

PERLINDUNGAN DATA PRIBADI DAN TANTANGANNYA



Prof. Dr. Henri Subiakto
Guru Besar FISIP Unair

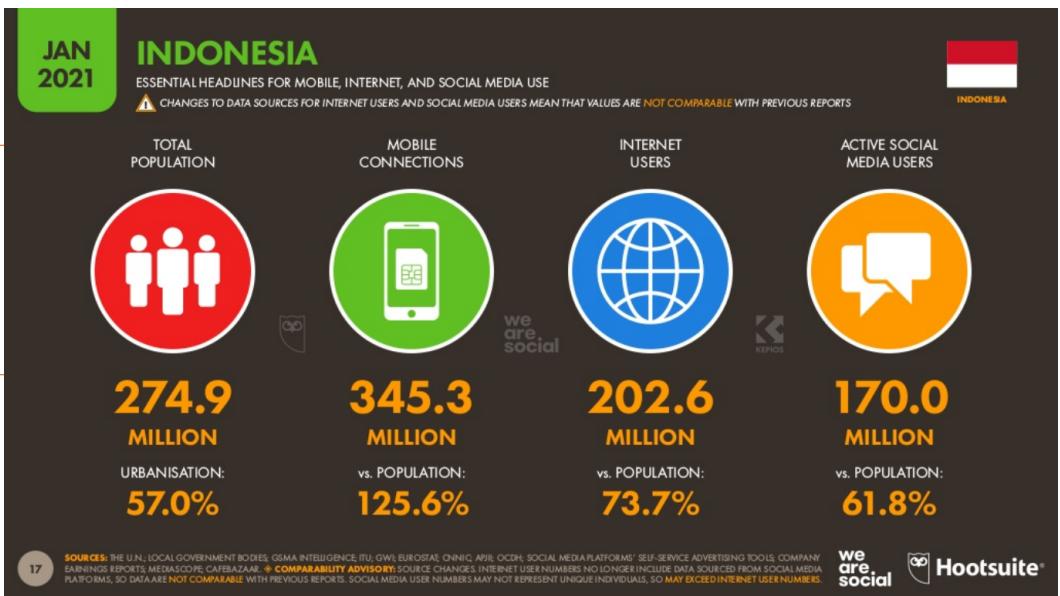
Indonesia di Era Digital

Setiap aktivitas warga di dunia digital selalu terkait dengan data pribadi. Pemanfaatan data pribadi tersebut memerlukan tata kelola yang baik dan akuntabel.

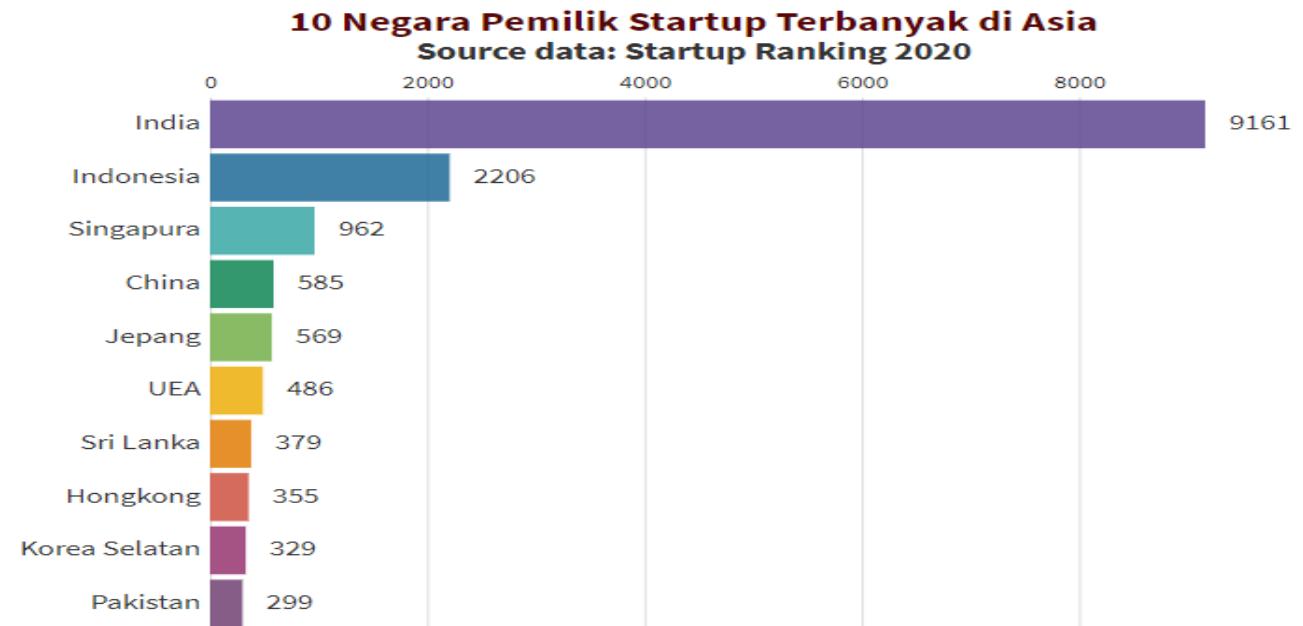
Dibutuhkan regulasi yang lengkap, kuat dan tegas. Sekaligus pentingnya kesiapan sumber daya manusia yang cerdas, tangguh dan adaptif.

