LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PENINGKATAN PERAN PEMERINTAH DALAM PERLINDUNGAN DATA PRIBADI DI RUANG DIGITAL GUNA MEMPERKUAT KEAMANAN NASIONAL

Oleh:

H. M. SABILUL ALIF, S.H., S.I.K., M.Si
KOMISARIS BESAR POLISI

KERTAS KARYA ILMIAH PERORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN (PPRA) LXIII
LEMHANNAS RI
TAHUN 2022

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur kehadirat Tuhan Yang Maha Esa serta atas segala rahmat dan petunjuk serta karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXIII tahun 2022 telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Perseorangan (Taskap) dengan judul: **"PENINGKATAN PERAN PEMERINTAH DALAM PERLINDUNGAN DATA PRIBADI DI RUANG DIGITAL GUNA MEMPERKUAT KEAMANAN NASIONAL."**

Pada kesempatan ini, perkenankan penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXIII tahun 2022 di Lemhannas RI. Ucapan yang sama juga penulis sampaikan kepada Pembimbing atau Tutor Taskap kami, yaitu Bapak Mayjen TNI Sugeng Santoso, S.I.P, Bapak/Ibu Tim Penguji Taskap, serta semua pihak yang telah membantu dan membimbing dalam penulisan dan penyusunan Taskap ini hingga selesai tepat waktu dan sesuai dengan ketentuan yang telah ditetapkan oleh Lemhannas RI.

Penulis menyadari, bahwa Taskap ini masih jauh dari kesempurnaan akademis. Oleh karena itu, dengan segala kerendahan hati mohon kiranya masukan maupun kritikan guna perbaikan-perbaikan dalam rangka penyempurnaan naskah ini. Besar harapan saya Taskap ini dapat bermanfaat sebagai sumbangan pemikiran dari penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya dalam rangka upaya perlindungan data pribadi di ruang digital guna memperkuat keamanan nasional.

Semoga Allah *Subhanahu wa Ta'ala*, Tuhan Yang Maha Esa senantiasa memberikan kekuatan, petunjuk, serta bimbingan kepada kita

semua dalam melaksanakan tugas dan pengabdian kepada masyarakat, bangsa, dan negara Indonesia yang kita cintai dan kita banggakan.

Sekian dan terima kasih.

Wassalamualaikum Warahmatullahi Wabarakatuh.

Jakarta, Agustus 2022

H. M. SABILUL ALIF, S.H., S.I.K., M.Si

KOMISARIS BESAR POLISI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini:

   Nama : H. M. Sabilul Alif, S.H., S.I.K., M.Si

   Pangkat : Komisaris Besar Polisi

   Jabatan : Pamen SSDM Polri (Ajudan Wakil Presiden RI)

   Instansi : SSDM Polri

   Alamat : Jl. Trunojoyo, No 3, Kebayoran Baru, Jakarta Selatan

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) LXIII tahun 2022 menyatakan dengan sebenarnya, bahwa:

   a. Kertas Karya Ilmiah Perseorangan (Taskap) yang saya tulis adalah asli.

   b. Apabila ternyata sebagian atau seluruhnya tulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus pendidikan.

2. Demikian pernyataan keaslian ini dibuat untuk dapat digunakan seperlunya.

TANHANA DHARMMA MANGRVA

Jakarta, Agustus 2022
Penulis Taskap

(Materai Rp. 10.000)

H. M. SABILUL ALIF, S.H., S.I.K., M.Si
KOMISARIS BESAR POLISI

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

LEMBAR PERSETUJUAN TUTOR TASKAP

Yang bertanda tangan di bawah ini Tutor Taskap dari:

Nama	:	Kombes. Pol. H. M. Sabilul Alif, S.H., S.I.K., M.Si
Peserta	:	Program Pendidikan Reguler Angkatan LXIII Tahun 2022
Judul Taskap	:	Peningkatan Peran Pemerintah Dalam Perlindungan Data Pribadi di Ruang Digital Guna Memperkuat Keamanan Nasional.

Taskap tersebut di atas telah ditulis "sesuai/~~tidak sesuai~~" dengan Petunjuk Teknis tentang Penulisan Ilmiah Peserta Pendidikan Lemhannas RI Tahun 2022, karena itu "layak/~~tidak layak~~" dan "disetujui/~~tidak disetujui~~" untuk diuji.

Jakarta, Agustus 2022
Tutor Taskap

SUGENG SANTOSO, S.I.P
MAYOR JENDERAL TNI

DAFTAR ISI

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1. Latar Belakang

Perkembangan bidang teknologi informasi yang memasuki era revolusi industri 4.0 telah mempengaruhi dan terhubung ke dalam berbagai dimensi kehidupan manusia. Terlebih dalam situasi pandemi *Corona Virus Disease 2019 (Covid-19)* dimana pemerintah membatasi mobilitas masyarakat, maka penggunaan internet dan media komunikasi berkembang demikian pesatnya. Ruang-ruang digital kini dipenuhi dengan data-data pribadi yang tersebar di media sosial, *e-commerce*, sistem pembayaran elektronik, dan lain sebagainya yang sebelumnya hanya digunakan untuk kepentingan administrasi, layanan sosial, bisnis, maupun sekadar hiburan. Dalam pertukaran data-data pribadi di ruang digital, dibutuhkan adanya keseimbangan antara hak privasi (hak pribadi), kepentingan ekonomi, dan juga kesejahteraan individu.[1]

Berdasarkan data *Internetworldstats*, Indonesia tercatat sebagai negara pengguna internet terbesar ketiga di Asia dengan jumlah pengguna internet sebanyak 204,7 (dua ratus empat koma tujuh) juta jiwa pada Januari 2022[2] dari total populasi Indonesia yang berjumlah 273,879 (dua ratus tujuh puluh tiga koma delapan ratus tujuh puluh sembilan) juta jiwa berdasarkan data kependudukan yang dirilis oleh Kemendagri melalui Direktorat Jenderal Dukcapil tahun 2021.[3] Berdasarkan laporan *Hootsuite* dan

[1] Anggi Kusumoningtyas, *et.all, Dilema Hak Perlindungan Data Pribadi dan Pengawasan Siber: Tantangan di Masa Depan*, Jurnal Legislasi Indonesia, Volume 17,Nomor 2, (Juni 2020), Sekolah Kajian Stratejik dan Global, Universitas Indonesia, hlm. 240.

[2] Viva Budy Kusnandar, 2021, *Pengguna Internet Indonesia Peringat Ke-3 Terbanyak di Asia,* https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia#:~:text=Berdasarkan%20data%20internetworldstats%2C%20pengguna%20internet,pengguna%20internet%20terbanyak%20di%20Asia, (diakses pada 29 Januari 2022, pukul 13.30 WIB).

[3] Dukcapil.kemendagri.go.id, 2022, 273 juta Penduduk Indonesia Terupdate Versi Kemendagri, https://dukcapil.kemendagri.go.id/berita/baca/1032/273-juta-penduduk-indonesia-terupdate-versi-kemendagri#:~:text=Jakarta%20%2D%20Kemendagri%20melalui%20Direktorat%20Jenderal,Indonesia%20adalah%20273.879.750%20jiwa, (diakses pada 28 Mei 2022, pukul 12.06 WIB).

