Dr. Udin Narsudin, S.H., Sp.N., M.Hum.

NOTARIS DI ERA DIGITAL



NOTARIS DI ERA DIGITAL

Dr. Udin Narsudin, S.H., Sp.N., M.Hum.

Penerbit :

CV KIMFA MANDIRI

Hak Cipta Dilindungi Undang-undang
Dilarang keras memperbanyak, memfotokopi sebagian atau
seluruh isi buku ini, serta
memperjualbelikannya tanpa mendapat izin tertulis dari Penerbit.
@2025, Penerbit CV. Kimfa Mandiri, Bandung
(95 halaman) 18,2 x 21 cm

NOTARIS DI ERA DIGITAL

Penulis:
Dr. Udin Narsudin, S.H., Sp.N., M.Hum.

Editor :
Prof. Dr. Mulyaningsih, M.Si

Desain Sampul dan Tata Letak :
Tim Penyusun

Penerbit:
CV. Kimfa Mandiri
JL. Raya Ciapus Rt 01 Rw 06 Desa. Ciapus Kec. Banjaran
Kab Bandung 40377
Telp: 022-85945637 - 085314983618 – 081220816826
Website: kimfamandiri.or.id
E-mail: kimfamandiriks@gmail.com

Januari, 2026
ISBN : 978-634-7487-05-6

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan buku yang berjudul: *Notaris Di Era Digital*.

Buku ini disusun dengan tujuan untuk memberikan pemahaman komprehensif mengenai peran, fungsi, tanggung jawab, serta etika profesi Notaris di Indonesia, terutama setelah berlakunya UU No. 2 Tahun 2014 tentang Perubahan atas UU No. 30 Tahun 2004 tentang Jabatan Notaris. Di tengah dinamisnya perkembangan hukum dan kebutuhan masyarakat akan kepastian hukum, profesi Notaris dituntut untuk lebih teliti, profesional, dan melek teknologi, serta tidak hanya sekadar formalitas belaka.

Penulis menyadari sepenuhnya bahwa buku ini masih jauh dari kesempurnaan karena keterbatasan kemampuan dan pengetahuan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari pembaca demi kesempurnaan buku ini di masa mendatang.

Akhir kata, penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dalam penyusunan buku ini. Semoga buku ini memberikan sumbangan pemikiran yang bermanfaat bagi dunia hukum kenotariatan di Indonesia.

Bandung, Januari 2026

Penulis

DAFTAR ISI

KATA PENGANTAR…….. i
DAFTAR ISI……. ii
BAB I. DISHARMONISASI REGULASI…….. 1
A. Penyebab Disharmonisasi……. 2
B. Dampak Negatif……... 9
C. Upaya Mengatasi……. 17

BAB II. KEAMANAN SIBER DAN PERLINDUNGAN DATA…… 30
A. Perbedaan Utama mengenai Keamanan Siber dan Perlindungan Data…… 31
B. Perbedaan Utama mengenai Ancaman Siber…….. 32
C. Perbedaan Utama mengenai Strategi Perlindungan Data Pribadi……. 36
D. Perbedaan Utama mengenai Kata Sandi… 38
E. Perbedaan Utama mengenai Autentikasi… 42
F. Perbedaan Utama mengenai Pembaruan... 44
G. Perbedaan Utama mengenai Kewaspadaan…… 46
H. Perbedaan Utama mengenai Perlindungan Data di Indonesia……. 48
I. Perbedaan Utama mengenai Pendekatan Sistem……. 50
J. Perbedaan Utama mengenai Keamanan…. 53

BAB III. MODERNISASI PENGAWASAN (2026)…… 56
A. Digitalisasi Layanan Pengawasan……. 56
B. Penguatan Peran MPN…… 59

C. Fokus pada Notaris Baru……. 61
D. Optimalisasi Organisasi Profesi……. 65
E. Sistem Pelaporan Online…… 69
F. Tujuan dari modernisasi……. 71

BAB IV. VALIDITAS HUKUM AKTA ELEKTRONIK ……. 74
A. Dasar Hukum & Validitas…… 74
B. Tantangan Konvensional…… 76
C. Aspek *Cyber Notary*…… 80
D. Validitas Alat Bukti…… 82

BAB V. ADAPTASI TEKNOLOGI (AI & BLOCKCHAIN)……. 84
A. Adaptasi Artificial Intelligence (AI) dalam Kenotariatan…….. 84
B. Adaptasi Blockchain dalam Kenotariatan…. 87
C. Dampak terhadap Peran Notaris (Cyber Notary)……. 89
D. Dasar Hukum di Indonesia…….. 91

Daftar Pustaka……. 94

BAB I.
DISHARMONISASI REGULASI

Disharmonisasi regulasi di Indonesia adalah kondisi tumpang tindih, konflik, atau ketidaksesuaian antarperaturan perundang-undangan, baik secara vertikal (hierarki) maupun horizontal (sektoral). Hal ini menyebabkan ketidakpastian hukum, menghambat efektivitas aturan, dan mempersulit investasi. Penyebab utamanya meliputi pendekatan sektoral yang kuat, kurangnya koordinasi antarlembaga, serta tingginya volume peraturan (over regulasi).

Disharmonisasi regulasi di Indonesia terjadi akibat tumpang tindih peraturan, pendekatan sektoral yang dominan, lemahnya koordinasi antarlembaga, serta tingginya volume peraturan (*over-regulation*). Faktor ini mengakibatkan ketidakpastian hukum, kebingungan di masyarakat, dan terhambatnya investasi. Akar masalah utamanya mencakup pembuatan peraturan oleh lembaga berbeda, pergantian pejabat, serta partisipasi publik yang terbatas.

A. **Penyebab Disharmonisasi:**

a. **Pendekatan Sektoral:** Lembaga pembentuk peraturan sering ego sektoral, mengutamakan kepentingan instansinya dibandingkan sistem hukum secara keseluruhan. Pendekatan sektoral adalah metode perencanaan dan pembangunan yang mengelompokkan aktivitas ekonomi atau pembangunan ke dalam sektor-sektor spesifik (seperti pertanian, industri, atau infrastruktur). Pendekatan ini menganalisis kebutuhan dan kinerja masing-masing sektor secara terpisah untuk mencapai tujuan pembangunan tertentu. Fokus utamanya adalah meningkatkan kinerja masing-masing sektor pembentuk pertumbuhan ekonomi.

Berikut adalah poin-poin penting terkait pendekatan sektoral:

Definisi: Pengelompokan aktivitas ekonomi ke dalam sektor primer, sekunder, dan tersier untuk dianalisis satu per satu.

Fokus utama: Penyelesaian masalah di sektor tertentu dan penyesuaian intervensi dengan karakteristik sektor tersebut.

Implementasi: Sering digunakan dalam perencanaan pembangunan yang membagi program berdasarkan sektor-sektor terkait.

Karakteristik: Membutuhkan data yang komprehensif, analisis mendalam pada sektor tersebut, dan seringkali memerlukan anggaran yang besar.

Kelemahan: Sering dianggap tidak selalu mampu menyelesaikan masalah kemiskinan dan ketimpangan pendapatan secara menyeluruh jika tidak dipadukan dengan pendekatan kewilayahan.

Kombinasi: Pendekatan ini sering dikombinasikan dengan pendekatan regional (wilayah) agar perencanaan lebih efektif.

Pendekatan ini berfokus pada pengembangan masing-masing sektor secara mandiri namun tetap harus terkoordinasi dalam pembangunan secara keseluruhan.

b. **Lemahnya Koordinasi:** Kurangnya sinkronisasi saat penyusunan peraturan antara instansi pusat maupun daerah. Disharmonisasi

(ketidakharmonisan/konflik) dalam kehidupan masyarakat, bernegara, maupun keluarga umumnya terjadi akibat lemahnya faktor-faktor pengikat sosial dan penegakan aturan.

Berikut adalah faktor-faktor penyebab utama lemahnya harmoni berdasarkan hasil pencarian:

- Lemahnya Penegakan Hukum dan Struktural

  Korupsi dan Intervensi Politik: Intervensi elit politik/oligarki dan korupsi melemahkan independensi penegak hukum, menciptakan ketidakadilan.

  Ketidakpastian Hukum: Disharmonisasi regulasi (peraturan yang tumpang tindih atau bertentangan) menimbulkan ketidakpastian hukum dan menghambat keadilan.

  Lemahnya Koordinasi: Lemahnya koordinasi antarlembaga pemerintahan menyebabkan fragmentasi peran, yang memicu disfungsi layanan publik.

- Masalah Sosial-Budaya dan Kurangnya Toleransi

Rendahnya Kesadaran Toleransi: Kurangnya kesadaran masyarakat untuk hidup rukun dan menghargai perbedaan keyakinan/budaya.

Etnosentrisme dan Sentimen Kedaerahan: Sikap memandang budayanya lebih unggul daripada budaya lain, serta prasangka sentimen kedaerahan yang tinggi.

Perubahan Nilai akibat Globalisasi: Perubahan sosial yang terlalu cepat seringkali membuat masyarakat tidak siap (culture shock) dan menimbulkan konflik nilai.

- Faktor Ekonomi dan Kesenjangan

  Ketimpangan Ekonomi: Kesenjangan sosial dan distribusi kekayaan yang tidak merata menciptakan kecemburuan sosial dan konflik antarkelompok.

  Perebutan Sumber Daya: Kompetisi yang tidak sehat dalam memperebutkan sumber daya (ekonomi, tanah, SDA).

- Faktor Politik dan Kepemimpinan

Manipulasi SARA: Politisasi isu SARA (Suku, Agama, Ras, Antargolongan) oleh elit politik untuk kepentingan elektoral.

Disharmonisasi Pemerintahan: Hubungan tidak harmonis antara pemimpin (contoh: Kepala Daerah dan Wakilnya) karena perbedaan kepentingan, bukan visi.

- Lemahnya Komunikasi dan Egoisme (Dalam Keluarga/Kelompok)

  Kurangnya Komunikasi: Minimnya komunikasi efektif menyebabkan salah paham, perselisihan, dan tidak terpenuhinya kebutuhan dasar emosional.

Sikap Egosentrisme: Masing-masing pihak lebih mengutamakan kepentingan pribadi di atas kepentingan bersama.

Secara ringkas, disharmonisasi berakar dari ketidakadilan, ketimpangan, serta gagalnya individu maupun kelompok dalam mengelola perbedaan dan menaati peraturan bersama.

c. **Over Regulasi:** Jumlah aturan yang terlalu banyak menyebabkan tumpang tindih. Over

regulasi dan disharmonisasi hukum di Indonesia ditandai dengan penumpukan lebih dari 52.000 peraturan yang sering bertentangan, tumpang tindih, dan tidak sinkron antarlembaga, menyebabkan ketidakpastian hukum dan menghambat investasi. Fenomena ini, yang sering disebut hyper-regulation, diatasi melalui penyederhanaan regulasi, metode omnibus law, evaluasi sistematik, dan pengujian peraturan yang konsisten.

Dampak dan Penyebab Over Regulasi & Disharmonisasi:

- **Alienasi Hukum:** Regulasi menjadi terasing dari masyarakat, sulit dipahami, dan rumit untuk dipatuhi, sering disebut "menghukum" masyarakat.
- **Tumpang Tindih:** Peraturan yang setingkat atau lebih tinggi bertentangan, menyebabkan dualisme atau ketidakpastian norma yang harus diikuti.
- **Faktor Penyebab:** Kurangnya koordinasi antarinstansi, ego sektoral, pergantian pejabat, rendahnya partisipasi publik dalam

penyusunan, dan tidak terpusatnya pengujian peraturan.

- **Hambatan Ekonomi:** Terlalu banyak aturan ketat mengurangi efisiensi dan persaingan pasar, menyulitkan usaha kecil/menengah.