↑ Besarnya jumlah pengguna internet

↑ Pesatnya pertumbuhan *digital startups*

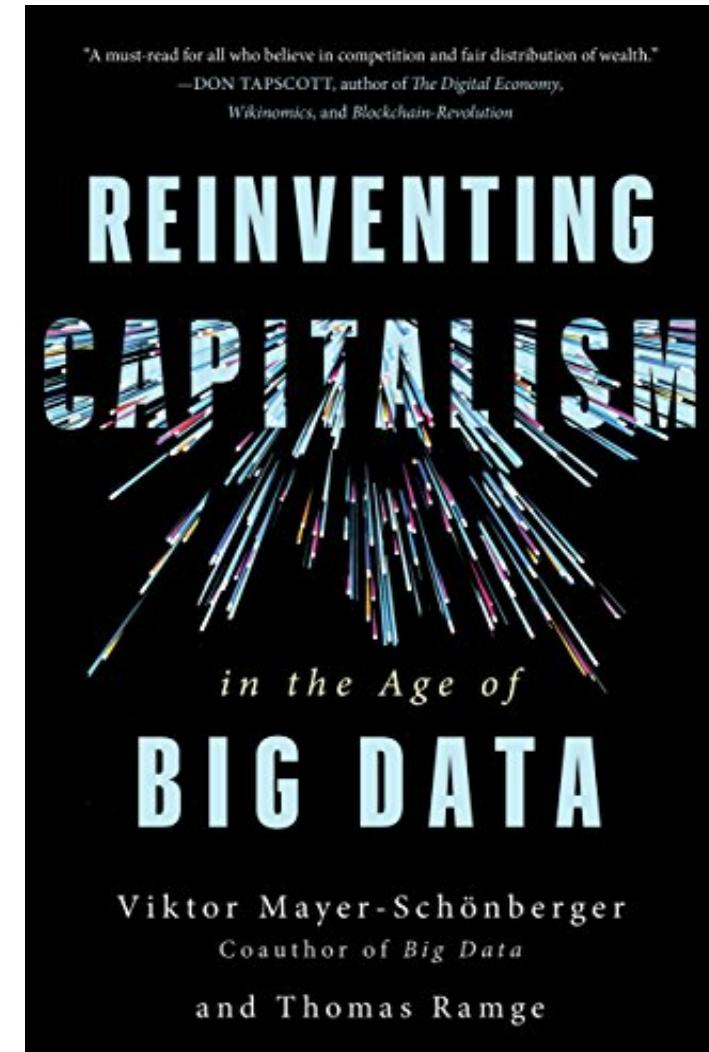


Sumber : We Are Social, 2021



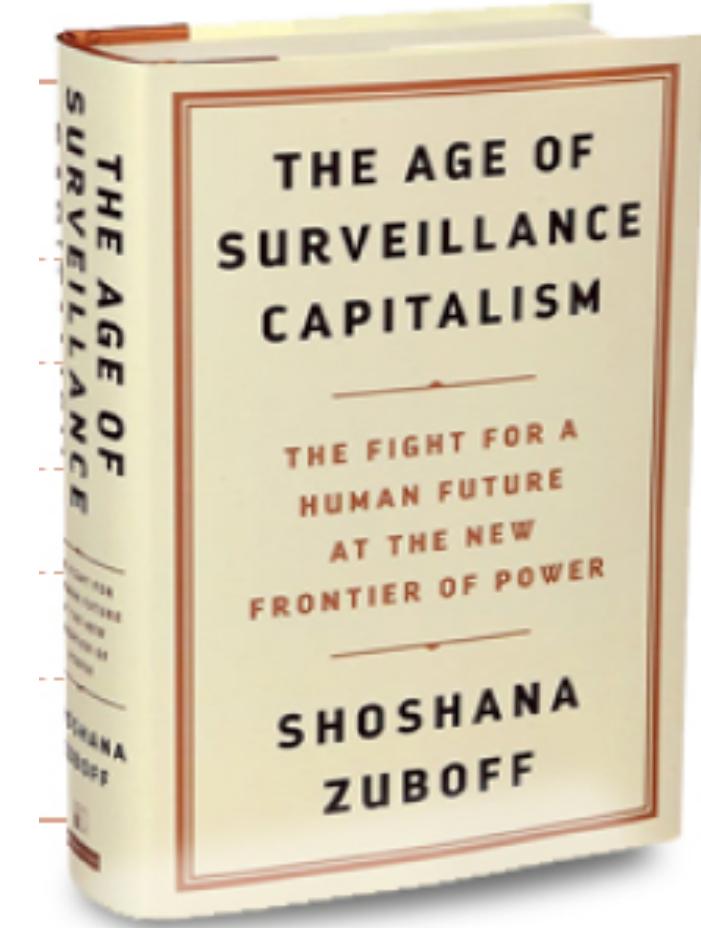
BIG DATA MENJADI KEKUATAN BISNIS DAN POLITIK

- Di era digital yang diperlukan kalangan kapitalis, adalah bagaimana menguasai data konsumen, pola perilaku masyarakat, dan komunikasi mereka di dunia maya. (Schonberger, Victor Mayer & Thomas Ramge, 2018)
- Big Data terkumpul lewat teknologi aplikasi telah mengubah wajah kapitalisme, tapi dengan karakter yang sama. Yaitu *greedy*. Dulu lewat penguasaan uang, sekarang penguasaan data. Tujuannya sama, berkuasa dan menguasai hidup manusia lain dengan cara lebih efektif.



FENOMENA GLOBAL : *THE AGE OF SURVEILLANCE CAPITALISM*

- Kapitalisme pengawasan, manusia menjadi sebatas komoditas ekonomi belaka. Dalam kapitalisme pengawasan, manusia terasing bukan karena pekerjaannya, melainkan karena ranah pribadinya (melalui data digital) telah dikuasai pihak ketiga.
- Zuboff (2019) menuding Google sebagai pelopor kapitalisme pengawasan dengan fitur mesin pencarian hingga sistem Android yang tersemat pada sebagian besar ponsel pintar di dunia. Riwayat pencarian pengguna, pesan suara, jejak rute peta perjalanan, atau kontak di surel dikonversi ke dalam data yang kemudian menjadi komoditas bagi perusahaan digital lainnya.



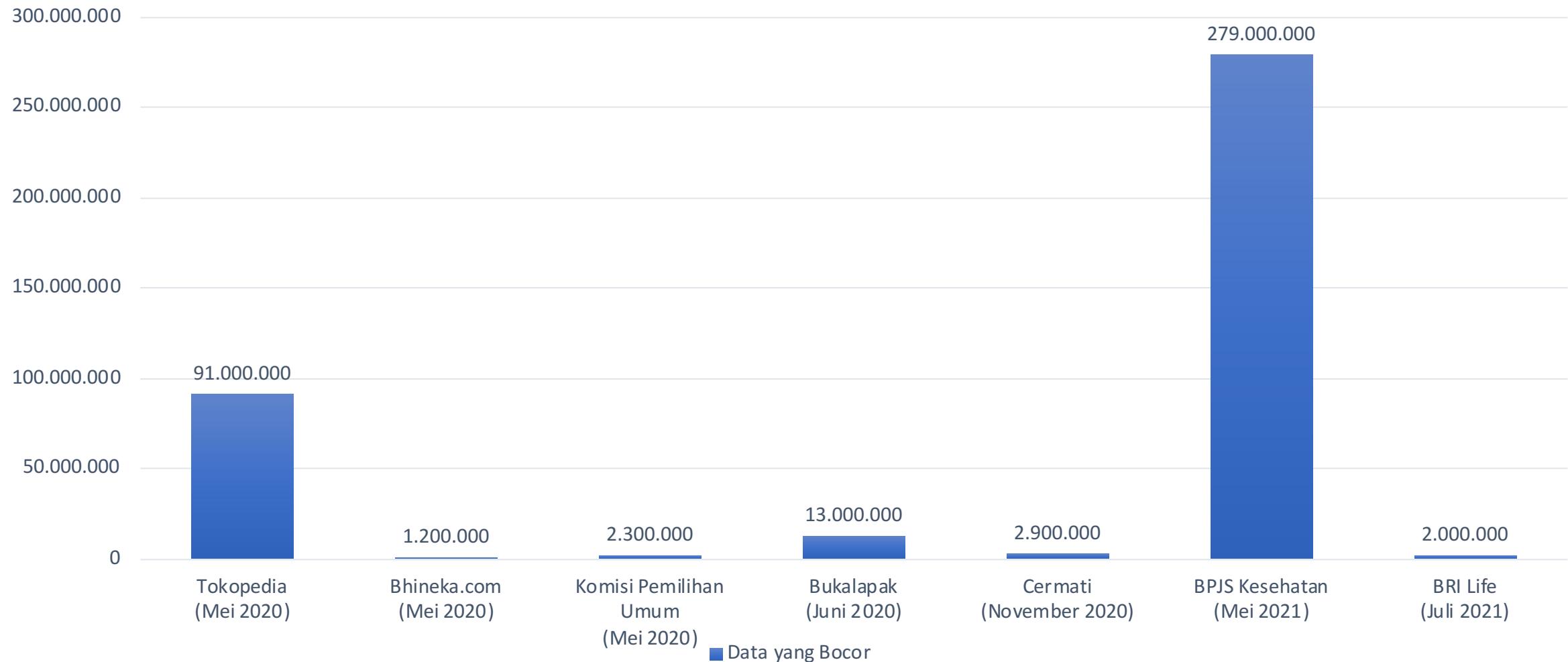
SERANGAN SIBER MENINGKAT 5X LIPAT



- Serangan siber ke Indonesia mengalami kenaikan dari tahun ke tahun. Pusat operasi keamanan siber nasional BSSN mencatat, adanya tren ini. Kasus percobaan pencurian data (*data breach*) sepanjang periode Januari hingga Agustus 2020, terdapat 190 juta serangan siber, dan 36.771 akun data yang tercuri, di sejumlah sektor, termasuk sektor keuangan. Serangan itu dicatat mengalami peningkatan lima kali lipat dari tahun 2019.
- Tahun 2021 juga semakin meningkat. Menurut Kapersky, perusahaan keamanan siber mengungkapkan 40% konsumen dari Asia Pasifik menghadapi insiden kebocoran data pribadi yang diakses orang lain tanpa persetujuan pemiliknya.
- Berdasar Perpres 28/2021 pasal (2) dan (3) BSSN adalah Badan yang bertugas membantu Presiden (Pemerintah) terkait keamanan Siber. Bertugas membuat **standar** dan **supervisi**.

DERETAN KEBOCORAN DATA DI INDONESIA

KEBOCORAN DATA DALAM KURUN WAKTU MEI 2020 – MEI 2021



PERETASAN WEBSITE/SITUS DPR RI



Situs DPR RI (www.dpr.go.id) sempat diretas awal Oktober 2020 lalu. Cuplikan gambar tersebut memperlihatkan halaman depan situs yang tulisan sebenarnya “Dewan Perwakilan Rakyat” diubah oleh peretas menjadi “Dewan Penghianat Rakyat”.

Peretasan tersebut didasari oleh penolakan pengesahan UU Ciptakerja atau *Omnibus Law*.

PERETASAN MEDIA ONLINE

Pemberangusan di Era Digital

PADA era Orde Baru, ancaman terbesar bagi media massa adalah pembredelan oleh penguasa. Di era digital, pembredelan sudah dilarang, tapi muncul ancaman baru berupa peretasan. Dampaknya lebih-kurang sama, yakni memberangus kerja wartawan.

Cekfakta.com

Peretasan situs Cekfakta.com terjadi pada 20 Februari 2019 pukul 05.00 WIB. Peretas diketahui mengubah ID pemilik situs Cekfakta.com menjadi bernama Elliot Alderton dengan surel thegreatfsociety@gmail.com.

