan administrasi yang berkaitan erat dengan pemerintah dan pemerintahan.

Secara umum diketahui bahwa yang dimaksud dengan Negara adalah suatu organisasi bangsa (*an organized political community controlled by on government*), yang paling tidak mempunyai empat elemen penting, yaitu bangsa, wilayah, pemerintahan dan sistem hukum. Sedangkan administrasi adalah kata benda yang berasal dari kata kerja *to administer* yang berarti mengelola atau mengatur suatu urutan tertentu dalam suatu organisasi (*to control the affairs of a business, an organization, etc; to manage something*); di mana administrasi juga bisa berarti memberikan suatu formalisasi atau memformalkan sesuatu (*to provide of give something formally*).⁴²

Dalam perkembangannya telah terjadi proses evolusi dari konsep maupun bentuk bangsa-negara dari waktu ke waktu. Berawal dari bentuk Negara Sebagai Penjaga Malam (*night watcher state atau police state*), berkembang menjadi bentuk Negara Kesejahteraan (*welfare state*), yang kemudian berkembang lagi menjadi bentuk Negara Yang Madani atau disebut juga *civil society*⁴³ yang lebih memberikan ruang bagi pelaku usaha, masyarakat dan pasar, atau pada sisi yang lain disebut juga *nation wealth creation*. Peranan tiga unsur penting tersebut yakni pemerintah, pelaku

⁴² Edmon Makarim (b), *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* (Jakarta : Rajawali Press, 2010), hlm. 45.

⁴³ Jimly Asshiddiqie, *Konstitusi dan Konstitusialisme Indonesia* (Jakarta : Sekeretariat Jemderal dan Kepaniteraan Mahkamah Konstitusi Republik Indonesia, 2006), hlm.81.

usaha dan masyarakat menjadi penentu dalam terciptanya penyelenggaraan negara yang baik dalam kerangka negara hukum modern.

Secara umum, konsep *Civil Society* ataupun *National Wealth Creation* tidak terlalu jauh berbeda dengan karakteristik Negara Kesejahteraan. Negara *cq* Pemerintah tetap dibenarkan atau ditugaskan untuk melakukan campur tangan atau interferensi demi mensejahterakan bangsa namun tetap dengan memperhatikan keberadaan pasar. Dalam pola ini, masyarakat dan pelaku usaha (swasta) diharapkan lebih aktif, sementara pemerintah diharapkan sebagai fasilitator saja. Namun, dengan melihat fakta bahwa pemerintah tetap dituntut oleh Publik untuk tidak lepas tangan dari suatu kondisi yang meskipun disukai pelaku usaha namun ternyata merugikan kepentingan umum, maka konsep *welfare state* menjadi pilihan.

Dalam konsep *welfare state* dimana negara yang direpresentasikan oleh pemerintah (administrasi negara) sebagai pengurus, maka tugas pemerintah tidak hanya membuat dan menegakan hukum, atau hanya menjaga ketertiban dan ketentraman saja, melainkan lebih luas dari pada itu yakni menyelenggarakan kepentingan umum seperti kesehatan rakyat, pendidikan, perumahan, dan lain sebagainya. Pemerintah juga diberikan tugas dan kewenangan untuk dapat bertindak atas inisiatif dirinya sendiri dalam menyelesaikan segala permasalahan yang ada pada warga masyarakat demi melindungi kepentingan umum itu sendiri.

Untuk menyelenggarakan kepentingan umum tersebut, secara garis besar menurut Stelinga, administrasi negara mempunyai kewenangan antara lain: (i) melakukan penetapan kebijakan, (ii) melakukan pengaturan/regeling, (iii) melakukan pengamanan, (iv) melakukan peradilan, dan (v) melakukan pelayanan kepada warga negara.⁴⁴ Sedangkan menurut Brown, kegiatan kepentingan umum adalah dilakukan dengan melakukan layanan publik yang merupakan kegiatan yang menggunakan (i) kewenangan publik, dan (ii) dilakukan untuk memenuhi kepuasan kebutuhan publik. Lebih lanjut, otoritas publik yang melakukan hal tersebut harus memenuhi prinsip-prinsip

⁴⁴ Prajudi Atmosodirjo, *Hukum Administrasi Negara*, cet. 10, (Jakarta: Ghalia Indonesia, 1983), hlm. 213.

antara lain (i) jujur atau tidak memihak, (ii) integritas, (iii) obyektif, (iv) seleksi dan promosi, dan (iv) akuntabilitas.⁴⁵

Terkait *government* dan *governance* sering dijumpai kerancuan dalam pemahaman, tentang perbedaan konsep dan arti dari keduanya. Konsep “*governance*” lebih inklusif daripada konsep “*government*”. Konsep ‘*government*’ hanya menunjuk pada suatu organisasi pengelolaan pemerintahan berdasarkan kewenangan tertinggi. Sementara konsep ‘*governance*’ melibatkan tidak sekedar Pemerintah dan negara, tapi juga peran berbagai aktor di luar Pemerintah dan negara, sehingga pihak yang terlibat juga sangat luas.

Secara umum, istilah *government* lebih mudah dipahami sebagai “Pemerintah” yaitu lembaga beserta aparturnya yang mempunyai tanggungjawab untuk mengurus negara dan menjalankan kehendak rakyat. Sementara ‘*Governance*’ adalah merupakan seluruh rangkaian proses pembuatan keputusan/kebijakan dan seluruh rangkaian proses dimana keputusan itu diimplementasikan atau tidak diimplementasikan.⁴⁶

2.2.2. Pelayanan Publik

Dalam kata pelayanan publik terdapat dua kata yang harus dijelaskan terlebih dahulu yakni kata-kata ‘Pelayanan’ dan ‘Publik’. Jika kata publik adalah bermakna kepada kepentingan publik yang merupakan kepentingan lebih luas dari sekedar kepentingan individu dan kepentingan masyarakat, maka dalam kata pelayanan adalah bermakna kepada pengertian tentang adanya suatu aktivitas atau serangkaian aktivitas yang bersifat tidak kasat mata (tidak dapat diraba) yang melibatkan usaha-usaha manusia dengan menggunakan peralatan.⁴⁷

Menurut Groon Ross sebagaimana dikutip oleh Ratminto dan Atik Septi Winarsih dalam bukunya tentang Manajemen Pelayanan, Pelayanan adalah suatu aktivitas atau serangkaian aktivitas yang terjadi sebagai akibat adanya interaksi antara konsumen dengan karyawan atau hal-hal lain yang

⁴⁵ Safri Nugraha et. al., *Hukum Administrasi Negara*, edisi revisi., (Depok: Center for Law and Good Governance Studies FHUI, 2007), hlm.81-82.

⁴⁶ Edmon Makarim (b), *op.cit*, hlm.54.

⁴⁷ *Ibid*, hlm.38.

disediakan oleh perusahaan pemberi pelayanan yang dimaksudkan untuk memecahkan permasalahan konsumen.⁴⁸

Dalam Keputusan Menteri Pendayagunaan Aparatur Negara No.81 Tahun 1993 yang kemudian disempurnakan dengan Keputusan Menteri Pendayagunaan Aparatur Negara No.63 Tahun 2003 telah mendefinisikan pelayanan umum sebagai Segala bentuk pelayanan yang dilaksanakan oleh Instansi Pemerintah Pusat, di Daerah, dan di lingkungan Badan Usaha Milik Negara atau Badan Usaha Milik Daerah dalam bentuk barang dan atau jasa, baik dalam rangka upaya pemenuhan kebutuhan masyarakat maupun dalam rangka pelaksanaan ketentuan peraturan perundang-undangan.

Pelayanan Publik menurut Edmon Makarim adalah serangkaian kegiatan administrasi negara dengan menggunakan peralatan tertentu sebagai hasil interaksi administrasi negara dengan publik yang ditujukan dalam rangka memenuhi kepentingan publik dalam rangka pelaksanaan ketentuan perundang-undangan.⁴⁹

Menurut Ratminto dan Atik, berdasarkan organisasi yang menyelenggarakannya, dapat dibedakan secara umum dua jenis layanan publik, yaitu (a) Pelayanan publik yang diselenggarakan oleh Organisasi Publik, dan (b) Pelayanan Publik yang diselenggarakan oleh organisasi privat. Selanjutnya Pelayanan Publik yang diselenggarakan oleh organisasi publik tersebut dapat dibedakan menjadi dua, yakni (i) yang bersifat primer dan (ii) yang bersifat sekunder.⁵⁰

Lebih lanjut mereka mencontohkan perbedaan ketiga jenis layanan publik tersebut sebagai berikut:

1. Pelayanan publik yang diselenggarakan oleh privat adalah semua penyediaan barang atau jasa publik yang diselenggarakan oleh swasta, seperti antara lain Rumah Sakit, Perguruan Tinggi, Perusahaan Transportasi dan lain sebagainya.

⁴⁸Ratminto dan Atik Septi Winarsih., *Manajemen Pelayanan: Pengembangan Model Konseptual, Penerapan Citizen's Charter dan Standar Pelayanan Minimal*, (Yogyakarta: Pustaka Pelajar, 2005), hlm.1-4.

⁴⁹ Edmon Makarim (b), *op.cit*, hlm.55.

⁵⁰ Ratminto dan Atik Septi Winarsih., *op.cit*, hlm.8-11.

2. Pelayanan Publik oleh Pemerintah yang bersifat primer, adalah semua penyediaan barang/jasa publik dimana Pemerintah adalah satu-satunya penyelenggara dan publik tidak bisa memilih yang lain, mau tidak mau mereka harus memanfaatkannya, seperti antara lain pelayanan imigrasi, KTP, SIM, dan pelayanan perizinan lainnya.
3. Pelayanan Publik oleh Pemerintah yang bersifat sekunder, adalah semua bentuk penyediaan barang/jasa publik dimana Pemerintah bukanlah satu-satunya penyedia sehingga publik masih bisa memilih penyelenggara yang lain. Misalnya adalah program asuransi tenaga kerja, program pendidikan dan pelayanan yang diberikan oleh BUMN, dan lain sebagainya.⁵¹

2.2.3. *E-Government*

E-Government merupakan bentuk pelayanan publik yang dilakukan oleh pemerintah dengan memanfaatkan teknologi informasi seperti internet. Sebagaimana telah diuraikan sebelumnya. Konsep *e-government* mulai mengemuka karena munculnya pelayanan publik oleh pihak swasta melalui internet, yang secara tidak langsung menuntut pemerintah untuk menerapkannya juga.

World Bank (www.worldbank.org) (AOEMA report) mendefinisikan *E-Government* sebagai “*the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions*”.⁵²

⁵¹ *Ibid*

⁵² Shailendra C. Jain Palvia dan Sushil S. Sharma, “E-Government and E-Governance : Definitions/Domain Framework and Status Around The World” http://www.iceg.net/2007/books/1/1_369.pdf. Diunduh 26 Maret 2012.

Sebuah kelompok kerja (Working Group) yang membahas *E-Government* dalam perkembangan dunia mendefinisikan *E-Government* sebagai “*the use of information and communication technologies (ICTs) to promote more efficient and effective government, facilitate more accessible government services, allow greater public access to information, and make government more accountable to citizens. E-government might involve delivering services via the Internet, telephone, community centers (self-service or facilitated by others), wireless devices or other communications systems*”.⁵³

Secara umum dapat disimpulkan bahwa *E-Government* adalah penggunaan/pemanfaatan teknologi informasi khususnya internet untuk meningkatkan pelayanan pemerintah kepada publik, pelaku usaha dan lembaga pemerintahan lainnya. *E-Government* memungkinkan warga Negara untuk berinteraksi dan menerima layanan dari pemerintah dua puluh empat jam sehari, tujuh hari dalam seminggu.

2.2.4. Sistem Administrasi Kependudukan sebagai bentuk pelaksanaan *E-Government* di Indonesia

Sistem Informasi Administrasi Kependudukan, yaitu suatu sistem informasi yang disusun berdasarkan prosedur-prosedur dan memakai standarisasi khusus yang bertujuan menata sistem administrasi kependudukan sehingga tercapai tertib administrasi di bidang kependudukan. Administrasi kependudukan meliputi Pendaftaran Penduduk dan Pencatatan Sipil.

Pada dasarnya Sistem Administrasi Kependudukan ini merupakan bentuk pelayanan publik yang dilakukan oleh pemerintah kepada warganya dalam bentuk penyediaan data – data kependudukan yang dapat diakses oleh warga negara yang memerlukan terkait dengan status pribadi dan status hukum seseorang. Oleh karena itu Sistem Administrasi Kependudukan (SIK) adalah bentuk pelaksanaan *E-Government*.

⁵³ *Ibid*

Selain Sistem Administrasi Kependudukan (SIAK) sebenarnya juga ada usulan pembuatan sistem lain terkait dengan catatan tindak criminal yang dirancang oleh Kepolisian Republik Indonesia, yaitu INAFIS yang rencananya berisi identitas warga Negara yang dilengkapi dengan catatan tindak kriminal, namun perkembangan selanjutnya proyek INAFIS ini dihentikan karena dianggap sama dengan SIAK dan juga terkait asas praduga tak bersalah setiap warga Negara, karena terkesan memiliki INAFIS pasti pernah melakukan tindak pidana.

2.2.5. *Electronic Identity*

Sebelum membahas mengenai *Electronic Identity* terlebih dahulu perlu dibahas mengenai identitas (*Identity*). Kata identitas sering digunakan sebagai penunjuk diri seseorang yang membedakannya dengan orang lainnya.

*Identity describes the distinction between an individual and a person, which can only be determined from the perspective of the person. The role then denominates the interrelation between activation of situation dependent identity properties and the corresponding form of the transmitting action.*⁵⁴

Secara sosiopsikologis identitas didefinisikan sebagai *permanent inner being one with oneself, the continuity of experience of one-self (self-identity) which is, for the most part, created by assuming certain social roles and membership in groups, as well as by recognition by someone who has assumed these roles or belongs to the respective group.*⁵⁵

Secara umum identitas (*Identity*) didefinisikan sebagai pengenal yang membedakan seseorang dengan seseorang lainnya serta peranannya dalam suatu kelompok masyarakat.

⁵⁴Independent Centre for Privacy Protection (ICPP) /Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG), "Identity Management Systems (IMS): Identification and Comparison Study" https://www.datenschutzzentrum.de/dmanage/study/ICPP_SNG_IMS-Study.pdf. Diunduh 29 Maret 2012.

⁵⁵ *Ibid*

Electronic Identity (E-ID) adalah identitas yang berbentuk/menggunakan media elektronik antara lain berbentuk smart card yang memuat data – data orang yang memiliki smart card tersebut.

2.2.6. Pengamanan *Electronic Identity*

2.2.6.1. Biometrik

Biometrik adalah metode pengukuran yang digunakan untuk mengidentifikasi kejelasan individu melalui ciri – ciri intrinsiknya secara fisik atau perilaku yang dapat berupa DNA, sidik jari, iris, retina, tangan atau geometri wajah, bentuk telinga, suara, bau badan, pola pembuluh darah, tulisan tangan dan pola menulis ataupun mengetik.⁵⁶

Penggunaan perangkat biometrik biasanya melibatkan proses perolehan, penyimpanan dan pengungkapan atau penggunaan. Proses pertama ialah menangkap sampel biometrik dalam bentuk digital, khususnya dari fitur biologis pada individu. Data biometrik tersebut kemudian diekstrasi dan dijadikan template untuk menjadi referensi yang kan digunakan untuk mengecek dan menentukan identitas seseorang

Secara teknis ketepatan teknik biometrik tidak dapat dikatakan bersifat mutlak karena fitur biologis cenderung akan berubah sesuai dinamika biologisnya, seteliti apapun teknis pengukurannya masih dimungkinkan terjadinya penyimpangan. Untuk mengakomodasi dinamika tersebut dilakukan penetapan ambang batas untuk pencocokan template referensi dengan data yang akan dicocokkan (data hasil ekstrasi)

Pengamanan *E-ID* menggunakan biometrik mempunyai resiko yang cukup besar, terutama menyangkut penyimpanan *template* referensi data biometrik yang dijadikan acuan untuk pencocokan. Jika data acuan tersebut diterobos oleh pihak yang tidak berwenang maka si pemilik atau pengguna data yang sah tidak punya cara lain selain mencabut data identifikasi tersebut. Oleh karena itu demi keamanan dan perlindungan hukum atas data acuan biometrik tersebut diperlukan aturan hukum untuk mencegah penyalahgunaan database biometrik tersebut.