Upaya Mengatasi Disharmonisasi:

- **Metode *Omnibus Law*:** Menggabungkan berbagai peraturan menjadi satu untuk menyederhanakan materi yang tumpang tindih.
- **Pengujian Satu Atap (*One-stop Simulation*):** Mengusulkan agar pengujian peraturan terpusat pada lembaga yudisial agar tidak terjadi putusan bertentangan.
- **Prinsip Hukum:** Menerapkan asas *Lex Superior Derogat Legi Inferiori* (peraturan tinggi mengalahkan rendah) dan *Lex Specialis Derogat Legi Generalis* (khusus mengalahkan umum).
- **Deregulasi:** Pemotongan jumlah peraturan yang tidak efektif secara masif.

Solusi konkret memerlukan sinkronisasi intensif dan kajian akademis yang mendalam sebelum peraturan disahkan, bukan sekadar kuantitas yang diutamakan melainkan kualitas.

d. **Dualisme Pengujian:** Putusan Mahkamah Agung dan Mahkamah Konstitusi yang berpotensi saling bertentangan dalam menguji aturan. Dualisme pengujian peraturan perundang-undangan di Indonesia merujuk pada pembagian kewenangan judicial review antara dua lembaga yudikatif, yaitu Mahkamah Konstitusi (MK) dan Mahkamah Agung (MA). Kondisi ini sering kali menimbulkan disharmonisasi putusan, ketidakpastian hukum, dan potensi konflik norma.

B. **Dampak Negatif:**

a. **Ketidakpastian Hukum:** Masyarakat dan penegak hukum kesulitan menentukan aturan yang berlaku. Ketidakpastian hukum, yang ditandai dengan peraturan tidak konsisten, tumpang tindih, atau sering berubah, berdampak negatif secara luas. Kondisi ini

menghambat investasi karena risiko bisnis yang tinggi, menurunkan kepercayaan publik terhadap aparat penegak hukum, merusak stabilitas nasional, serta meningkatkan kasus kriminalitas dan konflik sosial akibat kurangnya keadilan.

Dampak negatif dari ketidakpastian hukum meliputi:

- Ekonomi dan Investasi: Menghambat pertumbuhan ekonomi dan pembangunan nasional karena investor domestik maupun asing bersikap hati-hati. Risiko hukum, seperti pembatalan sepihak kontrak atau sanksi administrasi/pidana yang tidak konsisten, membuat bisnis tidak berjalan efektif.
- Kepercayaan Publik: Menurunkan kepercayaan masyarakat terhadap penegak hukum karena hukum dianggap tidak adil dan tidak melindungi.
- Ketidakstabilan Sosial: Tumpang tindih peraturan memicu konflik berkepanjangan dan ketimpangan sosial.

- Kepatuhan dan Hukum: Ketidakpahaman atas aturan yang berubah-ubah dapat meningkatkan risiko tindakan kriminal dan membuat masyarakat tidak mampu memperjuangkan hak-hak mereka.
- Inovasi: Regulasi yang membingungkan atau terlalu ketat menghambat inovasi teknologi dan memperlambat adaptasi terhadap tantangan baru.
- Penyelesaian memerlukan harmonisasi regulasi, sinkronisasi antarlembaga, dan peningkatan integritas aparat penegak hukum untuk menciptakan iklim hukum yang kondusif.

b. **Hambatan Pembangunan:** Menghambat masuknya investasi dan memperlambat laju ekonomi. Dampak negatif pembangunan sebagai hambatan utama meliputi kerusakan lingkungan (polusi, deforestasi, hilangnya habitat), ketimpangan sosial-ekonomi yang melebar, serta alih fungsi lahan yang tidak terkendali. Pembangunan yang tidak merata memperburuk jurang antara daerah maju dan tertinggal, serta seringkali menyebabkan

urbanisasi tidak terkendali, hilangnya nilai budaya lokal, dan ancaman kesehatan masyarakat.

Dampak Negatif Utama dan Hambatan Pembangunan:

- **Kerusakan Lingkungan & Ekosistem:** Pembangunan fisik sering mengorbankan lahan hijau, menyebabkan deforestasi, erosi, serta polusi udara dan air yang merusak kualitas hidup.
- **Ketimpangan Sosial-Ekonomi:** Ketidakseimbangan pembangunan menyebabkan pendapatan tidak merata, di mana orang kaya semakin kaya dan yang miskin semakin sulit mengakses fasilitas, memperlambat pertumbuhan ekonomi yang adil.
- **Alih Fungsi Lahan & Konflik Sosial:** Proyek pembangunan seringkali mengubah lahan pertanian menjadi kawasan industri, yang mengurangi lahan produktif dan menimbulkan konflik sosial.

- **Urbanisasi Tidak Terkendali:** Pembangunan terpusat memicu migrasi penduduk ke kota besar, yang menyebabkan kepadatan berlebih, kemacetan, dan tumbuhnya permukiman kumuh.
- **Hilangnya Identitas Budaya:** Pembangunan modern yang masif sering mengikis nilai-nilai budaya dan identitas lokal.

Pembangunan yang tidak berkelanjutan berisiko menciptakan kerusakan jangka panjang yang justru menghambat kemajuan ekonomi di masa depan.

c. **Inefisiensi Hukum:** Peraturan tidak berjalan efektif dan berpotensi menimbulkan korupsi. Inefisiensi hukum—di mana sistem hukum berjalan lambat, tidak konsisten, atau korup—menimbulkan dampak negatif yang luas bagi masyarakat, stabilitas negara, dan iklim ekonomi. Dampak-dampak tersebut berakar dari lambatnya proses peradilan, biaya yang tinggi, dan kurangnya kepastian hukum.

Berikut adalah dampak negatif utama dari inefisiensi hukum:

- **Krisis Kepercayaan Publik**
  - ✓ **Ketidakpercayaan terhadap Aparat:** Masyarakat kehilangan kepercayaan terhadap lembaga penegak hukum karena merasa keadilan sulit dicapai.
  - ✓ **Perilaku Anomi:** Individu merasa tidak terikat oleh norma atau aturan hukum, yang berpotensi memicu tindak kriminal karena merasa sistem tidak adil.
  - ✓ **Main Hakim Sendiri:** Kurangnya kepercayaan pada sistem memicu tindakan anarkis di mana masyarakat berusaha menghukum sendiri pelaku kejahatan.

- **Terhambatnya Pertumbuhan Ekonomi**
  - ✓ **Iklim Investasi Negatif:** Inefisiensi dalam penegakan hukum perdata dan kontrak menciptakan ketidakpastian bagi pelaku bisnis, sehingga menghambat pertumbuhan ekonomi.

- ✓ **Biaya Tinggi (High Cost Economy):** Proses hukum yang berbelit-belit meningkatkan biaya transaksi dan operasional, baik bagi individu maupun pelaku usaha.

- **Ketidakadilan Sosial dan Pelanggaran HAM**
  - ✓ **Keadilan yang Tertunda (Justice Delayed is Justice Denied):** Kasus yang berlarut-larut (lama) menyebabkan kerugian ganda bagi korban dan menyiksa terdakwa.
  - ✓ **Diskriminasi:** Sistem yang tidak efisien sering kali lebih merugikan kelompok miskin yang kurang memiliki akses atau daya tawar hukum dibandingkan kelompok kuat.
  - ✓ **Pelanggaran Hak Terdakwa:** Proses penahanan pra-peradilan yang terlalu lama sebelum vonis sah merupakan bentuk pelanggaran hak asasi manusia.

- **Instabilitas Stabilitas Sosial dan Politik**

- ✓ **Ketidakpastian Hukum:** Tumpang tindih regulasi dan inkonsistensi putusan menciptakan situasi di mana hukum sulit diprediksi, merusak kepastian hukum.
- ✓ **Konflik Berkepanjangan:** Kegagalan hukum dalam menyelesaikan konflik secara cepat sering kali memicu konflik sosial yang berkepanjangan.

- **Komodifikasi Penegakan Hukum**
  - ✓ **Korupsi di Lembaga Penegak Hukum:** Inefisiensi sering kali dipicu oleh korupsi, intervensi politik, dan lemahnya kapasitas aparat.
  - ✓ **Hukum sebagai Komoditas Politik:** Penegakan hukum yang diskriminatif dan tajam ke bawah tapi tumpul ke atas.

Inefisiensi hukum pada akhirnya menempatkan negara dalam posisi lemah, di mana kewajiban melindungi hak-hak dasar warga negara terabaikan, menyebabkan krisis multidimensi.

C. **Upaya Mengatasi:**

a. **Omnibus Law:** Metode penggabungan beberapa undang-undang untuk menyederhanakan peraturan. Upaya mengatasi masalah terkait *Omnibus Law* (khususnya UU Cipta Kerja) dapat dilakukan melalui tiga jalur utama: *judicial review* (uji materiil ke MK), *legislative review* (perubahan substansi oleh DPR dan Pemerintah), serta pemecahan UU menjadi kluster-kluster terpisah agar lebih mudah dipahami dan diimplementasikan. Partisipasi publik yang luas sangat krusial dalam setiap proses perbaikan tersebut.

Berikut adalah rincian upaya mengatasi *Omnibus Law* yang bermasalah:

- **Jalur Hukum (*Judicial Review*):** Menguji konstitusionalitas UU Cipta Kerja ke Mahkamah Konstitusi (MK) jika jalan musyawarah dengan pemerintah dan DPR buntu. Ini adalah langkah konstitusional terakhir untuk membatalkan pasal-pasal yang dianggap melanggar hak konstitusional warga negara.

- **Jalur Politik (*Legislative Review*):** DPR dan Presiden melakukan revisi terhadap substansi UU yang dianggap bermasalah. Langkah ini menuntut keterlibatan aktif stakeholder terkait (buruh, pengusaha, akademisi) untuk memastikan perubahan yang dihasilkan akomodatif.

- **Pemecahan UU (*Splitting*):** Memecah *Omnibus Law* menjadi beberapa undang-undang yang lebih kecil berdasarkan materi muatan sektoral (kluster). Misalnya, memisahkan kluster ketenagakerjaan, pertanahan, dan investasi menjadi UU tersendiri agar implementasinya lebih terarah dan mudah dipahami.

- **Optimalisasi Partisipasi Publik:** Memastikan revisi peraturan perundang-undangan (termasuk UU PPP) melibatkan partisipasi masyarakat yang bermakna (*meaningful participation*), bukan sekadar formalitas, untuk menghindari praktik pembentukan hukum yang buruk.

- **Penerbitan PERPU:** Presiden memiliki kewenangan menetapkan Peraturan Pemerintah Pengganti Undang-Undang (PERPU) jika situasi dinilai memenuhi unsur kegentingan yang memaksa.

  Langkah-langkah ini bertujuan memperbaiki tata kelola regulasi, memastikan kepastian hukum, serta menjamin keadilan dan kebermanfaatan peraturan bagi seluruh lapisan masyarakat.

b. **Harmonisasi:** Penyelarasan rancangan peraturan dengan peraturan yang lebih tinggi. Upaya mengatasi gangguan harmonisasi sosial (disharmoni) dalam masyarakat yang majemuk seperti Indonesia memerlukan pendekatan komprehensif, mulai dari dialog, pendidikan, hingga kebijakan yang inklusif. Harmonisasi sosial adalah keadaan seimbang di mana perbedaan suku, agama, ras, dan budaya dapat hidup berdampingan secara selaras.

  Berikut adalah beberapa upaya utama untuk mengatasi dan mencegah disharmoni sosial:

  1. **Penguatan Sikap Toleransi dan Sikap Sosial**

- **Saling Menghormati Perbedaan:** Menghargai keragaman budaya, agama, dan adat istiadat, serta tidak memaksakan kehendak.

- **Mengembangkan Solidaritas:** Meningkatkan kegiatan gotong royong dan aksi sosial bersama tanpa memandang perbedaan.

- **Menghindari Sikap SARA:** Menjaga ucapan dan tindakan agar tidak menyebarkan kebencian atau diskriminasi.

2. Dialog dan Komunikasi Terbuka

- **Membuka Ruang Dialog:** Mengadakan pertemuan, *Focus Group Discussion* (FGD), dan audiensi publik untuk menyelesaikan kesalahpahaman antarkelompok.