Suarapapua.com

Peretasan terjadi pada 26 Januari 2020. Pemimpin Redaksi Suarapapua.com, Arnold Belau, mengatakan situs beritanya sempat tak bisa diakses selama beberapa hari. Pembobolan terjadi tak lama setelah media ini menerbitkan berita seputar penembakan di Kabupaten Intan Jaya.

Magdalene.co

Situs yang rajin mengadvokasi persoalan kesetaraan gender, Magdalene, melaporkan peretasan sejak 15 Mei lalu. Modusnya dengan membanjiri server, sistem, dan jaringan, sehingga situs tersebut tak bisa diakses. Serangan terjadi lebih dari sebulan.

Tempo.co

Situs Tempo.co diretas pada 21 Agustus dinihari lalu. Pelaku mengganti tampilan depan laman Tempo.co menjadi gelap dan menuliskan kalimat bernada negatif. Peretasan juga pernah terjadi pada 2014 dan 2017.

Tirto.id

Portal berita Tirto.id diretas pada 21 Agustus dinihari lalu. Pelaku menghapus beberapa artikel ihwal calon obat Covid-19 dari Universitas Airlangga. Pembobolan juga mengubah isi naskah dan mengganti hyperlink di dalam tulisan.



SERANGAN SIBER DI INDONESIA



741.441.648

ANOMALI TRAFIK/SERANGAN SIBER
DI TAHUN 2021 (Januari – Juli)

Kategori Anomali Terbanyak:

1. Malware
2. Denial of Service (Mengganggu ketersediaan layanan)
3. Trojan Activity (Aktivitas Trojan)

Tren Serangan Siber:

1. Serangan Ransomware (Malware yang meminta tebusan)
2. Insiden Data Leaks (kebocoran data)

Sebaran sektor yang terkait dengan kebocoran data akibat malware pencuri informasi:



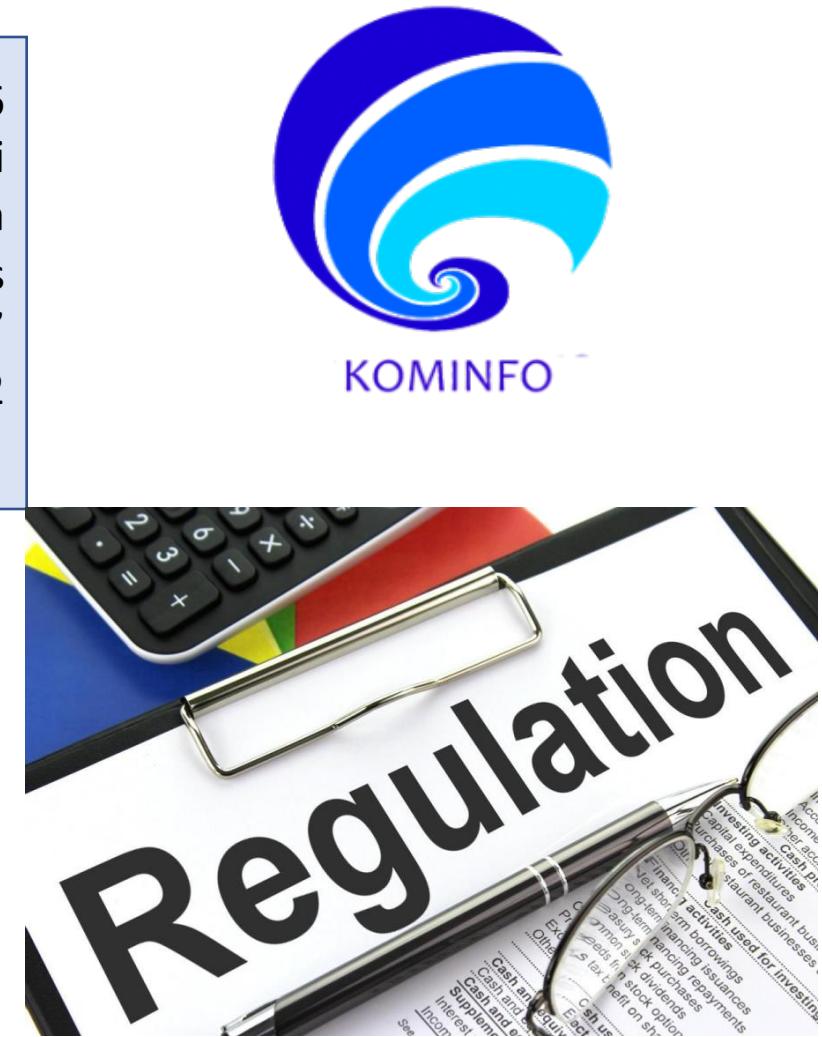
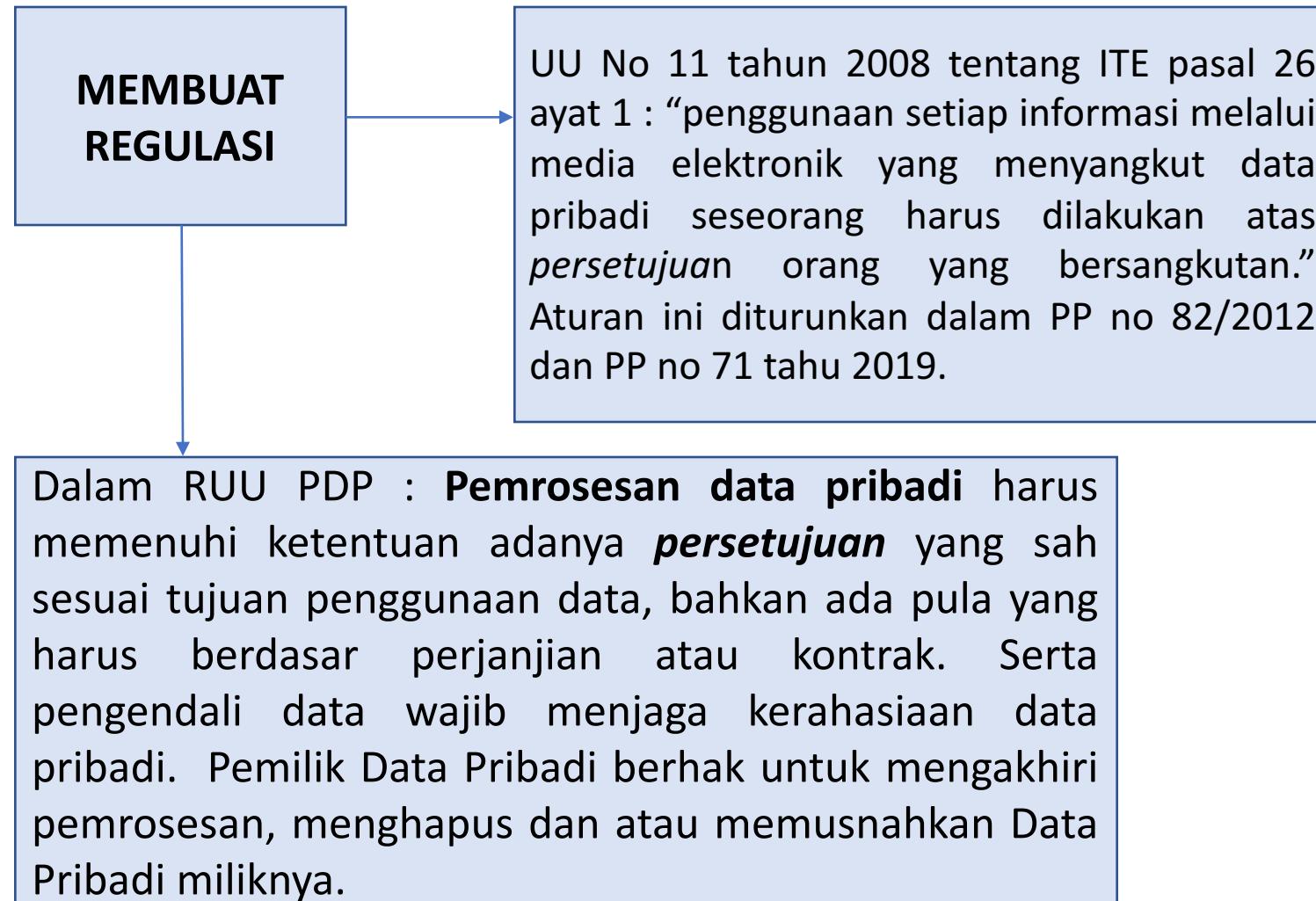
Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara (BSSN) mencatat jumlah serangan siber yang terjadi di Indonesia antara Januari hingga Juli 2021 sebanyak 741.441.648 kali. Jumlah serangan itu mengalami **peningkatan hampir dua kali lipat** dibandingkan seluruh anomali trafik yang dideteksi oleh lembaga siber tersebut selama tahun lalu yang mencapai kurang lebih 495 juta kali.