We Are Social, sekitar 191 (seratus sembilan puluh satu) juta jiwa di antara pengguna internet tersebut adalah pengguna aktif media sosial dengan penggunaan *mobile connection* rata-rata sebanyak 345,3 (tiga ratus empat puluh lima koma tiga) juta. Sebanyak 73,7% (tujuh puluh tiga koma tujuh persen) warga Indonesia kini sudah tersentuh oleh dunia maya. Jumlah perangkat *mobile* yang terkoneksi di Indonesia juga turut melonjak menjadi 345,3 (tiga ratus empat puluh lima koma tiga) juta.[4]

Pesatnya perkembangan data pribadi yang memenuhi ruang digital selain diakibatkan oleh kepentingan para pengguna media elektronik (secara sengaja), juga dapat diakibatkan adanya tindakan-tindakan abai terhadap perlindungan data pribadi (secara tidak sengaja) yang dilakukan oleh para pengguna media sosial. Data pribadi atau informasi pribadi dapat mengidentifikasi individu, termasuk tetapi tidak terbatas pada nama, alamat, tanggal lahir, status perkawinan, informasi kontak, ID dan tanggal kedaluwarsa, catatan keuangan, informasi kredit, riwayat kesehatan, lokasi bepergian, serta preferensi barang dan jasa.[5]

Di Indonesia sendiri telah terjadi beberapa kasus penyalahgunaan data pribadi, seperti kasus kebocoran data Bank Indonesia (BI) yang dilakukan oleh kelompok peretas asal Rusia bernama *Conti Ransomware,* yang meretas data dengan kapasitas 487 (empat ratus delapan puluh tujuh) MB *(Mega Bite)* dari 16 (enam belas) *Personal Computer* (PC) pada 21 Januari 2022.[6] Pernah juga terjadi kebocoran 297 (dua ratus sembilan puluh tujuh) juta data peserta Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, dimana data tersebut diperjualbelikan di *Raid Forums.*[7] Kasus-kasus lainnya adalah terjadinya kebocoran data pribadi dari 2 (dua) juta nasabah Bank Rakyat

---

[4] *Ibid.*

[5] Sinta Dewi Rosadi, *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional,* (Bandung: Widya Padjajaran, 2009), hlm. 13.

[6] Fahmi Ahmad Burhan, 2022, *Ahli IT: Data Bocor Bank Indonesia Berasal dari 200 Komputer,* https://katadata.co.id/desysetyowati/digital/61ee713f52c6d/ahli-it-data-bocor-bank-indonesia-berasal-dari-lebih-200-komputer, (diakses pada 29 Januari 2022, pukul 14.02 WIB).

[7] M. Ikhsan, 2021, *279 Juta Data Penduduk RI Diduga Bocor dan Dijual di Forum,* https://www.cnnindonesia.com/teknologi/20210520140736-185-644759/279-juta-data-penduduk-ri-diduga-bocor-dan-dijual-di-forum, (diakses pada 29 Januari 2022, pukul 15.12 WIB).

Indonesia (BRI) *Life*, kebocoran data akun pengguna Tokopedia, hingga kebocoran data pemilih dari Komisi Pemilihan Umum (KPU).[8]

Menurut Otoritas Jasa Keuangan (OJK), terdapat kerugian senilai Rp246 (dua ratus empat puluh enam) miliar rupiah akibat serangan siber *(cyber attack)* di bidang perbankan Indonesia pada semester I (satu) tahun 2020 hingga semester I (satu) tahun 2021. Di samping itu terdapat potensi kerugian yang mencapai hingga Rp208 (dua ratus delapan) miliar rupiah dari serangan yang sama pada periode yang sama. Sedangkan secara global, kerugian rata-rata mencapai US$100 (seratus) miliar dollar Amerika atau Rp1.430 (seribu empat ratus tiga puluh) triliun rupiah (dengan asumsi kurs Rp14.300/US$).[9]

Selain di dunia perbankan, kebocoran data pribadi juga menimpa *platform e-commerce,* salah satunya Tokopedia dimana sebanyak 91 (sembilan puluh satu) juta data pelanggan bocor dan disebar di forum internet oleh oknum yang tidak bertanggung jawab pada tahun 2020. Kebocoran data pribadi di ranah *e-commerce* tentunya merugikan berbagai pihak termasuk negara, karena kebocoran data berpotensi menimbulkan ketidakpercayaan *(distrust)* masyarakat terhadap *platform e-commerce* tersebut. Padahal, di era digital saat ini khususnya di tengah terjadinya pandemi *Corona Virus Disease 2019 (Covid-19),* mobilitas masyarakat dibatasi guna memutus rantai penularan virus. Pembatasan ini mengarahkan masyarakat untuk lebih banyak melakukan transaksi jual beli secara *online.* Namun, jika tingkat kepercayaan masyarakat terhadap *e-commerce* menurun, maka tingkat jual beli juga akan menurun, sehingga secara langsung atau tidak langsung akan berdampak pada perekonomian nasional.

Polisi Siber Mabes Polri mencatat terdapat sebanyak 182 (seratus delapan puluh dua) kasus pencurian data yang dilaporkan oleh masyarakat. Dalam kurun waktu 5 (lima) tahun terakhir (2016-2020), peningkatan laporan

---

[8] Caesar Akbar, 2021, *6 Kasus Kebocoran Data Pribadi di Indonesia,* https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia, (diakses pada 29 Januari 2022, pukul 15.18 WIB).

[9] Monica Wareza, 2021, *Ini Serius! Serangan Siber Bikin Bank-Bank RI Rugi Rp246M,* https://www.cnbcindonesia.com/market/20211026131120-17-286621/ini-serius-serangan-siber-bikin-bank-bank-ri-rugi-rp-246-m, (diakses pada 29 Januari 2022, pukul 14.25 WIB).

pencurian data meningkat sebesar 810% (delapan ratus sepuluh persen) dari 20 (dua puluh) laporan pada tahun 2016.[10] Memang, saat ini tata cara dan pengelolaan keamanan siber di Indonesia sifatnya masih cenderung parsial dan sektoral yang ditangani oleh masing-masing lembaga dan sektor-sektor swasta tertentu.

Hal ini menjadi tantangan tersendiri dalam penanganan permasalahan keamanan siber. Perlindungan data pribadi menjadi amat krusial dan strategis mengingat hak privasi seseorang yang menyangkut nama lengkap, alamat, *email*, nomor telepon, rekening bank, bahkan sampai dengan riwayat kesehatan telah dicuri atau dibocorkan. Ketika jumlahnya masif mencapai ribuan bahkan jutaan orang, maka hal ini berpotensi dapat mengancam keamanan nasional.[11] Kumpulan makro informasi pribadi dari masyarakat suatu wilayah apabila dikelola akan dapat merepresentasikan suatu keadaan ekonomi, sosial-politik, dan data-data lainnya. Apabila data ini disalahgunakan, maka dapat mengancam kedaulatan suatu negara, sehingga mengganggu keamanan nasional.

Berbagai upaya yang dilakukan oleh pemerintah terkait perlindungan data pribadi saat ini masih berorientasi pada tindakan represif. Pemerintah cenderung baru bertindak apabila kebocoran data sudah terjadi. Tindakan-tindakan yang dilakukan pun masih sebatas pemblokiran situs, sementara penangkapan dan pemidanaan baru dilakukan setelah kasus kebocoran data pribadi menjadi viral di media sosial. Upaya yang dilakukan oleh Kemkominfo melalui penerapan program Penyelenggara Sistem Elektronik (PSE) juga masih menuai pro dan kontra dari masyarakat. Sedangkan upaya preventif yang dilakukan adalah melalui penyusunan dan perumusan aturan-aturan terkait manajemen risiko pengelolaan data, tetapi masih terpisah-pisah dan diatur oleh masing-masing lembaga, sehingga belum ada aturan yang terintegrasi dan menjadi payung hukum bagi perlindungan data pribadi di

---

[10] Dwi Hadya Jayani, 2021, *Pencurian Data Pribadi Makin Marak Kala Pandemi,* https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi, (diakses pada 29 Januari 2022, pukul 16.27 WIB).

[11] Kominfo.go.id, *Memastikan Data Pribadi Aman,* https://www.kominfo.go.id/content/detail/37332/memastikan-data-pribadi-aman/0/artikel, (diakses pada 29 Januari 2022, pukul 17.02 WIB).

Indonesia. Upaya-upaya tersebut memang perlu dilakukan, tetapi dirasa belum cukup untuk dapat mewujudkan suatu perlindungan data pribadi dalam skala besar guna memperkuat keamanan nasional.

Aturan internal yang menjadi pedoman bagi masing-masing lembaga untuk melindungi data pribadi konsumen juga dirasa belum efektif, karena masih bersifat parsial dan sektoral. Padahal kebocoran data-data pribadi yang diakibatkan oleh diserangnya sistem penyimpanan data milik lembaga-lembaga negara tentunya menjadi ancaman yang bersifat vital dan strategis. Serangan-serangan demikian tidak hanya berasal dari dalam negeri, tetapi justru lebih sering berasal dari luar negeri dengan menggunakan virus komputer, jaringan *malware* tertentu, atau bahkan rekayasa sosial yang dapat memanipulasi pengguna media sosial.

