vedapraxis

UU PDP DALAM TUNTUTAN *DIGITAL TRUST*: NIAT BAIK ATAU SEKADAR LIPSTIK?

Di era digital yang penuh dinamika, pelindungan data pribadi menjadi isu krusial yang harus ditangani secara serius oleh para pemangku kepentingan, terutama oleh negara sebagai pembuat dan pengelola regulasi. Keseriusan ini perlu ditunjukkan dengan langkah-langkah konkret dan efektif, sehingga dampak positifnya dapat dirasakan oleh masyarakat sebagai *stakeholder* utama di negeri ini.

Dapat kita rasakan bersama, kehadiran teknologi informasi dan komunikasi membawa dampak signifikan terhadap cara kita menyimpan, mengelola, dan mendistribusikan data. Namun, dengan berbagai keuntungan yang ditawarkan, muncul pula tantangan besar, terutama terkait dengan pelindungan data pribadi. Di Indonesia, isu ini semakin mendapat perhatian setelah disahkannya Undang-Undang Pelindungan Data Pribadi (UU PDP) pada 20 September 2022. Tak lama berselang, muncullah kasus serangan *ransomware* yang menimpa Pusat Data Nasional (PDN). Artikel ini akan membahas tentang UU PDP, *data governance,* dan *digital trust* dengan merujuk pada kasus-kasus terkini di Indonesia, serta mengeksplorasi hipotesis apakah hadirnya UU PDP merupakan niat baik pemerintah yang efektif dalam mendorong digital trust masyarakat atau hanya sebatas 'lipstik' atau pencitraan semata.

Undang-Undang Pelindungan Data Pribadi

UU PDP disahkan pada tahun 2022 sebagai upaya Pemerintah Indonesia untuk memberikan perlindungan hukum terhadap data pribadi warga negara. Undang-undang ini mengatur berbagai aspek terkait pengumpulan, pengolahan, penyimpanan, dan distribusi data pribadi. Sebelumnya, pelindungan data pribadi di Indonesia masih bersifat parsial dan tersebar dalam berbagai peraturan perundang-undangan yang berbeda, sehingga menimbulkan kekosongan hukum dan ketidakpastian bagi pemilik data.

UU PDP bertujuan untuk memberikan kepastian hukum bagi individu terkait hak-hak mereka atas data pribadi yang dimiliki serta memberikan panduan bagi penyelenggara sistem elektronik dalam mengelola data pribadi secara aman dan bertanggung jawab. Dengan adanya undang-undang ini, diharapkan masyarakat Indonesia dapat lebih percaya dalam bertransaksi dan beraktivitas di dunia digital.

Hipotesis: Niat Baik atau Lipstik?

Dari serangkaian peristiwa seputar data, pengelolaan dan apa saja yang dilakukan oleh Pemerintah dalam rangka melakukan pelindungan data, wajar ketika sebagian kalangan melakukan penilaian. Tulisan ini juga mengajak kita untuk sedikit berhipotesis; apakah Pemerintah sudah cukup menunjukkan keseriusan dalam pengelolaan data masyarakat. Secara sederhana dapat kita pertanyakan, apakah upaya Pemerintah hingga saat ini adalah niat baik atau sekadar 'lipstik'?

Jika ini adalah Niat Baik

Jika UU PDP benar-benar merupakan wujud niat baik pemerintah yang efektif, maka setidaknya ada beberapa kondisi yang harus terpenuhi:

1. **SDM Teknologi dan Data yang memadai**

   Pemerintah perlu berinvestasi lebih banyak dalam pelatihan dan pengembangan sumber daya manusia (SDM) di bidang teknologi dan keamanan data. Kualitas SDM sangat penting dalam memastikan pengelolaan dan pelindungan data secara lebih efektif, terencana dan sistematis untuk efektivitas pelindungan data di Indonesia. Salah satu indikasi penting efektifnya pengelolaan dan pelindungan data adalah minimalnya risiko kebocoran data dan serangan siber. Tanpa SDM yang mumpuni, kebijakan pelindungan data seperti UU PDP tidak akan efektif karena implementasinya akan lemah dan rentan terhadap berbagai ancaman. Pendidikan dan pelatihan yang berkelanjutan dan terkoordinasi terkait Teknologi Informasi (TI) dan keamanan siber diperlukan untuk memastikan bahwa SDM dapat menangani kompleksitas dan dinamika ancaman digital yang terus berkembang.