⁵⁶ United Nations Commission on International Trade Law (UNCITRAL), *op.cit*, hlm.27 lihat juga Kai Ronnenberg, Dennis Royer, André Deuker, *op.cit*, hlm.138.

Selain adanya kemungkinan terjadinya penerobosan akses data biometrik oleh pihak yang tidak berwenang, juga perlu diakomodasi adanya akses pihak – pihak lain selain pemerintah khususnya pihak swasta yang melakukan kerjasama dengan pemerintah dalam menyelenggarakan suatu urusan kepada publik dan juga pihak lain yang memerlukan data – data kependudukan terkait dengan usaha/kegiatan yang dilakukannya misalnya perbankan yang memerlukan data kependudukan sebagai database nasabah. Oleh karena itu perlu dipastikan bahwa penggunaan data kependudukan (*E-ID*) oleh pihak – pihak tersebut dilakukan sesuai dengan kebutuhan dan rahasia.

2.2.6.2. Digital Signature (Tanda Tangan Digital)

Tanda tangan digital berbeda dengan tanda tangan elektronik. Tanda tangan elektronik mempunyai lingkup pengertian yang lebih luas yang mencakup semua metode autentifikasi secara elektronik di mana salah satunya adalah tanda tangan digital. Tanda tangan digital menggunakan teknologi asimetris kriptografi.⁵⁷

Kunci – kunci ini dikeluarkan sebagai digital certificates oleh *Certification Authority* (CA) yang bertindak sebagai seorang pihak ketiga yang dipercaya yang menjamin sertifikat – sertifikat digital yang mereka keluarkan. CA menjamin bahwa kedua pihak yang saling mempertukarkan informasi adalah benar – benar pihak yang mengklaim dirinya sebagai benar – benar pihak yang berkomunikasi.

CA tersebut “menandatangani” sertifikat tersebut yang secara yuridis mengikat sebagai bukti kepemilikan atas *public key* dari pemilik yang sesungguhnya. Hanya mereka yang dapat menunjukan sertifikat tersebut yang merupakan pemilik yang sesungguhnya dari *public key* tersebut, dan pemilik *public key* itu pula yang menjadi pemilik dan penyimpan *private key* yang disebutkan dalam sertifikat itu. Sertifikat tersebut

⁵⁷ Asimetris Kriptografi (*Asymmetric Cryptography*) adalah system pengacakan suatu pesan dengan menggunakan satu pasangan kunci yaitu kunci privat (*privat key*) dan kunci publik (*public key*). Disebut asimetrik karena kunci yang digunakan untuk mengenkripsi (*privat key*) dan mendeskripsi pesan (*public key*) berbeda, lihat Edmon Makarim (c), *Notaris dan Transaksi Elektronik (Kajian Hukum tentang Cyber notary atau Electronic Notary)* (Jakarta : Rajawali Pers, 2011), hlm.49.

memastikan bahwa hanya *public key* yang berasal dari sertifikat itu saja yang merupakan *public key* yang benar.⁵⁸

Meskipun kunci dari pasangan terkait secara matematis, namun jika penerapan *cryptosystem asimetris* telah dirancang dan diimplementasikan secara aman maka hampir tidak mungkin memperoleh kunci publik ataupun privat tanpa pengetahuan satu sama lainnya. Algoritma paling umum untuk enkripsi dengan menggunakan kunci publik dan privat didasarkan pada logika bilangan prima. Secara matematis akan sangat sulit, atau paling tidak akan memerlukan waktu yang sangat lama jika seseorang yang menerima *public key* akan dapat mencari sendiri pasangan kunci privat dari kunci tersebut. Jadi walaupun banyak orang mungkin memperoleh suatu kunci publik tidak berarti mereka dapat menemukan sendiri kunci privatnya dengan cara melakukan penerobosan terhadap algoritma pengamanannya.⁵⁹

Untuk menandatangani dokumen atau suatu informasi elektronik, penandatanganan harus melimitasi dulu batasan – batasan dari informasi yang akan ditandatangani. Kemudian dengan penggunaan software untuk melakukan fungsi *hash*⁶⁰ dilakukanlah pemadatan pesan (*digest*). Inti pesan tersebut kemudian dienkripsi dengan menggunakan kunci privat si penandatanganan sehingga menghasilkan suatu tandatangan digital. Kemudian tandatangan digital yang dihasilkan tersebut dikirimkan bersamaan dengan pesan atau dokumen yang dikirimkan baik dengan

⁵⁸ F. Lawrence Street dan Mark P. Grant, *Law of the Internet*, 2000 Edition, (Mathew Bedner & Company INC, 1999), hal 19.

⁵⁹ Edmon Makarim (c), *op.cit*, hlm.52.

⁶⁰ Fungsi *hash* adalah sebuah proses matematis untuk meringkaskan atau mengintisarikan suatu pesan secara elektronik (*message digest* atau *finger print*) agar ia menjadi terkompresi ke dalam bentuk suatu pesan yang lebih kecil sehingga dapat dikomunikasikan dengan lebih efisien dalam suatu komunikasi elektronik. Analoginya adalah sama dengan kepentingan seseorang yang melipat kertas suratnya untuk kemudian dimasukan ke dalam amplop untuk lebih mempermudah dan merahasiakan pesan yang dikirimkannya.

Fungsi *hash* juga menggunakan algoritma pengacakan pesan namun dengan tujuan yang berbeda dengan kunci publik dan privat. Enkripsi yang digunakan adalah simetris untuk membuat representasi digital atau bentuk pesan yang lebih terkompresi ke dalam bentuk suatu nilai – nilai pengacak ("*hash value*") atau hasil acak ("*hash result*") yang lebih pendek dari pesan aslinya namun tetap merepresentasikan substansial yang unik dari pesan itu sendiri. Setiap perubahan pesan selalu menghasilkan hasil *hash* yang berbeda meskipun fungsi *hash* yang sama digunakan., lihat *ibid* lihat juga Sutan Remy Syahdeini, *Kejahatan & Tindak Pidana Komputer* (Jakarta : Grafiti, 2009), hlm.209 -210.

dilekatkan pada dokumen itu sendiri (*fixed*) ataupun dikirimkan sebagai sebagai informasi (elemen data) terpisah yang tetap merupakan suatu pertautan tidak terpisahkan, terhubung atau terasosiasikan secara logis dengan pesan yang dikirimkan itu sendiri.

Tandatangan digital tersebut bersifat unik sehingga hanya dapat terbuka dengan pasangan kuncinya satu sama lain (privat dan publik) sehingga keberadaannya menjadi ukuran atau metode pengamanan pengiriman informasi itu sendiri, dari pihak pengirim kepada penerima. Jika suatu pesan disampaikan dengan kunci publik penerima, maka hanya si penerima saja tentunya yang dapat membukanya. Jika pesan yang telah dikunci dengan kunci privat si pengirim, maka hal tersebut berarti mengotentikasikan bahwa si pengirim adalah pihak yang bertanggungjawab terhadap pesan yang dikirim tersebut. Dengan kata lain, pengirim tidak dapat menampik atau menyangkal (*repudiation*) terhadap pesan yang dikirimkannya tersebut, kecuali jika si pengirim dapat membuktikan bahwa sistem penandatanganan tersebut ternyata tidak berjalan sebagaimana mestinya.

Suatu pesan yang terenkripsi yang dikirimkan kepada penerima/pihak yang dituju, maka pihak penerima harus melakukan verifikasi terhadap pesan dan tanda tangan digital tersebut. Proses verifikasi adalah proses pemeriksaan tandatangan digital dengan mengacu pada pesan asli yang dikirimkan.

Dengan menggunakan kunci public dilakukan suatu proses pembalikan atau dekripsi (*decrypt*) terhadap tanda tangan digital yang diterima oleh penerima hasilnya diperoleh suatu inti pesan yang kemudian dengan fungsi *hash* yang sama inti pesan tersebut diolah kembali ke dalam bentuk originalnya. Kemudian kedua pesan tersebut diperbandingkan satu sama lain. Jika informasi tersebut tidak berubah maka dapat dikatakan bahwa informasi tersebut aman dalam pengirimannya dan mengikat para pihak. Sementara itu jika pesan tersebut telah berubah dari bentuk aslinya maka pesan tersebut dianggap

telah mengalami perubahan dalam pengirimannya sehingga dapat dikatakan tidak aman dan tidak mengikat.

2.2.7. Identity Management System

Identity Management menurut Bauer, Meints dan Hansen serta Buitelaar, Meints dan van Alselooy terkait dengan beberapa hal yaitu :

1. Menghubungkan suatu pengenalan kepada seseorang tertentu
2. Identifikasi, otorisasi, autentifikasi dan kontrol akses atas aplikasi, teknologi informasi dan lingkungan
3. Manajemen siklus identitas seseorang (pendaftaran, pemberian hak, penggunaan, perubahan hak dan penghapusan dari register)
4. Menghubungkan suatu atribut/karakteristik dari satu grup (*group profiling*) atau perorangan (*individual profiling*) dari satu atau beberapa sumber, dan penggunaan profil, misalnya dengan mengkategorisasi atau mengklasifikasi setiap orang.
5. Aplikasi *pseudonymisation* dan teknik anonimisasi.
6. Penggunaan identitas untuk komunikasi.⁶¹

Secara ringkas manajemen identitas adalah semua kegiatan terkait dengan pengelolaan atas identitas seseorang yang dikumpulkan (register) untuk digunakan dalam berbagai kegiatan yang memerlukan identitas tersebut.

Sementara *Identity Management System* secara ringkas adalah sistem yang digunakan untuk melakukan manajemen/pengelolaan identitas.

2.2.8. Interoperabilitas dalam *Identity Management System*

Libon mendefinisikan interoperabilitas sebagai cara untuk bertukar informasi dan layanan antara sistem dan pemangku kepentingan yang berbeda tanpa adanya usaha tambahan dari para pihak.⁶² Kerangka interoperabilitas (*interoperability framework*) terdiri atas ketentuan, standar dan aturan yang menggambarkan bagaimana para pihak berinteraksi satu dengan yang lain.

⁶¹ Kai Ronnenberg, Dennis Royer, dan André Deuker, *op.cit*, hlm.131.

⁶² James Backhouse dan Michael Vanfleteren, *Future of Identity in the Information Society, Set of requirements for interoperability of Identity Management Systems* (FIDIS consortium - EC Contract No. 507512,2005), hlm.32.

Menurut Libon interoperabilitas memerlukan tiga hal yaitu :

1. Ketentuan dan tanggungjawab dari pihak – pihak yang terlibat.
2. Kesepakatan anatara para pihak atas ketentuan tersebut
3. Standarisasi proses dan pertukaran informasi⁶³

Lebih lanjut Libon menyatakan bahwa dalam proses interoperabilitas terdapat dua tahapan yang pertama adalah integrasi data sedangkan yang kedua adalah perancangan sinergi antara departemen dan lembaga terkait. Menurutnya pemerintah harus mempunyai suatu platform yang memungkinkan setiap departemen dan lembaga bertukar data. Untuk membuat platform ini diperlukan penstrukturan data dan pendefinisian istilah – istilah secara tepat dan disepakati bersama.⁶⁴ Adapun hal – hal yang menghambat terlaksananya interoperabilitas tersebut adalah masalah komunikasi yang tidak lancar antara para pihak dan perbedaan interpretasi/pemahaman para pihak atas informasi/data/istilah yang ada.

Jadi interoperabilitas dalam Identity Management System (IMS) adalah adanya konsolidasi dan sinergi di antara pihak – pihak yang terkait dalam IMS sehingga memungkinkan para pihak terkait saling bertukar data/informasi tanpa diperlukan adanya suatu prosedur atau sistem tambahan.

2.3 Notaris Sebagai Pejabat Umum yang Berwenang Membuat Akta Otentik

2.3.1 Notaris

Pemahaman mengenai siapakah notaris itu dapat dipahami dengan mencermati definisi notaris sebagaimana disebutkan dalam Peraturan Jabatan Notaris (PJN) dan UUJN. Pasal 1 PJN menyebutkan:

Notaris adalah pejabat umum yang satu-satunya berwenang untuk membuat akta otentik mengenai semua perbuatan, perjanjian dan penetapan yang diharuskan oleh suatu peraturan umum atau oleh yang berkepentingan dikehendaki untuk dinyatakan dalam suatu akta otentik, menjamin kepastian tanggalnya, menyimpan aktanya dan memberikan grosse, salinan dan kutipannya, semua sepanjang pembuatan akta itu oleh

⁶³ *Ibid*

⁶⁴ *Ibid*, hlm.33

suatu peraturan umum tidak juga ditugaskan atau dikecualikan kepada pejabat atau orang lain⁶⁵.

Sedangkan Pasal 1 angka 1 UUJN menyebutkan bahwa “Notaris adalah pejabat umum yang berwenang membuat akta otentik dan kewenangan lainnya sebagaimana dimaksud dalam Undang-Undang ini”.⁶⁶ Dengan demikian, dari kedua definisi peraturan tersebut dapat diketahui bahwa terdapat kesamaan dalam mendefinisikan kata notaris yaitu pejabat umum yang berwenang untuk membuat akta otentik.

2.3.2. Notaris Sebagai Pejabat Umum Dalam Kaitan Dengan Pasal 1868 KUHPerdata

Bila definisi notaris dikaitkan dengan ketentuan Pasal 1868 KUHPerdata yang menyebutkan bahwa suatu akta otentik ialah suatu akta yang, di dalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau di hadapan pegawai-pegawai umum yang berkuasa untuk itu di tempat di mana akta dibuatnya, maka dapat menimbulkan suatu pertanyaan apakah pegawai umum yang dimaksud dalam Pasal 1868 KUHPerdata ini adalah sama dengan pejabat umum yang dimaksud dalam Pasal 1 PJN dan Pasal 1 angka 1 UUJN. Mengenai hal ini, Dr, Habib Adjie, SH., M.Hum, menyebutkan bahwa istilah pejabat umum merupakan terjemahan dari kata *Openbare Ambtenaren* yang terdapat dalam Pasal 1 PJN dan Pasal 1868 KUHPerdata.⁶⁷ Jadi, apa yang dimaksud sebagai Pejabat Umum dalam Pasal 1 PJN dan Pasal 1 ayat (1) UUJN adalah sama dengan yang dimaksud sebagai Pegawai Umum dalam Pasal 1868 KUHPerdata, yang diartikan sebagai pejabat yang diberi kewenangan oleh undang-undang untuk melaksanakan sebagian fungsi publik dari negara dengan tugas pokok membuat akta otentik khusus dalam lingkup perdata, dan kualifikasi seperti itu diberikan kepada notaris. Dengan demikian, pegawai umum yang dimaksud dalam Pasal 1868 KUHPerdata adalah notaris sebagai pejabat

⁶⁵ G.H.R Lumban Tobing, *Peraturan jabatan Notaris*, cet 4 (Jakarta : Erlangga, 1996), hlm. 31.

⁶⁶ Indonesia (b), *loc.cit*, pasal 1 angka 1.

⁶⁷ Habib Adjie (a), *Hukum Notaris Indonesia Tafsir Tematik Terhadap UU No.30 Tahun 2004 Tentang Jabatan Notaris*, cet 1 (Bandung: Refika Aditama, 2008), hlm.12-13.

umum, sebagaimana yang diatur dalam Pasal 1 PJN dan Pasal 1 angka 1 UUJN.

2.3.3. Akta dan Akta Otentik

Tulisan adalah pengemban tanda baca yang mengandung arti serta bermanfaat untuk menggambarkan suatu pikiran⁶⁸ sedangkan tanda adalah suatu tulisan yang, tanpa memperhatikan isinya, secara lahiriah merupakan kesatuan lengkap.⁶⁹ Akta adalah suatu tulisan yang ditandatangani dan dibuat untuk dipergunakan sebagai bukti.⁷⁰

Surat-surat akta dapat dibedakan lagi antara akta otentik dan akta di bawah tangan. Philipus M. Hadjon berpendapat bahwa syarat akta otentik yaitu:⁷¹

1. Di dalam bentuk yang ditentukan oleh Undang-Undang (bentuknya baku);
2. Dibuat oleh dan di hadapan Pejabat Umum.

Pendapat lain dikemukakan oleh Irawan Surodjo, bahwa ada 3 (tiga) unsur esensial agar terpenuhinya syarat formal suatu akta otentik, yaitu:⁷²

1. Di dalam bentuk yang ditentukan Undang-Undang;
2. Dibuat oleh dan dihadapan Pejabat Umum;
3. Akta yang dibuat oleh atau dihadapan Pejabat Umum yang berwenang untuk itu dan ditempat di mana akta itu dibuat.