Oleh sebab itu, sudah semestinya melakukan upaya yang sistematis dan holistik (menyeluruh) dalam penanganan perlindungan data pribadi, termasuk ketersediaan instrumen dan infrastruktur keamanan digital yang memadai. Upaya sistematis yang dimaksud mencakup upaya pencegahan (preventif) yang bersifat edukatif kepada masyarakat dan pelaku transaksi digital sampai dengan mekanisme sanksi kepada pelaku. Keseluruhan ini selain harus didukung dengan infrastruktur teknologi dan sumber daya manusia, harus pula didasari oleh suatu instrumen hukum yang berkeadilan dan spesifik dalam mengatur tentang perlindungan data pribadi.

Berdasarkan penjabaran tersebut, maka peneliti tertarik untuk melakukan penelitian yang berjudul **"Peningkatan Peran Pemerintah Dalam Perlindungan Data Pribadi di Ruang Digital Guna Memperkuat Keamanan nasional."**

2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka peningkatan peran pemerintah dalam perlindungan data pribadi menjadi sangat penting, mengingat perkembangan dunia telah memasuki era revolusi industri 4.0 ditambah situasi pandemi *Covid-19* yang mendorong peningkatan penggunaan internet secara global. Penggunaan teknologi informasi dalam kehidupan sehari-hari memunculkan ancaman kejahatan pencurian data yang

dapat mempengaruhi keamanan nasional. Oleh karena itu, mencermati berbagai implikasi di atas, maka dapat diambil suatu rumusan masalah berupa: ***"Bagaimana Meningkatkan Peran Pemerintah Dalam Perlindungan Data Pribadi di Ruang Digital Guna Memperkuat Keamanan Nasional?"***

Merujuk pada rumusan masalah tersebut, maka dapat ditarik sejumlah pertanyaan kajian yang harus ditelaah lebih lanjut, yang terdiri dari:

a. Bagaimana menyusun regulasi perlindungan data pribadi di ruang digital?

b. Bagaimana menyiapkan infrastruktur perlindungan data pribadi di ruang digital?

c. Bagaimana membentuk kelembagaan khusus untuk perlindungan data pribadi di ruang digital?

d. Bagaimana membangun sistem dan metode dalam upaya melindungi data pribadi di ruang digital?

3. Maksud dan Tujuan

a. Maksud. Taskap ini dimaksudkan untuk membahas, mengkaji, dan menelaah mengenai pentingnya peningkatan peran pemerintah dalam perlindungan data pribadi di ruang digital guna memperkuat keamanan nasional.

b. Tujuan. Tujuan penulisan Taskap ini adalah untuk memberikan sumbangan pemikiran dan bahan masukan kepada pemerintah dalam melakukan berbagai kajian strategis berkaitan dengan masalah perlindungan data pribadi di ruang digital guna memperkuat keamanan nasional.

4. Ruang Lingkup dan Sistematika

Ruang lingkup penulisan Taskap ini dibatasi atau difokuskan pada peran pemerintah dalam perlindungan data pribadi di ruang digital dengan berlandaskan pada studi ketahanan nasional. Sebagaimana lazimnya penulisan Taskap Lemhannas, maka sistematika penulisannya disusun sebagai berikut:

Bab I, Pendahuluan. Bab ini berisikan tentang latar belakang penulisan, perumusan masalah, maksud dan tujuan, ruang lingkup dan sistematika, metode dan pendekatan yang digunakan, serta beberapa pengertian sebagai langkah untuk menyamakan persepsi dalam memahami pembahasan.

Bab II, Tinjauan Pustaka. Bab ini memuat dan menguraikan tentang semua pustaka yang digunakan sebagai sumber rujukan untuk melakukan pembahasan. Terdiri dari peraturan perundang-undangan, perspektif akan peran pemerintah dalam perlindungan data pribadi di ruang digital, konsepsi peran pemerintah dalam menangani kasus kebocoran data pribadi di ruang digital, kerangka teoritis, data dan fakta, faktor-faktor lingkungan strategis, serta referensi lain yang relevan dengan topik pembahasan untuk dapat menjawab pertanyaan-pertanyaan yang ada. Tinjauan pustaka yang digunakan dan diuraikan diharapkan mampu menjadikan Taskap ini sebagai tulisan akademis yang memiliki nilai strategis sebagai *strategic policy paper*.

Bab III, Pembahasan. Pada bab ini akan dijabarkan hasil analisis data dan fakta berdasarkan teori yang digunakan, sehingga akan ditemukan faktor-faktor yang mempengaruhi terjadinya/munculnya permasalahan dan dapat dirumuskan solusinya. Pembahasan pada bab ini meliputi 4 (empat) aspek dalam rumusan masalah, yang terdiri dari: (a) Regulasi perlindungan data pribadi di ruang digital; (b) Persiapan infrastruktur perlindungan data pribadi di ruang digital; (c) Pembentukan kelembagaan khusus untuk perlindungan data pribadi di ruang digital; serta (d) Sistem dan metode dalam upaya melindungi data pribadi di ruang digital.

Bab IV, Penutup. Pada bab ini penulis akan membuat simpulan dari keseluruhan pembahasan serta merekomendasikan langkah-langkah optimalisasi peningkatan peran pemerintah dalam perlindungan data pribadi di ruang digital guna memperkuat keamanan nasional.

5. Metode dan Pendekatan

a. Metode. Metode yang digunakan dalam penulisan Taskap ini adalah deskriptif analitis, yaitu metode yang menyajikan, menelaah, dan menjelaskan data maupun informasi yang berkaitan dengan materi

permasalahan, sekaligus analisis yang didasarkan pada tinjauan kepustakaan (*library research)*.

b. Pendekatan. Pendekatan yang digunakan adalah pendekatan komprehensif integral, yaitu penyelesaian masalah secara menyeluruh dengan menjangkau berbagai aspek yang terkait berdasarkan perspektif kepentingan nasional.

6. Pengertian

Guna memperoleh pengertian yang jelas dan tegas tentang beberapa istilah yang dikemukakan dalam penulisan Taskap ini dengan maksud menghindari salah tafsir serta untuk menyamakan persepsi, maka akan dicantumkan beberapa pengertian yang berkaitan dengan judul, yaitu:

a. Peran Pemerintah. Menurut Kamus Besar Bahasa Indonesia, definisi 'peran' adalah sesuatu yang dimainkan atau dijalankan. Secara terminologi, peran berarti seperangkat tingkah yang diharapkan dimiliki oleh yang berkedudukan di tengah masyarakat. Dalam Bahasa Inggris, peran disebut dengan istilah *'role'* yang bermakna *"person's task or duty in undertaking"* (tugas atau kewajiban seseorang dalam suatu usaha atau pekerjaan). Sedangkan pemerintah bermakna penyelenggara negara. Dengan demikian dapat dimaknai, bahwa peran pemerintah adalah suatu serangkaian tingkah laku yang diharapkan dimiliki oleh lembaga pemegang otoritas atau pemilik kewenangan di suatu negara.

b. Perlindungan. Istilah 'perlindungan' berasal dari kata dasar 'lindung' yang berarti menutupi supaya tidak terlihat atau tampak; tidak terkena panas, angin, udara dingin, dan sebagainya. Sementara perlindungan dapat dimaknai sebagai suatu proses, cara, dan perbuatan untuk melindungi.

c. Data Pribadi. Menurut *Organisation for Economic Co-operation and Development* (OECD) dalam *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, data pribadi adalah segala informasi yang berkaitan dengan individu (subjek data) yang diidentifikasi atau dapat mengidentifikasi. Sementara dalam EU *General Data Protection Regulation,* data pribadi dimaknai sebagai segala

informasi yang berkaitan dengan identifikasi atau dapat mengidentifikasi seorang individu (subjek data), baik secara langsung maupun tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal *online* satu atau lebih faktor spesifik untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya, atau identitas sosial dari orang tersebut.