2. **Penegakan Hukum yang Konsisten**

   Pemerintah harus menunjukkan komitmen yang kuat dalam menegakkan UU PDP. Ini termasuk melakukan penyelidikan dan memberikan sanksi tegas terhadap pelanggaran data pribadi, dengan menghindari banyak kompromi baik atas nama iklim investasi atau pertumbuhan ekonomi. Penegakan hukum yang konsisten akan membangun kepercayaan masyarakat bahwa pemerintah serius dalam melindungi data pribadi mereka.

3. **Sosialisasi dan Edukasi yang Luas**

   Pemerintah harus aktif dalam menyosialisasikan UU PDP kepada masyarakat dan organisasi. Edukasi tentang hak-hak pemilik data dan kewajiban pengendali data harus dilakukan secara terus-menerus. Masyarakat yang lebih paham teknologi dan keamanan data juga dapat menjadi pilar pendukung pelindungan data. Selain itu, pemberian pemahaman dan informasi yang valid kepada masyarakat tentang upaya Pemerintah melakukan pelindungan data akan menambah kepercayaan yang signifikan, bahwa upaya yang dilakukan oleh Pemerintah serius dan akan berdampak positif bagi keamanan data masyarakat.

4. **Infrastruktur Keamanan yang Memadai**

   Pemerintah harus berinvestasi dalam meningkatkan keamanan infrastruktur digitalnya. Ini termasuk penguatan sistem keamanan di PDN dan lembaga-lembaga pemerintah lainnya. Infrastruktur yang kuat akan mengurangi risiko kebocoran data dan meningkatkan kepercayaan masyarakat.

5. **Kolaborasi dengan Sektor Swasta**

   Pemerintah harus bekerja sama dengan sektor swasta untuk memastikan kepatuhan terhadap UU PDP. Sektor swasta, terutama perusahaan teknologi dan penyedia layanan digital, memiliki peran penting dalam melindungi data pribadi pengguna mereka. Kolaborasi yang baik akan menciptakan ekosistem digital yang lebih aman dan terpercaya.

Jika ini adalah Lipstik atau Pencitraan

Sebaliknya, jika UU PDP hanya sebatas 'lipstik' atau pencitraan, beberapa kondisi berikut mungkin dapat kita saksikan:

1. **Kompetensi SDM Teknologi dan Data Rendah**

   Pada suatu wawancara di stasiun televisi nasional, bulan Juni 2024, Wakil Rektor Institut Teknologi Tangerang Selatan (ITTS) Profesor Ono Purbo menyampaikan fakta yang cukup mengejutkan, bahwa dari 21.000 peserta kursus gratis terkait keamanan data yang beliau selenggarakan, hanya 22 orang yang dianggap lulus dan memiliki kecakapan yang memadai. Ini menunjukkan perlunya peningkatan kualitas pendidikan dan pelatihan di bidang ini untuk memastikan keberhasilan implementasi UU PDP. Jika tidak ada upaya untuk meningkatkan kapasitas dan keterampilan SDM di bidang teknologi dan data, terutama di lembaga pemerintahan, maka penerapan UU PDP akan kurang efektif. SDM yang tidak terlatih dan tidak kompeten akan menghambat implementasi kebijakan dan prosedur yang diperlukan untuk melindungi data pribadi.