- **Penyelesaian Konflik secara Damai:** Mengembangkan sistem penyelesaian perselisihan secara damai dan tidak menggunakan kekerasan.

- **Mediasi yang Bijaksana:** Menggunakan pihak netral untuk menengahi konflik antarkelompok agar tercapai keadilan bagi semua pihak.

3. Pendidikan dan Edukasi Multikultural

- **Pendidikan Multikultural:** Menanamkan nilai-nilai kebangsaan, toleransi, dan kebhinekaan melalui pendidikan sejak dini untuk merajut kerukunan.

- **Pendidikan Kewarganegaraan:** Menggunakan PKn sebagai alat untuk memahami pentingnya harmoni dalam keberagaman.

- **Bijak Bermedia Sosial:** Mengedukasi masyarakat untuk tidak mudah terprovokasi hoaks yang dapat memecah belah persatuan.

4. Kebijakan dan Tindakan Pemerintah/Lembaga

- **Kebijakan Inklusif:** Pemerintah perlu membuat kebijakan yang merangkul semua kelompok masyarakat dan tidak diskriminatif.

- **Pemberdayaan Masyarakat:** Menginisiasi program pemberdayaan untuk mengatasi kesenjangan sosial yang sering menjadi akar konflik.

- **Kampanye Sosial Persatuan:** Menyebarkan pesan-pesan positif tentang pentingnya kebersamaan melalui seminar, media sosial, dan podcast.

5. Penguatan Kearifan Lokal

- **Memaksimalkan Organisasi Lokal:** Menggunakan organisasi sosial kemasyarakatan untuk mengikat kerukunan antar etnik.

- **Gotong Royong:** Memperkuat tradisi gotong royong yang menjadi akar budaya untuk menjaga keharmonisan.

Dengan menerapkan langkah-langkah tersebut secara konsisten, potensi konflik dapat diredam, dan harmoni sosial dapat dipertahankan atau dipulihkan kembali.

c. **Asas Hukum:** Penerapan asas *Lex superior derogat legi inferiori* (peraturan tinggi

mengesampingkan rendah) dan *Lex specialis derogat legi generalis* (khusus mengesampingkan umum). Upaya mengatasi pertentangan atau konflik antar asas hukum, maupun konflik norma yang didasarkan pada asas hukum, umumnya dilakukan melalui mekanisme penafsiran hukum, penerapan hierarki peraturan, atau uji materiil.

Berikut adalah upaya-upaya utama untuk mengatasi konflik asas hukum:

1. **Penerapan Tiga Asas Utama (Asas Derogasi)**

   Dalam sistem hukum, khususnya hukum tertulis, konflik antara aturan atau asas diselesaikan dengan tiga prinsip utama:

   - ***Lex Superior Derogat Legi Inferiori***: Peraturan yang lebih tinggi mengesampingkan peraturan yang lebih rendah. Asas yang berakar dari konstitusi lebih kuat dari undang-undang, dan seterusnya.

   - ***Lex Specialis Derogat Legi Generali***: Peraturan yang bersifat khusus

mengesampingkan peraturan yang bersifat umum (jika setara).

- ***Lex Posterior Derogat Legi Priori***: Peraturan yang baru mengesampingkan peraturan yang lama (jika setara).

2. Mekanisme Uji Materiil (*Judicial Review*)

Jika pertentangan asas mengakibatkan satu peraturan bertentangan dengan peraturan di atasnya, dilakukan langkah hukum:

- **Mahkamah Konstitusi (MK)**: Menguji undang-undang terhadap UUD 1945.
- **Mahkamah Agung (MA)**: Menguji peraturan di bawah undang-undang (seperti PP, Perpres, Perda) terhadap undang-undang.

3. Interpretasi dan Penafsiran Hukum oleh Hakim

Hakim memiliki peran krusial dalam mengatasi asas yang bertentangan di lapangan melalui:

- **Interpretasi Sistematis**: Menafsirkan peraturan dengan mengaitkannya dengan peraturan lain yang setara atau lebih tinggi.
- **Interpretasi Teleologis/Sosiologis**: Menafsirkan tujuan hukum dengan melihat rasa keadilan yang berkembang di masyarakat (*living law*), bukan hanya kaku pada asas legalitas formal.
- **Asas *Salus Populi Suprema Lex Esto***: Menggunakan prinsip bahwa keselamatan rakyat adalah hukum tertinggi jika asas hukum formal menemui jalan buntu.

4. Upaya Hukum (Litigasi)

Jika terjadi sengketa konkret akibat benturan asas:

- **Banding dan Kasasi**: Membawa perkara ke tingkat yang lebih tinggi untuk menguji ketepatan penerapan hukum.
- **Peninjauan Kembali (PK)**: Upaya hukum luar biasa jika ditemukan bukti baru atau kekhilafan hakim yang nyata.

5. Penyelesaian Non-Litigasi (Alternatif)

- **Negosiasi dan Mediasi**: Penyelesaian sengketa melalui diskusi untuk mencari kesepakatan yang adil, yang sering kali lebih fleksibel dalam mengakomodasi asas-asas hukum yang saling berbenturan.

  Upaya-upaya ini memastikan bahwa sistem hukum tetap konsisten, harmonis, dan tetap berorientasi pada keadilan substansial.

d. **Pengujian Satu Atap:** Wacana penyatuan lembaga pengujian peraturan untuk menghindari putusan bertentangan. Upaya mengatasi pengujian satu atap (one-stop testing/judicial review satu atap) di Indonesia, terutama dalam konteks ketatanegaraan (dualisme MA dan MK), difokuskan pada harmonisasi regulasi, efisiensi waktu, dan kepastian hokum. Berdasarkan kajian hukum dan hasil penelusuran, berikut adalah langkah-langkah untuk mengatasi kendala dalam pengujian satu atap:

1. **Penyatuan Kewenangan (Single Door/One-Stop Method)**
   - **Mengalihkan Kewenangan ke MK:** Salah satu solusi utama adalah menjadikan Mahkamah Konstitusi (MK) sebagai pelaku tunggal dalam pengujian peraturan perundang-undangan (judicial review), baik terhadap UUD 1945 maupun peraturan di bawah UU.
   - **Mengurangi Beban MA:** Dengan menyerahkan pengujian peraturan di bawah UUD ke MK, beban perkara di Mahkamah Agung (MA) dapat dikurangi, sehingga penanganan perkara lebih terfokus.
   - **Menghindari Dualisme Putusan:** Penyatuan atap mencegah terjadinya pertentangan norma antara putusan MA dan MK yang kerap menimbulkan ketidakpastian hukum.

2. **Digitalisasi Proses Pengujian**
   - **Implementasi SIJURI (Sistem Judicial Review Indonesia):** Menggunakan

sistem digital yang *user-friendly* dan *open access* untuk mempermudah masyarakat mengajukan pengujian, sekaligus meningkatkan transparansi dan kecepatan proses.

3. **Reformasi Kelembagaan dan Prosedur**
   - **Harmonisasi Putusan:** Memastikan bahwa putusan hukum bersifat integral, di mana penafsiran keabsahan produk hukum tidak terpecah, sehingga tidak multitafsir.
   - **Optimalisasi Penataan Regulasi:** Menata ulang jenis dan hierarki peraturan agar lebih sinkron sebelum masuk ke tahap pengujian, yang juga berfungsi mengurangi penumpukan perkara.

4. **Batasan Waktu Penyelesaian**
   - **Penerapan *Time Limit* yang Tegas:** Menerapkan batas waktu penyelesaian yang ketat, misalnya maksimal 3 bulan setelah perkara diterima

oleh majelis hakim untuk memastikan kepastian hukum.

5. Penguatan Posisi Lembaga

- **Penyetaraan Kedudukan:** Pengujian satu atap di MK juga bertujuan menegaskan kembali posisi MA dan MK sejajar, di mana MA berfokus pada perkara perorangan (administrasi/pidana/perdata) dan MK berfokus pada konsistensi regulasi terhadap UUD 1945.

Tujuan Akhir: Upaya ini bertujuan agar tidak ada lagi putusan *judicial review* yang berbeda atau bertentangan, sehingga tercipta kepastian hukum yang lebih baik bagi rakyat dan bangsa Indonesia.

BAB II.
KEAMANAN SIBER DAN PERLINDUNGAN DATA

Meningkatnya risiko kejahatan siber, seperti kebocoran data pribadi dan manipulasi tanda tangan elektronik, menjadi beban baru bagi notaris dalam menjaga kerahasiaan protokol. Notaris kini diwajibkan memahami standar teknis keamanan digital yang jauh lebih kompleks.

Keamanan siber dan perlindungan data adalah praktik krusial untuk melindungi sistem, jaringan, dan informasi sensitif dari serangan digital, pencurian, atau akses tidak sah. Keamanan siber berfokus pada pertahanan infrastruktur (termasuk CIA Triad: kerahasiaan, integritas, ketersediaan),

sementara perlindungan data memastikan privasi dan kepatuhan informasi. Langkah wajib meliputi penggunaan kata sandi kuat, autentikasi dua faktor (2FA), pembaruan perangkat lunak, dan kewaspadaan terhadap phishing.

A. Perbedaan Utama mengenai Keamanan Siber dan Perlindungan Data:

Keamanan siber melindungi aset dari ancaman luar (menghentikan intrusi), sedangkan perlindungan data fokus pada keamanan informasi di dalamnya.

Pernyataan bahwa keamanan siber melindungi aset dari ancaman luar (menghentikan intrusi), sedangkan perlindungan data fokus pada keamanan informasi di dalamnya adalah sebagian benar, tetapi terlalu menyederhanakan perbedaan antara keduanya.

Keamanan siber berfokus pada perlindungan sistem, jaringan, dan program dari serangan digital eksternal, seperti peretasan, malware, dan phishing. Tujuannya adalah membangun pertahanan dan menghentikan akses tidak sah.

Perlindungan data adalah istilah yang lebih luas dan merupakan bagian dari keamanan informasi. Ini mencakup semua aspek melindungi data, baik dalam bentuk digital maupun fisik, dari akses tidak sah, korupsi, atau kehilangan. Fokus utamanya adalah memastikan kerahasiaan, integritas, dan ketersediaan data (dikenal sebagai triad CIA), terlepas dari sumber ancamannya (internal atau eksternal).

Perlindungan data juga mencakup aspek kepatuhan terhadap peraturan perundang-undangan (seperti GDPR atau undang-undang privasi lokal) yang mengatur cara data dikumpulkan, disimpan, dan digunakan, serta hak-hak pengguna atas data mereka.

Singkatnya, keamanan siber menyediakan mekanisme teknis untuk melindungi dari ancaman digital, sedangkan perlindungan data adalah pendekatan holistik yang memastikan keamanan dan privasi informasi secara keseluruhan, termasuk aspek teknis, kebijakan, dan kepatuhan.

B. Perbedaan Utama mengenai Ancaman Siber:

Serangan yang umum terjadi meliputi ransomware, phishing, pencurian identitas, dan kebocoran data yang dapat merugikan secara finansial dan merusak reputasi.

Ancaman siber (cyber threats) adalah segala jenis tindakan jahat yang bertujuan untuk mendapatkan akses tidak sah, merusak, mencuri data, atau mengganggu jaringan dan sistem komputer. Perbedaan utama di antara berbagai ancaman siber terletak pada tujuan pelaku, metode serangan, dan dampak yang ditimbulkan.

Berikut adalah perbedaan utama dari jenis-jenis ancaman siber yang paling umum:

1. Malware (Malicious Software)

   Definisi: Perangkat lunak berbahaya yang dirancang khusus untuk merusak, memata-matai, atau mengeksploitasi sistem.

   Metode: Menyusup melalui unduhan, lampiran email, atau perangkat lunak rentan.

   Contoh: Virus, Worm, Trojan, Spyware.

Tujuan Utama: Merusak sistem atau mencuri data secara diam-diam.

2. Ransomware

   Definisi: Jenis malware spesifik yang menyandera data pengguna dengan mengenkripsi (mengunci) file.