KASUS THE GRAET HACK OF PERSONAL DATA

- Kasus Facebook yang datanya digunakan *Cambridge Analytica* merupakan *evidence* dari sisi hitam media sosial mempengaruhi kualitas Pemilu Presiden AS 2016.
- Bukti nyata bagaimana negara maju seperti AS berhasil digunakan jutaan data pribadi milik warga negaranya yang ada di FB dipakaiuntuk mempengaruhi politik.
- Kasus ini juga mempertanyakan integritas Mark Zuckerberg antara apa yang dia ucapkan dengan apa yang benar-benar terjadi terhadap data pribadi pengguna FB.



APA YANG DILAKUKAN NEGARA DALAM MENGHADAPI RESIKO KEAMANAN DATA?



CYBER SECURITY SANGAT PENTING UNTUK MENGURANGI RISIKO KEAMANAN DATA

- *Cyber security*, terkait, talent, proses dan teknologi.
- Kita butuh banyak ahli dan perusahaan yang mampu menghadapi resiko *cyber security*.
- *Cyber Security* bagian dari program yang harus melekat bahkan di depan, terkait proses, infrastruktur maupun teknologi (OS).
- Indonesia kekurangan talenta *cyber security* dibanding perkembangan digital dan kebutuhan.
- Terjadi gap antara kebutuhan *cyber security* dengan keadaan di Indonesia.
- Butuh peran Pemerintah, Industri, Perguruan Tinggi untuk mengatasi persoalan *cyber security*.
- Pentingnya program *up skilling* kemampuan *cyber security talent* dan literasi publik.



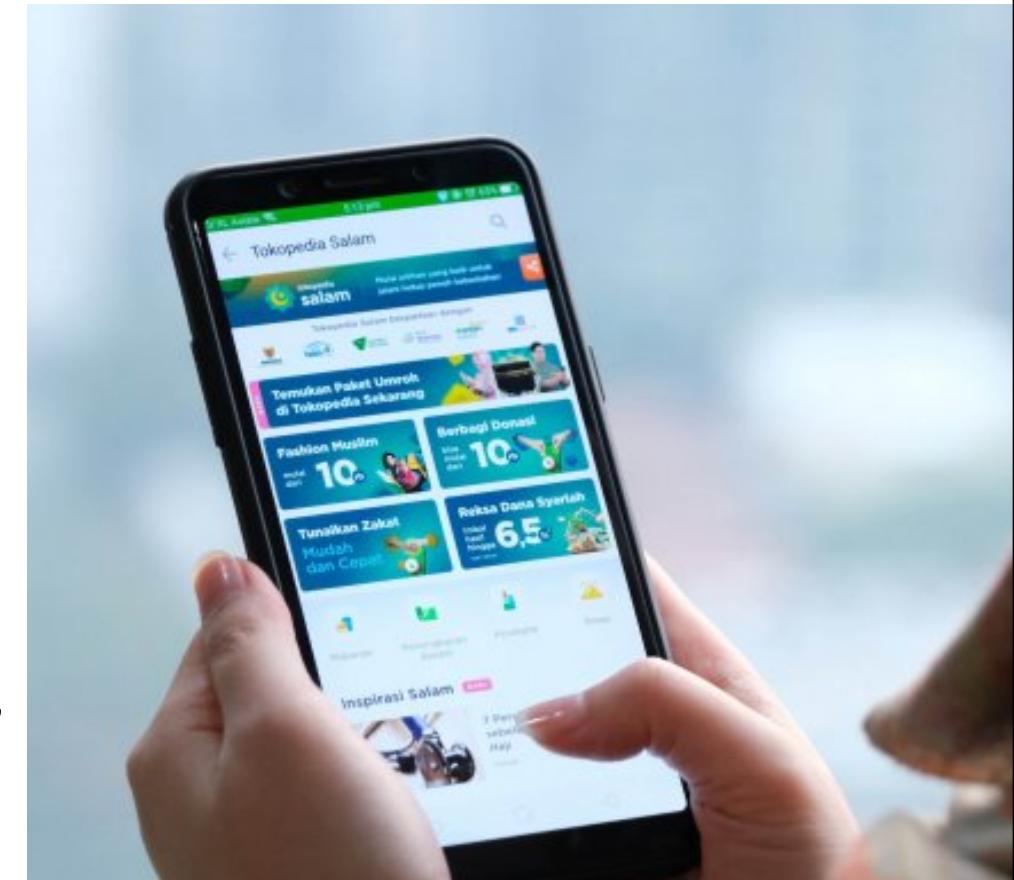
ALASAN PERETASAN DATA PRIBADI

- **PROFIT** : Keuntungan Pribadi, Organisasi, Perusahaan, atau Lembaga tertentu.
- **DATA ANALYSIS** : Untuk kepentingan analisis data (*Data mining, profiling dll*).
- **LOW BUG BOUNTY PRICE** : Hacker kecewa terkait reward.
- **POLITICS**, persaingan antar kelompok, kompetitor.
- **PENIPUAN/PHISING** : Penipuan.
- **TELEMARKETING** : Data pribadi diperjual belikan untuk telemarketing.



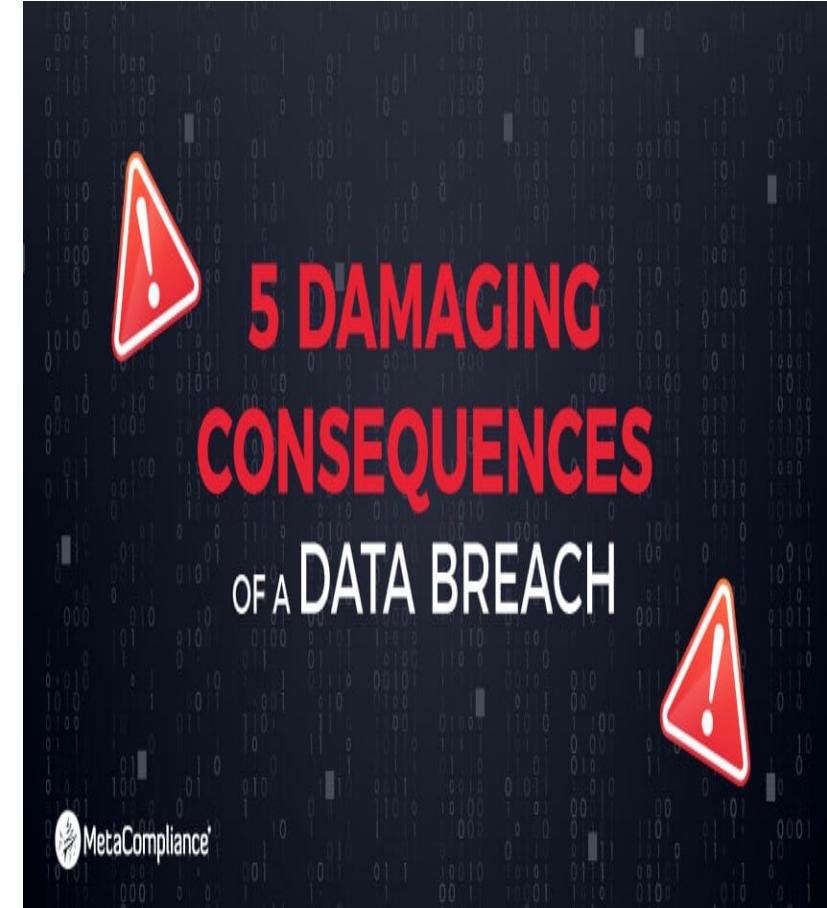
BERBAGAI BENTUK KEMUNGKINAN PERETASAN

- ***Structured Query Language (SQL)/NoSQL Injection*** : Hacker mengakses data server melalui kesalahan pada filter input.
- ***IDOR (Insecure Direct Object References)*** : Hacker mengakses data akun pengguna lain melalui akun pribadi (*Brute force ID*).
- ***CVE (Common Vulnerabilities and Exposures)*** : Aplikasi yang dipakai tidak ter-update, atau hardware yang memiliki vulnerability.
- ***Human Error*** : Minimnya edukasi kerahasiaan data, atau kejahatan individu pekerja (illegal access).
- ***Lain Lain*** : Seluruh aspek yang munculkan celah keamanan.