2. **Tantangan pada Upaya Penegakan Hukum**

   Jika penegakan UU PDP lemah dan pelanggaran data pribadi tidak ditindak secara tegas, masyarakat akan menganggap bahwa Pemerintah tidak serius dalam melindungi data pribadi mereka. Hal ini akan menurunkan tingkat kepercayaan masyarakat terhadap pemerintah dan UU PDP itu sendiri.

3. **Minimnya Sosialisasi dan Edukasi**

   Jika Pemerintah tidak melakukan sosialisasi dan edukasi yang memadai, masyarakat dan organisasi mungkin tidak memahami hak-hak dan kewajiban mereka terkait data pribadi. Ketidaktahuan ini akan mengurangi efektivitas UU PDP dan menciptakan ketidakpercayaan.

4. **Infrastruktur Keamanan yang Lemah**

   Jika infrastruktur keamanan digital pemerintah tidak ditingkatkan, risiko kebocoran data akan tetap tinggi. Kejadian seperti serangan ransomware di PDN akan terus terjadi, menunjukkan bahwa pemerintah tidak mampu melindungi data pribadi secara efektif. Presiden RI Joko Widodo mengatakan bahwa saat ini terdapat 27 ribu aplikasi milik kementerian, lembaga dan pemerintah daerah yang berjalan sendiri-sendiri, sehingga tidak sinkron dan bahkan tumpang tindih. Jika tak dikoordinasikan dan dilakukan maintenance dengan baik, banyaknya aplikasi ini juga berpotensi mengakibatkan kerentanan terhadap serangan siber dan kebocoran data. Hal ini menunjukkan bahwa meskipun ada banyak upaya untuk membangun infrastruktur digital, efektivitas dan keamanan dari aplikasi-aplikasi ini masih jauh dari memadai sehingga mengurangi kepercayaan masyarakat terhadap kemampuan Pemerintah mengelola data pribadi dengan aman.

5. **Kurangnya Kolaborasi dengan Sektor Swasta**

   Jika Pemerintah tidak bekerja sama dengan sektor swasta, implementasi UU PDP akan menemui banyak tantangan. Sektor swasta yang tidak terlibat dalam proses pelindungan data pribadi akan menciptakan celah dalam sistem keamanan dan mengurangi kepercayaan masyarakat.

Data governance di Era Digital

Data governance yang baik adalah kunci dalam mengelola dan melindungi data pribadi di era digital. *Data governance* mencakup serangkaian proses, kebijakan, dan prosedur yang dirancang untuk memastikan bahwa data dikelola secara efektif, efisien, dan aman. Dengan *data governance* yang baik, organisasi dapat meminimalkan risiko kebocoran data, menjaga integritas data, dan memastikan ketersediaan data saat dibutuhkan.

Di Indonesia, implementasi *data governance* masih menghadapi berbagai tantangan. Banyak organisasi yang belum memiliki kebijakan dan prosedur *data governance* yang memadai. Selain itu, kesadaran akan pentingnya pelindungan data pribadi masih relatif rendah. Oleh karena itu, diperlukan upaya yang lebih besar untuk meningkatkan pemahaman dan kesadaran akan pentingnya *data governance,* baik di sektor publik maupun swasta.