   Metode: Masuk ke sistem, mengenkripsi file, dan menampilkan pesan tebusan.

   Tujuan Utama: Meminta uang tebusan (biasanya cryptocurrency) sebagai imbalan kunci dekripsi.

3. Phishing

   Definisi: Teknik rekayasa sosial (social engineering) untuk menipu pengguna agar memberikan informasi sensitif.

   Metode: Menggunakan email, situs palsu, atau pesan yang menyamar sebagai entitas tepercaya.

   Tujuan Utama: Mencuri nama pengguna, kata sandi, informasi kartu kredit, atau data pribadi.

4. Social Engineering (Rekayasa Sosial)

Definisi: Manipulasi psikologis manusia untuk membocorkan informasi rahasia.

Metode: Manipulasi, penyamaran, atau penipuan (termasuk phishing).

Tujuan Utama: Memanfaatkan kelalaian manusia, bukan kelemahan teknis sistem.

5. DDoS (Distributed Denial of Service)

   Definisi: Serangan yang membanjiri lalu lintas jaringan agar sistem tidak dapat diakses.

   Metode: Menggunakan jaringan komputer yang terinfeksi (botnet) untuk membanjiri server dengan lalu lintas palsu.

   Tujuan Utama: Melumpuhkan layanan atau situs web agar tidak bisa digunakan.

   Perbedaan Antara Ancaman Siber dan Serangan Siber

   Penting untuk memahami perbedaan istilah ini:

   Ancaman Siber (Threat): Potensi atau indikasi risiko adanya serangan.

   Serangan Siber (Attack): Tindakan nyata yang dilakukan peretas untuk melaksanakan ancaman tersebut.

Memahami perbedaan ini membantu dalam menerapkan strategi keamanan yang tepat, seperti penggunaan antivirus untuk malware, backup data untuk ransomware, dan pelatihan kesadaran keamanan untuk phishing.

C. Perbedaan Utama mengenai Strategi Perlindungan Data Pribadi:

Perbedaan utama dalam strategi perlindungan data pribadi sering kali terletak pada fokus operasional (teknis vs. legal), pendekatan (proaktif vs. reaktif), dan kepatuhan terhadap regulasi (seperti GDPR vs. UU PDP Indonesia).

Berikut adalah perincian perbedaan utama mengenai strategi perlindungan data pribadi:

1. Fokus Utama: Privasi Data vs. Keamanan Data

   Meskipun sering digunakan bersamaan, keduanya memiliki pendekatan berbeda:

   Privasi Data (Data Privacy): Fokus pada bagaimana data dikumpulkan, digunakan, dibagikan, dan diproses sesuai pedoman etika dan hukum. Strateginya meliputi transparansi

kebijakan (privacy policy), manajemen persetujuan (consent management), dan pembatasan data.

Keamanan Data (Data Security): Fokus pada langkah teknis untuk melindungi data dari akses tidak sah, pencurian, atau serangan siber. Strateginya meliputi enkripsi, firewall, kontrol akses, dan backup data.

2. Pendekatan: Proaktif vs. Reaktif

   Privacy by Design (Proaktif): Pendekatan yang mengintegrasikan perlindungan privasi sejak awal pengembangan sistem, bukan sebagai tambahan di akhir.

   Perlindungan Reaktif: Strategi yang berfokus pada respons setelah terjadi insiden (data breach), seperti pemulihan data dan penanganan pelanggaran.

3. Lingkup Strategi: Data Pribadi vs. Data Umum

   Strategi Perlindungan Data Pribadi: Secara khusus menargetkan informasi yang dapat mengidentifikasi individu (Nama, NIK, Biometrik, Kesehatan).

Strategi Keamanan IT/Data Umum: Melindungi seluruh aset informasi, termasuk data perusahaan yang tidak sensitif.

4. Perbedaan Kepatuhan: Regulasi (GDPR vs. UU PDP/APRA)

   Strategi sering kali disesuaikan dengan regulasi yang berlaku:

   GDPR (Eropa): Mewajibkan persetujuan eksplisit (opt-in), penunjukan Data Protection Officer (DPO), dan penilaian dampak perlindungan data (DPIA).

   UU PDP (Indonesia): Berlaku efektif penuh pada Oktober 2024, menuntut pemrosesan data yang sah, persetujuan pengguna, dan kewajiban notifikasi pelanggaran dalam 72 jam.

   APRA (AS - Proposal): Lebih condong ke model opt-out dan fokus pada konsumen tertentu dibandingkan pendekatan menyeluruh GDPR.

5. Komponen Strategis (Teknis vs. Manajerial)

   Strategi Teknis: Enkripsi, masking data, data loss prevention (DLP), dan manajemen akses.

Strategi Manajerial: Pelatihan kesadaran karyawan (awareness), kebijakan tata kelola data (governance), dan manajemen risiko.

D. Perbedaan Utama mengenai Kata Sandi:

Gunakan kombinasi huruf, angka, simbol, dan unik untuk setiap akun. Kata sandi biasanya berisi kombinasi karakter khusus, huruf, dan angka dengan panjang yang bervariasi. Sebagian besar sekitar 10 karakter.

Frasa sandi pada dasarnya adalah kata sandi yang lebih panjang, biasanya minimal 14 karakter, dengan spasi di antara kata-kata. Baik kata sandi maupun frasa sandi dapat digunakan untuk mengenkripsi data dan menjaga akses aman ke situs web, perangkat lunak, dan sistem perangkat keras.

Kata sandi adalah serangkaian karakter yang diperlukan untuk mengakses suatu sistem.

Kata sandi adalah metode umum untuk mengenkripsi atau mengamankan data, serta informasi rahasia, hak milik, dan pribadi. Berbagai

situs dan program memiliki persyaratan kata sandi yang berbeda-beda, termasuk panjangnya, penyertaan angka dan huruf, penggunaan huruf besar dan kecil, serta simbol khusus.
Kata sandi bisa terlihat seperti ini: 4jli$oju?A.

Frasa sandi pada dasarnya adalah bentuk kata sandi yang lebih aman. Orang menggunakan frasa sandi untuk alasan dan cara yang sama seperti kata sandi. Frasa sandi biasanya lebih panjang dan mengandung spasi. Frasa sandi juga dapat mengandung simbol, dan tidak perlu benar secara tata bahasa.

Seringkali lebih baik jika kata-kata dalam frasa sandi benar-benar acak. Arti frasa sandi tidak boleh mudah ditebak atau berupa frasa yang umum atau lazim. Menggunakan frasa acak membuat frasa sandi lebih kuat.membuka di tab baruContoh kata sandi bisa berupa “flow cat, bo0k through there!” Kata sandi harus mudah diingat tetapi sulit ditebak dan dibobol oleh peretas.

Baik kata sandi maupun frasa sandi dapat dibuat aman. Namun secara umum, frasa sandi yang kuat dan acak dikatakan memiliki entropi yang lebih tinggi dan karenanya lebih aman daripada kata sandi biasa. Kata sandi yang lebih panjang (14 karakter atau lebih) juga dapat memiliki tingkat entropi yang tinggi, sehingga lebih sulit untuk diretas melalui serangan brute force, tetapi juga lebih sulit untuk diingat.

Sebagian besar aturan kode sandi dan standar keamanan mengizinkan penggunaan frasa sandi sebagai pengganti kata sandi. Secara keseluruhan, menggunakan frasa sandi lebih aman dan memberikan ketenangan pikiran yang lebih baik. Dalam kedua kasus tersebut, FBImembuka di tab baruDisarankan untuk membuat kata sandi atau frasa sandi sepanjang mungkin yang diizinkan oleh sistem untuk keamanan optimal. Tips untuk membuat frasa sandi: Saat membuat frasa sandi yang kuat, ikuti aturan berikut:

Jangan memilih frasa atau pepatah yang populer.

Hindari lirik lagu.

Pertimbangkan kata-kata yang tidak bermakna.

Buat frasa tersebut minimal sepanjang 15 karakter.

Lima kata lebih baik daripada empat.

Tambahkan simbol dan huruf.

Pilih kata secara acak.

Gunakan frasa yang berbeda untuk setiap akun.

Ingatlah bahwa kata sandimembuka di tab baruTidak perlu berupa kalimat yang tepat atau bahkan mengikuti aturan tata bahasa dasar.

E. Perbedaan Utama mengenai Autentikasi:

Aktifkan autentikasi dua faktor (2FA).

Autentikasi dua faktor (2FA) adalah metode keamanan yang mengharuskan penggunaan dua bukti identitas berbeda (misalnya, kata sandi + kode OTP) untuk masuk ke akun, meningkatkan perlindungan secara signifikan dibanding satu faktor. Perbedaan utama 2FA dari MFA (Multi-

Factor) adalah 2FA tepat menggunakan dua faktor, sementara MFA bisa menggunakan dua atau lebih.

Berikut adalah perbedaan utama mengenai 2FA:

a. Jumlah Faktor: 2FA wajib menggunakan dua faktor berbeda (pengetahuan, kepemilikan, atau biometrik).
b. Keamanan: 2FA memberikan perlindungan kuat, terutama terhadap serangan phishing dan brute force, karena peretas butuh dua elemen yang berbeda untuk membobol akun.
c. Jenis Faktor: Biasanya kombinasi dari:
    - Sesuatu yang Anda ketahui (kata sandi/PIN).
    - Sesuatu yang Anda miliki (smartphone/aplikasi autentikator/token).
    - Sesuatu yang melekat pada diri Anda (sidik jari/wajah).
    - vs. MFA: Semua 2FA adalah autentikasi multifaktor (MFA), tetapi tidak semua MFA adalah 2FA (karena MFA bisa memakai 3+ faktor).

d. Kesesuaian: 2FA sangat cocok untuk akun pribadi, email, dan media sosial, menawarkan keseimbangan antara keamanan tinggi dan kemudahan penggunaan.

Mengaktifkan 2FA sangat penting karena Microsoft menunjukkan bahwa >99,9% akun yang diretas tidak menggunakan autentikasi faktor tambahan.

F. Perbedaan Utama mengenai Pembaruan:

Selalu perbarui sistem operasi dan perangkat lunak untuk menambal celah keamanan.

Pembaruan (update) sistem operasi (OS) dan perangkat lunak aplikasi sama-sama krusial untuk menambal celah keamanan, namun memiliki fokus dan ruang lingkup yang berbeda. Berikut adalah perbedaan utamanya:

Ruang Lingkup dan Dampak: Pembaruan sistem operasi (seperti Windows, Android, iOS) berdampak pada seluruh fondasi perangkat, mencakup komponen tingkat rendah (kernel, driver) dan keamanan sistem secara keseluruhan.

Sementara itu, pembaruan aplikasi (aplikasi pihak ketiga, web browser, dll.) hanya menambal celah pada perangkat lunak tertentu tanpa mempengaruhi sistem operasi secara langsung.

Keamanan vs. Fungsionalitas: Pembaruan sistem operasi sering kali berfokus pada perbaikan celah kritis (security patches) untuk mencegah akses tidak sah ke sistem inti. Pembaruan aplikasi selain menambal keamanan, lebih sering membawa peningkatan fitur, bug fix, dan peningkatan antarmuka pengguna.

Prioritas Pembaruan: Pembaruan OS dianggap lebih mendesak karena celah di tingkat OS dapat memberi peretas akses total (hak akses tertinggi) ke seluruh perangkat. Pembaruan aplikasi penting untuk aplikasi yang sering berinteraksi dengan internet (seperti browser atau aplikasi perbankan) untuk mencegah pencurian data.

Frekuensi dan Pengelola: Pembaruan OS biasanya dikelola oleh vendor perangkat (Microsoft, Google, Apple) dan bersifat menyeluruh. Pembaruan aplikasi bisa berasal dari berbagai

pengembang berbeda (pihak ketiga) dan sering kali membutuhkan interaksi pengguna untuk pembaruan manual.

Mengapa Keduanya Harus Diperbarui?

Menunda pembaruan—baik OS maupun aplikasi—meninggalkan celah yang diketahui (vulnerabilities) yang dapat dieksploitasi oleh malware, virus, atau ransomware. Pembaruan rutin adalah langkah pertama dalam pertahanan siber.