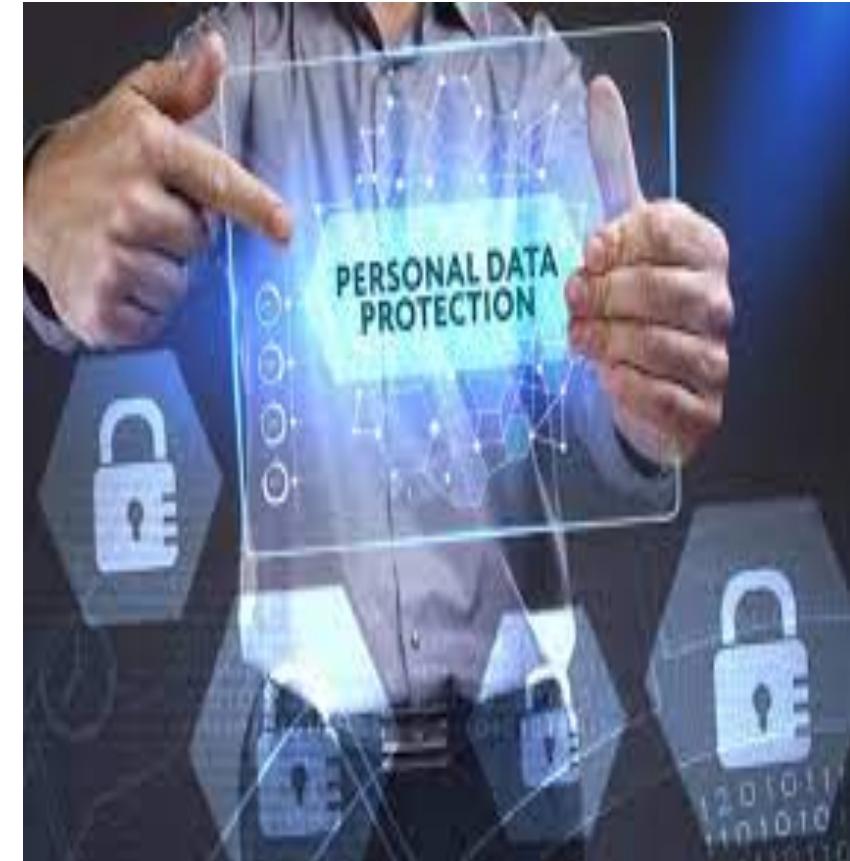
AKIBAT PERETASAN DATA PRIBADI PADA LEMBAGA YANG TERKENA

- **OPERATIONAL DOWNTIME** : Operations may need to be completely shut down until investigators get all the answers they need.
- **LEGAL LIABILITY** : Organisasi dan negara dinilai lalai melindungi data Pribadi, berpotensi muncul *legal dispute*.
- **BUSINESS REPUTATION** : Korban peretasan reputasinya dan kepercayaan jatuh, pada pengguna, investor dan pemerintah.
- **LOST PRODUCTIVITY** : Kehilangan produktivitas, ide, inovasi diambil alih Kompetitor.
- **FINANCIAL LOSS** : Biaya meneliti kasusnya, menerapkan sistem keamanan baru, kompensasi Pelanggan dll.



SIAPA YANG HARUS TANGGUNG JAWAB TERHADAP KEBOCORAN DATA?

- Di pasal 15 UU ITE ; “*Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya system elektronik sebagaimana mestinya.*”
- PP 71 tahun 2019 pasal 24 ayat (1) Penyelenggara Sistem Elektronik (PSE) wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan Sistem Elektronik dalam menghindari gangguan, kegagalan, dan kerugian.
- Ayat (2) PSE wajib menyediakan sistem pengamanan yang mencakup prosedur dan system pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.
- Ayat (3) Dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan dari pihak lain terhadap Sistem Elektronik, PSE wajib mengamankan Informasi Elektronik dan/atau Dokumen Elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan Kementerian atau Lembaga terkait.



Sumber : Prof. Henry Subiakto 2021

PENANGANAN DUGAAN KEBOCORAN DATA PRIBADI

- Pemerintah, dalam hal ini Kementerian Kominfo melakukan penanganan dugaan kebocoran data terhadap 36 Penyelenggara Sistem Elektronik (PSE) sejak 2019 sampai 31 Agustus 2021. Dari jumlah tersebut, 31 kasus telah selesai dilakukan investigasi dengan perincian: 4 PSE telah dikenai sanksi teguran tertulis, 18 PSE diberikan rekomendasi teknis peningkatan tata kelola data dan Sistem Elektronik, sedangkan 9 PSE lainnya dalam proses pemberian keputusan akhir terkait sanksi.
- Upaya pengawasan kepatuhan terhadap pengelola sistem PeduliLindungi, pihak yang mengelola data, serta para pengguna, akan terus dilakukan oleh Kementerian Kominfo dengan berkoordinasi bersama Kementerian Kesehatan, BSSN, serta pihak terkait lainnya.
- Sedang terhadap pelaku kejahatannya, dikenakan sanksi pidana sesuai ketentuan UU ITE.



KASUS SERTIFIKAT VAKSIN PRESIDEN DI PEDULI LINDUNGI

- Sertifikat Vaksinasi Covid-19 di sistem PeduliLindungi mensyaratkan menyertakan nomor handphone dan 5 parameter (nama, Nomor Identitas Kependudukan (NIK), tanggal lahir, tanggal vaksin, dan jenis vaksin). Belakangan nomer hp dihilangkan.
- Informasi terkait NIK dan tanggal vaksinasi Covid-19 milik Presiden Joko Widodo digunakan untuk mengakses Sertifikat Vaksinasi di Sistem PeduliLindungi. Informasi NIK ada di situs Komisi Pemilihan Umum. Informasi tanggal vaksinasi Presiden dapat ditemukan di pemberitaan media massa.
- Kementerian Kesehatan, sebagai Wali Data bertanggung jawab agar pemanfaatan data di Pedulilindungi terintegrasi dengan Pusat Data Nasional (PDN) sesuai PP No. 71 Tahun 2019 tentang PSTE serta Perpres No. 39/2019 tentang Satu Data Indonesia.
- BSSN sebagai Lembaga yang berwenang melaksanakan kebijakan teknis keamanan siber bertanggungjawab melakukan pemulihian, dan manajemen risiko keamanan siber sesuai PP PSTE dan Perpres No. 28 Tahun 2021 tentang BSSN.
- Kementerian Kominfo selaku regulator, melakukan langkah strategis pemutakhiran tata kelola data Sistem Pedulilindungi sesuai PP PSTE, PM Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, serta Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
- Kementerian Kominfo, telah melakukan migrasi Sistem PeduliLindungi ke Pusat Data Nasional (PDN) 28 Agustus 2021. Migrasi tersebut meliputi migrasi sistem, layanan aplikasi, dan juga database aplikasi. Migrasi turut dilakukan terhadap Sistem Aplikasi SiLacak dan Sistem Aplikasi PCare.



PENTINGNYA LITERASI KEAMANAN INFORMASI

- Selalu mengganti *password* secara berkala, dan tidak menggunakan *password* yang mudah ditebak.
- Jangan membuka *email* atau *link* yang mencurigakan, atau yang tidak dikenal.
- Menggunakan *software* yang legal sehingga selalu ada update keamanan untuk OS yang kita pakai.
- Pelajari semua aplikasi yang kita pakai dan selalu di-update.
- Gunakan koneksi internet dan protokol yang aman, jangan di Wifi sembarangan.
- Tidak menunjukkan data pribadi atau sisi privasi untuk umum.
- Pelajari hak hukum dan regulasi terkait keamanan data dan privasi.