Digital Trust: Membangun Kepercayaan di Era Digital

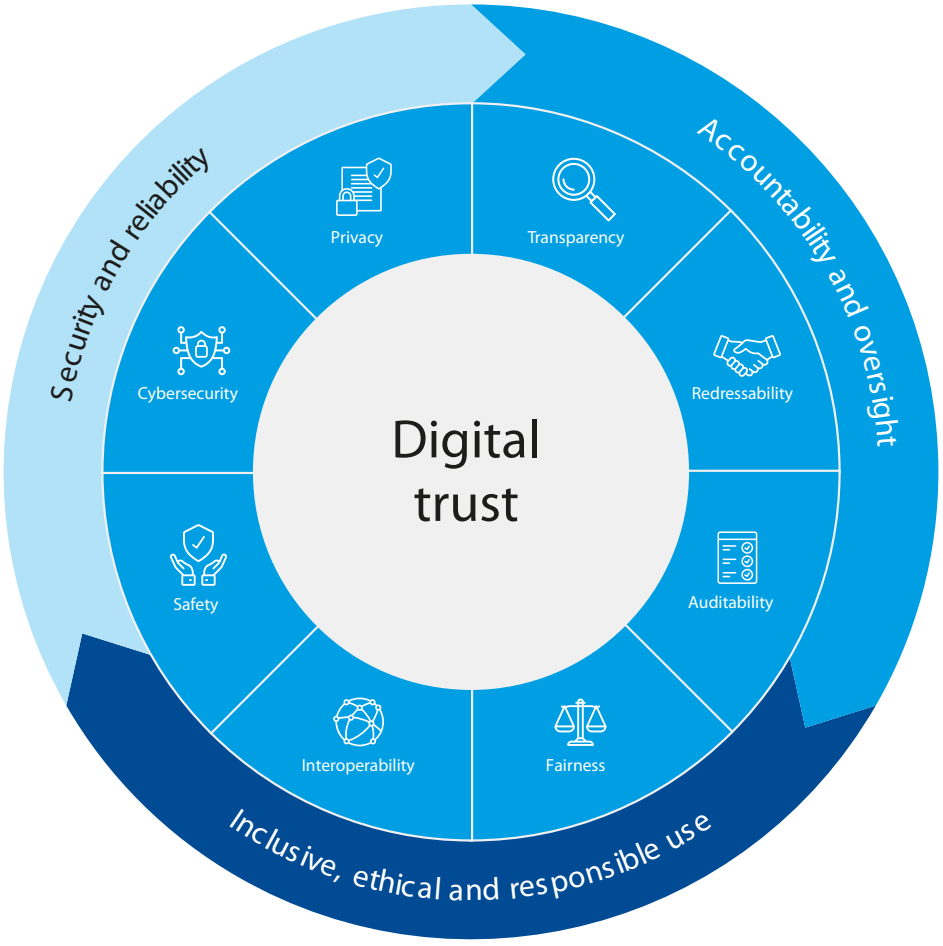
Kepercayaan digital atau *digital trust* merujuk pada tingkat kepercayaan yang diberikan individu atau organisasi terhadap sistem dan layanan digital. ISACA mendefinisikan *digital trust* sebagai tingkat kepercayaan secara utuh atas hubungan, interaksi, dan transaksi antara *supplier* atau *provider* dengan nasabah dalam konteks ekosistem digital.

Kepercayaan ini didasarkan pada keyakinan bahwa data pribadi mereka akan dilindungi, diolah dengan cara yang aman, dan tidak disalahgunakan. *Digital trust* sangat penting karena tanpa kepercayaan, individu akan ragu untuk bertransaksi dan berinteraksi di dunia digital, yang pada akhirnya dapat menghambat perkembangan ekonomi digital.

McKinsey & Company, dalam survei yang dirilis 12 September 2022, bahkan mengatakan bahwa konsumen sangat concern terhadap *digital trust*. Salah satu hasil dari survei tersebut mengatakan bahwa lebih dari separuh konsumen menaruh kepercayaan kepada perusahaan yang memiliki kebijakan yang jelas dalam melindungi data mereka.

Faktor-Faktor Digital Trust

Banyak pakar dan sejumlah penelitian yang mengerucutkan faktor-faktor yang mempengaruhi *digital trust,* salah satunya yang bersumber dari *world economic forum 4*, seperti dapat dilihat dari gambar di bawah ini:



Gambar:
Framework Digital Trust dari World Economic Forum, 2022

Berdasarkan ilustrasi di atas, faktor yang memengaruhi *digital trust* termasuk:

1. **Keamanan:** Sistem dan layanan digital harus mampu melindungi data pribadi dari ancaman keamanan, seperti serangan siber dan kebocoran data.
2. **Transparansi:** Organisasi harus transparan dalam mengelola data pribadi, termasuk memberikan informasi yang jelas tentang bagaimana data dikumpulkan, diolah, dan digunakan.
3. **Kepatuhan:** Mematuhi peraturan dan standar yang berlaku, seperti UU PDP, merupakan salah satu cara untuk membangun kepercayaan digital.
4. **Pengalaman Pengguna:** Memberikan pengalaman pengguna yang baik dan responsif juga dapat meningkatkan kepercayaan digital.