G. Perbedaan Utama mengenai Kewaspadaan:

Hindari Wi-Fi publik dan jangan sembarangan mengeklik tautan mencurigakan.

Perbedaan utama mengenai kewaspadaan antara menghindari Wi-Fi publik dan tidak sembarangan mengeklik tautan mencurigakan terletak pada sumber ancaman dan tindakan pencegahan yang diperlukan.

Hindari Wi-Fi publik berfokus pada keamanan jaringan (infrastruktur), sementara hindari tautan mencurigakan berfokus pada keamanan perilaku pengguna (social engineering).

Berikut adalah rincian perbedaannya:

1. Hindari Wi-Fi Publik (Keamanan Infrastruktur)

Risiko Utama: Data disadap (sniffing), serangan Man-in-the-Middle (penyerang berada di antara pengguna dan router), dan hotspot palsu.

Target: Informasi yang sedang dikirim atau diterima (kata sandi, detail kartu kredit, chat).

Tindakan Waspada: Jangan gunakan untuk transaksi perbankan, gunakan VPN, hindari jaringan tanpa kata sandi, dan matikan fitur auto-connect.

Fokus: Menghindari penggunaan jaringan yang tidak terenkripsi.

2. Jangan Mengeklik Tautan Mencurigakan (Keamanan Perilaku)

Risiko Utama: Phishing (pencurian kredensial), instalasi malware otomatis (ransomware/spyware), dan pengalihan ke situs palsu.

Target: Memancing pengguna untuk memberikan informasi secara sukarela atau mengunduh virus.

Tindakan Waspada: Periksa URL sebelum diklik, waspadai urgensi (pesan "akun Anda

diblokir"), dan jangan klik tautan dari pengirim tidak dikenal.

Fokus: Menghindari manipulasi psikologis dan klik impulsif.

Keduanya penting, tetapi Wi-Fi publik lebih berbahaya pada keamanan koneksi, sedangkan tautan mencurigakan berbahaya pada tindakan pengguna.

H. Perbedaan Utama mengenai Perlindungan Data di Indonesia:

Diatur melalui kerangka hukum yang mewajibkan organisasi menjaga privasi data pribadi pengguna guna mematuhi regulasi yang berlaku.

Perlindungan data pribadi di Indonesia diatur utamanya melalui UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang mewajibkan pengendali data (organisasi) menjaga privasi pengguna dengan persetujuan eksplisit, hak subjek data, serta sanksi administratif dan pidana bagi pelanggar. Perbedaan utamanya dengan regulasi lama seperti UU ITE adalah cakupan yang

lebih komprehensif, standar internasional, dan fokus pada hak individu atas data pribadinya.

Perbedaan Utama Perlindungan Data di Indonesia (UU PDP) dan Konteks Hukum

Landasan Hukum Utama: UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi aturan komprehensif utama, menggeser pendekatan tersebar pada UU ITE.

Subjek Data dan Hak Individu: Individu memiliki hak untuk mengakses, memperbaiki, menghapus, dan membatasi pemrosesan data mereka, serta berhak menggugat penyalahgunaan.

Pengendali vs. Prosesor Data: UU PDP membedakan tanggung jawab Pengendali Data Pribadi (yang menentukan tujuan) dan Prosesor Data Pribadi (yang memproses atas perintah pengendali), dengan kewajiban mematuhi aturan persetujuan.

Sanksi dan Kepatuhan: Pelanggaran dapat berakibat sanksi administratif (denda administratif) dan pidana, serta mengharuskan adanya

persetujuan jelas (persetujuan) sebelum data diproses.

Kesesuaian Internasional: Meskipun disesuaikan dengan standar internasional (serupa GDPR), regulasi Indonesia memiliki penekanan spesifik pada kedaulatan data warga negara Indonesia.

UU PDP mewajibkan organisasi menjaga keamanan data melalui langkah-langkah teknis dan administratif, serta memberikan kewenangan kepada lembaga pengawas untuk mengawasi pemrosesan data pribadi.

I. Perbedaan Utama mengenai Pendekatan Sistem:

Melibatkan kombinasi manusia (kesadaran keamanan), proses, dan teknologi.

Pendekatan sistem dalam keamanan informasi (sering disebut sebagai kerangka kerja People, Process, Technology - PPT) adalah strategi holistik yang tidak hanya mengandalkan satu elemen saja, melainkan kombinasi harmonis dari tiga pilar utama.

Perbedaan utamanya terletak pada pergeseran dari perlindungan berbasis teknologi semata (tradisional) menuju perlindungan komprehensif yang melibatkan budaya kesadaran manusia dan prosedur yang ketat.

Berikut adalah rincian perbedaan utama dari masing-masing elemen:

1. Manusia (Kesadaran Keamanan)

Peran: Manusia sering menjadi titik lemah sekaligus garis pertahanan pertama (frontline).

Perbedaan: Pendekatan sistem tidak hanya memasang teknologi, tetapi berfokus pada pelatihan, edukasi, dan membangun budaya keamanan (security culture) agar karyawan dapat mengenali ancaman seperti phishing.

Contoh: Pelatihan kesadaran keamanan (security awareness training) dan simulasi phishing.

2. Proses (Prosedur & Kebijakan)

Peran: Menyediakan struktur dan konsistensi dalam operasional keamanan.

Perbedaan: Proses memastikan tindakan keamanan dilakukan secara seragam dan terukur, bukan berdasarkan tindakan ad-hoc atau kebetulan.

Contoh: Kebijakan Manajemen Kata Sandi, Rencana Respons Insiden (Incident Response Plan), dan prosedur otorisasi akses.

3. Teknologi (Perangkat Keamanan)

Peran: Backbone atau tulang punggung pertahanan untuk mendeteksi dan mencegah ancaman siber.

Perbedaan: Teknologi digunakan untuk mengotomatisasi perlindungan dan memantau sistem secara real-time, yang tidak bisa dilakukan manusia secara manual.

Contoh: Firewall, Sistem Deteksi Intrusi (IDS), enkripsi data, dan Security Information and Event Management (SIEM).

Mengapa Pendekatan Sistem (Kombinasi) Penting?

Pendekatan ini menciptakan sinergi. Jika satu pilar diabaikan, pertahanan akan lemah:

Teknologi + Proses (Tanpa Manusia): Sistem aman, tetapi karyawan bisa tertipu phishing.

Manusia + Teknologi (Tanpa Proses): Karyawan sadar keamanan tetapi tidak tahu prosedur penanganan insiden yang benar.

Manusia + Proses (Tanpa Teknologi): Prosedur ada, orang sadar, tetapi sistem mudah ditembus malware.

Kesimpulan Utama: Pendekatan sistem/holistik memastikan keamanan seimbang, di mana teknologi yang canggih didukung oleh prosedur yang disiplin dan kesadaran manusia yang tinggi, sehingga menciptakan pertahanan yang tangguh (robust) dan adaptif.

J. Perbedaan Utama mengenai Keamanan

Siber bukan lagi pilihan, melainkan keharusan untuk melindungi aset digital, menjaga kepercayaan, dan memastikan kelangsungan operasional.

Pernyataan bahwa keamanan siber bukan lagi pilihan, melainkan keharusan, menandai pergeseran paradigma dari "keamanan sebagai biaya" menjadi

"keamanan sebagai investasi strategis". Perbedaan utama terletak pada tingkat kepentingan, dampak, dan pendekatan terhadap risiko.

Berikut adalah rincian perbedaan utama tersebut:

1. Keamanan Siber sebagai Pilihan (Paradigma Lama)

   Pendekatan: Reaktif (menangani masalah setelah serangan terjadi).

   Fokus: Kepatuhan dasar atau sekadar pemenuhan syarat administratif.

   Investasi: Dianggap sebagai beban biaya (cost center) yang mengurangi profit.

   Dampak: Kebocoran data hanya merugikan sebagian kecil aset, jarang berdampak pada kelangsungan bisnis utama.

2. Keamanan Siber sebagai Keharusan (Paradigma Saat Ini/Kebutuhan Utama)

   Pendekatan: Proaktif dan preventif (pencegahan sebelum terjadi serangan).

   Fokus: Perlindungan komprehensif atas aset digital, reputasi, dan kepercayaan pelanggan.

Investasi: Dianggap sebagai enabler bisnis yang krusial untuk inovasi dan pertumbuhan.

Dampak: Serangan siber dapat menyebabkan terhentinya operasional (downtime), kerugian finansial yang signifikan, hingga kebangkrutan.

Mengapa Keamanan Siber Menjadi Keharusan:

Melindungi Aset Digital: Melindungi kekayaan intelektual, data sensitif, dan sistem dari pencurian.

Menjaga Kepercayaan: Pelanggan hanya akan bertransaksi dengan perusahaan yang dapat menjamin keamanan data mereka.

Kelangsungan Operasional: Memastikan bisnis tidak terhenti akibat serangan ransomware atau gangguan jaringan.

Di era digital, keamanan siber adalah fondasi yang memungkinkan transformasi digital berjalan aman, terutama mengingat ancaman yang semakin canggih dan meningkat secara global.

BAB III.
MODERNISASI PENGAWASAN (2026)

Mulai Januari 2026, sistem pembinaan dan pengawasan notaris mengalami transformasi signifikan melalui digitalisasi layanan oleh Majelis Pengawas Daerah Notaris (MPDN). Hal ini menuntut notaris untuk segera beradaptasi dengan pelaporan protokol secara elektronik.

Modernisasi pengawasan notaris pada tahun 2026 di Indonesia berfokus pada digitalisasi layanan, penguatan peran Majelis Pengawas Notaris (MPN), dan restrukturisasi keanggotaan untuk meningkatkan profesionalisme dan integritas. Langkah ini diambil pasca diterbitkannya Peraturan Menteri Hukum dan HAM (Permenkumham) Nomor

24 Tahun 2025 tentang Penetapan, Pembinaan, dan Pengawasan Organisasi Notaris.

A. Digitalisasi Layanan Pengawasan:

MPN (khususnya MPDN Kota Bogor dan wilayah lain) menerapkan sistem berbasis teknologi untuk memantau kinerja, memproses laporan, dan memeriksa protokol notaris secara elektronik.

Digitalisasi pengawasan notaris di era digital, seperti implementasi aplikasi SIEMON (Sistem Manajemen Pengawasan Notaris), mentransformasi pembinaan dari manual menjadi digital yang lebih profesional, akuntabel, efisien, dan aman. Pengawasan difokuskan pada keamanan akun notaris dari mafia, digitalisasi protokol, serta penggunaan cyber notary untuk menjamin integritas akta.

Ada beberapa yang terkait digitalisasi layanan pengawasan notaris di era digital:

a. Sistem Pengawasan Berbasis Digital (SIEMON): Implementasi SIEMON oleh Kemenkumham (khususnya di DIY) mempermudah pembinaan dan pengawasan

notaris agar lebih terstandar, akuntabel, efektif, dan efisien.

b. Pengamanan Akun dan Protokol: Dirjen AHU mendorong pengawasan ketat, termasuk reset akun nasional, sistem autentikasi baru, dan audit berkala untuk menangkal "mafia akun" dan menyalahgunakan akses notaris.
c. Cyber Notary dan Digitalisasi Protokol: Penerapan cyber notary mencakup alih media arsip fisik menjadi elektronik (digitalisasi protokol), memungkinkan penyimpanan aman, konsultasi, dan laporan digital.
d. Keamanan dan Legalitas: Tantangan utama meliputi legalitas akta elektronik, keamanan data, dan risiko pemalsuan. Penggunaan tanda tangan digital, enkripsi, dan teknologi blockchain diusulkan untuk verifikasi dan mencegah manipulasi data.
e. Efisiensi Layanan: Digitalisasi mempercepat proses notaris dari hitungan hari menjadi jam, memangkas biaya fisik, dan mempermudah akses layanan.