d. Keamanan Nasional. Dalam Kamus Bahasa Indonesia, 'Keamanan Nasional' berarti kekuatan suatu bangsa untuk melindungi negaranya terhadap ancaman atau bahaya, baik dari dalam maupun dari luar negeri. Edy Prasetyono (2005) mengemukakan, bahwa keamanan nasional dapat diartikan sebagai kebijakan politik pemerintah yang bertujuan untuk menegakkan situasi yang aman dan kondusif bagi terselenggaranya pemerintahan, sehingga mampu mempertahankan tujuan vital nasional dari segala gangguan dan ancaman. Dengan demikian, keamanan nasional perlu dilihat dalam hubungannya dengan upaya untuk mencapai kepentingan nasional.[12] Keamanan nasional (kamnas) dapat dimaknai dari 2 (dua) sisi, yakni: (1) Sebagai kondisi, yaitu terciptanya rasa aman yang mencakup rasa nyaman, damai, tenteram, dan tertib; serta (2) Sebagai fungsi, yaitu merujuk pada kebijakan publik untuk memastikan terjaminnya keselamatan dan keamanan negara melalui penggunaan kuasa ekonomi dan militer serta upaya diplomasi, baik dalam kondisi damai maupun perang.

[12] Susi, 2019, *Memahami Konsep Keamanan,* https://tribratanews.kepri.polri.go.id/2019/07/17/memahami-konsep-keamanan-3/, (diakses pada 6 Mei 2022, pukul 19:00 WIB).

BAB II
TINJAUAN PUSTAKA

7. Umum

Pada bab ini akan diuraikan mengenai sumber-sumber kepustakaan yang merujuk pada pembahasan yang terdiri dari peraturan perundang-undangan; kerangka teoretis; data/fakta mengenai perlindungan data pribadi di Indonesia; serta perkembangan lingkungan strategis, baik secara global, regional, maupun nasional. Kemajuan teknologi informasi dan media sosial dewasa ini membawa perubahan dan sangat berpengaruh terhadap setiap aspek kehidupan manusia. Media komunikasi digital yang secara meluas digunakan oleh seluruh lapisan masyarakat termasuk Indonesia, secara sengaja maupun tidak sengaja akan memuat informasi-informasi mengenai data pribadi, dimana informasi tersebut seyogianya mendapat perlindungan secara khusus, karena mengandung hak privat di dalamnya. Ketidakamanan data pribadi yang secara masif dan terus menerus dibiarkan dapat berdampak negatif terhadap stabilitas negara, berupa terjadinya disintegrasi bangsa yang berpotensi mengancam keamanan nasional.

8. Peraturan Perundang-Undangan

Peran pemerintah dalam perlindungan data pribadi di ruang digital guna memperkuat keamanan nasional harus berlandaskan pada regulasi yang berlaku dan diterapkan di Indonesia, antara lain:

a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Di dalam UUD NRI 1945, kebebasan untuk berkomunikasi dijamin oleh negara, termasuk hak mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi melalui penggunaan segala jenis saluran yang tersedia, termasuk melalui media telekomunikasi, sebagaimana tertuang dalam pasal 28F. Dalam Pasal 28H ayat (4) juga disebutkan, bahwa terdapat penjaminan hak bagi setiap orang untuk memiliki hak milik pribadi yang tidak boleh diambilalih secara sewenang-wenang oleh siapa pun, yang dalam hal ini berarti termasuk pada perlindungan data pribadi sebagai hak privat (hak pribadi). Sementara dalam konteks upaya mempertahankan keamanan nasional dituangkan

dalam konstitusi Pasal 30 ayat (1) dan ayat (2). Pasal ini mengalami perubahan setelah amandemen kedua UUD 1945 melalui Sidang tahunan MPR 7-18 Agustus 2000. Jika sebelum amandemen Pasal 30 ayat (1) menyebutkan, bahwa setiap warga negara berhak dan wajib ikut serta dalam usaha pembelaan negara, maka setelah amandemen pasal ini berubah bunyinya menjadi menyatakan, bahwa tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara. Usaha tersebut dilaksanakan melalui sistem pertahanan dan keamananrakyat semesta oleh Tentara Nasional Indonesia (TNI) dan Kepolisian Negara Republik Indonesia (Polri) sebagai kekuatan utama, dan rakyat sebagai kekuatan pendukung perlindungan negara.

b. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Perlindungan mengenai data pribadi dalam undang-undang ini diatur dalam Pasal 84 dan Pasal 85. Pasal 85 ayat (1) secara tegas menyebutkan, bahwa data pribadi penduduk wajib disimpan dan dilindungi oleh negara. Kemudian dalam ayat (3) disebutkan, bahwa data pribadi penduduk harus dijaga dan dilindungi kebenaran dan kerahasiaannya oleh penyelenggara dan instansi pelaksana sesuai dengan peraturan perundang-undangan yang berlaku.

c. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Pada dasarnya undang-undang ini bertujuan untuk menciptakan suatu sistem pemerintahan dengan keterbukaan informasi publik guna mewujudkan *good governance*, yaitu yang transparan, efektif dan efisien, akuntabel, serta dapat dipertanggungjawabkan. Hal ini diamanatkan dalam Pasal 3 huruf d. Namun, secara tegas dalam Pasal 17 huruf f juga diatur mengenai jenis-jenis informasi yang dikecualikan untuk dibuka aksesnya bagi masyarakat umum/pemohon, termasuk informasi publik yang jika dibocorkan akan dapat mengungkap rahasia pribadi. Secara tegas pula dalam Pasal 17 huruf c disebutkan, bahwa salah satu informasi yang dikecualikan untuk dibuka aksesnya adalah informasi publik yang dapat membahayakan pertahanan dan keamanan negara.

d. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dalam undang-undang ini diatur, bahwa penggunaan setiap informasi yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan yang bersangkutan sebagaimana tertuang dalam Pasal 26 ayat (1). Pada bagian penjelasan pasal tersebut dijelaskan, bahwa yang dimaksud dengan data pribadi adalah salah satu bagian dari hak pribadi *(privacy rights).* Dalam pasal 30 juga menyebutkan larangan mengenai perbuatan seseorang dengan sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

e. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Aturan ini secara terbatas tetapi tegas mengatur mengenai perlindungan data pribadi yang harus dilakukan oleh penyelenggara sistem elektronik. Dalam Pasal 14 ayat (1) angka 3 disebutkan, bahwa penyelenggara sistem elektronik wajib melaksanakan prinsip perlindungan data pribadi dalam melakukan pemrosesan data pribadi, yakni dengan memberikan perlindungan keamanan data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau pengrusakan data pribadi.

f. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Dalam Pasal 2, yang dimaksud dengan perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Pengelolaan perlindungan data pribadi dalam sistem elektronik ini dititikberatkan pada setiap penyelenggara sistem elektronik, sebagaimana tercantum dalam Pasal 5.

g. Surat Keputusan Bersama Menteri Komunikasi dan Informatika Republik Indonesia, Jaksa Agung Republik Indonesia, dan Kepala Kepolisian Negara Republik Indonesia Nomor 229 Tahun 2021,

Nomor 154 tahun 2021, Nomor KB/2/VI/2021 tentang Pedoman Implementasi Atas Pasal Tertentu Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Sebagaimana Telah Diubah Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik. Surat Keputusan Bersama ini merupakan hasil pengkajian komprehensif oleh kementerian dan lembaga di bidang informasi dan transaksi elektronik dengan melibatkan unsur masyarakat, akademisi, Dewan Perwakilan Rakyat (DPR), dan pers. Surat Keputusan Bersama ini menjadi pedoman implementasi bagi aparat penegak hukum dalam melaksanakan tugas dan kewajibannya, sehingga dapat tercipta dan terjaga ruang digital yang bersih, sehat, beretika, produktif, dan berkeadilan.