Pendapat – pendapat tersebut sesuai dengan ketentuan pasal 1868 KUH Perdata, yang menentukan bahwa :

Suatu akta otentik adalah suatu akta yang didalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau dihadapan pegawai-pegawai umum yang berkuasa untuk itu ditempat dimana akta dibuatnya.⁷³

⁶⁸ Tan Thong Kie, *Studi Notariat & Serba – Serbi Praktek Notaris*, Cet 1 (Jakarta : Ichtiar Baru Van Hoeve, 2007), hal 441

⁶⁹ *ibid.*

⁷⁰ *ibid*

⁷¹ Habib Adjie (b), *Sanksi Perdata dan Administratif Terhadap Notaris Sebagai Pejabat Publik*, cet. 2. (Bandung: Refika Aditama, 2009), hal. 56.

⁷² *Ibid*

⁷³ Kitab Undang Undang Hukum Perdata (*Burgerlijk Wetboek*) diterjemahkan oleh R. Subekti dan R. Tjitrosudibio, cet.32, (Jakarta : Pradnya Paramita, 2004), ps.1868.

2.3.4. Syarat Otentisitas Akta Notaris

Akta notaris merupakan alat bukti tertulis yang diharapkan oleh para pihak yang meminta untuk dibuatkan agar dapat dipakai sebagai alat bukti yang sempurna atas setiap perbuatan yang dituangkannya dalam akta tersebut. Agar suatu akta notaris dapat dijadikan sebagai alat bukti yang sempurna maka akta notaris harus dibuat dalam bentuk tertentu yang dapat menjadikannya sebagai akta otentik

Sesuai ketentuan pasal 1868 KUHPPerdata sebagaimana telah diuraikan di atas, maka agar akta Notaris menjadi akta yang otentik maka, akta notaris harus dibuat dalam bentuk yang ditentukan oleh Undang Undang, dibuat oleh dan di hadapan pejabat umum dan pejabat umum oleh atau di hadapan siapa akta itu dibuat, harus mempunyai wewenang untuk membuat akta itu⁷⁴.

Pasal 1 angka 7 UUJN dengan jelas menegaskan bahwa akta notaris adalah akta otentik yang dibuat oleh atau di hadapan notaris menurut bentuk dan tata cara yang ditetapkan dalam UUJN. Dan sebagai akta otentik maka akta yang dibuat oleh atau di hadapan notaris ini memberikan di antara para pihak beserta ahli warisnya atau orang-orang yang mendapat hak daripada mereka, suatu bukti yang sempurna tentang apa yang dimuat di dalamnya.⁷⁵

Agar suatu akta notaris dapat dikatakan sebagai akta otentik, maka terhadap pembuatan akta notaris haruslah dibuat oleh atau di hadapan notaris sesuai dengan bentuk yang yang dikehendaki oleh undang-undang agar terpenuhi syarat-syarat keotentisitasannya sebagaimana yang ditetapkan oleh Pasal 1868 KUHPPerdata. Implementasi terhadap ketentuan persyaratan akta otentik yang dikehendaki oleh Pasal 1868 KUHPPerdata dalam UUJN dapat diuraikan sebagai berikut:

1. Akta harus dibuat dalam bentuk yang ditentukan oleh undang-undang. Bentuk akta notaris sebagai akta otentik telah diatur secara tegas dalam ketentuan Pasal 38 UUJN yang mengatur bahwa suatu akta notaris harus dibuat dalam format yang terdiri atas:

⁷⁴ G.H.S Lumban Tobing, *op.cit*, hal 48.

⁷⁵Kitab Undang Undang Hukum Perdata (*Burgerlijk Wetboek*) diterjemahkan oleh R. Subekti dan R. Tjitrosudibio, cet.32, (Jakarta : Pradnya Paramita, 2004), ps.1870.

- a. Awal akta atau kepala akta, memuat:
 1. judul akta, apakah itu akta jual beli, akta sewa menyewa, akta perjanjian pranikah, dan lain sebagainya;
 2. nomor akta, yang urutannya dibuat berdasarkan buku repertorium;
 3. jam, hari, tanggal, bulan dan tahun; dan
 4. nama lengkap dan tempat kedudukan notaris. Dalam hal terdapat notaris pengganti, notaris pengganti khusus dan pejabat sementara notaris, maka dalam akta juga disebutkan nomor dan tanggal penetapan pengangkatan, serta pejabat yang mengangkatnya
- b. Badan akta, memuat:
 1. Komparisi yang terdiri dari:
 - 1.1. nama lengkap, tempat dan tanggal lahir, kewarganegaraan, pekerjaan, jabatan, kedudukan, tempat tinggal para penghadap dan/atau orang yang mereka wakili (identitas para pihak);
 - 1.2. keterangan mengenai kedudukan bertindak penghadap, disebutkan apakah dalam hal ini bertindak untuk diri sendiri, atau kuasa, atau mewakili perusahaan selaku direksi dan lain sebagainya.
 2. Isi akta yang merupakan kehendak dan keinginan dari pihak yang berkepentingan, memuat:
 - 2.1. premise atau penjelasan, yang menerangkan tentang penjelasan atau alasan yang menjadi dasar tujuan dibuatnya akta tersebut;
 - 2.2. esensial dari perjanjian yang dituangkan dalam akta, berupa klausul-klausul para pihak.
 3. Nama lengkap, tempat dan tanggal lahir, serta pekerjaan, jabatan, kedudukan dan tempat tinggal dari tiap-tiap saksi pengenal (*attesterend*), bila ada.

Pengertian kenal dalam akta ini tidaklah sama dengan kenal secara pribadi, melainkan kenal secara hukum/yuridis, yaitu kenal berdasarkan identitas yang sah, yang memuat secara benar nama, alamat, tempat dan tanggal lahir yang dikenal oleh umum/masyarakat sebagai benar bahwa itu adalah orang yang bersangkutan sehingga ia dapat dibedakan dan diindividualisasi dari orang – orang lain di dalam masyarakat.⁷⁶ Jaminan bahwa notaris mengenal orang yang bersangkutan adalah adanya pernyataan dalam akta ‘bahwa para penghadap saya, notaris kenal.’ Pernyataan notaris ini dijamin kebenarannya, sebab notaris adalah pejabat umum yang menyandang jabatan sebagai pejabat publik sehingga notaris dapat dipercaya.

Terkait hal mengenal penghadap, J.C.H Melis seperti dikutip oleh Tan Thong Kie menyatakan bahwa dengan menyatakan mengenal penghadap, Notaris harus menanggung bahwa nama penghadap yang tertulis dalam akta benar – benar melekat pada orang itu dan tidak pada orang lain. Tuntutan undang – undang tidak lebih daripada orang yang tersebut dalam akta sebagai Tuan A juga disebut Tuan A oleh masyarakat. Misalnya seseorang yang bertahun – tahun hidup di masyarakat dengan nama palsu misalnya X dan semua orang mengenalnya dengan nama X serta tidak ada yang tahu bahwa nama tersebut sebenarnya palsu, jika dalam akta disebut sebagai Tuan X maka penyebutan tersebut benar, oleh karena notaris dan masyarakat mengenalnya dengan nama itu.⁷⁷

Selain identitas si penghadap di dalam masyarakat, mengenal di sini juga berarti yang bersangkutan (penghadap) mempunyai wewenang untuk melakukan suatu tindakan hukum yang akan disebutkan dalam akta.⁷⁸

c. Akhir atau penutup akta, memuat:

⁷⁶ Tan Thong Kie, *op.cit*, hlm.499.

⁷⁷ *Ibid*, hlm.499-500.

⁷⁸ Habib Adjie (a), *op.cit*, hlm.148.

1. uraian tentang akta itu sendiri, apakah dibuat sebagai minuta atau sebagai akta in originali;
2. uraian tentang pembacaan akta sebagaimana dimaksud dalam pasal 16 ayat (1) huruf 1 yakni pembacaan akta di hadapan penghadap dengan dihadiri oleh paling sedikit 2 (dua) orang saksi dan ditandatangani pada saat itu juga oleh penghadap, saksi dan notaris, atau pasal 16 ayat (7) yakni bahwa pembacaan akta tidak wajib dilakukan, jika penghadap menghendaki agar akta tidak dibacakan karena penghadap telah membaca sendiri, mengetahui dan memahami isinya, dengan ketentuan bahwa hal tersebut dinyatakan dalam penutup akta serta pada setiap halaman minuta akta diparaf oleh penghadap, saksi dan notaris. Dalam hal demikian, maka notaris harus mengirimkan terlebih dahulu draft akta ke para pihak, kemudian para pihak akan membubuhkan paraf di setiap halaman. Setelah draft tersebut disepakati oleh para pihak notaris akan mengetik ulang draft tersebut untuk dibuat minutanya. Dan setelah minuta jadi notaris tidak perlu membacakannya dengan syarat di akhir akta ditulis bahwa notaris tidak membacakan akta di hadapan para penghadap oleh karena para penghadap telah membaca sendiri, mengetahui dan memahami isinya. Kemudian draft minuta tersebut dijahit pada minuta sebagai bukti;
3. uraian tentang penandatanganan dan tempat penandatanganan atau penerjemah akta bila ada;
4. nama lengkap, tempat dan tanggal lahir, pekerjaan, jabatan, kedudukan dan tempat tinggal dari tiap-tiap saksi. Saksi yang dimaksud dalam hal ini bukanlah saksi *at testerend* (saksi pengenalan) melainkan saksi *instrumetaire*, yaitu saksi yang hadir di hadapan notaris untuk menyaksikan pembacaan akta oleh notaris di hadapan para penghadap dan penandatangan akta oleh para penghadap. Dalam hal terdapat saksi *instrumentaire*

yang dikenal oleh notaris dan terdapat juga saksi *instrumentaire* yang tidak dikenal oleh notaris, maka dalam bagian akhir akta penyebutannya dilakukan dengan urutan pertama saksi tidak dikenal, kemudian baru dilanjutkan dengan saksi yang dikenal.

5. uraian tentang tidak adanya perubahan yang terjadi dalam pembuatan akta atau uraian tentang adanya perubahan yang dapat berupa penambahan, pencoretan atau penggantian.

Uraian mengenai format akta notaris dari awal akta hingga akhir akta tersebut di atas secara singkat dapat disebut sebagai suatu rangkaian tindakan *verlijden*, yaitu suatu rangkaian tindakan menyusun akta sesuai dengan bentuk yang ditentukan oleh undang-undang, kemudian membacakannya di hadapan para pihak dan saksi-saksi, dan seketika dilakukan penandatanganan oleh para pihak, saksi-saksi dan notaris.

2. Akta harus dibuat oleh atau dihadapan pejabat umum

Syarat kedua agar suatu akta notaris dapat disebut sebagai akta otentik adalah bahwa akta tersebut harus dibuat oleh atau di hadapan seorang pejabat umum. Seperti telah diuraikan dalam sub bab sebelumnya, disebutkan bahwa notaris adalah pejabat umum, sehingga dengan demikian notaris berwenang untuk membuat akta otentik. Hal ini dipertegas dengan ketentuan yang termaktub dalam Pasal 1 angka 1 juncto Pasal 1 angka 7 UUJN yang menyebutkan bahwa notaris adalah pejabat umum yang berwenang untuk membuat akta otentik, akta mana dibuat oleh atau di hadapan notaris menurut bentuk dan tata cara yang ditetapkan dalam UUJN.

Akta notaris sebagai akta otentik dibuat oleh atau di hadapan notaris atas permintaan para pihak yang berkepentingan agar perbuatan hukum mereka itu dituangkan dalam bentuk akta otentik. Berdasarkan kewenangannya notaris boleh membuat akta otentik dalam lingkup hukum perdata mengenai semua jenis perbuatan, perjanjian, dan ketetapan yang diharuskan oleh peraturan perundang-undangan dan/atau yang dikehendaki oleh pihak-pihak yang berkepentingan untuk dinyatakan dalam akta otentik, sepanjang pembuatan akta-akta

itu tidak ditugaskan kepada pejabat lain. Dan terhadap akta-akta itu notaris wajib untuk membuatnya dalam bentuk minuta akta dan menyimpannya sebagai bagian dari protokol notaris serta memberikan salinannya kepada para pihak yang berkepentingan.

3. Pejabat umum oleh atau di hadapan siapa akta itu dibuat, harus mempunyai wewenang untuk membuat akta itu.

Kewenangan notaris selaku pejabat umum dalam membuat akta meliputi 4 (empat) hal, yaitu:⁷⁹

- a. Notaris harus berwenang sepanjang yang menyangkut akta yang harus dibuatnya;

Wewenang Notaris dalam pembuatan akta otentik sepanjang tidak dikecualikan kepada pihak atau pejabat lain, atau Notaris juga berwenang membuatnya disamping dapat dibuat oleh pihak atau pejabat lain, mengandung makna bahwa wewenang Notaris dalam membuat akta otentik mempunyai wewenang yang umum, sedangkan pihak lainnya mempunyai wewenang terbatas.

Pasal 15 UUJN telah menentukan wewenang Notaris. Wewenang ini merupakan suatu batasan, bahwa Notaris tidak boleh melakukan suatu tindakan diluar wewenang tersebut. Sebagai contoh, apakah Notaris dapat memberikan *Legal Opini* secara tertulis atas permintaan para pihak? Jika dilihat dari wewenang tersebut dalam pasal 15 UUJN, pembuatan *Legal Opinion* ini tidak termasuk wewenang Notaris. Pemberian *Legal Opinion* merupakan pendapat pribadi Notaris yang mempunyai kapasitas keilmuan dibidang hukum dan kenotarisan, bukan dalam kedudukannya menjalankan tugas jabatan sebagai Notaris. Sehingga jika dari *Legal Opinion* tersebut menimbulkan permasalahan hukum, harus dilihat dan diselesaikan tidak berdasarkan kepada tatacara yang dilakukan oleh Majelis Pengawas atau Majelis Pemeriksa yang dibentuk oleh Majelis Pengawas, tapi diserahkan kepada prosedur biasa, yaitu jika menimbulkan kerugian dapat digugat secara perdata. Hal ini

⁷⁹ G.H.S Lumban Tobing, *op.cit*, hal 49, lihat juga Habib Adjie (a), *op.cit*, hal 130-134.

harus dibedakan dengan kewajiban Notaris memberikan penyuluhan hukum yang berkaitan dengan akta yang akan dibuat oleh atau dihadapan Notaris yang bersangkutan.

- b. Notaris harus berwenang sepanjang mengenai orang -orang untuk kepentingan siapa akta itu dibuat.

Meskipun Notaris dapat membuat akta untuk setiap orang, tapi agar menjaga netralitas Notaris dalam pembuatan akta, ada batasan menurut Pasal 52 UUJN bahwa notaris tidak diperkenankan untuk membuat akta untuk diri sendiri, isteri/suami atau orang lain yang mempunyai hubungan kekeluargaan dengan Notaris, baik karena perkawinan maupun hubungan darah dalam garis keturunan lurus ke bawah dan/atau ke atas tanpa pembatasan derajat, serta dalam garis kesamping sampai dengan derajat ketiga, serta menjadi pihak untuk diri sendiri, maupun dalam suatu kedudukan ataupun dengan perantaraan kuasa.

Mengenai orang dan untuk siapa akta dibuat, harus ada keterkaitan yang jelas, misalnya jika akan dibuat akta pengikatan jual beli yang diikuti dengan akta kuasa untuk menjual, bahwa pihak yang akan menjual mempunyai wewenang untuk menjual kepada siapapun. Untuk mengetahui ada keterkaitan semacam itu, sudah tentu Notaris akan melihat (asli surat) dan meminta fotokopi atas identitas dan bukti kepemilikannya. Salah satu tanda bukti yang sering diminta oleh Notaris dalam pembuatan akta Notaris, yaitu Kartu Tanda Penduduk (KTP) dan sertipikat tanah sebagai bukti kepemilikannya. Ada kemungkinan antara orang yang namanya tersebut dalam KTP dan sertipikat bukan orang yang sama, artinya pemilik sertipikat bukan pemilik orang yang sesuai dengan KTP. Hal ini bisa terjadi (di Indonesia), karena banyak kesamaan nama dan mudahnya membuat KTP, serta dalam sertipikat hanya tertulis nama pemegang hak, tanpa ada penyebutan identitas lain. Dalam kejadian seperti ini bagi notaris tidak menimbulkan permasalahan apapun , tapi dari segi yang lain Notaris oleh pihak yang berwajib

(kepolisian/penyidik) dianggap memberikan kemudahan untuk terjadinya suatu tindak pidana. Berkaitan dengan identitas diri penghadap dan bukti kepemilikannya yang dibawa dan aslinya diperlihatkan ternyata palsu, maka hal ini bukan tanggungjawab Notaris, tanggung jawabnya diserahkan kepada para pihak yang menghadap.