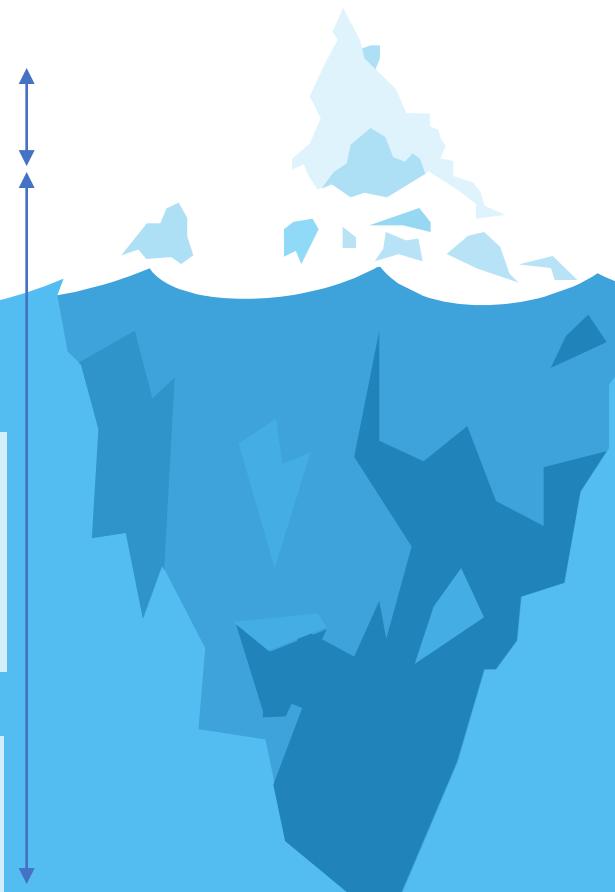


UU PDP Mempersempit Penyalahgunaan Data Pribadi, Kebocoran Hingga Jual Beli

Kasus pelanggaran terhadap Data Pribadi

Banyak **kasus pelanggaran data pribadi** baik di dalam maupun di luar negeri yang memberikan **dampak kerugian** yang **signifikan** bagi masyarakat

RUU Perlindungan Data Pribadi merupakan instrumen hukum yang disusun untuk melindungi data pribadi **warga negara** dari praktik penyalahgunaan data pribadi



Disebabkan oleh

Serangan siber

Human Error (negligent insider)

Outsourcing Data ke Pihak ketiga

Kesengajaan Perbuatan orang dalam

Kegagalan sistem

Rendahnya Awareness

Tidak peduli dengan kewajiban regulasi

Regulasi Perlindungan Data Pribadi di Indonesia

Tersebar pada berbagai macam sektor (keuangan, kesehatan, kependudukan, telekomunikasi, perbankan perdagangan, dan lain-lain) pada kurang lebih **32** regulasi.

Penyelenggara layanan publik memiliki standar dan acuan perlindungan data pribadi yang berbeda.

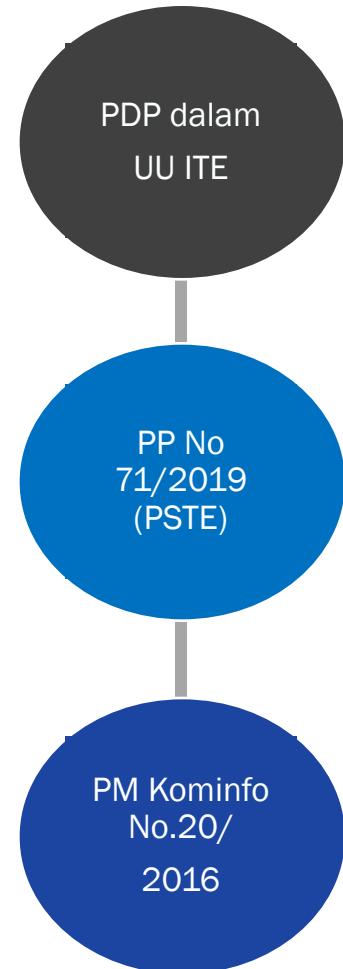
Kebutuhan peraturan yang lebih komprehensif untuk perlindungan data pribadi di Indonesia



RUU
PDP

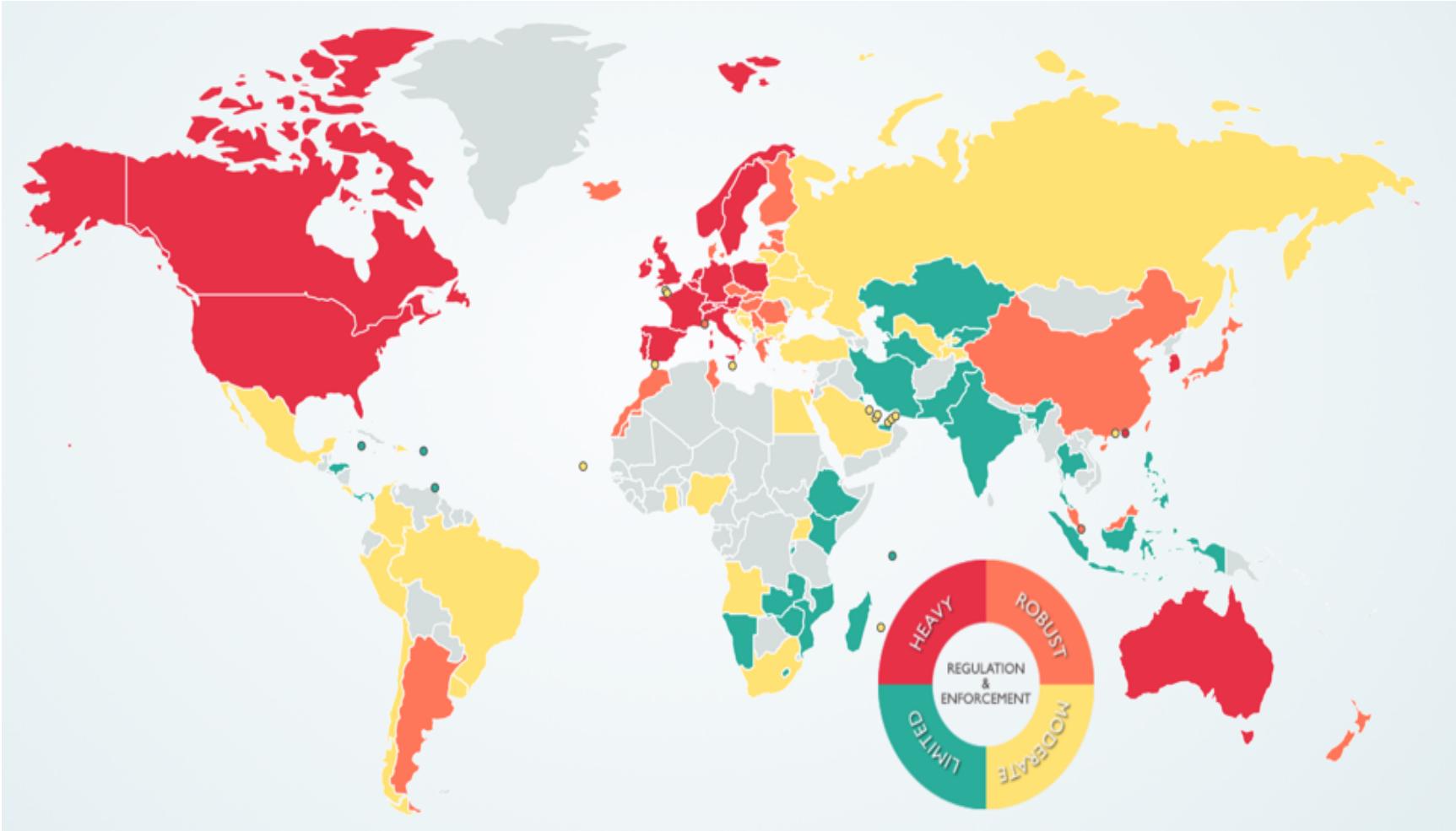
Rancangan Undang-Undang
tentang
Perlindungan Data Pribadi

Perlindungan Data Pribadi Sistem Elektronik



Regulasi Perlindungan Data Pribadi di Dunia

Gambaran Peraturan Perlindungan Data Pribadi di Berbagai Negara



Source: <https://www.dlapiperdataprotection.com/index.html>

Lebih dari **132** negara telah memiliki instrumen hukum yang secara khusus mengatur mengenai privasi dan data pribadi warga negaranya.

– Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills* (6th Ed January 2019)

Beberapa negara **ASEAN** juga telah memiliki aturan khusus perlindungan data pribadi, misalnya:



Malaysia (2010)



Singapura (2012)



Filipina (2012)



Thailand (2019)

Disebabkan?

- Penyalahgunaan data pribadi
- Jual beli data pribadi
- Penipuan yang menggunakan data pribadi milik orang lain

Belakangan ini, baik di dalam maupun di luar negeri telah terjadi banyak kasus kebocoran data pribadi yang memberikan dampak kerugian yang signifikan bagi masyarakat

Kasus pelanggaran terhadap Data Pribadi

Oleh karena itu, RUU Perlindungan Data Pribadi merupakan instrumen hukum yang disusun untuk melindungi data pribadi warga negara dari praktik penyalahgunaan data pribadi sebagaimana disebutkan di atas.