Digitalisasi ini menuntut notaris untuk aktif memverifikasi penghadap dan menjaga kredensial akun, memastikan marwah kenotariatan tetap terjaga.

B. Penguatan Peran MPN.

Restrukturisasi keanggotaan MPN dilakukan untuk memastikan pengawasan lebih proaktif, terutama dalam mencegah tindak pidana pencucian uang (TPPU) dan tindak pidana pendanaan terorisme (TPPT).

Penguatan peran Majelis Pengawas Notaris (MPN)—terdiri dari MPD, MPW, dan MPPN—sangat krusial di era digital untuk memastikan notaris tetap mematuhi kode etik dan Undang-Undang Jabatan Notaris (UUJN), terutama dalam mengadopsi teknologi cyber notary dan tanda tangan elektronik. MPN berperan mengawal integritas profesi dari potensi pelanggaran yang timbul akibat digitalisasi layanan.

Hal-hal penting penguatan peran MPN di era digital:

1. Sinergi Pengawasan dan Pembinaan (2025-2028)

   Fokus pada Integritas: Pelantikan MPPN dan MKNP (Majelis Kehormatan Notaris Pusat) periode 2025-2028 menekankan penguatan pengawasan untuk menjaga integritas notaris di tengah disrupsi teknologi.

   Pengawasan Siber: MPN meningkatkan pengawasan atas kepatuhan notaris dalam mengadopsi cyber notary dan tanda tangan elektronik agar sesuai dengan standar hukum yang berlaku.

   Rakor Pengawasan: Kemenkumham aktif menggelar Rapat Koordinasi (Rakor) MPW dan MPD untuk memperkuat pengawasan atas perilaku notaris di dunia digital.

2. Adaptasi terhadap Cyber Notary

   Keamanan Data: MPN harus memastikan notaris mampu menjaga kerahasiaan dan privasi data pribadi klien dalam proses notarisasi online.

Penerbitan Akta Elektronik: Mengawasi tata cara kerja dan etika notaris, khususnya dalam pembuatan akta yang menggunakan tanda tangan elektronik.

3. Tantangan Baru bagi MPN

Adaptasi Hukum: MPN menghadapi tantangan dalam harmonisasi aturan, mengingat regulasi cyber notary di Indonesia masih tertinggal dan masih mengacu pada kehadiran fisik (UUJN Pasal 1868 KUHPerdata).

Integritas Digital: Pengawasan terhadap potensi penyalahgunaan tanda tangan elektronik oleh notaris.

4. Reformasi Kode Etik

Pembaruan Etika: MPN berperan dalam mendorong reformasi kode etik agar relevan dengan era digital, termasuk mengatur promosi jabatan di media sosial.

Secara keseluruhan, penguatan peran MPN di era digital bertujuan untuk menjamin kepastian hukum, mencegah pelanggaran etika dan teknis

dalam layanan digital, serta meningkatkan kepercayaan masyarakat.

C. Fokus pada Notaris Baru.

Kemenkumham (misalnya Kanwil Jabar dan Kalbar) memperketat pengawasan terhadap notaris baru untuk menjamin kepatuhan terhadap aturan dan kode etik.

Era digital membawa pergeseran fundamental dalam praktik kenotariatan di Indonesia, terutama bagi Notaris Baru yang memulai karier di tahun 2025-2026. Notaris tidak lagi hanya berurusan dengan kertas fisik, tetapi dituntut untuk menguasai teknologi, blockchain, dan AI (Artificial Intelligence) untuk menjamin keamanan hukum di ruang siber.

Berikut adalah fokus utama bagi Notaris Baru di Era Digital:

1. Transformasi Menuju Cyber Notary
    a. Definisi Operasional: Cyber Notary bukan sekadar membuat dokumen digital, melainkan penerapan teknologi dalam verifikasi identitas (biometrik), proses

pembuatan akta elektronik, hingga penyimpanan arsip digital yang aman.

b. Layanan Daring: Notaris baru diharapkan mahir menggunakan sistem AHU Online, SABH (Sistem Administrasi Badan Hukum), dan e-Notary untuk pengesahan badan hukum, pendaftaran wasiat, dan fidusia.
c. Tanda Tangan Elektronik: Penggunaan Tanda Tangan Elektronik (TTE) tersertifikasi menjadi wajib untuk menjamin otentisitas dokumen.

2. Tantangan Spesifik Notaris Baru
   a. Keamanan Data Klien: Notaris bertanggung jawab penuh atas privasi dan keamanan data digital klien dari risiko peretasan.
   b. Teknologi Blockchain: Penggunaan blockchain untuk verifikasi akun dan akta mulai menjadi tren untuk mencegah pemalsuan.
   c. Adaptasi Hukum & AI: Meskipun AI berkembang, peran manusia dalam "aspek kehati-hatian" dan validasi identitas tetap tak

tergantikan. Notaris baru harus cepat beradaptasi dengan disrupsi teknologi.

3. Peluang di Era Digital
    a. Efisiensi Layanan: Proses menjadi jauh lebih cepat, akurat, dan transparan.
    b. Perjanjian Modern: Tren baru seperti perjanjian pranikah digital, transaksi aset digital, dan kontrak pintar (smart contracts) membuka ceruk pasar baru.
    c. Fleksibilitas: Memungkinkan pelayanan dari jarak jauh tanpa mengurangi keabsahan hukum, selama sesuai dengan prosedur cyber notary.
4. Etika dan Pengawasan
    a. Kode Etik Digital: Meskipun aktif di media sosial untuk membangun branding, notaris baru harus mematuhi kode etik terkait promosi dan publikasi diri.
    b. Pengawasan Digital: MPPN (Majelis Pembina Pusat Notaris) dan MKNP (Majelis Kehormatan Notaris Pusat) semakin

memperkuat sistem pembinaan dan pengawasan notaris berbasis digital.

c. Kesimpulan untuk Notaris Baru: Kunci sukses notaris baru di era digital adalah kecepatan beradaptasi, keamanan siber (cyber security), dan pemahaman mendalam tentang regulasi ITE, tanpa meninggalkan prinsip kehati-hatian hukum.

D. Optimalisasi Organisasi Profesi:

Ikatan Notaris Indonesia (INI) semakin ditegaskan sebagai satu-satunya organisasi notaris yang diakui dan diatur kewenangannya dalam pembinaan, sebagai tindak lanjut dari revisi UU Jabatan Notaris.

Optimalisasi organisasi profesi notaris (seperti Ikatan Notaris Indonesia/INI) di era digital sangat krusial untuk memastikan notaris tetap relevan, profesional, dan berintegritas di tengah disrupsi teknologi. Di tahun 2025, fokus utama adalah adaptasi terhadap blockchain, Kecerdasan Buatan (AI), dan penerapan cyber notary untuk

meningkatkan kecepatan serta keamanan layanan hukum.

Berikut optimalisasi organisasi profesi notaris di era digital berdasarkan hasil studi:

1. Penguatan Cyber Notary dan Infrastruktur Digital

   Organisasi profesi harus mendorong anggotanya untuk tidak hanya memahami hukum konvensional, tetapi juga menguasai teknologi digital.

   Penerapan Cyber Notary: Melibatkan penggunaan teknologi digital dalam verifikasi identitas (biometrik), pembuatan dokumen, hingga penyimpanan arsip secara elektronik.

   Tanda Tangan Elektronik (E-Signature): Mengintegrasikan tanda tangan digital yang sah sesuai UU ITE dalam akta notaris untuk kepastian hukum.

   Sistem Keamanan Data: Memastikan penggunaan sistem enkripsi tingkat tinggi untuk menjaga kerahasiaan dan integritas dokumen.

2. Peningkatan Kompetensi dan Literasi Digital

Organisasi profesi wajib mengadakan pelatihan berkelanjutan agar notaris adaptif dengan revolusi teknologi.

Pelatihan AI dan Blockchain: Notaris perlu memahami cara kerja blockchain dan AI agar tidak tergerus oleh otomatisasi hukum.

Sertifikasi Digital: Mendorong notaris memiliki sertifikasi tanda tangan elektronik dan pemahaman mendalam tentang keamanan siber.

3. Reformasi Kode Etik dan Regulasi

   Perlunya penyesuaian aturan perilaku notaris agar sesuai dengan praktik digital.

   Revisi Kode Etik: Memperbarui kode etik jabatan notaris agar relevan dengan branding digital dan pemasaran online yang etis.

   Adaptasi UU Jabatan Notaris (UUJN): Mendorong perubahan aturan yang mendukung pelaksanaan notaris elektronik (e-notary) tanpa menghilangkan prinsip kehati-hatian (prudent principle).

4. Sinergi dengan Pemerintah (Ditjen AHU Online)

Organisasi profesi berperan sebagai jembatan antara notaris dan Kementerian Hukum dan HAM.

Pemanfaatan Sistem Elektronik: Memaksimalkan penggunaan sistem yang diinisiasi Ditjen AHU (AHU Online) untuk pendaftaran badan hukum, PT, dan pelayanan lainnya.

Penyatuan Data: Mengintegrasikan data akta elektronik untuk mempermudah verifikasi dan meningkatkan efisiensi layanan publik.

5. Perlindungan Integritas dan Profesi

Di era digital, peran notaris bergeser dari sekadar saksi fisik menjadi penjamin autentisitas dokumen digital.

Menjaga Kepercayaan Publik: Memastikan bahwa meskipun akta dibuat secara digital, nilai pembuktiannya tetap kuat dan tidak menjadi akta di bawah tangan.

Penanganan Sengketa Digital: Organisasi profesi harus menyediakan panduan bagi

notaris dalam menghadapi sengketa akta elektronik.

Dengan optimalisasi ini, Ikatan Notaris Indonesia diharapkan mampu mengawal anggotanya bertransformasi dari praktik konvensional menuju digital notary yang handal, efisien, dan tetap menjaga keluhuran martabat jabatan.

E. Sistem Pelaporan Online

Pengawasan proaktif dilakukan melalui transformasi digital untuk memantau pelanggaran wilayah jabatan notaris secara sistematis.

Sistem pelaporan online notaris di era digital, seperti SIMPALNOT dan SIEMON, mengoptimalkan transparansi dan efisiensi melalui pelaporan bulanan, monitoring, serta pengaduan berbasis elektronik yang terintegrasi ke Kementerian Hukum dan HAM. Inovasi ini mendukung Cyber Notary, mempercepat layanan, serta mempermudah pengawasan melalui data real-time.

Sistem Pelaporan dan Layanan Digital Utama terbagi menjadi:

a. SIMPALNOT & SIEMON: Aplikasi untuk membuat laporan bulanan ke majelis pengawas daerah dan sistem monitoring notaris yang efektif serta terintegrasi.
b. Cyber Notary: Inovasi digitalisasi akta, penyimpanan protokol secara elektronik, serta tanda tangan dan segel tersertifikasi yang aman.
c. Aplikasi PASTI: Digunakan di Kanwil Kemenkumham DKI Jakarta untuk memperkuat akuntabilitas digital dan pengawasan notaris.
d. Portal AHU Online: Digunakan untuk mengecek profil dan keterdaftar notaris secara resmi.

Manfaat dan Dampak di Era Digital, seperti:

a. Efisiensi Tinggi: Mempercepat proses pembuatan dan penandatanganan dokumen serta mengurangi birokrasi.
b. Transparansi & Keamanan: Pengawasan menjadi lebih terstandar, serta menjaga integritas dokumen melalui tanda tangan elektronik.

c. Penghematan Biaya: Mengurangi biaya perjalanan dan penyimpanan dokumen fisik.
d. Aksesibilitas: Memungkinkan notarisasi jarak jauh tanpa kendala geografis.

Sistem ini memindahkan paradigma pengawasan dari manual ke digital, memastikan notaris profesional dan akuntabel di era modern.

F. Tujuan dari modernisasi.

Tujuan untuk meningkatkan akuntabilitas, transparansi, dan efektivitas pembinaan, sehingga notaris dapat menjalankan tugasnya secara profesional dan bertanggung jawab di era digital.