- c. Notaris harus berwenang sepanjang mengenai tempat, dimana akta itu dibuat.

Notaris harus berwenang sepanjang mengenai tempat, dimana akta tersebut dibuat. Pasal 18 ayat (1) UUJN menentukan bahwa Notaris harus berkedudukan di daerah kabupaten atau kota. Setiap Notaris sesuai dengan keinginannya mempunyai tempat kedudukan dan berkantor di daerah kabupaten atau kota (Pasal 19 ayat (1) UUJN). Notaris mempunyai wilayah jabatan meliputi seluruh wilayah propinsi dari tempat kedudukannya (Pasal 18 ayat (2) UUJN). Pengertian pasal-pasal tersebut bahwa Notaris dalam melaksanakan tugas jabatannya tidak hanya berada di tempat kedudukannya, karena Notaris mempunyai wilayah jabatan di seluruh propinsi, misalnya notaris yang berkedudukan di Kota Bogor, maka dapat membuat akta di Kabupaten atau kota lain dalam wilayah Propinsi Jawa Barat. Hal ini dapat dijalankan dengan ketentuan:

1. Notaris ketika menjalankan tugas jabatannya (membuat akta) di luar tempat kedudukannya, maka Notaris tersebut harus berada di tempat akta akan dibuat. Contoh Notaris yang berkedudukan di Kota Bogor akan membuat akta di Bandung, maka Notaris yang bersangkutan harus membuat dan menyelesaikan akta tersebut di Bandung.
2. Pada akhir akta harus disebutkan tempat (kota atau kabupaten) pembuatan dan penyelesaian akta.
3. Menjalankan tugas jabatan di luar tempat kedudukan Notaris dalam wilayah jabatan satu propinsi tidak merupakan satu keteraturan atau tidak terus menerus (Pasal 19 ayat (2) UUJN)

4. Ketentuan tersebut dalam praktek memberikan peluang kepada Notaris untuk merambah dan melintasi batas tempat kedudukan dalam pembuatan akta. Meskipun bukan suatu hak yang dilarang untuk dilakukan, karena yang dilarang menjalankan tugas jabatannya di luar wilayah jabatannya atau di luar propinsi (Pasal 17 huruf a UUJN), tapi untuk saling menghormati sesama Notaris di kabupaten atau kota lain lebih baik hal seperti itu tidak dilakukan.
- d. Notaris harus berwenang sepanjang mengenai waktu pembuatan akta itu.

Notaris dalam menjalankan tugas jabatannya harus dalam keadaan aktif, artinya tidak dalam keadaan cuti, sakit atau berhalangan sementara untuk menjalankan tugas jabatannya. Agar tidak terjadi kekosongan, maka Notaris yang bersangkutan dapat menunjuk Notaris Pengganti (Pasal 1 angka 3 UUJN). Seorang Notaris dapat mengangkat seorang Notaris Pengganti, dengan ketentuan tidak kehilangan kewenangannya dalam melaksanakan tugas jabatannya, dengan demikian dapat mengangkat Notaris Pengganti, yaitu Notaris yang cuti, sakit atau berhalangan sementara, yang setelah cuti habis protokolnya dapat diserahkan kembali kepada Notaris yang digantikannya. Sedangkan tugas jabatan Notaris dapat dilakukan oleh Pejabat Sementara Notaris⁸⁰, hanya dapat dilakukan untuk Notaris yang kehilangan kewenangannya dengan alasan:

1. Meninggal dunia;
2. Telah berakhir masa jabatannya;
3. Minta sendiri;
4. Tidak mampu secara rohani dan/atau jasmani untuk melaksanakan tugas jabatan sebagai Notaris secara terus menerus lebih dari 3 (tiga) tahun;

⁸⁰ Dalam pasal 62 UUJN dalam pengangkatan Pejabat Sementara Notaris di samping alasan – alasan tersebut di atas, ada alasan yang tidak tepat untuk dimasukkan sebagai alasan untuk mengangkat Pejabat Sementara Notaris, yaitu diangkat sebagai pejabat negara atau jabatan-jabatan lain yang tidak dapat dirangkat dengan jabatan Notaris, lihat Habib Adjie (a), *op.cit*, hal 134.

5. Pindah wilayah jabatan;
6. Diberhentikan sementara; atau
7. Diberhentikan dengan tidak hormat.

Selain ketentuan pada pasal 1868 KUHPerdara keabsahan akta Notaris juga ditentukan oleh syarat – syarat *verlijden*, yaitu :

1. Akta tidak boleh kosong, melainkan disusun atas keterangan penghadap. Akta harus disusun dan dipersiapkan untuk dibacakan kepada penghadap (hal ini diatur dalam pasal 42 ayat (2) UUJN yang menentukan ruang dan sela kosong dalam akta digaris.
2. Dibacakan kepada para penghadap oleh Notaris dihadiri oleh dua orang saksi. Pada saat dibacakan, bila ada kesalahan dapat diperbaiki/*direnvooi*. Selain pada saat pembacaan akta kepada para pihak sebelum ditandatangani, akta tidak boleh dirubah (hal ini diatur pada pasal 16 ayat (1) jo pasal 44 ayat (1) jo pasal 49 jo pasal 50 ayat (3) UUJN.
3. Ditanda tangani oleh oleh para penghadap, saksi – saksi dan Notaris. Tandatangani dimaksudkan agar para pihak terikat dengan isi akta (ketentuan mengenai kewajiban tandatangan terdapat pada pasal 44 ayat (1) dan juga pasal 38 ayat (4) b UUJN)

Dalam hal penghadap tidak bisa menandatangani akta karena alasan tertentu maka penghadap menyatakan pada Notaris alasan tidak bisa tandatangan yang dinyatakan di bagian penutup akta yang berfungsi sebagai *surogaat* (pengganti tandatangan) yang kekuatannya sama dengan tandatangan.

Dalam hal syarat – syarat tersebut tidak dipenuhi maka akta Notaris tersebut tidak memiliki kekuatan pembuktian yang sempurna sebagaimana akta yang otentik melainkan hanya sebagai akta di bawah tangan.

2.3.5 Pengawasan Terhadap Notaris

Jabatan identik dengan wewenang dan kekuasaan, dan Notaris merupakan pejabat umum yang wewenangnya diatur dengan Undang-undang. Pelaksanaan wewenang dalam pelaksanaan tugas jabatan tersebut

sudah tentu perlu diawasi agar tidak terjadi penyalahgunaan kekuasaan dan wewenang (*abuse of power*).

Tujuan dari pengawasan terhadap Notaris ialah agar para Notaris sebanyak mungkin memenuhi persyaratan-persyaratan yang berkaitan dengan pelaksanaan tugas dan jabatan Notaris, yang ditetapkan undang-undang demi pengamanan dari kepentingan masyarakat umum. Notaris diangkat bukan untuk kepentingan sendiri, akan tetapi untuk kepentingan masyarakat yang dilayaninya. Untuk itu oleh undang-undang diberikan kepercayaan yang begitu besar dan secara umum dapat dikatakan bahwa setiap pemberian kepercayaan terhadap seseorang meletakkan tanggungjawab di atas bahunya, baik berdasarkan hukum maupun berdasarkan moral.⁸¹

Mekanisme pengawasan terhadap Notaris saat ini dilakukan dengan 2 cara yaitu :

1. Pengawasan Internal

Pengawasan Internal adalah pengawasan yang dilakukan oleh Organisasi Notaris (IKATAN NOTARIS INDONESIA) terhadap Notaris yang dilakukan secara berjenjang mengenai pelaksanaan kode etik yang berlaku terhadap notaris. Pengawasan Internal tersebut diatur dalam pasal 7 Kode Etik Notaris.

Pasal 7 Kode Etik Notaris menentukan bahwa pengawasan atas pelaksanaan Kode Etik itu dilakukan dengan cara sebagai berikut:

1. Pada tingkat pertama oleh Pengurus Daerah Ikatan Notaris Indonesia dan Dewan Kehormatan Daerah;
2. Pada tingkat banding oleh Pengurus Wilayah Ikatan Notaris Indonesia dan Dewan Kehormatan Wilayah;
3. Pada tingkat terakhir oleh Pengurus Pusat Ikatan Notaris Indonesia dan Dewan Kehormatan Pusat.

Selanjutnya, jika Notaris diduga melakukan pelanggaran kode etik maka terhadap notaris tersebut dilakukan pemeriksaan dan jika terbukti dalam pemeriksaan bahwa notaris yang bersangkutan melakukan pelanggaran

⁸¹ G.H.S Lumban Tobing, *op.cit*, hlm.301.

terhadap kode etik, maka terhadap Notaris tersebut akan dijatuhkan sanksi.

Kewenangan memeriksa dan menjatuhkan sanksi terhadap notaris yang terbukti melakukan pelanggaran kode etik berada di tangan Dewan Kehormatan. Hal ini tersebut diatur dalam pasal 8 Kode etik Notaris.

Selanjutnya dalam Pasal 9, Pasal 10, dan Pasal 11 Kode Etik Notaris diatur mekanisme pemeriksaan dan Penjatuhan Sanksi kepada Notaris oleh Dewan Kehormatan yang dilakukan secara berjenjang, yaitu pada tingkat pertama oleh Majelis Kehormatan Daerah (Pasal 9), Pemeriksaan dan penjatuhan sanksi pada tingkat banding oleh Dewan Kehormatan Wilayah (Pasal 10), dan pemeriksaan dan penjatuhan sanksi pada tingkat terakhir oleh Dewan Kehormatan Pusat (pasal 11).

Sanksi terhadap pelanggaran kode etik yang dapat dijatuhkan oleh Dewan Kehormatan kepada Notaris diatur dalam Pasal 13 Kode Etik Notaris. Bentuk sanksi tersebut bisa berupa pemecatan sementara sebagai anggota perkumpulan Notaris (INI) atau bahkan pemecatan permanen sebagai anggota INI.

2. Pengawasan Eksternal

Pengawasan baik preventif dan represif diperlukan bagi pelaksanaan tugas Notaris sebagai pejabat umum. Sebelum berlakunya UUJN, kewenangan pengawasan dan pembinaan atas Notaris dilakukan oleh Pengadilan Negeri. Namun setelah Pengadilan Negeri diintegrasikan satu atap di bawah Mahkamah Agung, maka kewenangan yang bersifat non-litigasi yang dilakukan oleh Pengadilan, dalam hal ini pengawasan dan pembinaan terhadap Notaris beralih kepada Menteri Hukum dan Hak Asasi Manusia, sebagaimana diamanatkan dalam pasal 67 ayat (1) dan ayat (2) UUJN, yang menyatakan bahwa Menteri berwenang melakukan pengawasan terhadap Notaris. yang dalam pelaksanaannya Menteri membentuk MPN (Majelis Pengawas Notaris). Ketentuan terhadap pengawasan Eksternal terhadap Notaris ini diatur dalam UUJN, khususnya dalam pasal 67 sampai dengan Pasal 81. Majelis Pengawas sebagaimana diatur dalam pasal 67 ayat (3) UUJN terdiri dari 9 orang,

yang komposisinya berasal dari 3 unsur dengan umlah yang sama, yaitu 3 orang dari unsur pemerintah, 3 orang mewakili organisasi notaris, dan 3 orang mewakili ahli (akademisi). Pengawasan terhadap Notaris melalui Majelis Pengawasan dilakukan secara berjenjang sebagaimana diatur dalam Pasal 68 UUJN. Di Tingkat daerah Kabupaten/kota dilakukan oleh Majelis Pengawas Daerah (MPD), kemudian dilanjutkan oleh Majelis Pengawas Wilayah (MPW) yang berada di tingkat Propinsi, dan terakhir berujung di Majelis Pengawas Pusat (MPP) yang berkedudukan di ibukota Negara di Jakarta.



BAB III
PERLINDUNGAN DATA PRIBADI DI INDONESIA DAN TANGGUNG
JAWAB NOTARIS DALAM AKSES INTEROPERABILITAS DATA
KEPENDUDUKAN

3.1. Perlindungan Data Pribadi di Indonesia

Sama dengan Amerika Serikat hingga saat ini di Indonesia belum ada undang – undang mengenai perlindungan data pribadi, tetapi aspek – aspek atas perlindungan data pribadi terdapat dalam beberapa peraturan perundang – undangan seperti Undang Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang Undang Nomor 43 tahun 2009 tentang Kearsipan, Undang Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang Undang Nomor 23 Tahun 1992 tentang Kesehatan, dan Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

1. Undang Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Pasal 14 ayat (2) menentukan bahwa salah satu hak mengembangkan diri adalah hak untuk mencari, memperoleh, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia.⁸²

Ketentuan ini menunjukkan adanya hak untuk mengembangkan diri termasuk mengontrol informasi/data.

2. Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 26 menentukan kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

⁸² Indonesia (e), *Undang-Undang Hak Asasi Manusia*, UU No.39 tahun 1999, LN No.165 Tahun 1999, TLN No. 3886 , Ps. 14 ayat (2).

Setiap Orang yang dilanggar haknya dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Kemudian penjelasan pasal 26 menentukan Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:

- a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
- b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
- c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.⁸³

Pasal 40 Ayat (2) menentukan Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.⁸⁴

3. Undang Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Dalam pasal 1 angka 22, data pribadi didefinisikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.⁸⁵

Pasal 84 ayat (1) menentukan data Pribadi Penduduk yang harus dilindungi memuat:

- a. nomor KK;
- b. NIK;
- c. tanggal/bulan/tahun lahir;
- d. keterangan tentang kecacatan fisik dan/atau mental;
- e. NIK ibu kandung;
- f. NIK ayah; dan

⁸³ Indonesia (d), *loc.cit*, Ps. 26 dan penjelasannya.

⁸⁴ *Ibid.*, Ps. 40 ayat (2).

⁸⁵ Indonesia (a), *loc.cit*, Ps. 1 angka 22.

g. beberapa isi catatan Peristiwa Penting.⁸⁶

Pasal 85 ayat (1) menentukan data pribadi Penduduk sebagaimana dimaksud dalam Pasal 84 wajib disimpan dan dilindungi oleh negara.

Pasal 86 ayat (1) menentukan Menteri sebagai penanggung jawab memberikan hak akses kepada petugas pada Penyelenggara dan Instansi Pelaksana untuk memasukkan, menyimpan, membaca, mengubah, meralat dan menghapus, mengkopi Data serta mencetak Data Pribadi.

Pasal 87 ayat (1) menentukan Pengguna Data Pribadi Penduduk dapat memperoleh dan menggunakan Data Pribadi dari petugas pada Penyelenggara dan Instansi Pelaksana yang memiliki hak akses.⁸⁷

Terkait dengan perolehan dan penggunaan Data Pribadi Penduduk dalam Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (PP No 37 Tahun 2007) di mana pada pasal 61 ayat (1) ditentukan bahwa untuk memperoleh data pribadi penduduk, pengguna harus memiliki izin dari Menteri, gubernur, atau bupati/walikota sesuai dengan lingkup data yang diperlukan. Kemudian pada ayat (2) ditentukan data pribadi penduduk yang diperoleh sebagaimana dimaksud pada ayat (1), hanya dapat digunakan sesuai dengan keperluannya yang tercantum dalam surat izin, jadi penggunaan data di luar apa yang tertulis dalam surat izin tidak diperbolehkan.⁸⁸

Sementara mengenai tata cara perolehan izin akses data tersebut diatur dalam pasal 62 PP No 37 Tahun 2007 tersebut di mana pada ayat (1) ditentukan data pribadi penduduk dapat diperoleh dengan cara: (a). pengguna mengajukan permohonan izin kepada Menteri, gubernur, atau bupati/walikota dengan menyertakan maksud dan tujuan penggunaan data

⁸⁶ Dalam penjelasan pasal 85 disebutkan bahwa Yang dimaksud dengan "beberapa isi catatan Peristiwa Penting" adalah beberapa catatan mengenai data yang bersifat pribadi dan berkaitan dengan Peristiwa Penting yang perlu dilindungi sedangkan pasal 1 butir 17 menyatakan bahwa peristiwa penting adalah kejadian yang dialami oleh seseorang meliputi kelahiran, kematian, lahir mati, perkawinan, perceraian, pengakuan anak, pengesahan anak, pengangkatan anak, perubahan nama dan perubahan status kewarganegaraan.