9. Kerangka Teoritis

Adapun teori yang akan digunakan, adalah sebagai berikut:

a. Teori Peran Pemerintah. Menurut Soerjono Soekanto, efektivitas suatu hukum ditentukan oleh 5 (lima) faktor, yang meliputi: (1) Hukum itu sendiri (undang-undang); (2) Penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum; (3) Sarana atau fasilitas yang mendukung penegakan hukum; (4) Masyarakat, yakni lingkungan di mana hukum tersebut berlaku atau diterapkan; serta (5) Kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.[13] Dalam hal peran pemerintah, Soerjono Soekanto (2002:243) berpendapat, bahwa peran merupakan aspek dinamis kedudukan (status) seseorang dimana jika ia melaksanakan kewajibannya sesuai dengan kedudukannya, maka ia menjalankan suatu peranan. Peran juga dapat dirumuskan sebagai rangkaian perilaku yang timbul dari jabatan tertentu. Faktor kepribadian turut mempengaruhi bagaimana peran tersebut dijalankan. Peran adalah

[13] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, (Jakarta: PT Raja Grafindo Persada), 2008, hlm. 8.

tindakan atau perilaku seseorang pada suatu posisi dalam status sosial. Miftha Thoha (2005:10) berpendapat, bahwa peranan merupakan suatu rangkaian perilaku yang ditimbulkan oleh suatu jabatan. Dengan demikian, peran merupakan suatu rangkaian kegiatan teratur yang timbul dari adanya suatu jabatan.

Menurut Henry J. Abraham (Tjokroamidjojo, 1988:18), peranan pemerintah digambarkan dalam 3 (tiga) bentuk, yang terdiri dari:

1) Mula-mula peranan pemerintah adalah sebagai penjaga keamanan dan ketertiban dalam perkembangan.
2) Selanjutnya timbul pengertian tentang *service state*, dimana peranan pemerintah merupakan abdi sosial dari keperluan-keperluan yang perlu diatur dalam masyarakat.
3) Kemudian terdapat peranan pemerintah sebagai *entrepreneur* atau pendorong inisiatif usaha pembaharuan dan pembangunan masyarakat. Pemerintah menjadi *'development agent'* atau unsur pendorong pembaharuan/pembangunan.

Dalam Tjokroamidjojo (1988:19) disebutkan, bahwa klasifikasi lain dari cara pelaksanaan peranan pemerintah dapat dirumuskan melalui pendapat Irving Swerdlow, bahwa keterlibatan pemerintah dalam proses perkembangan kegiatan masyarakat dapat dilakukan dengan 5 (lima) cara, yang terdiri dari:

1) Operasi langsung *(operation)*: Pemerintah menjalankan sendiri kegiatan-kegiatan tertentu.
2) Pengendalian langsung *(direct control)*: Penggunaan perizinan, lisensi (untuk kredit, kegiatan ekonomi lain), penjatahan, dan lain sebagainya. Dilakukan oleh badan-badan pemerintahan yang telah atau berusaha menjadi *'action ladern'* (yang berwenang dalam berbagai perizinan, alokasi, tarif, dan lain sebagainya).
3) Pengendalian tidak langsung *(indirect control)*: Memberikan pengaturan dan syarat-syarat tertentu.
4) Pemengaruhan langsung *(direct influence)*: Melakukan persuasi dan nasihat misalnya supaya golongan masyarakat tertentu dapat turut menggabungkan diri dalam koperasi atau program tertentu.

5) Pemengaruhan tidak langsung *(indirect influence)*: Merupakan bentuk ketererlibatan yang paling sederhana, misalnya pemberian informasi, penyuluhan, dan pembinaan untuk dapat menerima hal-hal yang baru *(promoting a receptive attitude toward innovation).*

b. Teori Keamanan Nasional *(National Security).*[14] Keamanan secara umum dapat diartikan sebagai '*security.'* Awalnya konsep keamanan *(security)* terbatas pada pengertian tentang keamanan suatu negara yang melingkupi wilayah teritorial dan keselamatan populasi (warga negara) di negara tersebut. Komisi Konstitusi (2004) mengutip pendapat Patrick J. Garrity mengemukakan, bahwa pengertian *security* adalah *"closely tied to a state's defense of sovereign interest by military means. At its most fundamental level, the term security has meant the effort to protect a population and territory against organized force while advancing state interest through competitive behavior."*[15]

Dalam diskursus tradisional, para ilmuwan menafsirkan keamanan secara sederhana, yaitu suasana yang bebas dari segala bentuk ancaman bahaya, kecemasan, dan ketakutan, atau sebagai suatu kondisi dimana tidak terdapat ancaman fisik (militer) yang berasal dari luar.[16] Sementara diskursus kontemporer mendefinisikan keamanan secara fleksibel dan longgar dengan memasukkan unsur dan perspektif yang tidak terdapat dalam diskursus tradisional. Menurut Caroline Thomas dan Jessica Mathews, keamanan bukan hanya berkaitan dengan *nexus military-external*, tetapi juga menyangkut dimensi-dimensi lain yang menentukan eksistensi suatu negara.[17] Berdasarkan pengertian ini, maka diskursus kontemporer memandang keamanan nasional sebagai suatu upaya untuk memantapkan keamanan internal bangsa, ketersediaan pangan, fasilitas kesehatan dan pendidikan, uang,

---

[14] Mukhtar Sidratahta, *Pemberantasan Terorisme di Indonesia dan Dampaknya Terhadap Keamanan Nasional,* Makalah Seminar Sehari, Departemen Ilmu Hubungan Internasional, Universitas Hasanuddin, (2009), Makassar, hlm. 5.

[15] Susi, 2019*, Op. Cit.*

[16] Kusnanto Anggoro, *Keamanan Nasional, Pertahanan Negara, dan Ketertiban Umum,* Makalah Pembanding Seminar Pembangunan Hukum Nasional VIII, (Juli 2003), Departemen Kehakiman dan HAM RI, hlm.1.

[17] *Ibid.*

perdagangan, pengembangan alutsista, serta kepentingan warga negara yang dalam hal ini juga menyangkut keamanan data pribadi sebagai hak atas privasi.

Titik temu antara diskursus kontemporer dengan diskursus tradisional merupakan *state adequateness*. Sebagai perwakilan masyarakat dalam melaksanakan kebijakan negara, pemerintah harus memiliki memenuhi elemen kenegaraan yang memadai *(adequate stateness)*, terutama dalam menciptakan keseimbangan antara kemampuan menggunakan kekerasan *(coercive capacity)*, kekuatan infrastruktural *(infrastructural power),* dan legitimasi tanpa syarat *(unconditional legitimacy).*[18]

Barry Buzan mengelompokkan keamanan ke dalam 5 (lima) kategori umum, yaitu: (1) Keamanan militer; (2) Keamanan politik; (3) Keamanan lingkungan; (4) Keamanan ekonomi; dan (5) Keamanan sosial. Buzan beranggapan, bahwa keamanan tidak semata merujuk pada sudut pandang negara *(state security)* secara sempit dimana jika kebutuhan pokok masyarakat terpenuhi dan rakyat dianggap sejahtera, maka secara otomatis akan tercipta keamanan. Seiring perkembangannya, konsep keamanan nasional turut mengalami pergeseran makna, dari yang semula mengusung konsep keamanan berpusat pada negara *(state centered security)* menjadi berkonsep keamanan berpusat pada orang/masyarakat *(people centered security)*. Perubahan tersebut kini mengacu pada pandangan, bahwa keamanan nasional harus mencakup *state security* (keamanan negara), *public security* (keamanan masyarakat), dan *human/people security* (keamanan manusia).