Modernisasi dan digitalisasi dalam pembinaan notaris di Indonesia bertujuan untuk menciptakan ekosistem layanan hukum yang lebih modern, cepat, dan aman, sejalan dengan era Society 5.0. Berikut adalah tujuan utama dari modernisasi tersebut:

a. Peningkatan Akuntabilitas dan Transparansi: Digitalisasi (seperti AHU Online, e-Notary, dan Cyber Notary) memungkinkan pengawasan

yang lebih baik, efisien, dan transparan terhadap kinerja notaris.

b. Efektivitas Pembinaan dan Pengawasan: Berdasarkan Permenkumham Nomor 24 Tahun 2025, digitalisasi pengawasan (layanan MPDN) dilakukan untuk memperketat pengawasan, meningkatkan profesionalisme, dan memastikan kepatuhan notaris terhadap kode etik.
c. Profesionalisme di Era Digital: Notaris didorong untuk menguasai teknologi (digital literacy) agar tetap mampu menjaga kepercayaan publik (public trust) sebagai custodian of justice di tengah arus disrupsi digital.
d. Peningkatan Layanan Hukum: Modernisasi mengurangi kendala geografis, mempercepat waktu proses, dan menurunkan biaya, sehingga memberikan kemudahan bagi masyarakat dalam mengakses layanan notaris.
e. Penguatan Hukum dan Keamanan: Penggunaan teknologi seperti tanda tangan

digital, biometrik, dan blockchain memastikan keamanan data dan integritas akta otentik.

Dengan adanya Permenkumham Nomor 24 Tahun 2025 dan kebijakan terkait, Ikatan Notaris Indonesia (INI) semakin mempertegas peran notaris dalam memberikan perlindungan dan kepastian hukum yang adaptif terhadap perkembangan teknologi.

BAB IV.
VALIDITAS HUKUM AKTA ELEKTRONIK

Masih adanya perdebatan hukum mengenai kekuatan pembuktian akta otentik yang dibuat secara elektronik di hadapan pengadilan, mengingat yurisprudensi Indonesia yang masih bertumpu pada bukti fisik.

Akta elektronik yang dibuat notaris memiliki validitas hukum yang kuat melalui tanda tangan digital dan sertifikat elektronik, yang didukung oleh UU ITE dan PP 71/2019. Meskipun menjanjikan

efisiensi, penerapannya masih menghadapi tantangan yuridis, karena UU Jabatan Notaris (UUJN) secara konvensional mengharuskan kehadiran fisik. Keabsahan akta elektronik memerlukan harmonisasi aturan lebih lanjut agar memenuhi syarat formil dan autentik.

A. **Dasar Hukum & Validitas:**

UU No. 19 Tahun 2016 (perubahan UU ITE) dan PP No. 71 Tahun 2019 memberikan legalitas pada dokumen elektronik dan tanda tangan digital.

Akta elektronik di Indonesia sah secara hukum sebagai alat bukti berdasarkan UU ITE, selama menggunakan tanda tangan elektronik tersertifikasi dan memenuhi syarat sah perjanjian (Pasal 1320 KUHPerdata). Meskipun UUJN masih menitikberatkan fisik, peraturan teknis seperti Permenkumham No. 24 Tahun 2021 memfasilitasi legalitasnya.

Berikut adalah poin-poin mengenai validitas hukum akta elektronik:

a. Dasar Hukum:

- UU No. 1 Tahun 2024 (Perubahan UU ITE): Mengakui dokumen dan tanda tangan elektronik sebagai alat bukti yang sah.
- KUHPerdata (Pasal 1320): Syarat sahnya perjanjian tetap berlaku (kesepakatan, kecakapan, hal tertentu, kausa yang halal).
- Permenkumham No. 24 Tahun 2021: Mengatur penggunaan dokumen elektronik dan Tanda Tangan Elektronik (TTE) dalam layanan jasa hukum.
- PP No. 71 Tahun 2019: Penyelenggaraan sistem dan transaksi elektronik.

b. Validitas dan Syarat:
   - Otentikasi & Integritas: Tanda tangan digital harus tersertifikasi untuk menjamin identitas penandatangan (otentikasi) dan mencegah perubahan isi dokumen (integritas).
   - Kekuatan Pembuktian: Sesuai UU ITE Pasal 5 ayat 2, hasil cetak/dokumen elektronik merupakan alat bukti hukum yang sah.
   - Tantangan Hukum: Saat ini, akta otentik (notariil) masih menghadapi kendala regulasi fisik, namun tanda tangan elektronik (TTE) telah diakui sah.

Keabsahan akta elektronik sangat bergantung pada penerapan TTE yang tersertifikasi dan pemenuhan unsur-unsur dalam hukum perdata.

B. **Tantangan Konvensional:**

UUJN (UU No. 30/2004 dan No. 2/2014) menegaskan akta harus berbentuk fisik dan dibacakan langsung. Tanda tangan elektronik belum secara eksplisit diatur untuk akta autentik, sehingga ada risiko ketidakpastian hukum.

Validitas hukum akta elektronik di Indonesia telah diakui secara hukum melalui UU Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya (UU No. 1 Tahun 2024), namun menghadapi tantangan konvensional yang signifikan karena bertentangan dengan prinsip-prinsip hukum perdata kolonial yang masih berlaku, seperti keharusan kehadiran fisik (Pasal 1868 KUHPerdata). Akta elektronik, terutama yang menggunakan tanda tangan elektronik tersertifikasi, sah secara hukum, tetapi kedudukannya sebagai akta otentik sering dipertanyakan dalam praktik kenotariatan konvensional.

Berikut adalah analisis validitas hukum akta elektronik dan tantangan konvensionalnya:

1. Dasar Hukum Validitas Akta Elektronik

   UU ITE: Pasal 5 ayat (1) UU ITE menetapkan bahwa informasi/dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

   Tanda Tangan Elektronik (TTE): TTE yang tersertifikasi memiliki kekuatan hukum yang setara dengan tanda tangan basah, selama memenuhi persyaratan teknis (Pasal 11 UU ITE).

   Cyber Notary: Peraturan Menteri Hukum dan HAM Nomor 24 Tahun 2021 mengatur tata cara penggunaan dokumen elektronik dan tanda tangan elektronik dalam layanan jasa hukum, yang memfasilitasi peran notaris dalam era digital.

2. Tantangan Konvensional (Hambatan)

   Akta elektronik menghadapi tantangan besar karena hukum kenotariatan (UUJN) dan hukum perdata masih berakar pada dokumen fisik:

Keharusan Kehadiran Fisik (Pasal 1868 KUHPerdata): Hukum perdata Indonesia (civil law) menuntut notaris dan para pihak hadir secara fisik untuk penandatanganan akta otentik.

Resistensi Konvensional: Hakim atau praktisi hukum yang konservatif mungkin enggan menerima bukti non-fisik (digital) jika terjadi sengketa, menganggap akta elektronik tidak memiliki kekuatan otentik yang sama dengan akta kertas.

Cacat Hukum: Akta elektronik yang dibuat tanpa memenuhi persyaratan ketat (contoh: tidak menggunakan TTE tersertifikasi) berisiko turun nilainya menjadi "akta di bawah tangan".

Keamanan dan Keaslian: Kekhawatiran akan pemalsuan, peretasan, dan manipulasi data elektronik masih menjadi tantangan, meskipun sistem digitalisasi terus dikembangkan.

3. Kekuatan Pembuktian

Meskipun diakui, akta elektronik dapat dilumpuhkan dengan adanya bukti lawan

(tegenbewijs) di persidangan. Kekuatan pembuktiannya sangat bergantung pada:

- Sertifikasi TTE yang digunakan.
- Pemahaman hakim terhadap teknologi.
- Pemenuhan prinsip cyber notary yang diakui pemerintah.

Kesimpulan

Validitas hukum akta elektronik di Indonesia sah, tetapi masih berada dalam tahap transisi. Akta tersebut sering dianggap memiliki kekuatan "akta di bawah tangan" jika belum memenuhi standar otentikasi konvensional, sehingga memerlukan harmonisasi peraturan (UUJN) dan pemahaman hukum yang lebih adaptif agar memiliki kekuatan pembuktian yang setara dengan akta konvensional.

C. **Aspek *Cyber Notary*:**

Penggunaan *cyber notary* bertujuan meningkatkan efisiensi dan keamanan, namun wajib mempertahankan prinsip kehati-hatian, verifikasi identitas (non-repudiation), dan otentikasi yang ketat.

Akta elektronik dalam konsep cyber notary di Indonesia valid secara hukum jika memenuhi standar keamanan tinggi, autentikasi biometrik, dan tanda tangan digital, sesuai UU ITE dan UUJN. Meskipun sah, akta elektronik masih menghadapi kendala regulasi yang mewajibkan kehadiran fisik para pihak, sehingga berpotensi dianggap sebagai akta di bawah tangan daripada akta autentik penuh.

a. Validitas Hukum dan Aspek Cyber Notary:
   Dasar Hukum: UU Jabatan Notaris (UUJN) Pasal 15 ayat (3) memberi ruang untuk sertifikasi transaksi elektronik (Cyber Notary), namun belum diatur rinci dalam peraturan pelaksana.
   Aspek Cyber Notary: Proses ini mencakup autentikasi dokumen, tanda tangan digital (TTE) yang sah, dan penyimpanan aman, dengan prinsip kehati-hatian tinggi.
b. Tantangan: Pasal 16 ayat (1) huruf m UUJN masih mewajibkan kehadiran fisik dan pembacaan akta secara langsung.
c. Status Akta: Jika akta elektronik dibuat tanpa memenuhi syarat fisik (kehadiran) menurut UUJN, akta tersebut berpotensi turun derajat

menjadi akta di bawah tangan, meskipun tanda tangan digitalnya valid.

d. Peluang: Penggunaan teknologi GPS dan verifikasi identitas berbasis biometrik dapat meningkatkan validitas dan keamanan akta elektronik.

Regulasi yang lebih komprehensif diperlukan untuk menyelaraskan UUJN dengan perkembangan digital guna menjamin kepastian hukum autentikasi elektronik.

D. **Validitas Alat Bukti:**

Akta elektronik memiliki kekuatan pembuktian yang kuat, setara dengan dokumen fisik, selama disahkan melalui prosedur elektronik dan menggunakan tanda tangan digital yang tersertifikasi.

Akta elektronik memiliki validitas hukum sebagai alat bukti yang sah dan mengikat di Indonesia, setara dengan dokumen tertulis konvensional, sebagaimana diatur dalam UU ITE (Nomor 11 Tahun 2008 jo. UU 19/2016 jo. UU 1/2024). Dokumen ini sah selama dapat diakses, ditampilkan,

dijamin keutuhannya (integritas data), dan dapat dipertanggungjawabkan.

Poin Penting Validitas Akta Elektronik:

Landasan Hukum: Pasal 5 ayat (1) dan (2) UU ITE menegaskan informasi/dokumen elektronik merupakan perluasan alat bukti yang sah.

Syarat Keabsahan: Akta elektronik harus memenuhi persyaratan teknis seperti autentikasi, integritas data, dan menggunakan tanda tangan elektronik yang tersertifikasi untuk menjamin keasliannya.

Kedudukan: Dalam perkara perdata, ini adalah alat bukti surat/tertulis. Dalam pidana, ini termasuk alat bukti perluasan yang sah menurut hukum acara.

Tanda Tangan Elektronik: Menjadi elemen krusial untuk memastikan validitas dan tanggung jawab para pihak dalam perjanjian/akta elektronik.

Akta elektronik tidak terbatas pada email, tetapi mencakup hasil cetakan, rekaman, dan dokumen digital lain yang terkait dengan transaksi atau tindak pidana.

BAB V.
ADAPTASI TEKNOLOGI (AI & BLOCKCHAIN)

Munculnya teknologi baru seperti *Artificial Intelligence* dan *Blockchain* memaksa profesi notaris untuk mereformasi kode etik agar tetap relevan dalam menjaga moralitas jabatan di tengah otomatisasi layanan hukum.