⁸⁷ Indonesia (a), *loc.cit*, Ps. 84 ayat (1), Ps. 85 ayat 91), Ps. 86 ayat (1) dan Ps. 87 ayat (1)

⁸⁸ Indonesia (k), Peraturan Pemerintah Pelaksanaan Undang Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, PP No.37 Tahun 2007, LN No.80 Tahun 2007, TLN No 4736, Ps. 61 ayat (1) dan (2).

pribadi penduduk; (b). Menteri, gubernur, atau bupati/walikota melakukan seleksi untuk menentukan pemberian izin. Tanggapan atas permohonan izin tersebut diberikan paling lambat 14 (empat belas) hari setelah permohonan diterima. Jika permohonan diterima petugas penerima akses memberikan data penduduk sesuai dengan izin yang diperoleh.⁸⁹

4. Undang Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Pasal 6 Ayat (3) menentukan Informasi Publik yang tidak dapat diberikan oleh Badan Publik adalah: ... (c) informasi yang berkaitan dengan hak-hak pribadi...

Pasal 17 menentukan setiap Badan Publik wajib membuka akses bagi setiap Pemohon Informasi Publik untuk mendapatkan Informasi Publik, kecuali: Informasi Publik yang apabila dibuka dapat mengungkapkan isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang; Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkap rahasia pribadi, yaitu:

1. riwayat dan kondisi anggota keluarga;
2. riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang;
3. kondisi keuangan, aset, pendapatan, dan rekening bank seseorang;
4. hasil-hasil evaluasi sehubungan dengan kapabilitas, intelektualitas, dan rekomendasi kemampuan seseorang; dan/atau
5. catatan yang menyangkut pribadi seseorang yang berkaitan dengan kegiatan satuan pendidikan formal dan satuan pendidikan nonformal.⁹⁰

5. Undang Undang Nomor 43 Tahun 2009 tentang Kearsipan

Pada pasal 81 ditentukan bahwa setiap orang yang dengan sengaja menguasai dan/atau memiliki arsip negara sebagaimana dimaksud dalam Pasal 33 untuk kepentingan sendiri atau orang lain yang tidak berhak dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp250.000.000,00 (dua ratus lima puluh juta rupiah).

⁸⁹ *Ibid*, Ps.62 ayat (1),(2) dan (3).

⁹⁰ Indonesia (f), *Undang-Undang Keterbukaan Informasi Publik*, UU No.14 tahun 2008, LN No.61 Tahun 2008, TLN No. 4846 , Ps. 22 dan Ps. 42 ayat (1).

Pada pasal 82 ditentukan bahwa setiap orang yang dengan sengaja menyediakan arsip dinamis kepada pengguna arsip yang tidak berhak sebagaimana dimaksud dalam Pasal 42 ayat (1) dipidana dengan pidana penjara paling lama 3 (tiga) tahun atau denda paling banyak Rp125.000.000,00 (seratus dua puluh lima juta rupiah).

Dalam hal ini perlu diperhatikan definisi arsip dalam Undang Undang tentang Kearsipan tersebut yaitu Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara.⁹¹

Oleh karena itu bisa saja rekaman kegiatan/peristiwa yang dibuat dan diterima oleh lembaga Negara pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan merupakan data pribadi, misalnya data kependudukan yang dikumpulkan oleh Kementrian Dalam Negeri.

6. Undang Undang Nomor 10 Tahun 1998 tentang Perbankan

Pasal 40 menentukan Bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan Simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 43, Pasal 44 dan Pasal 44A.⁹²

Keterangan Nasabah disini termasuk dalam lingkup data pribadi karena data nasabah dapat digunakan untuk mengidentifikasi seseorang.

7. Undang Undang Nomor 23 Tahun 1992 tentang Kesehatan

Pasal 52 ayat (2) dinyatakan bahwa tenaga kesehatan dalam melakukan tugasnya berkewajiban untuk mematuhi standar profesi dan menghormati hak pasien.⁹³

⁹¹ Indonesia (g), *Undang-Undang Kearsipan*, UU No.43 tahun 2009, LN No.152 Tahun 2009, TLN No. 5071 , Ps. 3, Ps. 81, Ps. 82.

⁹² Indonesia (h), *Undang-Undang Perbankan*, UU No.10 tahun 1998, LN No.182 Tahun 1998, TLN No. 3790 , Ps. 3, Ps. 81, Ps. 82.

⁹³ Indonesia (i), *Undang-Undang Kesehatan*, UU No.23 tahun 1992, LN No.100 Tahun 1992, TLN No. 3495 , Ps. 52 ayat (2).

Salah satu hak pasien adalah hak atas privasi dan kerahasiaan penyakit yang diderita termasuk data-data medisnya. Dalam Bab yang mengatur mengenai kewajiban Dokter dinyatakan pula bahwa dokter wajib merahasiakan segala sesuatu yang diketahuinya tentang seorang penderita bahkan juga setelah penderita itu meninggal dunia

Dalam hal ini yang merupakan data pribadi adalah rekam medis yang memuat riwayat kesehatan pasien.

8. Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal 22 menentukan bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau manipulasi (a) akses ke jaringan telekomunikasi; dan atau (b) akses ke jasa telekomunikasi; dan atau (c) akses ke jaringan telekomunikasi khusus. Bagi pelanggar ketentuan tersebut diancam pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp. 600 juta.

Pasal 42 ayat (1) mengatur kewajiban penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya. Bagi penyelenggara yang melanggar kewajiban tersebut diancam pidana penjara maksimal 2 tahun dan/atau denda maksimal Rp. 200 juta.⁹⁴

Dari uraian tersebut sangat jelas, bahwa walaupun belum ada peraturan/ketentuan khusus yang mengatur mengenai perlindungan data pribadi di Indonesia, di dalam beberapa peraturan perundang – undangan terdapat pasal yang mengatur serta memberikan perlindungan atas data pribadi walaupun tidak secara spesifik.

Sementara itu terkait perlindungan data pribadi dalam akses data kependudukan terdapat ketentuan dalam Undang Undang Adminduk dan ITE walaupun jika dibandingkan dengan ketentuan di Uni Eropa ketentuan tersebut masih kurang lengkap karena hanya memberikan perlindungan terhadap data pribadi sebatas izin akses dan pengaksesan sedangkan penggunaan dan pemrosesannya belum diatur.

⁹⁴ Indonesia (j), *Undang-Undang Telekomunikasi*, UU No.36 tahun 1999, LN No.154 Tahun 1999, TLN No. 3881 , Ps. 22 dan Ps. 42 ayat (1).

3.2. Urgensi Akses Data Kependudukan Oleh Notaris

Salah satu syarat otentisitas akta Notaris adalah bahwa penghadap dikenal oleh Notaris sebagaimana disyaratkan oleh pasal 39 UUJN ayat (2) yang merupakan bagian dari ketentuan mengenai badan akta oleh karena itu apabila ternyata penghadap tidak dikenal oleh Notaris maka akta yang telah dibuat tersebut dapat menjadi akta bawah tangan.

Sebagaimana telah diuraikan, bahwa pengertian dikenal bukan berarti kenal akrab seperti kenal dalam kehidupan sehari – hari melainkan kenal dalam arti hukum/yuridis yaitu identitas penghadap, yaitu kenal berdasarkan identitas yang sah, yang memuat secara benar nama, alamat, tempat dan tanggal lahir yang dikenal oleh umum/masyarakat sebagai benar bahwa itu adalah orang yang bersangkutan sehingga ia dapat dibedakan dan diindividualisasi dari orang – orang lain di dalam masyarakat serta bahwa yang bersangkutan (penghadap) berwenang melakukan tindakan dalam akta.

Selama ini Notaris sangat bergantung kepada Kartu Tanda Penduduk (KTP) sebagai sumber identitas untuk mengenal penghadap. Namun pada prakteknya seseorang dapat memiliki lebih dari satu KTP bahkan KTP juga dapat dipalsukan. Seseorang dapat dengan mudah memperoleh KTP dan melakukan penyalahgunaan atas KTP tersebut. Masih belum rapinya sistem data kependudukan dan keterbatasan akses atas sistem tersebut akan menimbulkan masalah bagi Notaris dikemudian hari dalam kaitannya dengan pengenalan penghadap oleh Notaris. Khususnya jika orang yang menghadap kepada Notaris adalah orang yang menggunakan identitas palsu. Hal tersebut terbukti dengan adanya tuntutan dari pihak yang dicuri identitasnya tersebut kepada Notaris yang bersangkutan dengan tuntutan pemalsuan surat yang dilakukan oleh Notaris.

Padahal jika dianalisa lebih jauh, dalam hal ini sebenarnya Notaris justru adalah korban penipuan, tetapi justru Notaris yang dipersalahkan membuat surat palsu atau melakukan pemalsuan surat. Untuk mengatasi hal tersebut, Notaris mencoba melakukan tindakan preventif dengan mengabadikan penghadap dalam foto, videocam ataupun kamera CCTV sebagai alat bukti jika nantinya ternyata penghadap tersebut menggunakan identitas palsu.

Namun upaya ini tetap tidak cukup untuk memperjelas dan menunjukkan validitas identitas subyek hukum (penghadap).

Untuk menjaga dan melindungi Notaris dari kemungkinan tuntutan terkait pemalsuan identitas oleh penghadap yang membuat akta pada Notaris, tentunya diperlukan suatu media yang memungkinkan Notaris untuk melakukan penelusuran data identitas seseorang yang dapat diakses oleh Notaris sebagai pejabat umum yang menjalankan sebagian fungsi publik dari Negara dalam hal pembuatan alat bukti atas transaksi yang dilakukan oleh masyarakat di bidang hukum perdata.

Saat ini di beberapa Negara di Eropa telah mengembangkan sistem *Electronic ID (e-ID)* manajemen dengan baik dan telah memberikan akses kepada Notaris untuk menelusuri validitas orang yang menghadapnya dengan pengecekan atas identitas penghadap melalui suatu basis data (*database*) kependudukan yang berisi identitas warga Negara di mana dengan menggunakan perangkat tertentu Notaris dapat mengecek validitas identitas penghadap yang menghadap kepadanya, apakah benar atau tidak.

Di Indonesia, saat ini dengan adanya Perpres KTP berbasis NIK/Perpres *e-KTP*, *e-ID* saat ini sedang dikembangkan oleh pemerintah yang dijalankan oleh Kementerian Dalam Negeri (dalam bentuk Sistem Administrasi Kependudukan) dan saat ini tengah dalam tahap pengumpulan identitas penduduk. Dengan adanya *e-KTP* ini diharapkan akan ada basis data penduduk yang valid yang bisa dijadikan rujukan.

Sehubungan dengan adanya basis data penduduk/data kependudukan yang tengah disusun dan dirancang oleh Kementerian Dalam Negeri tersebut dikaitkan dengan wewenang Notaris sebagai pejabat publik yang melaksanakan sebagian fungsi Negara dalam pelayanan publik, maka Notaris sangat memerlukan akses atas basis data penduduk tersebut agar dapat mengecek validitas identitas penghadap yang menghadap kepadanya yang merupakan salah satu syarat otentisitas akta.

Mengenai akses Notaris atas data kependudukan tersebut seperti diuraikan sebelumnya pada uraian mengenai perlindungan data pribadi di Indonesia, dimungkinkan dengan meminta izin kepada Menteri, Gubernur atau Walikota

dengan menyebutkan maksud dan tujuan akses atas data kependudukan tersebut, dalam hal ini tentunya adalah untuk mengecek validitas identitas penghadap yang menghadap kepada Notaris.

Mengenai hal tersebut dapat dibuat semacam formulir isian yang harus diisi oleh Notaris terkait dengan akses atas data kependudukan tersebut (yang termasuk di dalamnya data pribadi yang dilindungi) yang antara lain berisi tanggal dan waktu akses, maksud dan tujuan akses dan kemudian sebagai laporan mengenai valid tidaknya identitas penghadap dalam formulir disediakan kolom yang menerangkan apakah identitas penghadap yang disampaikan (*e-KTP*) sesuai dengan data yang ada dalam data kependudukan, sehingga tentunya dapat menjadi masukan bagi petugas penerima akses untuk melakukan perbaikan/koreksi atas data kependudukan.⁹⁵

Mengenai hal ini ada yang perlu diperhatikan terkait dengan isi dari data kependudukan dalam *e-KTP* yang akan dicocokkan oleh Notaris terkait identitas penghadap yaitu data alamat, karena dimungkinkan bahwa seseorang mempunyai lebih dari satu rumah sehingga tentu saja alamatnya/tempat tinggalnya lebih dari satu. Sehingga dalam pengecekan identitas bisa saja si penghadap menyebutkan alamat yang berbeda dengan data dalam *e-KTP*, namun menurut bapak Andi Kihorman hal tersebut tidak menjadi persoalan, karena pada dasarnya seseorang dapat memilih di mana dia akan membuat *e-KTP* yang akan menjadi tempat kedudukan/domisilinya⁹⁶ dan tempat di mana ia dapat mengubah dan memperbaharui data pribadinya dengan memberitahukan kepada petugas yang berwenang merubah/memperbaiki data kependudukan. Tidak menjadi masalah bahwa ia punya banyak tempat tinggal, pada dasarnya tempat kedudukan/domisilinya hanya satu dan ini yang

⁹⁵ Dalam wawancara dengan Bapak Andi Kihorman, Kepala Bidang Hubungan Masyarakat Kemendagri di Kementerian Dalam Negeri, Senin 4 Juni 2012, disampaikan olehnya bahwa dalam Sistem SIAK nanti akan ada logging data siapa yang mengakses data kependudukan, sehingga dapat diketahui siapa yang mengakses yang juga berfungsi sebagai rekap akses data kependudukan.

⁹⁶ Menurut pasal 17s/d 25 Kitab Undnag Undang Hukum Perdata sebagaimana dinyatakan oleh Wienarsih Imam Subekti dan Sri Soesilomahdi, tempat kediaman/domisili adalah tempat di mana seseorang dianggap selalu hadir dalam hal melakukan hak – haknya dan memenuhi kewajibannya walaupun senyatanya ia tidak berada di situ, lihat Wienarsih Imam Subekti dan Sri Soesilowati Mahdi, *Hukum Perorangan dan Kekeluargaan Perdata Barat*, (Jakarta: Gitama Jaya, 2005), hlm.12.

digunakan pada setiap saat seseorang melakukan perbuatan hukum, hal ini sesuai dengan asas tunggal dalam *E-KTP* di mana seseorang hanya dapat memiliki satu buah *e-KTP* yang nomor induk kependudukannya unik (berbeda untuk setiap orang).⁹⁷

Jadi walaupun seseorang memiliki rumah lebih dari satu/bertempat tinggal lebih dari satu, dalam melakukan perbuatan hukum alamat yang dia gunakan tetap sama yaitu tempat tinggalnya yang ada dalam data *e-KTP* dan alamat inilah yang nantinya dicocokkan oleh Notaris dalam pengecekan identitas penghadap yang membuat akta.⁹⁸

Dengan adanya akses ini, maka setidaknya Notaris benar – benar dapat memastikan kebenaran identitas orang yang menghadap hendak membuat akta, jika setelah dicek ternyata *e-KTP* yang disampaikan penghadap tidak sesuai dengan data kependudukan, tentunya Notaris dapat menunda pembuatan akta hingga adanya kejelasan atas identitas penghadap, apakah terjadi kesalahan pada input data kependudukan sehingga identitas dalam *e-KTP* tidak sesuai dengan data kependudukan atau memang data pada *e-KTP* yang diserahkan penghadap tidak valid/benar. Sehingga apabila nanti ternyata diketahui bahwa si penghadap menggunakan identitas palsu/tidak benar maka Notaris dapat menghindarkan dirinya dari tuntutan pembuatan surat palsu, karena data identitas yang diperoleh Notaris sesuai dengan data yang ada dalam data kependudukan, karena jika data *e-KTP* yang disampaikan tidak sesuai dengan data kependudukan, Notaris tentunya menolak untuk membuat akta.