10. Data dan Fakta

a. Pelanggaran Data Pribadi Sebagai Hak Privasi

Perkembangan bisnis yang turut merambah dunia digital telah memasuki era *data driven economy,* yaitu industrialisasi dengan memanfaatkan teknologi digital berbasis utilisasi data *(big data).* Entitas

[18] *Ibid.*

yang memiliki akses pada *big data* akan meraih *information advantage* lebih besar daripada entitas yang tidak memiliki akses tersebut. Di era ini, data berperan sebagai objek yang bernilai untuk diperdagangkan. Akuisisi data direkam menggunakan *platform realtime* seperti media sosial, mesin pencari, dan lain sebagainya.[19]

Data pribadi merupakan hak milik setiap orang sebagai hak asasi manusia atau dapat disebut sebagai hak privasi. Oleh sebab itu, data pribadi seseorang tidak boleh dihimpun dan disebarluaskan secara bebas, apalagi tanpa seizin pemilik data pribadi tersebut. Potensi pelanggaran hak privasi yang paling banyak menimbulkan kerugian adalah kegiatan pengumpulan data pribadi yang dilakukan secara massal *(digital dossier).* Melalui internet, pihak swasta maupun para penyelenggara sistem transaksi elektronik lainnya menjadi pelaku *digital dossier*.[20] Suatu penyelenggara sistem transaksi elektronik dapat memperoleh informasi konsumen dengan cara membeli informasi tersebut dari jasa perusahaan pengumpul data.[21]

Hal ini menciptakan potensi pelanggaran serius, seperti halnya kasus bobolnya data pengguna *iCloud* (komputasi awan yang disediakan oleh *Apple*) yang kemudian menyebar di beberapa media massa. Kasus ini mendapat banyak perhatian publik, karena beberapa data yang bocor adalah milik beberapa selebritis terkenal Hollywood, seperti Jennifer Lawrence, Jenny McCarthy, Rihanna, Kate Upton, Mary Elizabeth Winstead, Kristen Dunst, Ariana Grande, dan Victoria Justice.[22]

Potensi pelanggaran privasi di media sosial tidak hanya disebabkan adanya praktik jual beli yang dilakukan oleh pihak swasta maupun penyelenggara transaksi elektronik, tetapi lebih jauh lagi potensi

---

[19] Johny G Plate, *Rencana Pengaturan Perlindungan Data Pribadi sebagai Penyeimbang Pesatnya Perkembangan Teknologi Digital di Sektor Jasa Keuangan*, pemaparan disampaikan pada Webinar Indonesia Banking School, Kementerian Komunikasi dan Informatika RI, (Jakarta, 20 Agustus 2021).

[20] Solove, Daniel J, *The Digital Person, Technology and Privacy in the Information Age,* (New York: West Group Publication, New York University Press, 2004), hlm. 13-17, sebagaimana dikutip dalam Naskah Akademik RUU Perlindungan Data Pribadi, 2021, hlm. 4.

[21] *Ibid.*

[22] Naskah Akademik RUU Perlindungan Data Pribadi, (Jakarta, 2019), hlm. 43.

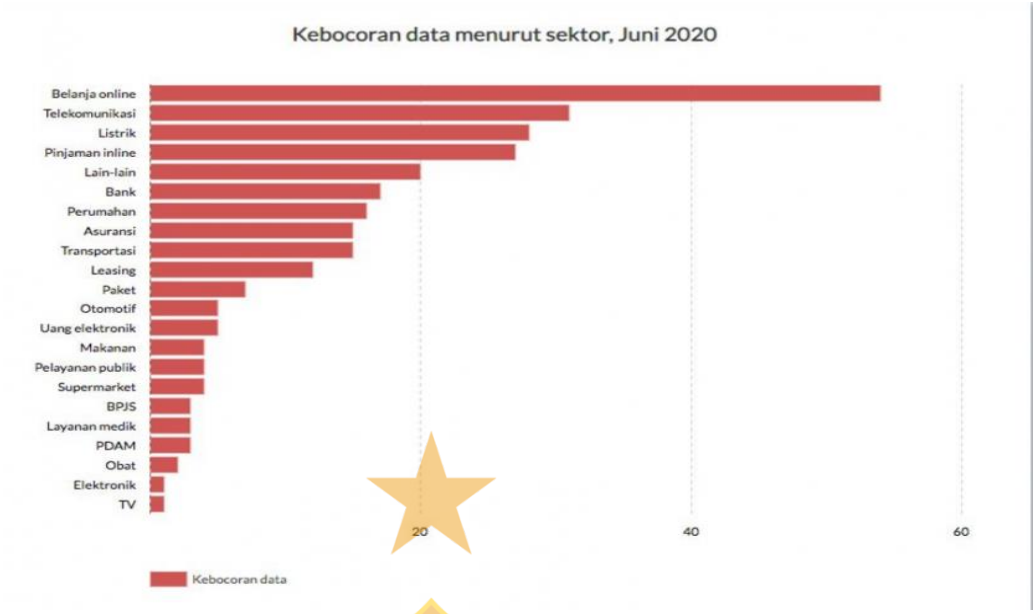
pelanggaran privasi juga dapat muncul melalui program yang digulirkan oleh pemerintah dengan keterlibatan pihak swasta, seperti program KTP elektronik (e-KTP), kesehatan elektronik *(e-health),* dan sejenisnya. Berdasarkan informasi kebocoran dari *Kawat Wikileaks* yang merilis presentasi sebuah perusahaan Inggris *ThorpeGlen* pada tahun 2008, e-KTP justru membuat keberadaan dan aktivitas masyarakat dapat terlacak dengan mudah.[23] Pemanfaatan metode e-KTP membuat negara bisa dengan leluasa dan mudah mengamati kehidupan pribadi setiap warganya, sehingga kebebasan sipil dilanggar dengan semena- mena.[24]

Khususnya di Indonesia, kasus kebocoran data pribadi kerap terjadi, salah satu yang menyita perhatian publik adalah bocornya 279 (dua ratus tujuh puluh sembilan) juta data pengguna BPJS (Badan Penyelenggara Jaminan Sosial) pada pertengahan Mei 2021. Data yang bocor meliputi Nomor Induk Kependudukan (NIK), nama, alamat, nomor telepon, alamat *e-mail,* dan foto pengguna BPJS dimana data tersebut dijual di situs *Raid Forums* senilai 0,15 (nol koma lima belas) BTC atau setara dengan Rp70-80 (tujuh puluh sampai dengan delapan puluh) juta rupiah. Kasus kebocoran data ini bukan yang pertama kali terjadi di Indonesia. Tahun sebelumnya, sebanyak 91 (sembilan puluh satu) juta data pengguna dan 7 (tujuh) juta data *merchant* Tokopedia diretas dan dijual di situs daring. Begitu pula dengan 2,3 (dua koma tiga) juta data Pemilu tahun 2014 milik KPU (Komisi Pemilihan Umum) dan 230 (dua ratus tiga puluh) ribu data pasien *Corona Virus Disease 2019 (Covid-19).*[25]

[23] Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privacy di Internet-Beberapa Penjelasan Kunci,* (Jakarta: Elsam, 2014), hlm. 23

[24] Naskah Akademik RUU Perlindungan Data Pribadi, *Op. Cit.,* hlm. 40.

[25] Andrea Lidwina, 2021, *Kebocoran Data Pribadi yang Terus Berulang,* Kebocoran Data Pribadi yang Terus Berulang - Infografik Katadata.co.id, (diakses pada 13 Februari 2022, pukul 21.07 WIB).



Gambar 1. Kebocoran Data Pribadi Berdasarkan Sektor, Juni 2022
Sumber: https://retizen.republika.co.id/posts/12998/kebocoran-data- pribadi-urgensi-pengesahan-ruu-perlindungan-data-pribadi

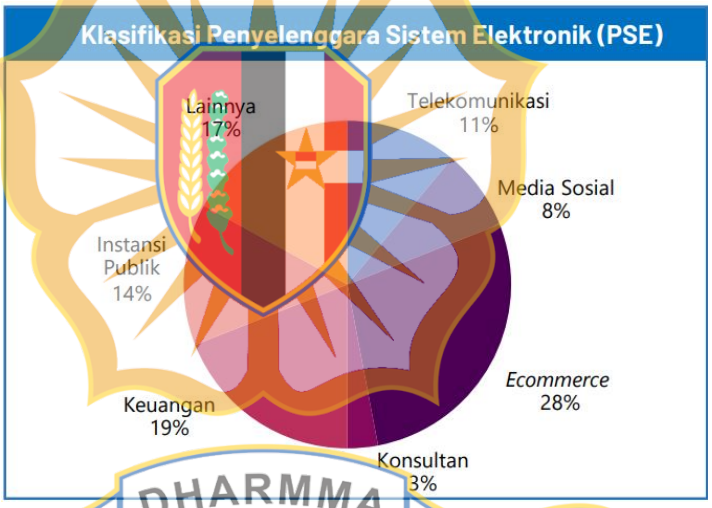
Berdasarkan data yang dirilis oleh Yayasan Lembaga Konsumen Indonesia di atas terlihat, bahwa pengaduan mengenai kebocoran data pribadi pada Juni 2020 paling banyak dialami oleh industri belanja *online (e-commerce),* yakni sebanyak 54 (lima puluh empat) kasus. Sejak Januari hingga Juni, total kasus kebocoran data mencapai hingga 277 (dua ratus tujuh puluh tujuh) kasus. Industri telekomunikasi menjadi industri kedua yang paling rentan mengalami kebocoran data, yakni 31 (tiga puluh satu) kasus.