Semua faktor *digital trust* akhirnya bermuara pada kepercayaan masyarakat. Dalam dimensi layanan publik oleh Pemerintah, seberapa besar faktor-faktor digital trust ini dijaga dan dipertahankan, maka sebesar itu pula kepercayaan yang akan tertanam pada benak masyarakat. Semakin tinggi kepercayaan digital, maka semakin kredibel Pemerintah di mata masyarakat dalam mengelola dan melindungi kepentingan masyarakat terkait data.

Kasus Terkini: Serangan *Ransomware* di Pusat Data Nasional Sementara

Pada tahun 2023, Indonesia dikejutkan oleh serangan *ransomware* yang menimpa Pusat Data Nasional Sementara (PDNS). Serangan ini menyebabkan sejumlah besar data pribadi milik warga negara Indonesia terancam bocor. Para pelaku serangan berhasil mengenkripsi data pada PDNS dan menuntut tebusan dalam bentuk mata uang kripto untuk membuka kembali akses ke data tersebut.

Dinamika terjadi, di mana pada akhirnya, sang peretas memberikan kunci deskripsi atas data yang sebelumnya mereka sandera, tanpa tebusan uang sepeser pun. Hal ini cukup ganjil pada praktik *hacking* di dunia selama ini. Oleh karena itu, perlu upaya serius untuk mengungkap ihwal motif dan hakikat serangan yang sempat berpengaruh pada sejumlah layanan publik ini.

Terlepas dari misteri dan teori konspirasi atas hal tersebut, serangan *ransomware* ini menunjukkan betapa rentannya infrastruktur digital kita terhadap ancaman siber. Selain itu, kejadian ini juga menyoroti pentingnya penerapan *data governance* yang baik dan pelindungan data yang memadai. PDNS mengelola sejumlah besar data dari 282 layanan kementerian/lembaga negara. Hal ini tentu membuat posisi PDNS sangat strategis sekaligus riskan terhadap isu keamanan data. Upaya peretasan data sangat berpotensi terulang, sehingga perlu upaya yang sistematis, preventif, dan menyeluruh untuk melindungi data secara efektif.

Langkah Strategis dalam Mengatasi Ancaman Siber

Serangan siber terhadap *Domain Name System* (DNS) publik dapat menyebabkan gangguan besar dalam layanan internet, mengarah pada masalah akses, keamanan, dan integritas data. Untuk menanggulangi dan memitigasi risiko terkait serangan ini, Pemerintah dan masyarakat perlu mengambil tindakan strategis. Berikut adalah beberapa langkah yang dapat dilakukan:

Langkah-langkah Strategis untuk Pemerintah:

1. **Menetapkan Infrastruktur Keamanan**
   - ***Update dan Patch:*** Pastikan bahwa semua perangkat keras dan perangkat lunak yang terkait dengan DNS selalu diperbarui dengan *patch* keamanan terbaru.
   - **Redundansi dan Distribusi:** Implementasikan solusi DNS yang terdistribusi dan *redundant* untuk memastikan bahwa jika satu server terpengaruh, yang lain tetap berfungsi.
2. **Pengembangan Kebijakan dan Regulasi**
   - **Standar Keamanan:** Kembangkan dan terapkan standar keamanan untuk penyedia layanan DNS dan perusahaan teknologi yang relevan.
   - **Penegakan Hukum:** Perkuat hukum dan regulasi terkait kejahatan siber untuk menangani pelaku serangan secara efektif.
3. **Koordinasi dan Kerjasama**
   - **Kolaborasi Internasional:** Bekerja sama dengan negara lain untuk bertukar informasi tentang ancaman dan solusi keamanan siber.
   - **Koordinasi Antar Lembaga:** Tingkatkan koordinasi antara lembaga pemerintah yang bertanggung jawab atas keamanan siber dan penyedia layanan DNS.
4. **Pendidikan dan Kesadaran**
   - **Kampanye Kesadaran:** Lakukan kampanye untuk meningkatkan kesadaran tentang pentingnya keamanan DNS dan cara-cara melindungi diri dari serangan siber.
   - **Pelatihan:** Berikan pelatihan kepada pegawai pemerintah dan sektor terkait tentang penanganan dan pencegahan serangan siber.
5. **Pemantauan dan Respons**
   - **Sistem Pemantauan:** Implementasikan sistem pemantauan *real-time* untuk mendeteksi aktivitas mencurigakan dan serangan siber pada DNS.
   - **Tim Respons Insiden:** Bentuk tim khusus untuk menangani dan merespons insiden keamanan siber dengan cepat.

Langkah yang dapat diambil oleh Masyarakat:

1. **Pendidikan dan Kesadaran Individu**
    - **Penggunaan DNS yang Aman:** Gunakan layanan DNS yang aman dan tepercaya, seperti DNS yang mendukung DNS Security Extensions (DNSSEC).
    - **Kesadaran *Phishing:*** Waspadai potensi serangan *phishing* dan hindari mengeklik tautan atau membuka lampiran yang mencurigakan.
2. **Keamanan Jaringan Pribadi:**
    - **Pengaturan *Router:*** Pastikan *router* dan perangkat jaringan pribadi dikonfigurasi dengan benar dan menggunakan kata sandi yang kuat.
    - ***Firewall* dan Antivirus:** Gunakan *firewall* dan perangkat lunak antivirus untuk melindungi perangkat dari serangan siber.
3. **Pelaporan dan Kolaborasi**
    - **Pelaporan Insiden:** Segera laporkan setiap aktivitas mencurigakan atau potensi serangan kepada penyedia layanan internet atau otoritas terkait.
    - **Kolaborasi dengan Komunitas:** Bergabung dengan komunitas atau forum yang membahas keamanan siber untuk berbagi informasi dan strategi perlindungan.
4. **Pemeliharaan Perangkat**
    - ***Update* Perangkat Lunak:** : Pastikan perangkat lunak dan sistem operasi selalu diperbarui untuk menutup celah keamanan yang dapat dimanfaatkan oleh pelaku serangan.

Menanggulangi serangan siber terhadap PDNS memerlukan pendekatan *multi-layer* yang melibatkan berbagai pihak. Pemerintah harus fokus pada penguatan infrastruktur, kebijakan, dan koordinasi, sedangkan masyarakat harus berfokus pada praktik keamanan pribadi dan pelaporan insiden. Dengan upaya bersama, ancaman terhadap PDNS dapat diminimalkan dan ketahanan terhadap serangan siber dapat ditingkatkan.

Meskipun akhir dari drama penyanderaan data ini berakhir dengan penyerahan kunci deskripsi oleh palaku peretasan sendiri tanpa tebusan, tetap perlu proses panjang untuk melakukan pemulihan data tersebut, terutama untuk memastikan bahwa kunci deskripsi yang diberikan valid dan lengkap serta memastikan pemulihan semua data kembali pada kondisi normal.

Selain itu, ada potensi kondisi yang lebih kompleks, yakni bahwa *copy* data yang disandera sangat mungkin telah dibuat oleh peretas dan kita tidak tahu apa yang akan terjadi dengan hal ini. Pemerintah perlu memikirkan cara untuk memitigasi kondisi tersebut, sekaligus menciptakan rangkaian sistem pengendalian dan perlindungan agar hal ini tidak terjadi lagi di kemudian hari.