Terkait dengan pengecekan validitas antara data kependudukan dengan *e-KTP* Notaris sebagai pihak ketiga yang berada di luar Kementerian Dalam Negeri dan pihak yang terlibat langsung dalam perancangan dan penyusunan data kependudukan juga dapat difungsikan sebagai pemeriksa validitas data kependudukan, apakah ada kesesuaian antara data kependudukan dengan *e-KTP* yang dipegang oleh penduduk dengan kata lain Notaris berfungsi

⁹⁷ Disampaikan oleh Bapak Andi Kihorman, Kepala Bidang Hubungan Masyarakat Kemendagri di Kementerian Dalam Negeri, dalam wawancara pada Senin 4 Juni 2012.

⁹⁸ Hal ini salah satunya terjadi dalam hal seseorang menikah lebih dari satu kali (poligami) dan mempunyai lebih dari satu rumah.

sebagai penyelia/penyaring data kependudukan. Tentunya dengan adanya fungsi tambahan ini, Notaris harus diberikan akses khusus atas data kependudukan, tidak lagi melalui jalur permohonan izin tetapi lewat suatu ketentuan khusus yang memungkinkan Notaris memperoleh akses atas data kependudukan tentunya Notaris harus tetap menjaga kerahasiaan data kependudukan tersebut dan tidak menyalahgunakan wewenang akses yang diperolehnya terkait fungsinya sebagai penyelia data.

Adanya peran Notaris sebagai penyelia data ini akan membantu tugas petugas penerima akses data kependudukan dalam memperbaiki dan memperbaharui data kependudukan dan tentunya mengurangi dampak akibat adanya kesalahan input oleh petugas, karena dilakukan pengecekan ulang oleh Notaris atas data yang diinput pada saat pengumpulan data (pembuatan *e-KTP*) dengan *e-KTP* yang dimiliki oleh masing – masing penduduk.

3.3. Hak dan Kewajiban Notaris Sebagai Pengakses Data Kependudukan

Terkait akses Notaris atas data kependudukan yang bertujuan untuk menjamin validitas/kebenaran identitas penghadap yang menghadap kepada Notaris, Notaris mempunyai hak dan juga kewajiban.

Adapun hak Notaris adalah memperoleh kewenangan akses atas data kependudukan sesuai dengan izin akses yang diperolehnya merujuk pada ketentuan PP Adminduk yang tentunya diberikan setelah Notaris mengajukan permohonan terlebih dahulu. Selain itu Notaris juga berhak untuk melapor secara berkala terkait akses data yang dilakukan apakah data yang ada di data kependudukan sesuai dengan data *e-KTP* yang disampaikan oleh penghadap. Hal ini diperlukan agar Notaris dapat melaporkan apa yang ditemuinya saat melakukan pengecekan data kependudukan. Adapun karena Notaris berada di bawah Kementrian Hukum dan Hak Asasi Manusia (Kemenhukham), maka laporan ditujukan pada Kemenhukham, baru kemudian Kemnhukham yang akan menyampaikan kepada Kemendagri terkait temuan Notaris untuk ditindaklanjuti. Bentuk penindaklanjutan dapat berupa perbaikan data kependudukan, jika terjadi kesalahan input atau penarikan *e-KTP* yang tidak benar serta penindakan kepada pihak yang menyerahkan *e-KTP* yang tidak

benar tersebut sesuai dengan ketentuan yang berlaku seperti dinyatakan oleh Bapak Martua Batubara, Sekretaris MPPN⁹⁹.

Sementara kewajiban Notaris atas adanya kewenangan akses data kependudukan tersebut adalah:

1. Melakukan akses atas data kependudukan sesuai dengan izin yang diperoleh untuk menghindari terjadinya akses berlebihan mengingat dalam data kependudukan terdapat data pribadi yang harus dilindungi terkait privasi seseorang.
2. Menggunakan data kependudukan (terutama yang merupakan data pribadi) sesuai dengan kebutuhan/keperluan yaitu untuk pengecekan identitas penghadap tidak untuk hal – hal lain yang tidak ada hubungannya.
3. Tidak menyimpan data kependudukan yang diperoleh untuk jangka waktu yang lama, jika akta yang berkaitan dengan data kependudukan yang diakses dan diperoleh telah selesai dan telah ditandatangani oleh para pihak (dengan demikian diasumsikan bahwa identitas penghadap sesuai dengan data kependudukan) maka data kependudukan yang diperoleh harus dihapus.
4. Sedapat mungkin memastikan bahwa data yang diperoleh adalah data terbaru yang telah diperbaharui.
5. Menjaga kerahasiaan data kependudukan yang diakses dan diperoleh berdasarkan izin yang diperoleh agar tidak diketahui oleh pihak lain selain oleh penghadap yang merupakan pemilik data kependudukan tersebut (yang mempunyai hak atas perlindungan privasi atas data dirinya) dan oleh Notaris sendiri.
6. Melaporkan secara berkala aktivitas akses data kependudukan yang dilakukan untuk memperoleh data kependudukan untuk memastikan bahwa izin akses dipergunakan sebagaimana mestinya dan tidak disalahgunakan.

Selain laporan berkala, Notaris juga wajib melaporkan laporan secara insidental apabila ditemukan dalam proses pencocokan antara data yang

⁹⁹ Hasil wawancara dengan Bapak Martua Batubara, Sekretaris Majelis Pengawas Pusat Notaris, di Kementerian Hukum dan hak Asasi Manusia, Senin, 4 Juni 2012.

diperoleh dari penghadap (*e-KTP*) dengan data kependudukan dalam Sistem Administrasi Kependudukan (SIAK) tidak sesuai.

Oleh karena itu laporan Notaris terkait akses data kependudukan ini dapat berupa laporan berkala dan laporan yang sifatnya insidental (jika ada ketidaksesuaian data). Adapun terkait dengan laporan, dapat dibuat formulir yang antara lain berisi tanggal akses data, data yang diperoleh, sesuai tidaknya data antara data kependudukan dengan data *E-KTP* dan pemanfaatan/penggunaan data yang diperoleh misalnya untuk pembuatan suatu akta, sehingga dapat dicek apakah akses yang dilakukan oleh Notaris telah sesuai dengan izin akses yang diberikan dan apakah data dalam data kependudukan sesuai dengan data *E-KTP*.

Terkait laporan ini ada baiknya juga selain diberikan kepada Kemenhukham juga diberikan salinan laporan kepada Majelis Pengawas Daerah (MPD) sebagai pengawas Notaris pada tingkat yang terbawah. Hal ini terkait dengan fungsi pengawasan yang dimiliki oleh MPD.

Terkait kewajiban Notaris terkait akses data kependudukan tersebut ada baiknya ditentukan Standar Operasional (SOP) bagi Notaris terkait dengan akses data kependudukan untuk mengecek kebenaran data kependudukan yang diperoleh berdasarkan izin dari Menteri, Gubernur ataupun Walikota sebagai pedoman bagi Notaris dalam pelaksanaannya.

Terkait hal ini menurut Bapak Martua Batubara, perlu dilakukan revisi terlebih dahulu pada UUJN sebagai landasan bagi peraturan di bawahnya agar memuat ketentuan terkait adanya kewajiban Notaris untuk melaporkan akses terhadap data kependudukan kepada Kementrian Hukum dan HAM.¹⁰⁰

3.4. Tanggung Jawab Notaris Sebagai Pengakses Data Kependudukan

Sebelum membahas mengenai tanggungjawab Notaris sebagai pengakses data kependudukan, perlu dipahami bahwa pada saat Sistem Admintrasi Kependudukan (SIAK) yang menjadi sumber data kependudukan selesai dirancang dan input/pemasukan data telah selesai maka pihak yang mengakses data tersebut tidak hanya Notaris saja melainkan ada pihak lainnya seperti Kemenhukham, Kemeninfo, Perpajakan, Perbankan dan lain –

¹⁰⁰ Disampaikan dalam wawancara dengan Bapak Martua Batubara, Sekretaris Majelis Pengawas Pusat Notaris, di Kementrian Hukum dan hak Asasi Manusia, Senin, 4 Juni 2012

lain, sehingga akses dilakukan secara interoperabilitas, oleh karena itu atas akses data kependudukan tidak hanya Notaris yang dibebani tanggungjawab.

Selain itu juga perlu dipahami bahwa dalam akses data kependudukan ini, Notaris bukan merupakan pihak yang terlibat langsung melainkan hanya pengakses data (*user/pengguna*). Pihak yang terlibat langsung adalah pihak perancang (*Developer*) sistem yang digunakan untuk akses interoperabilitas dan pihak yang menjadi pelaksana proyek sistem akses tersebut, mereka inilah yang seharusnya bertanggungjawab terkait adanya masalah yang disebabkan oleh sistem misalnya *bug* (cacat pada pemrograman mengakibatkan sistem tidak berjalan sebagaimana mestinya)

Perlu juga diketahui bahwa terdapat juga pihak yang menjadi penyelenggara sistem yaitu petugas pelaksana dari kemendagri yang diberikan tugas dan wewenang untuk melakukan pemrosesan data kependudukan (memasukan, menyimpan, membaca, merubah, menghapus, mengkopi dan mencetak) sebagaimana ditentukan dalam pasal 86 ayat (1) UU Adminduk.

Oleh karena itu pertanggungjawaban para pihak terkait dengan akses atas Sistem Informasi Kependudukan dapat diuraikan sebagai berikut :

1. Tanggungjawab Konsultan Perancang dan/atau pengembang (*Developer*)
Perancang dan/atau pengembang di sini adalah pihak yang membuat Sistem Administrasi Kependudukan yang pada dasarnya merupakan penerapan ilmu pengembangan sistem informasi (Sistem Informasi dan Teknik Informasi) yang pada dasarnya membuat sistem sesuai pesanan atau mengerjakan sistem yang memang diinginkan oleh si developer itu sendiri.

Tanggungjawab mereka adalah apabila ada cacat pada sistem yang mereka buat sehingga tidak bekerja sebagaimana seharusnya seperti terjadinya *error* atau *not responding* sistem pada saat sistem digunakan yang bukan karena kesalahan dalam pengoperasian atau penggunaan sistem melainkan karena adanya kesalahan pada saat sistem tersebut dibuat misalnya kesalahan dalam kode pemrogramannya ataupun pada *Graphical User Interface* (GUI).

Akibat dari adanya cacat pada sistem adalah sistem tidak dapat bekerja pada saat digunakan yang tentunya berdampak besar, karena pengguna (*user*) tidak dapat mengakses data yang diperlukan karena sistem tidak bekerja.

2. Tanggungjawab Pelaksana Proyek (Kontraktor)

Kontraktor di sini adalah pihak yang mendapatkan proyek untuk pengerjaan sistem, mereka inilah yang kemudian terhubung dengan developer sebagai pembuat sistemnya. Kontraktor adalah pihak yang muncul pada saat terjadi tender atas suatu proyek, di mana si pemesan menentukan kriteria dari produk yang ia inginkan dan kontraktor menyatakan bersedia melakukan sesuai permintaan pemesan. Dalam hal ini ada kontrak antara pemesan dan kontraktor terkait produk yang dipesan, bagaimana fiturnya, spesifikasinya dan juga kinerjanya

Tanggungjawab kontraktor adalah, apabila ia mengerjakan proyek yang ia peroleh ternyata tidak sesuai dengan permintaan pemesan, sehingga apa yang menjadi keinginan pemesan tidak terpenuhi. Dalam hal ini si kontraktor dapat dikategorikan tidak memenuhi ketentuan yang telah disepakati dalam kontrak dengan si pemesan.

3. Tanggungjawab Penyelenggara (Operator/Provider)

Dalam SIAK, penyelenggara ada dua pihak, yang pertama adalah penyedia akses internet/*Internet Service Provider* (ISP) dan yang lainnya adalah petugas pelaksana yang melakukan pemrosesan terhadap data kependudukan.

Tanggungjawab ISP adalah terkait dengan konektivitas jaringan (*network*) yang merupakan media yang digunakan agar sistem SIAK dapat senantiasa diakses di seluruh wilayah Indonesia. Adanya permasalahan konektivitas tentunya mengakibatkan kegagalan akses data. Oleh karena itu ISP bertanggungjawab atas permasalahan yang timbul terkait konektivitas, misalnya kerusakan server atau infrastruktur lain yang diperlukan dalam suatu *network*.

Tanggungjawab petugas pelaksana adalah terkait pada pemrosesan data yang dilakukan olehnya, misalnya adanya kesalahan pemasukan data atau

pemuktahiran data yang dilakukan, selain itu juga terkait pemeliharaan/perawatan sistem (*maintenace*).¹⁰¹

Adanya kesalahan input data mengakibatkan pengguna memperoleh data yang salah dan tidak akurat yang berakibat kemungkinan kerugian bila akses data tersebut digunakan untuk keperluan lain, misalnya Notaris yang menggunakan data tersebut terkait tugasnya membuat akta, kesalahan pemasukan data akan mengakibatkan data yang ada tidak sesuai dengan *e-KTP* yang diperoleh Noataris dari penghadap.

4. Tanggungjawab Pengguna (*User*)

User adalah pihak yang menjadi pengguna yang melakukan akses terhadap sistem untuk memperoleh data yang diperlukan, dalam SIAK, pengguna di sini ada beberapa pihak, seperti yang telah diuraikan terkait akses interoperabilitas antara lain Kemenhukham, Kemeninfo, Notaris, perbankan, perpajakan dan lain – lain.

Tanggungjawab pengguna adalah terkait pada pengaksesan dan penggunaan data sesuai dengan kebutuhan masing – masing dan juga menjaga kerahasiaan yang terkait erat dengan aspek perlindungan privasi. Selain itu juga menggunakan data dengan benar sesuai dengan data yang diperoleh, tidak merubah atau memanipulasinya serta tidak menggunakan data yang diperoleh untuk hal – hal lain yang di luar kewenangan yang diberikan kepadanya.

Terkait dengan akses atas data kependudukan selain sistem SIAK juga ada sistem lain yang digunakan Notaris untuk mengakses SIAK tersebut yang terintegrasi aksesnya dengan SIAK. Hingga saat ini belum dikembangkan sistem tersebut.

Dalam perkembangannya terkait sistem, Ikatan Notaris Indonesia (INI) dengan perusahaan swasta yaitu Averin telah mengembangkan sistem administrasi kenotariatan bernama INI-SAN, saat INI-SAN telah menyediakan beberapa fungsi terkait kenotariatan yaitu administrasi

¹⁰¹ Terkait dengan pemuktahiran data ini, menurut Bapak Andi Kihorman, pemilik data dimungkinkan untuk mengkoreksi kesalahan input data yang terjadi di tempat di mana ia membuat *e-KTP*, hanya saja menurutnya pemilik data tidak dapat langsung mengganti datanya sendiri tetapi pembetulan data tersebut tetap dilakukan oleh petugas yang memiliki hak akses atas SIAK sesuai ketentuan perundang – undangan yang ada.

notaris, pembuatan akta Notaris dan PPAT dimulai dari pembuatan, penandatanganan, pengurusan dan penyerahan, keuangan Notaris yang berisi pemasukan, pengeluaran serta tagihan, dokumentasi termasuk pengarsipan akta Notaris yang menyediakan juga fitur/fungsi pencarian baik berkas maupun dokumen hingga fungsi pengamanan akta. Hanya saja sistem ini hanya dapat terkoneksi dalam satu kantor notaris saja jadi akses interoperabilitas belum dimungkinkan.

Untuk ke depannya diharapkan akan ada sistem yang bisa terintegrasi dengan SIAK yang kini dikembangkan oleh Kemendagri, sehingga memungkinkan Notaris untuk mengakses secara interoperabilitas data kependudukan.

Dengan adanya sistem yang terintegrasi ini maka tanggungjawab terkait sistem berada pada pihak yang merancang dan mengembangkan sistem sesuai dengan ketentuan dalam perjanjian pengembangan sistem tersebut. Sedangkan tanggungjawab operasional dibebankan pada pihak yang nantinya mengoperasikan sistem tersebut. Notaris, sekali lagi di sini hanya merupakan pengguna sehingga tanggungjawab Notaris hanyalah sebatas atau terkait masalah penggunaan dan pemanfaatan data. Notaris tidak dapat diminta pertanggungjawaban apabila terjadi kesalahan pada input data, karena Notaris hanya mengakses data yang ada untuk dicocokkan apakah sesuai dengan data yang diperoleh dari penghadap.