b. Pengguna Internet di Indonesia

Menurut data dari *We Are Social* pada bulan Januari 2022, sekitar 204,7 (dua ratus empat koma tujuh) juta dari total populasi Indonesia yang berjumlah 273.879.750 (dua ratus tujuh puluh tiga juta delapan ratus tujuh puluh sembilan ribu tujuh ratus lima puluh) jiwa adalah pengguna internet, dimana sekitar 191 (seratus sembilan puluh satu) juta jiwa di antaranya adalah pengguna aktif media sosial. Jumlah ini mengalami peningkatan sebesar 12,35% (dua belas koma tiga puluh lima persen) dibandingkan tahun 2021.

Dalam data tersebut juga ditemukan, bahwa rata-rata waktu yang dihabiskan seseorang untuk menggunakan internet melalui semua alat *(devices)* adalah selama 8 (delapan) jam 52 (lima puluh dua) menit dalam sehari. Secara spesifik penggunaan media sosial menghabiskan rata-rata 3 (tiga) jam 14 (empat belas) menit dalam sehari hanya untuk mengunjungi atau menggunakan layanan media sosial.

Penyelenggaraan sistem elektronik dan digital telah menyentuh hampir seluruh aspek kehidupan manusia. Dilansir dari pemaparan Menteri Komunikasi dan Informatika Republik Indonesia, Johny G Plate, klasifikasi penyelenggara sistem elektronik terdiri dari bidang Telekomunikasi, Media Sosial, *E-Commerce,* Konsultan, Keuangan, Instansi Publik, dan bidang-bidang lainnya.[26] Besaran perbandingan masing-masing tersaji dalam diagram berikut:



Gambar 2.1 Klasifikasi Penyelenggara Sistem Elektronik
Sumber: Paparan Menteri Kominfo Republik Indonesia

Masifnya penggunaan media internet, baik itu aplikasi media sosial maupun aplikasi pencarian *(browsing)* lainnya tidak sekadar menawarkan fasilitas untuk berkomunikasi interaktif, tetapi juga telah merambah pada aspek komersial, *influencing,* edukasi, hiburan, politik, kesehatan, dan lain sebagainya. Melalui sumber data yang sama, jumlah dana yang diinvestasikan untuk kepentingan marketing melalui *social media ads* (iklan yang diunggah di media sosial) mencapai $432.5 (empat ratus tiga puluh dua koma lima) juta dollar. Sedangkan jumlah

[26] Johny G Plate, *Op. Cit.*

audiens yang dapat dijangkau oleh *Instagram* mencapai 85 (delapan puluh lima) juta jiwa dan *Facebook* mencapai 31 (tiga puluh satu) juta jiwa.[27] Hal ini menunjukkan, bahwa di era digital saat ini, mau atau tidak mau, setuju atau tidak setuju, pada kenyataannya hampir semua aspek kehidupan manusia telah bergeser ke arah dominasi digitalisasi.

c. Kebocoran Data Situs Pemerintah

Menurut laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Sandi dan Siber Negara (BSSN), serangan siber tidak hanya terbatas ditujukan kepada pribadi maupun sistem penyelenggara transaksi elektronik (swasta) tertentu. BSSN melaporkan di tahun 2021 terdapat 4.224 (empat ribu dua ratus dua puluh empat) kasus aduan siber. Laporan didominasi oleh institusi pemerintah dengan 52% (lima puluh dua persen) dari keseluruhan laporan. Serangan siber dari institusi pemerintahan pada tahun 2019 diperkirakan mencapai 2.197 (dua ribu seratus sembilan puluh tujuh) kasus.[28]

Adapun contoh-contoh kasus yang melibatkan data pribadi masyarakat yang dipegang oleh instansi pemerintah adalah sebagai berikut:

a. Kasus kebocoran data Nomor Induk Kependudukan (NIK) dan Kartu Keluarga (KK) dalam proses registrasi Surat Izin Mengemudi (SIM) pada tahun 2018.[29]

b. Kasus pembobolan rekening bank milik wartawan senior Ilham Bintang, karena datanya yang terdaftar di sistem daring Otoritas Jasa Keuangan (OJK) disalahgunakan.[30]

---

[27] Kemas Ahmad, 2021, *Media Sosial 2021: 170 Juta dari 274,9 Juta Jiwa Adalah Pengguna Media Sosial, https://www.kompasiana.com/kemasahmadadnan6029/608a22fa8ede480b3e5165a3/media-sosial-2021-170-juta-dari-274-9-juta-jiwa-adalah-pengguna-media-sosial,* (diakses pada 13 Februari 2022, pukul 21.18 WIB).

[28] Dandi, 2022, *Kebocoran Data Situs Pemerintah,* Kebocoran Data Situs Pemerintah (republika.co.id, (diakses pada 13 Februari 2022, pukul 21.29 WIB).

[29] Kustin Ayuwuragil, 2018, *Kominfo Akui 'Pencurian' NIK dan KK Saat Registrasi Kartu SIM,* https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/ kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim, (diakses pada 15 Februari 2022, pukul 17:00).

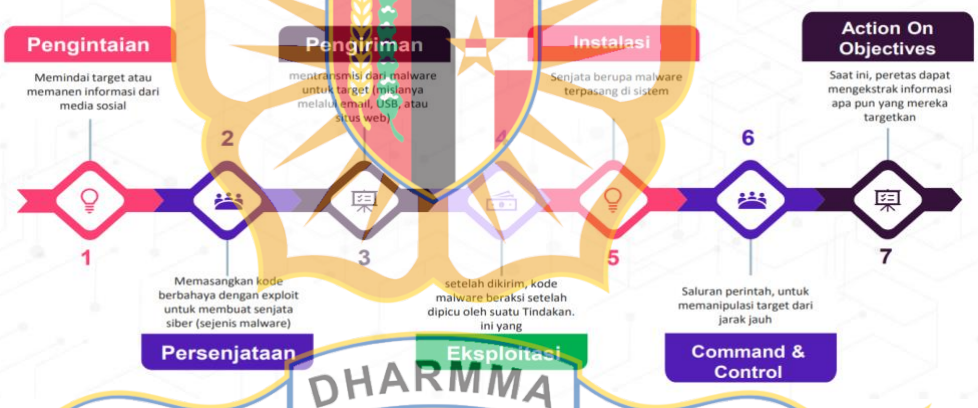
c. Kebocoran 2,3 (dua koma tiga) juta data kependudukan dalam daftar pemilih tetap Pemilu 2014 yang dipegang oleh Komisi Pemilihan Umum (KPU).[31]

d. Kebocoran data pasien *Covid-19* beberapa waktu lalu.[32]

Kasus-kasus ini hanya sebagian dari berbagai kasus kebocoran data yang terjadi di Indonesia. Apabila dibiarkan, kondisi ini selain menciptakan ketidakamanan di tengah masyarakat, juga berpotensi disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, sehingga dapat mengancam keamanan nasional.