Urgensi RUU Perlindungan Data Pribadi di Indonesia

01

Tumpang tindih
peraturan

02

Peraturan tidak
komprehensif

03

Kesulitan
implementasi
dan penegakan
hukum

04

Meningkatnya
pelanggaran DP

05

Kesadaran
publik rendah

Urgensi RUU Perlindungan Data Pribadi di Indonesia

RUU Perlindungan Data Pribadi merupakan instrumen hukum yang perlu segera hadir di dalam sistem hukum di Indonesia.
Isu-isu utama yang hendak direspon dengan adanya RUU PDP:

- 1 Menjawab kebutuhan atas regulasi yang komprehensif untuk melindungi data pribadi sebagai bagian dari hak asasi manusia.
- 2 Keseimbangan dalam tata kelola pemrosesan data pribadi dan jaminan perlindungan hak dan kesadaran subjek data .
- 3 Pencegahan dan penanganan kasus pelanggaran data pribadi.
- 4 Membangun ekosistem ekonomi digital yang aman dengan memberikan kepastian hukum bagi bisnis dan meingkatkan kepercayaan konsumen.
- 5 Kesetaraan dalam aturan PDP secara internasional yang mendukung pertumbuhan ekonomi digital melalui pengaturan *cross-border data flow*.

Urgensi Regulasi Perlindungan Data Pribadi



Adequate Protection
Between Countries



Data Free Flow with
Trust (DFFT)



Security
in digital economy

Kebutuhan peraturan perlindungan data pribadi yang komprehensif

RUU Perlindungan Data Pribadi ini akan menjadi **kerangka regulasi** yang lebih kuat dan **komprehensif** dalam memberikan perlindungan hak asasi manusia, khususnya terkait data pribadi

Tatakelola

RUU PDP akan menciptakan keseimbangan dalam tata kelola pemrosesan data pribadi dan jaminan perlindungan hak subjek data, serta menyediakan prinsip-prinsip dan syarat sah dalam pemrosesan data pribadi yang harus ditaati pengendali dan pemroses data pribadi

Kepastian Hukum

RUU PDP akan menjadi instrumen hukum kunci dalam pencegahan dan penanganan kasus pelanggaran data pribadi yang masih banyak terjadi dan menjadi tantangan bersama

Pertukaran Data Lintas Batas Negara

RUU PDP akan menciptakan kesetaraan dalam aturan PDP secara internasional yang mendukung pertumbuhan ekonomi digital melalui pengaturan cross-border data flow

Ekosistem Ekonomi Digital

RUU PDP akan mempercepat pembangunan ekosistem ekonomi digital dan meningkatkan iklim investasi yang aman dengan memberikan kepastian hukum bagi bisnis dan meningkatkan kepercayaan konsumen

Data Pribadi sebagai bagian dari HAM (amanat UUD 1945)

Pasal 28 G ayat (1)

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"

Pasal 28 H ayat (4)

"Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun"

RUU Perlindungan Data Pribadi

Substansi Pengaturan

JENIS DATA PRIBADI

HAK PEMILIK DATA PRIBADI

PEMROSESAN DATA PRIBADI

KEWAJIBAN PENGENDALI
DATA PRIBADI DAN
PROSESOR DATA PRIBADI
DALAM PEMROSESAN DATA
PRIBADI

TRANSFER DATA PRIBADI

SANKSI ADMINISTRATIF

LARANGAN DALAM
PENGGUNAAN DATA PRIBADI

PEMBENTUKAN PEDOMAN
PERILAKU PENGENDALI DATA
PRIBADI

PENYELESAIAN SENGKETA
DAN HUKUM ACARA

KERJA SAMA INTERNASIONAL

PERAN PEMERINTAH DAN
MASYARAKAT

KETENTUAN PIDANA

RUU Perlindungan Data Pribadi memberikan landasan hukum bagi Indonesia untuk menjaga **kedaulatan negara, keamanan negara, dan perlindungan** terhadap data pribadi milik **warga negara** Indonesia dimanapun data pribadi tersebut berada.



Dalam wilayah NKRI



Luar wilayah NKRI

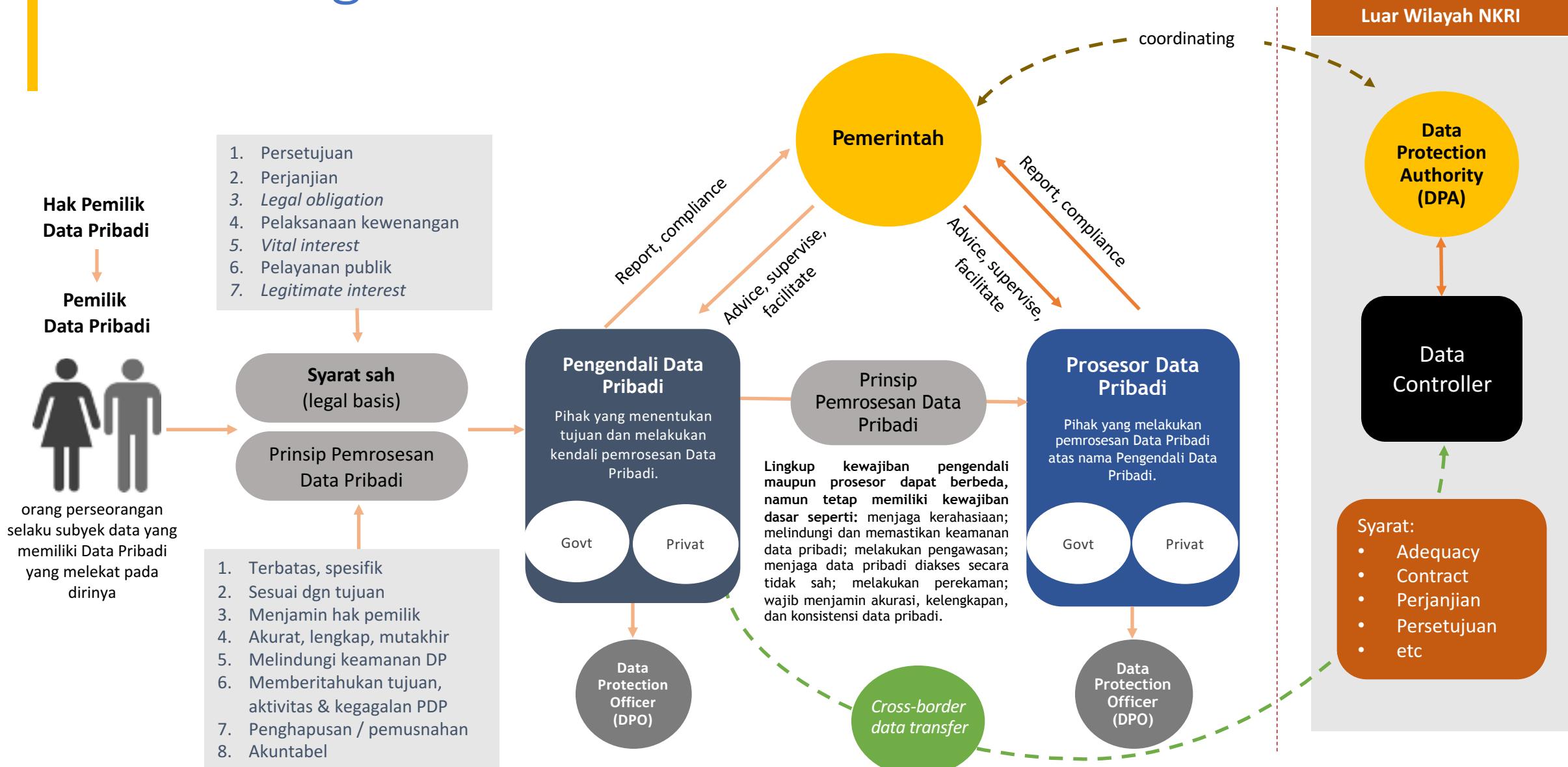


Pemerintah /
Sektor Publik



Sektor Privat

Konsep Pengaturan Perlindungan Data Pribadi



Lingkup Pemrosesan Data Pribadi

 Perolehan dan pengumpulan

 Pengolahan dan penganalisisan

 Penyimpanan

 Perbaikan dan pembaharuan

Penampilan, Pengumuman, Transfer, Penyebarluasan, atau Pengungkapan

 Penghapusan atau pemusnahan

Pemrosesan Data Pribadi harus mematuhi prinsip dan syarat sah pemrosesan

Prinsip Perlindungan Data Pribadi

1 **Terbatas, spesifik**

pengumpulan dilakukan secara **terbatas dan spesifik**, sah secara hukum, patut, dan transparan

2 **sesuai dengan tujuannya**

3 **menjamin hak Pemilik Data Pribadi**

4 **Akurat**

akurat, lengkap, tidak menyesatkan, mutakhir, dpt dipertanggungjawabkan

5 **melindungi keamanan data pribadi**

6 **memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan PDP**

7 **Penghapusan / Pemusnahan (retensi)**

Pemusnahan dan/atau penghapusan data pribadi setelah **masa retensi** berakhir atau berdasarkan **permintaan** Pemilik Data Pribadi (kecuali ditentukan lain oleh Peraturan Per-UU)