Seperti diuraikan sebelumnya, tanggungjawab Notaris lebih terkait pada pemanfaatan data dan penggunaan serta masalah kewajiban merahasiakan data yang merupakan unsur hak seseorang atas privasi. Adapun secara rinci, tanggungjawab Notaris dalam akses interoperabilitas informasi data kependudukan adalah :

1. Melakukan akses data kependudukan sesuai dengan izin yang diperoleh berdasarkan ketentuan dalam PP Adminduk, yaitu mengakses data sesuai dengan keperluan yang tercantum dalam surat izin akses data yang diberikan. Misalnya Notaris meminta izin akses untuk melihat data kependudukan terkait nama, tanggal lahir, alamat dan pekerjaan

makan Notaris tidak boleh melihat data kependudukan yang lain dan tidak berhubungan.

2. Menggunakan data kependudukan yang diperoleh sesuai dengan tujuan permohonan akses data, dan tidak menggunakannya untuk hal lain yang tidak ada dalam ketentuan perolehan akses data dalam surat izin akses yang diberikan pada Notaris. Selai itu juga menggunakan data apa adanya tidak dirubah/dimodifikasi sehingga data menjadi berbeda dengan apa yang sebenarnya.
3. Merahasikan data – data kependudukan yang diperoleh dalam akses untuk pengecekan identitas penghadap dari orang lain. Dalam hal ini Notaris tidak boleh memberitahukan informasi data kependudukan yang diperoleh kepada orang lain.
4. Merawat peralatan/perangkat yang digunakan untuk mengakses data kependudukan agar selalu berfungsi dengan baik, karena apabila terjadi kesalahan akses data kependudukan karena perangkat yang digunakan tidak bekerja dengan baik akibat tidak adanya tindakan perawatan yang dilakukan oleh Notaris sebagai pengguna, maka hal tersebut menjadi tanggungjawab Notaris.

Mengenai sistem yang digunakan untuk mengakses data kependudukan ada baiknya jika dilakukan sinergi antara Kementerian Komunikasi dan Informasi (Kominfo) sebagai pihak yang memberi izin atas suatu sistem informasi, Kemenhukham sebagai pihak yang melakukan tugas pengawasan atas Notaris dan juga INI sebagai organisasi profesi Notaris. Sehingga fungsi interoperabilitas dalam akses data kependudukan bisa terlaksana dengan lebih baik.¹⁰²

¹⁰² Terkait hal ini menurut Bapak Martua Batubara, Beliau berpendapat bahwa lebih baik Sistem Akses tersebut dibuat atas kerjasama Ikatan Notaris Indonesia, sebagai wadah kegiatan para Notaris dengan Kemendagri sebagai pelaksana Sistem Informasi Data Kependudukan sedangkan Kemenhukham hanya melakukan pengawasan berdasarkan pemeriksaan rutin ataupun insidental. Adapun menurut Bapak Andi Kihorman, hal tersebut akan dibahas dalam sosialisasi dan pengenalan *E-KTP* antara bulan Juni dan Juli 2012 dengan mengundang para pihak yang terkait.

BAB 4 PENUTUP

4.1. Kesimpulan

1. Pengaturan perlindungan atas data pribadi dan kewenangan akses data kependudukan saat ini hanyalah sebatas adanya ketentuan mengenai data pribadi harus dilindungi dan diperlukannya izin bagi pengguna untuk mendapatkan/memperoleh akses atas data pribadi tersebut. Selain itu juga terdapat kewajiban pengguna untuk memastikan bahwa akses yang digunakan sesuai dengan izin yang diberikan. Ketentuan lebih lanjut terkait perlindungan data pribadi terkait dengan masalah pemrosesan, lama penyimpanan data yang diakses serta pelaporan mengenai akses data belum diatur secara rinci.
2. Terkait dengan tugas Notaris sebagai pelaksana sebagian peran pemerintah dalam pelayanan publik yaitu pembuatan akta, guna menjaga agar akta yang dibuat adalah akta otentik yang mempunyai kekuatan pembuktian sempurna maka Notaris membutuhkan kepastian kebenaran identitas para pihak yang membuat akta.

Terkait kebutuhan atas kepastian identitas tersebut sehubungan dengan adanya proyek *e-KTP* yang saat ini tengah dikembangkan oleh pemerintah, maka akses Notaris atas sistem yang memuat identitas penduduk merupakan hal yang diperlukan, karena dengan adanya akses tersebut, Notaris dapat mencocokkan apakah data yang diperoleh dari para pihak yang datang hendak membuat akta sesuai dengan data yang ada pada administrasi kependudukan. Dengan melakukan pencocokan data tersebut, Notaris akan memperoleh kepastian bahwa data yang diperolehnya dari penghadap adalah benar sesuai dengan data yang ada di administrasi kependudukan.

Sebagai konsekuensi adanya hak akses atas data kependudukan yang dilakukan secara interoperabilitas, maka Notaris memiliki tanggungjawab sebagai pengakses data. Namun tanggungjawab Notaris adalah hanya terkait dengan pengaksesan data dan penggunaan data

serta kerahasiaan data. Dalam hal ini, notaris bertanggungjawab untuk melakukan akses sesuai dengan izin yang diberikan terkait permohonan akses yang diajukan serta menggunakan data yang diperoleh hanya untuk keperluan Notaris saja terkait validasi identitas penghadap.

Hal – hal lain termasuk masalah kesalahan pemasukan (input) data atau ketidak akuratan data yang ada bukan merupakan tanggungjawab Notaris, karena Notaris hanya sebagai pihak pengguna data saja.

4.2. Saran

Berdasarkan analisa dan pembahasan di atas maka penulis menyarankan :

1. Perlu dilakukan revisi ketentuan pasal 16 UUJN, mengenai kewajiban Notaris dengan menambahkan kewajiban Notaris untuk melaporkan pengaksesan data kependudukan kepada Kementerian Hukum dan Hak Asasi Manusia atau disusun Peraturan Menteri yang mengatur mengenai adanya kewajiban Notaris untuk melaporkan pengaksesan data kependudukan.
2. Perlu dilakukan revisi ketentuan dalam Undang Undang Adminduk dan PP pelaksanaannya, terkait perlindungan atas data pribadi di mana tidak hanya pengaksesannya yang sesuai izin, tetapi juga penggunaan datanya juga sesuai kebutuhan dan tidak disalah gunakan atau digunakan untuk pemrosesan data lebih lanjut yang tidak ada hubungannya dengan tujuan semula.
3. Perlu disusun peraturan yang dibuat bersama antara pihak – pihak yang terkait dengan akses Data Kependudukan dalam Sistem Administrasi Kependudukan yang berisi masala ketentuan akses dan pertanggungjawaban masing – masing pihak atas akses tersebut.
4. Perlu disusun Standar Operasional pengaksesan data kependudukan oleh Notaris, sehingga mudah untuk mengecek apakah Notaris melakukan akses terhadap data kependudukan sesuai dengan ketentuan yang berlaku.

DAFTAR REFERENSI

Buku

- Adjie, Habib. *Sanksi Perdata dan Administratif Terhadap Notaris Sebagai Pejabat Publik*, cet. 2. Bandung: Refika Aditama, 2009.
- _____. *Hukum Notaris Indonesia Tafsir Tematik Terhadap UU No.30 Tahun 2004 Tentang Jabatan Notaris*, cet 1. Bandung : Refika Aditama, 2008.
- Hadjon, Philipus M. et al. *Pengantar Hukum Adminstrasi Indonesia*. Yogyakarta : Gajah Mada University Press, 1994.
- Hildebrandt, Mireille dan Serge Gatwirth. Ed. *Profiling the European Citizen Cross Dicipinary Prespectives*. Germany : Springer Science + Bussiness Media BV, 2008.
- Leenes, Ronald, Bert Joop Koops dan Paul De Hert.Ed. *Information and Technology & Law Series Constitutional Rights and New Technologies A Comparative Study*. Hague Netherlands : TMC Asser Press, 2008.
- Makarim, Edmon. *Notaris dan Transaksi Elektronik (Kajian Hukum tentang Cyber notary atau Electronic Notary)*. Jakarta : Rajawali Pers, 2011.
- _____. *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Jakarta : Rajawali Pers, 2005.
- _____. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta : Rajawali Pers, 2010.
- Mamudji,Sri, et al. *Metode Penelitian Dan Penulisan Hukum*. Jakarta : Badan Penerbit Fakultas Hukum Universitas Indonesia, 2005.
- Prins, J.E.J. ed. *Designing e-Government: On the Crossroads of Technological Innovation and Institutional Change*. The Netherlands: Kluwer Law International, 2001.
- Ratminto dan Winarsih, Atik Septi. *Manajemen Pelayanan : Pengembangan Model Konseptual, Penerapan Citizen's Charter dan Standar Pelayanan Minimal*. Yogyakarta:Pustaka Pelajar, 2005.
- Reed, Chris. *Internet Law Text and Materials Second Editions*. Cambridge, United Kingdom : Press Syndicate of The University of cambridge, 2004.

- Ronnenberg, Kai, Dennis Royer dan André Deuker. Ed. *The Future of Identity in the Information Society Challenges and Opportunities*. Berlin Heidelberg : Springer – Verlag, 2009.
- Nugraha, Safri et. al. *Hukum Administrasi Negara*. Edisi Revisi. Depok : Center of Law and Good Governance Studies, FHUI, 2007.
- Sanusi , M. Arsyad. *Konvergensi Hukum & Teknologi Informasi [Sebuah Torehan Empiris – Yuridis]*. Jakarta : The Indonesian Reach, 2007.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. cet. 3. Jakarta: UI – Press, 1986.
- Street F.,Lawrence dan Grant,Mark P. *Law of the Internet*.2000 Edition. Mathew Bedner & Company INC, 1999.
- Supriadi. *Etika dan Tanggungjawab Profesi Hukum di Indonesia*. Jakarta : Sinar Grafika,2006.
- Syahdeini , Sutan Remy. *Kejahatan & Tindak Pidana Komputer*. Jakarta : Grafiti, 2009.
- Tan Thong Kie. *Studi Notariat & Serba – Serbi Praktek Notaris*, Cet 1. Jakarta : Ihtiar Baru Van Hoeve,2007.
- Tobing, G.H.R Lumban. *Peraturan jabatan Notaris*, cet 4. Jakarta : Erlangga, 1996.
- United Nations Comission On International trade Law. *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods*. Vienna : United Nations Publications, 2009.

Artikel/Makalah

- Agung, Harijadi Joko. “Developing E-Government, The Case of Indonesia.” Makalah disampaikan pada E-Government Workshop APECTEL29, Hongkok China, 24 Maret 2004.
- Maule, Michael R. “Applying Strict Products Liability To Computer Software.” *Tulsa Law Jornal*, Summer, 1992.

Rundle, Mary “International Data Protection and Digital Identity Management Tools.” Makalah disampaikan pada IGF Athens Privacy Workshop.

Ramsay, Hayden. “Privacy, Privacies and Basic Needs.” *The Heythrop Journal*, vol.51, Februari 2010.

Peraturan Perundang - undangan

Indonesia. Peraturan Pemerintah Pelaksanaan Undang Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. PP No 37 Tahun 2007. LN No 80 Tahun 2007. TLN No 4736.

Indonesia. Undang Undang Jabatan Notaris. UU No 30 Tahun 2004. LN No 117 Tahun 2004. TLN No 4432.

_____. Undang-Undang Administrasi Kependudukan. UU No.23 Tahun 2006. LN No.124 Tahun 2006. TLN No. 4674, Ps. 1.

_____. Undang-Undang Kearsipan. UU No.43 tahun 2009. LN No.152 Tahun 2009. TLN No. 5071.

_____. Undang-Undang Pelayanan Publik. UU No.25 tahun 2009. LN No.112 Tahun 2009. TLN No. 5038.

_____. Undang Undang Tentang Informasi dan Transaksi Elektronik. UU No. 11. LN No. 58 tahun 2008. TLN No. 4843.

Presiden Republik Indonesia. Peraturan Presiden Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional. Perpres No.26 Tahun 2009.

_____. Peraturan Presiden Perubahan Peraturan Presiden Nomor 26 Tahun 2009 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional. Perpres No.35 Tahun 2010.

Kitab Undang Undang Hukum Perdata (*Burgerlijk Wetboek*). diterjemahkan oleh R. Subekti dan R. Tjitrosudibio. cet.32. Jakarta : Pradnya Paramita, 2004.

One Hundred Seventh Congress of the United States of America. E-Government Act of 2002.

The European Parliament. DIRECTIVE 2002/58/EC On The Processing OF Personal Data And The Protection Of Privacy In The Electronic Communications Sector.

_____. DIRECTIVE 2002/22/EC on Universal Service and Users' Rights Relating To Electronic Communications Networks and Services.

_____. DIRECTIVE 2009/136/EC Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating To Electronic Communications Networks and Services.

_____. DIRECTIVE 1995/46/EC on *The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*.

_____. DIRECTIVE 2001/45/EC Amending Directive 2002/22/EC on *The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*.

Internet

“*Digital & Electronic Signature FAQ*”. Co Sign ARX. <http://www.arx.com/digital-signatures-faq/digital-signatures-faq>. Diakses 23 Maret 2012.

Antonio Joia, Luis. “*A Framework for Developing Regional E-Government Capacity*” The Massachusetts Institute of Technology Information Technologies and International Development Volume 2, Number 4, Summer 2005. <http://itidjournal.org/itid/article/download/211/81>. Diunduh 26 Maret 2012.

Backhouse, James dan Vanfleteren, Michael. “Set of Requirements for Interoperability of Identity Management Systems”. Future of Identity in the Information Society. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.2.set_of_requirements.pdf. Diunduh 29 Maret 2012.

Jain Palvia , Shailendra C dan S. Sharma, Sushil. “E-Government and E-Governance: Definitions/Domain Framework and Status around the World” Computer Society of India. http://www.iceg.net/2007/books/1/1_369.pdf. Diunduh 26 maret 2012.

- Buitelar, J.C. Martin Meints dan E.Kindt. Ed. "Towards requirements for privacy-friendly identity management in eGovernment". Future of Identity in the Information Society. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_06_14_Fidis_D16.3_Reqs_PF_eGov_v1.2_final.pdf.
Dunduh 29 Maret 2012.
- Cameron, Kim. "The Laws of Identity". <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>. Diunduh 29 Maret 2012.
- D. Atkinson, Robert. "Turbo-Government: A Bold New Vision for E-Government" Information Technology and Innovation Foundation, Washington. <http://www.itif.org/index.php?id=68>. Diunduh 23 Maret 2012.
- Kementrian Dalam Negeri Republik Indonesia : Dirjen Adminsitrasi Kependudukan. <http://adminduk.depdagri.go.id>. Terakhir diakses 11 Juni 2012.
- Hansen, Marit, Ari Schwartz dan Alissa Cooper. "Privacy and Identity Management" IEEE Computer Society. <https://www.cdt.org/privacy/2008schwartzcooper.pdf>. Diunduh 29 maret 2012.
- Independent Centre for Privacy Protection (ICPP) /Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG). "Identity Management Systems (IMS): Identification and Comparison Study". https://www.datenschutzzentrum.de/dmanage/study/ICPP_SNG_IMS-Study.pdf. Diunduh 29 Maret 2012.
- Gasson, Mark. Martin Meints dan Kevin Warwick. Ed. "A Study On PKI and Biometrics" Future of Identity in the Information Society. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3_del3.2.study_on_PKI_and_biometrics.pdf. Dunduh 29 Maret 2012.
- _____. "Overview on IMS" Future of Identity in the Information Society. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3_del3.1.overview_on_IMS.final.pdf. Dunduh 29 Maret 2012.
- Kindt, Els dan Müller Lorenz. "The Privacy Legal Framework For Biometrics". Future of Identity in the Information Society. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf.
Diunduh 29 maret 2012.