Kolaborasi dan Peran Sektor Swasta dalam Mengatasi Ancaman Siber

Selain pemerintah, sektor swasta juga memegang peran penting dalam menjaga keamanan data pribadi dan membangun kepercayaan digital. Perusahaan teknologi dan penyedia layanan digital harus mengambil langkah proaktif dalam melindungi data pengguna mereka. Ini termasuk investasi pada teknologi keamanan siber, pelatihan keamanan bagi karyawan, dan penerapan praktik terbaik dalam manajemen data. Kunci utama keberhasilan pengamanan data untuk ekosistem digital adalah kolaborasi. Semua pihak harus mengoptimalkan perannya dalam mewujudkan ekosistem digital yang aman, nyaman dan bermanfaat untuk semua. Menurut artikel Jawa Pos, Syahraki Syahrir, selaku Presiden ISACA Indonesia *Chapter* menjelaskan bahwa di tengah situasi dan kondisi keamanan siber Indonesia saat ini, ekosistem digital kita membutuhkan dukungan dari semua pihak, baik regulator, industri, maupun penyedia layanan. Hal ini perlu dilakukan untuk bisa bersama-sama membangun *trust,* agar kita memiliki ekosistem yang baik yang bisa memberikan jaminan kenyamanan bertransaksi dan berinteraksi digital lebih jauh.

Peran Pendidikan dalam Meningkatkan Kesadaran Keamanan Data

Pendidikan dan pelatihan juga memegang peranan kunci dalam meningkatkan kesadaran akan pentingnya pelindungan data pribadi. Institusi pendidikan dapat memasukkan topik keamanan siber dan *data governance* ke dalam kurikulum mereka, sehingga generasi muda lebih siap menghadapi tantangan digital di masa depan. Selain itu, program pelatihan dan sertifikasi di bidang keamanan siber juga dapat membantu meningkatkan keterampilan profesional dalam menjaga keamanan data.

Masa Depan Pelindungan Data Pribadi di Indonesia

Serangan *ransomware* di PDN menjadi pengingat akan pentingnya pelindungan data pribadi dan *data governance* yang baik di Indonesia sebagai elemen-elemen penting yang saling terkait dalam menciptakan ekosistem digital yang aman dan tepercaya untuk membangun *digital trust*. Untuk itu, diperlukan kerja sama antara pemerintah, sektor swasta, dan masyarakat dalam menerapkan praktik-praktik terbaik dalam pengelolaan dan pelindungan data pribadi.

Dengan adanya UU PDP, Indonesia telah mengambil langkah besar menuju pelindungan data pribadi yang lebih baik. Namun, masih banyak tantangan, termasuk dalam hal implementasi dan penegakan hukum. Kerja sama antara pemerintah, sektor swasta, dan masyarakat sangat penting untuk memastikan keberhasilan undang-undang ini. Di masa depan, kita dapat mengharapkan perkembangan lebih lanjut dalam regulasi dan teknologi yang mendukung pelindungan data pribadi, seiring dengan meningkatnya kesadaran dan tuntutan akan keamanan data pribadi di masyarakat.

Hadirnya UU PDP bisa menjadi niat baik yang efektif dalam mendorong *digital trust* masyarakat, namun juga bisa hanya sebatas 'lipstik' atau pencitraan jika tidak diiringi dengan implementasi dan penegakan hukum yang kuat. Waktu dan tindakan nyata yang akan menentukan hasil akhirnya.

PROFIL PENULIS

Deden Darajat Muharam

Deden, yang kini menjadi Partner Sharia Digital Advisory di Veda Praxis, menyelesaikan studi sarjana di bidang Akuntansi di Universitas Padjadjaran, Bandung, dan meraih gelar Magister Perbankan dan Keuangan Syariah dari Indonesia Banking School, Jakarta.

Berbekal keahlian yang meliputi digital syariah, keuangan syariah, pemasaran keuangan syariah, perbankan syariah, teknologi keuangan, kepemimpinan, dan business process improvement, dia telah dipercaya sebagai konsultan dalam berbagai proyek pengembangan bisnis dan keuangan syariah.