Adaptasi teknologi *Artificial Intelligence* (AI) dan *Blockchain* dalam profesi notaris di Indonesia merupakan keniscayaan menuju era *cyber notary*. Teknologi ini tidak menggantikan peran manusia secara penuh, melainkan berfungsi sebagai alat bantu untuk meningkatkan efisiensi, keamanan, dan transparansi dalam pembuatan akta serta penyimpanan dokumen.

A. Adaptasi Artificial Intelligence (AI) dalam Kenotariatan.

AI digunakan untuk otomatisasi tugas-tugas administratif dan repetitif.

- **Penyusunan Draf Otomatis:** AI membantu menyusun draf kontrak atau akta secara cepat, yang kemudian diverifikasi oleh notaris. Penyusunan draf otomatis dalam praktik notaris di Indonesia kini semakin berkembang seiring dengan digitalisasi hukum dan penggunaan Kecerdasan Buatan (AI) untuk meningkatkan efisiensi dan akurasi. Teknologi ini memungkinkan notaris menghasilkan draf akta dalam hitungan menit, bukan hari.

- **Analisis Dokumen:** AI mampu menganalisis dokumen hukum dalam jumlah besar dan mendeteksi kesalahan atau ketidakkonsistenan data. Notaris adalah pejabat umum berwenang membuat akta autentik dan dokumen hukum, yang bertindak berdasarkan UUJN (UU No. 2 Tahun 2014) untuk menjamin kepastian tanggal, para pihak, dan isi perjanjian. Analisis dokumen notaris mencakup verifikasi identitas, legalitas substansi, serta kewajiban menyimpan minuta akta. Pelanggaran dapat berakibat sanksi perdata, administratif, atau pidana.

- **Efisiensi Pelayanan:** Aplikasi berbasis AI memungkinkan pemrosesan dokumen yang

lebih cepat, mengurangi waktu tunggu bagi klien. Efisiensi pelayanan notaris di Indonesia terus ditingkatkan melalui digitalisasi, seperti penggunaan tanda tangan elektronik, arsip digital, dan sistem pelaporan online (e-protocol/SIMPALNOT) untuk mempercepat proses administratif, mengurangi kertas, dan meminimalisir kesalahan manual. Langkah ini meningkatkan transparansi, mempercepat integrasi dengan lembaga hukum (e-court), dan meningkatkan akurasi data. Meskipun demikian, diperlukan pembaruan regulasi untuk mendukung keabsahan penuh akta digita

- **Batasan:** AI berfungsi sebagai alat bantu (*tool*), bukan pengganti notaris manusia yang memiliki kewenangan hukum formal. Batasan mengenai notaris di Indonesia diatur terutama dalam UU No. 2 Tahun 2014 (perubahan atas UU No. 30 Tahun 2004) tentang Jabatan Notaris, mencakup batasan usia maksimal 70 tahun, wilayah jabatan setingkat provinsi, larangan rangkap jabatan (seperti advokat, ASN, pegawai BUMN/BUMD/swasta), serta wajib merahasiakan isi akta. Notaris harus berdomisili

di kabupaten/kota, namun kewenangannya meliputi seluruh wilayah provinsi tempat kedudukannya.

B. Adaptasi Blockchain dalam Kenotariatan.

Blockchain menawarkan teknologi penyimpanan data yang aman, transparan, dan tidak dapat diubah (*immutable*).

- **Notarisasi Digital & Timestamping:** Blockchain memastikan keaslian dokumen digital dan memberikan stempel waktu (*timestamp*) yang jelas, melindungi dari pemalsuan. Notarisasi digital dan timestamping merupakan komponen utama dari konsep Cyber Notary di Indonesia, yang memungkinkan notaris untuk memproses, menandatangani, dan menyimpan dokumen secara elektronik dengan kekuatan hukum yang sah. Teknologi ini bertujuan meningkatkan efisiensi, keamanan, dan aksesibilitas layanan notaris di era digital.

- **Smart Contracts:** Notaris dapat berperan sebagai *trusted third party* dalam verifikasi *smart contract* yang direkam di blockchain, memastikan kontrak digital tersebut valid secara hukum. Smart contracts (kontrak pintar) adalah program komputer berbasis blockchain yang mengeksekusi perjanjian secara otomatis tanpa perantara, menawarkan efisiensi tinggi, keamanan kriptografi, dan biaya lebih rendah. Dalam dunia notaris, smart contracts dapat digunakan untuk notarisasi digital, sewa, dan transaksi properti. Meski otomatis, peran notaris tetap krusial sebagai trusted third party untuk memverifikasi identitas, kepatuhan hukum, dan memberikan kepastian hukum.

- **Keamanan Data:** Setiap blok dalam blockchain dihubungkan dengan enkripsi, membuat data transaksi akta tidak bisa diubah atau dihapus tanpa konsensus. Keamanan data di lingkungan notaris wajib mematuhi UU Jabatan Notaris (UUJN) dan UU Perlindungan Data Pribadi (UU PDP), di mana notaris bertindak sebagai Pengendali Data Pribadi yang bertanggung jawab atas kerahasiaan akta. Pada era digital,

notaris harus menggunakan sistem enkripsi, autentikasi ganda (2FA), penyimpanan awan bersertifikat (ISO 27001), dan tanda tangan elektronik resmi untuk mencegah kebocoran data.

C. Dampak terhadap Peran Notaris (Cyber Notary)

- **Peralihan ke Digital:** Notaris di Indonesia diwajibkan mengadopsi teknologi digital untuk verifikasi identitas, pembuatan dokumen, dan penyimpanan arsip elektronik. Peralihan notaris ke ranah digital (Cyber Notary) di Indonesia merupakan transformasi mutlak untuk meningkatkan efisiensi, kecepatan, dan akurasi layanan hukum di era modern. Proses ini melibatkan transisi dari metode konvensional berbasis kertas menuju sistem elektronik terintegrasi, seperti penggunaan AHU Online untuk pengesahan badan hukum.

    - **Peningkatan Integritas:** Penggunaan teknologi seperti tanda tangan digital berbasis biometrik meningkatkan keamanan dan kepastian hukum. Penerapan Cyber Notary (notaris elektronik) di Indonesia

membawa dampak signifikan terhadap pergeseran peran notaris dari metode konvensional ke digital, yang secara langsung menuntut peningkatan integritas dan kehati-hatian (prinsip kehati-hatian) dalam menjaga otentisitas akta. Integritas notaris dalam era cyber bukan lagi sekadar kehadiran fisik, melainkan jaminan keamanan data, validasi identitas digital, dan kerahasiaan dalam sistem hukum elektronik.

- **Tantangan Hukum & Etika:** Notaris harus tetap mematuhi prinsip kehati-kehati-hatian, kerahasiaan data, dan kode etik profesi meskipun menggunakan AI. Penerapan Cyber Notary di Indonesia menghadapi tantangan hukum utama berupa kewajiban fisik (tatap muka) dalam UUJN yang berpotensi menurunkan akta digital menjadi akta di bawah tangan. Etika profesi terancam oleh risiko kebocoran data, siber, dan sulitnya memverifikasi identitas asli para pihak. Diperlukan reformasi UUJN agar mengakomodasi tanda tangan elektronik dan

menjamin kepastian hukum, sembari menjaga integritas etika notaris.

D. Dasar Hukum di Indonesia

- **UU No. 2 Tahun 2014 (UUJN):** Mengatur dasar jabatan notaris. UU No. 2 Tahun 2014 tentang Perubahan atas UU No. 30 Tahun 2004 tentang Jabatan Notaris (UUJN-P) adalah landasan hukum utama yang mengatur profesi notaris di Indonesia, yang berfokus pada peningkatan kepastian, perlindungan hukum, dan profesionalisme. UU ini memperketat tanggung jawab notaris, mengatur kewajiban, larangan, serta sanksi administratif bagi notaris.

- **UU ITE (Nomor 19 Tahun 2016):** Mengatur informasi dan transaksi elektronik. UU ITE No. 19 Tahun 2016 merupakan perubahan atas UU No. 11 Tahun 2008, yang menjadi dasar hukum utama aktivitas di ruang digital Indonesia. UU ini mengatur tata cara penggunaan teknologi, transaksi elektronik, dan sanksi pidana atas penyebaran informasi

bohong (hoaks), ujaran kebencian SARA, serta intersepsi ilegal.

- **UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022):** Penting dalam pengelolaan data digital. UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah payung hukum komprehensif utama di Indonesia yang disahkan pada 17 Oktober 2022 (berlaku penuh 17 Oktober 2024) untuk melindungi hak privasi individu atas data pribadi dari pemrosesan tidak sah oleh pihak ketiga. Undang-undang ini menjamin keamanan data, mengatur sanksi administratif/pidana, serta memberikan hak bagi subjek data.

- **PP No. 28 Tahun 2025:** Mengakui blockchain sebagai bagian dari infrastruktur digital nasional. Peraturan Pemerintah (PP) Nomor 28 Tahun 2025 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko, yang berlaku mulai Juni 2025, menggantikan PP Nomor 5 Tahun 2021. PP ini mengintegrasikan seluruh izin dasar dan sektoral melalui sistem OSS RBA,

memberikan kepastian hukum, mempercepat proses melalui Service Level Agreement (SLA), serta menyesuaikan aturan dengan Undang-Undang Cipta Kerja untuk menyederhanakan birokrasi bagi UMKM maupun pelaku usaha besar.

Secara keseluruhan, notaris masa depan diharapkan menjadi "Notaris Digital" yang terampil menggunakan teknologi untuk meningkatkan akuntabilitas dan efisiensi, tanpa melepaskan tanggung jawab hukumnya.

DAFTAR PUSTAKA

Akbar, Muhammad Rizqy Ali, Soesi Idayanti, and Bha'iq Roza Rakhmatullah. Due Diligence oleh Notaris dalam Pendaftaran Jaminan Fidusia secara Online. Penerbit NEM, 2024.

Akbar, Muhammad Rizqy Ali, Soesi Idayanti, and Bha'iq Roza Rakhmatullah. Due Diligence oleh Notaris dalam Pendaftaran Jaminan Fidusia secara Online. Penerbit NEM, 2024.

Emirzon, H. Joni, and M. SH. Pembaharuan Hukum Nasional Indonesia di Era Industri 4.0 (Beberapa Catatan UU Cipta Kerja)-Rajawali Pers. PT. RajaGrafindo Persada, 2023.

HS, H. Salim, and MS SH. Teknik Pembuatan Akta Badan Usaha di Era Digital. Sinar Grafika, 2021.

Katharina, Riris. Pelayanan publik & pemerintahan digital Indonesia. Yayasan Pustaka Obor Indonesia, 2021.

Kusmiati, N. Ike, M. SH, and S. H. Elly Ruslina. HUKUM INVESTASI DALAM KONSENTRASI EKONOMI. Greenbook Publisher, 2025.

Muta'ali, Luthfi. Dinamika peran sektor pertanian dalam pembangunan wilayah di Indonesia. Ugm Press, 2019.

Nugraheni, Wahyu Pudji, et al. Public Private Mix dalam Layanan Kesehatan. CV Eureka Media Aksara, 2025.

Press, U. G. M. Tata Kelola Penanganan COVID-19 di Indonesia: Kajian Awal. UGM PRESS, 2024.

Rustiyana, Rustiyana, et al. Pemanfaataan AI dalam Keamanan Siber. PT. Sonpedia Publishing Indonesia, 2025.

Waluyo, Bambang. Penegakan hukum di Indonesia. Sinar Grafika, 2022.

Wibowo, Afrizal Mukti, et al. Perkembangan Hukum Keperdataan di Era Digital. Sada Kurnia Pustaka, 2024.

NOTARIS DI ERA DIGITAL



Penerbit:
CV. Kimfa Mandiri
JL. Raya Ciapus Rt 01 Rw 06 Desa. Ciapus Kec. Banjaran Kab. Bandung 40377
Telp: 022-85945637 - 085314983618 – 081220816826
Website: kimfamandiri.or.id
E-mail: kimfamandiriks@gmail.com

ISBN 978-634-7487-05-6