Kreek, Kristel. "Electronic Signatures and E-invoicing; legislative approaches to electronic authentication and integrity of data" <http://www.virtuallawjournal.net/?nodeid=39&lang=en>. diakses 23 Mei 2011

WAWANCARA

Hasil wawancara dengan Bapak Andi Kihorman dari bagian Kepala Bidang Hubungan Masyarakat Kementerian Dalam Negeri Republik Indonesia bertempat di Kementerian Dalam Negeri Republik Indonesia pada hari senin, tanggal 4 Juni 2012. Jam 13.50

Hasil wawancara dengan Bapak Martua Batubara dari Pusat Notaris, bertempat di Kementerian Dalam Negeri Republik Indonesia pada hari senin, tanggal 4 Juni 2012. Jam 13.50



Lampiran 1 Tampilan Sistem Administrasi Kependudukan

KEMENTERIAN DALAM NEGERI
REPUBLIK INDONESIA

Provinsi * : JAWA TIMUR (35)
 Kecamatan * : PULIHAN
 Kabupaten/Kota * : 72 - KOTA BLITAR
 Desa/Kelurahan * :
 Cari berdasarkan : NOMOR KK : Jenis KTP : BARU : Kata Kunci : Data per Halaman : 10

TAMPAKAN

NO.	NOMOR KK	NIK (tidak ada foto)	NAMA LENGKAP	TEMPAT & TANGGAL LAHIR	ALAMAT	KTP		PHOTO	
						POS	3PK		
1.	3572031705061275	3572034608930003	NURUL HADYAH	BLITAR, 06-08-1993	J. PADANG NO 36 RT: 002 RW: 001	WA	3PK	0	<input type="checkbox"/>
2.	3572031705060285	3572035009950001	LAVINA SYIFAULHA	TULUNGAGUNG, 30-08-1995	SINGOLODRO NO 17 RT: 004 RW: 003	WA	3PK	0	<input type="checkbox"/>
3.	3572031607300003	3572032309899001	SEPTOKHO	BLITAR, 23-09-1988	J. RIAU NO. 45 RT: 004 RW: 002	WA	3PK	0	<input type="checkbox"/>
4.	3572033605069452	3572035908633002	SRI SUBENTYANS	BLITAR, 14-08-1987	J. KENARU NO 38 RT: 001 RW: 003	WA	3PK	0	<input type="checkbox"/>
5.	3572031605069452	3572031203813001	YUSUF WITOMO	BLITAR, 23-03-1983	J. KEMBAR NO 99 RT: 001 RW: 003	WA	3PK	0	<input type="checkbox"/>
6.	3572033605069452	357203121132001	MUKASTO	BLITAR, 11-11-1983	J. KEMBAR NO 99 RT: 001 RW: 003	WA	3PK	0	<input type="checkbox"/>

Total : 42627 Riwayat | Total : 4263 Riwayat

REGISTRASI SIAK KTP / KARTU TANDA PENDUDUK F-1.21 MENU

KEMENTERIAN DALAM NEGERI
REPUBLIK INDONESIA

DATA KELUARGA

No. KK * : PERKADA Nama Kepala Keluarga * :
 Alamat Keluarga * : No. RT :
 No. RT : Nama Dusun/Kampung/Dukuh :
 Kode Pos : Telepon :
 Provinsi * : Kabupaten/Kota * :
 Kecamatan * : Desa/Kelurahan * :

DATA INDIVIDU

NIK * : Nama Lengkap * :
 Gelar * : Akademis Kebangsaan Keagamaan Lainnya :
 No. KTP/Aspen : Tempat Tanggal Sebelumnya :
 No. Paspor : Tanggal Berakhir Paspor (dd-mm-yyyy) :
 Jenis Kelamin * : Tempat Lahir * :
 Tanggal Lahir (dd-mm-yyyy) * : Alita Lahir/Surat Kematian Lahir * :
 Golongan Darah * : Agama * :
 Status Perkawinan * : Alita Perkawinan/Buku Nikah :
 Tanggal Perkawinan (dd-mm-yyyy) : Alita Perkawinan/Surat Cerai :
 Tanggal Perorangan (dd-mm-yyyy) : Status Hubungan dengan Keluarga * :
 Kelainan Fisik dan Mental * : Penyandang Cacat :
 Pendidikan Terakhir * : Jenis Pekerjaan * :
 Foto : Tanda Tangan :

DATA ORANG TUA

NIK Ibu : Nama Lengkap Ibu * :
 NIK Ayah : Nama Lengkap Ayah * :

DATA ADMINISTRASI

Nama Ketua RT : Nama Ketua RW :
 Nama Petugas Registrasi * : NIP Petugas Registrasi :
 Nama & NIP Petugas Entry Data : <Administrator (Blitar) <123456789> Tanggal Entry Data : <2017-01-01>

DATA KELUARGA

- Data warga diambil berdasarkan data Kartu Keluarga (KK)

DATA INDIVIDU

- Data diisi sesuai dengan form isian formulir yang didapat pemohon.

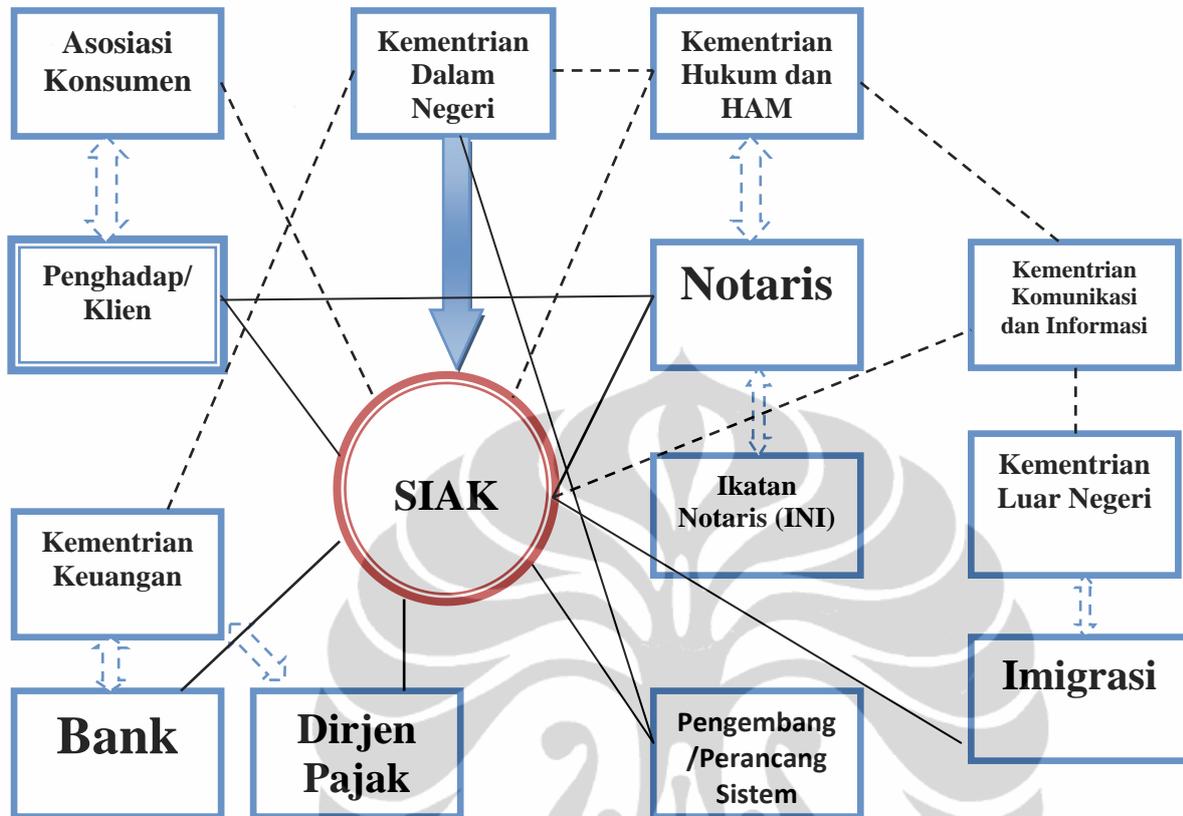
DATA ORANGTUA

- Nama lengkap Orangtua IBU & AYAH
- NIK Orangtua, IBU & AYAH

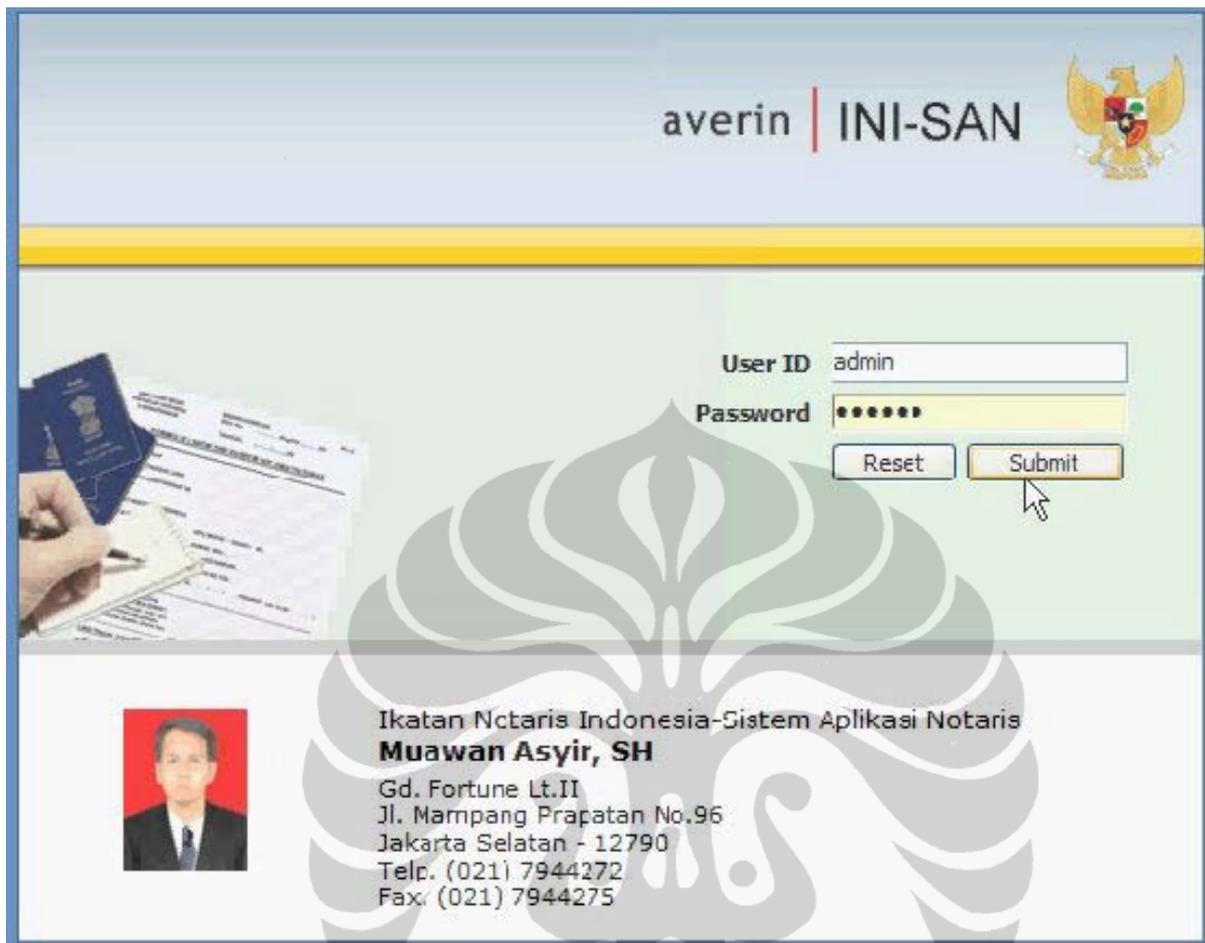
DATA ADMINISTRASI

- Nama Ketua RT/RW Domisili
- Tanggal Registrasi dan NIP Petugas

Lampiran 2 Skema Prediksi Hubungan Antara Para Pihak Dalam Sistem Administrasi Kependudukan (SIAK)



Lampiran 3 Sistem INI-SAN Adminstrasi Notaris Secara Elektronik



Ikatan Notaris Indonesia-Sistem Aplikasi Notaris
Ikatan Notaris Indonesia

Averin | INI-SAN

Modul: Tools Dashboard Informasi Ganti Password Administrator Logout

Admin		User				Tambah User
No.	Can	Nama Pegawai	User ID	Nama Notaris	Group User	Status
1.			admin	Administrator	Super Administrator	Aktif
2.			an	Asisten Notaris	Assistant Notaris	Aktif
3.			asep	Asep Yudhi	Keuangan	Aktif
4.			filling	Filing dan Dokumentasi	Filing & Dokumentasi	Aktif
5.			fo	front office	Front Office	Aktif
6.			keuangan	keuangan	Keuangan	Aktif
7.			laura	Laura	Front Office	Aktif
8.			muawan	Administrator	Notaris	Aktif
9.			nura	Nura	Assistant Notaris	Aktif
10.			sinta	Sinta	Filing & Dokumentasi	Aktif

Ikatan Notaris Indonesia-Sistem Aplikasi Notaris
Ikatan Notaris Indonesia

Averin | INI-SAN

Tools Dashboard Informasi Ganti Password Filling dan Dokumentasi Logout

Modul Filling & Dokumentasi

Filling & Dokumentasi

- Entry Dokumen
- Peminjaman Dokumen
- Pengembalian Dokumen

SURAT MEYURAT BULAN FEBRUARI 2011

- Terdapat 1 Surat Masuk
- Terdapat 2 Surat Keluar
- Terdapat 2 Fax Masuk
- Terdapat 1 Fax Keluar
- Terdapat 1 Email Terima
- Terdapat 1 Email Kirim
- Terdapat 1 Orang yang terdaftar pada Buku Tamu

ARSIP

- 4 Perwimanan Dokumen Fisik Februari 2011
- 3 Perwimanan Dokumen Elektronik Februari 2011
- 1 Peminjaman Arsip Februari 2011
- 1 Pengembalian Arsip Februari 2011

GRAFIK STATUS FEBRUARI 2010

DATA ORDER BULAN FEBRUARI 2011

Kategori	Status Order
Akta Notaris	26
PPAT	8
Legal	3
Waarmerking	2

DATA STATUS

Surat Masuk

No.	No.Agenda	Tanggal	Pengirim	Nomor	Kepada	Hal
1.	1	05-02-2011	Sae'ul	1111	Muawan Asyir, SH	Undangan

Halaman 1 dari 1 | Terdapat 1 Record | Ke Halaman

MODUL NOTARIS

STATUS ORDER FEBRUARI 2011

- 25 Order Akta Notaris
- 8 Order Akta PPAT
- 2 Order Legalisasi
- 3 Order Waarmerking
- 32 Order belum ditandatangani
- 6 Order sudah ditandatangani

STATUS ADM FEBRUARI 2011

- 1 Surat Masuk
- 2 Surat Keluar
- 2 Fax Masuk
- 1 Fax Keluar
- 1 Email Terima
- 1 Email Kirim
- 1 Orang tercatat di Buku Tamu
- Tercatat 4 Dokumen Fisik
- Tercatat 3 Dokumen Elektronik
- 1 Peminjaman Arsip
- 1 Pengembalian Arsip

STATUS KEUANGAN FEBRUARI 2011

- 1 Klient belum bayar
- 3 Klient yang membarar

GRAFIK ORDER FEBRUARI 2011

DATA ORDER BULAN FEBRUARI 2011

Kategori	Status Order
Akta Notaris	25
PPAT	8
Legal	2
Waarmerking	3

DATA STATUS

ORDER AKTA

No.	Nama Klient	Jenis Pekerjaan	Tgl Order	Tgl Persetujuan	Tgl Penyerahan	
1.	TIRTA SENTOSA	Akta Badan Hukum (Pendirian Perusahaan)	05-02-2011	05-02-2011	05-02-2011	Penyere
2.	ABADI SENTOSA	Akta Badan Hukum (Pendirian Perusahaan)	05-02-2011	05-02-2011	05-02-2011	Penyere
3.	EKA JAYA	Akta Badan Hukum (Pendirian Perusahaan)	05-02-2011	05-02-2011		Penguru
4.	MITRA SEJATI	Akta Badan Hukum (Pemberitahuan Perubahan AD Perusahaan)	04-02-2011			Proses f

Halaman 1 dari 5 | Terdapat 25 Record | Ke Halaman

Lampiran 4 Diagram Flow dan Fitur INI-SAN