8 **Akuntabel**

dilakukan secara **bertanggung jawab** dengan memenuhi pelaksanaan **prinsip perlindungan Data Pribadi** dan dapat **dibuktikan** secara jelas

Syarat Sah Pemrosesan Data Pribadi

Persetujuan

persetujuan yang sah dari Pemilik Data Pribadi untuk satu atau beberapa tujuan tertentu yang telah disampaikan kepada Pemilik Data Pribadi

Perjanjian

pemenuhan kewajiban perjanjian dalam hal Pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Pemilik Data Pribadi pada saat akan melakukan perjanjian

Legal obligation

pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan

Vital Interest

pemenuhan perlindungan kepentingan yang sah (vital interest) Pemilik Data Pribadi

Pelaksanaan kewenangan

pelaksanaan kewenangan Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan

Pelayanan Publik

pemenuhan kewajiban Pengendali Data Pribadi dalam pelayanan publik untuk kepentingan umum

Legitimate Interest

pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Pemilik Data Pribadi

Transfer Data Pribadi ke luar wilayah NKRI

Pengendali Data Pribadi dapat mentransfer Data Pribadi kepada Pengendali Data Pribadi di luar wilayah hukum Negara Kesatuan Republik Indonesia dalam hal:

Negara/organisasi tujuan memiliki tingkat perlindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam UU ini;

terdapat perjanjian internasional antarnegara;

terdapat kontrak antar Pengendali Data Pribadi yang memiliki standar dan/atau jaminan pelindungan data pribadi; dan/atau

mendapat persetujuan Pemilik Data Pribadi.

Issue Model Lembaga Pengawas PDP

Model Lembaga Tersendiri

Model Lembaga Yang Telah ada

Model Lembaga di Bawah
Koordinasi Pemerintah

Penyelenggaraan Pelindungan Data Pribadi dalam RUU PDP

Pasal 58

- 1) Pemerintah berperan dalam mewujudkan penyelenggaraan pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini.
- 2) Penyelenggaraan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh **Menteri**.
- 3) Ketentuan mengenai penyelenggaraan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (2) diatur dalam **Peraturan Pemerintah**.



OPSI BENTUK KELEMBAGAAN PDP

1. Berdasarkan pembahasan Panja RUU PDP, Fraksi mengusulkan perlu ada pembentukan Badan secara tegas selaku pelaksana dan pengawas UU PDP.
2. Menanggapi hal tersebut, Pemerintah perlu menyiapkan struktur kelembagaan PDP di bawah fungsi eksekutif.
3. Beberapa opsi struktur kelembagaan PDP:
 - a. Di bawah Presiden langsung → Badan PDP dibentuk oleh Perpres
 - b. Di bawah Presiden yang pertanggungjawabannya melalui kementerian
 - c. Di bawah Menteri → Menteri Membentuk Badan berdasarkan PM

TUGAS DAN FUNGSI BADAN PDB

- REGULATORY, Membuat Regulasi dan Kebijakan, keputusannya berlaku mengikat.
- SURVEILLANCE, Pengawasan dan Penegakkan Hukum. Evaluasi compliance, penyelesaian sengketa dan penegakkan hukum.
- COOPERATION, kerjasama dengan institusi lain, nasional maupun internasional.
- DEVELOPMENT, pengembangan ekosistem.
- PROMOTION, promosi, sosialisasi dan edukasi pada publik.



PERTANYAAN YANG HARUS KITA JAWAB

- Di masa depan siapa yang akan paling banyak mengendalikan Data Pribadi? Negara (Pemerintah) atau Korporasi?
- Yang makin kuat mengawasi aktivitas kehidupan umat manusia itu Surveillance Capitalism atau Surveillance Government?
- Lalu yang harus mengawasi dan melindungi kepentingan warga negara itu siapa?
- Siapa yang pantas berhadapan untuk “mengawasi dan mengurus” Korporasi Global seperti Google, Facebook dll?



STAND POINT PEMERINTAH TENTANG BADAN PDB

- Kalau ada Badan Baru yg diamanatkan UU, maka penetapan dan pemilihan pejabat di dalamnya didasarkan atas Perpres. Sekarang sudah ada 400 posisi pejabat yg dipilih DPR, sehingga melemahkan sistem presidensial.
- Jika perlu Badan Baru, sesuai prinsip sistem Presidensiel, maka Presiden yang berwenang membentuknya dan Presiden bertanggung jawab terhadap kinerja Lembaga tersebut.
- Badan Baru independent, menjadi isu hampir di tiap UU dengan alasan kemandirian lembaga pengawas dan penegak hukum.
- Institusi Penegakkan Hukum sudah ada. *State auxiliary institution* justru mengacaukan sistem presidensiel. Penegakkan administrasi tidak harus Badan tersendiri.
- Lembaga pengawas sektor juga sudah ada, dengan sistem yang sudah jalan, misal sector perbankan dan jasa keuangan, (ada OJK dan BI).
- Saat berhubungan dengan negara lain, atau institusi internasional, dan korporasi global, pemerintah telah memiliki jaringan yang kredible dan sarana yang memadahi.



Prof. Dr. H. Henry Subiakto, SH, MA

Staf Ahli Menteri Kominfo RI

Guru Besar FISIP Universitas Airlangga

Twitter : @henrysubiakto (Communication Corner)

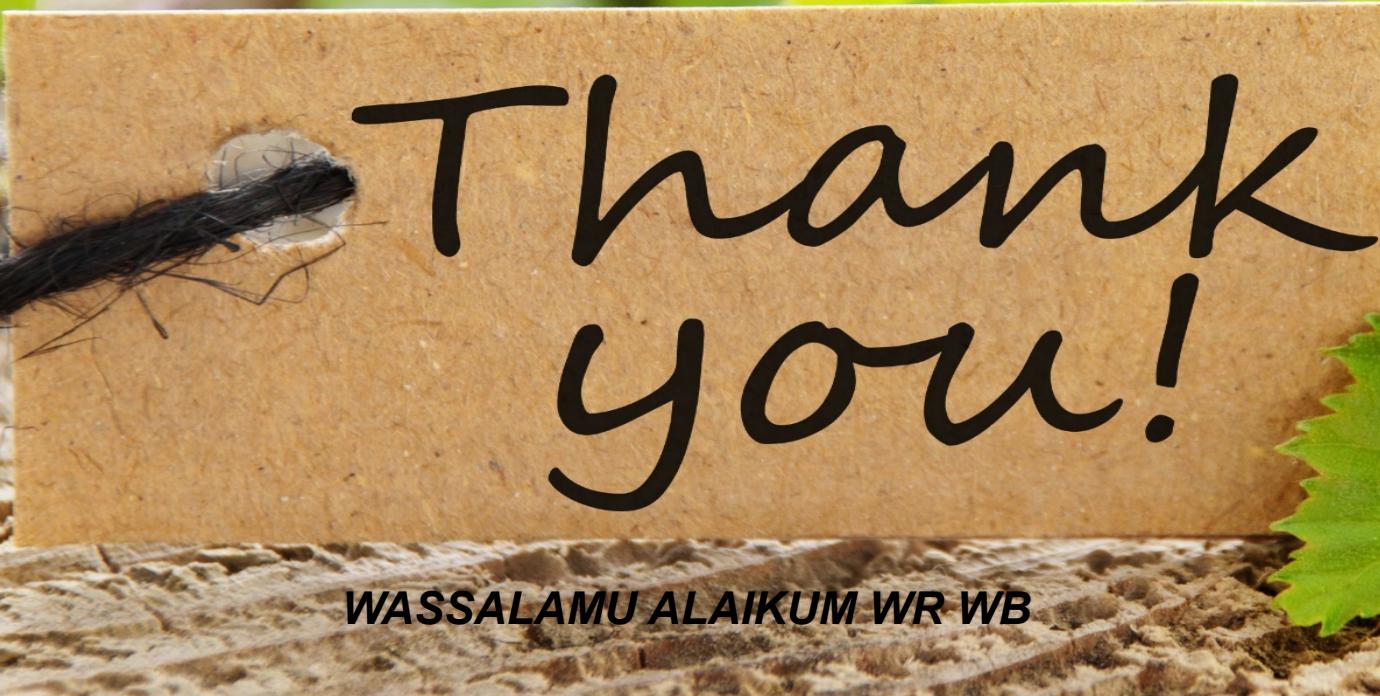
Face Book : Henri Subiakto

Instagram : Henri_Subiakto

Website : henrisubiakto.com

WA /line : 0818522902

You Tube : Henri Subiakto



WASSALAMU ALAIKUM WR WB