Berdasarkan pemaparan Dr. Pratama Persadha (*Chairman* Lembaga Riset Keamanan Siber CISSRec), setidaknya terdapat 7 (tujuh) tahapan serangan siber, yang meliputi: (1) Pengintaian; (2) Persenjataan; (3) Pengiriman; (4) Eksploitasi; (5) Instalasi; (6) *Command & Contro*l; hingga akhirnya pada tahap (7) *Action on Objectives.*[33]

Masing-masing dijelaskan dalam gambar berikut:



Gambar 3. Tujuh Tahapan Serangan Siber
Sumber: Paparan Lembaga Riset Siber Indonesia

Peretasan dan kebocoran informasi tentunya memiliki dampak yang berbahaya dan mengancam kedaulatan dan keamanan nasional. Dampak yang secara langsung dapat terjadi, antara lain: (1) *Reputation*

---

[30] CNN Indonesia, 2020, *Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank,* https://www.cnnindonesia.com/nasional/20200205211241-12-472073/ pembobolan-rekening-ilham-bintang-data-dijual-orang-bank, (diakses pada 15 Februari 2022, pukul 17:22).

[31] *Ibid.*

[32] *Ibid.*

[33] Pratama Persadha, *Kewaspadaan Nasional Terhadap Perkembangan Siber dan Ancamannya*, Paparan disampaikan sebagai *chairman* Lembaga Riset Keamanan Siber CISSReC, 2022.

loss (kehilangan reputasi/kepercayaan); (2) *Financial loss* (kerugian finansial)*;* (3) *Intellectual property loss* (kerugian hak kekayaan intelektual); (4) *Legislative breaches leading to legal actions* (pelanggaran legislatif terhadap pembuatan hukum*)*; (5) *Loss of public confidence* (Kehilangan privasi/kerahasiaan publik); dan (6) *Service interruption costs* (kerugian akibat biaya gangguan layanan).[34]

11. Perkembangan Lingkungan Strategis

Perkembangan lingkungan strategis yang terkait dengan Peningkatan Peran Pemerintah Dalam Perlindungan Data Pribadi di Ruang Digital Guna Memperkuat Keamanan Nasional, adalah sebagai berikut:

a. Pengaruh Perkembangan Lingkungan Strategis Global

Pertumbuhan dan perkembangan teknologi komputer termasuk jaringannya telah mendigitalisasi pola hidup manusia, sehingga muncul dunia baru yang disebut dengan dunia digital. Dunia digital atau domain siber ini berkembang sedemikian cepat, sehingga hanya dalam kurun waktu 20 (dua puluh) tahun, sekitar 60% (enam puluh persen) penduduk dunia telah terhubung di dunia digital.[35]

Pada tataran global diketahui, bahwa setiap menitnya terjadi sekitar 500 (lima ratus) ribu serangan siber di seluruh dunia.[36] Sebagaimana yang disampaikan oleh *Country Lead Azure Business Group Microsoft,* bahwa kejahatan siber saat ini menjadi isu keamanan nasional yang mengincar pos-pos kritis di suatu negara, seperti sektor kesehatan hingga sektor institusi keuangan. Tidak ada sektor yang tidak tersentuh oleh serangan siber.[37]

Selain itu, spionase siber juga menjadi hal yang patut dikhawatirkan. Berdasarkan laporan *Microsoft* pada Oktober 2021, secara global target spionase siber saat ini meliputi berbagai sektor,

---

[34] Pratama Persadha, *Ibid.*

[35] Tim Pokja, *Bahan Ajar Bidang Studi Hubungan Internasional,* (Jakarta: Lembaga Ketahanan Nasional Republik Indonesia, 2022), hlm. 97.

[36] *Ibid.*

[37] Leo Dwi Jatimiko, 2021, *Microsoft: Serangan SIber, Lahan Bisnis Baru Buat Peretas,* https://teknologi.bisnis.com/read/20211124/84/1470012/waduh-microsoft-serangan-siber-lahan-bisnis-baru-buat-peretas, (diakses pada 18 Maret 2022, pukul 18:30 WIB).

yakni sektor pemerintahan, Lembaga Swadaya Masyarakat (LSM) dan lembaga penelitian; Sektor pendidikan; (4) Sektor organisasi lingkungan; (5) Sektor Informasi dan Teknologi (IT); (6) Sektor media; (7) Sektor kesehatan; (8) Sektor energi; dan sektor-sektor lainnya.[38]

Faktanya spionase siber *(cyber espionage)* kini memiliki peran penting dalam peperangan modern. Dengan peralihan kegiatan masyarakat termasuk pemerintah suatu negara menjadi menggunakan metode digital, maka data yang tersimpan dalam jaringan akan sangat besar serta bersifat vital dan krusial. Dalam dunia digital saat ini, dikenal suatu istilah peperangan siber *(cyber war)* sebagai suatu bentuk perang yang baru. Subjeknya pun tidak lagi terbatas pada negara atau kelompok militer tertentu, tetapi dapat juga perseorangan, badan, atau kelompok tertentu. Beberapa negara-negara di dunia khususnya negara-negara maju telah memberikan perhatian khusus terhadap sistem digitalisasi dan dunia maya, karena hal ini jelas-jelas dapat menimbulkan ancaman terhadap pertahanan dan keamanan nasional jika tidak terwadahi sebagaimana mestinya.

b. Pengaruh Perkembangan Lingkungan Strategis Regional

Di tengah pandemi *Covid-19,* kerja sama antar negara-negara ASEAN tetap terjalin dengan baik. Walaupun mobilitas antar warga negara dibatasi sedemikian rupa, tetapi interaksi sosial termasuk juga kerja sama bisnis dan pemerintahan tetap terjadi melalui transaksi digital dan media informasi digital lainnya. Hal ini menjadi perhatian khusus bagi pemerintah Indonesia, khususnya bidang keamanan siber dalam menjaga interaksi antar negara-negara di ASEAN. Pertemuan kementerian-kementerian telekomunikasi di Asia Tenggara tahun 2021 mengagendakan pembuatan *landscape* digital dengan mengadopsi

[38] Microsoft.com, 2021, *Microsoft Digital Defense Report,* https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report, (diakses pada 7 Maret 2022, pukul 14:00 WIB).

ASEAN Digital Masterplan 2025.[39] Dalam forum tersebut, Menteri Komunikasi dan Informatika, Johnny G Plate, menekankan pentingnya perlindungan data pribadi dan keamanan data di kawasan ASEAN. Mengingat saat ini data memiliki nilai ekonomi yang signifikan, maka dibutuhkan pengelolaan dan pemanfaatan dengan menjunjung prinsip kedaulatan data, yakni *a reciprocal, lawful, fair, and transparent manner.*[40]

c. Pengaruh Perkembangan Lingkungan Strategis Nasional

Di bidang keamanan, perkembangan transaksi elektronik dan penggunaan media digital juga sangat mempengaruhi dinamika kehidupan nasional, baik dari sisi masyarakat dalam ranah privat, iklim bisnis, dan juga tentunya pemerintahan. Pandemi *Covid-19* mengubah pola mobilitas interaksi masyarakat yang sebelumnya masih didominasi pertemuan fisik menjadi mayoritas melalui pertemuan dan interaksi secara digital. Hal ini juga berdampak pada gangguan keamanan dan ketertiban dalam negeri yang semula hanya berupa pelanggaran hukum dan aksi-aksi kejahatan biasa atau kejahatan konvensional, saat ini berubah menjadi kejahatan melalui media sosial atau kejahatan terhadap informasi digital itu sendiri (seperti halnya pencurian data pribadi). Belum lagi kejahatan luar biasa yang terorganisir *(extra ordinary organized crime)* dan lintas negara yang semakin rentan dan mudah terjadi dengan pesatnya perkembangan teknologi informasi. Seiring dengan perkembangan ini, keamanan dalam negeri juga kini menghadapi ancaman berdimensi teknologi siber *(cyber crime)*. Ciri utama dari *cyber crime* adalah pelaku kejahatan yang sebelumnya bersifat konvensional dan tradisional berubah menjadi menggunakan teknologi internet, sehingga kejahatan tersebut bisa dilakukan di mana saja (tidak harus *on-site*), cepat, murah *(low cost),* dapat diulang-ulang, dapat dikerjakan di ruang tersembunyi dan aman, *anonymous and*

[39] Fauziah Mursid, 2021, *Menkominfo Tekankan Pentingnya Perlindungan Data di ASEAN,* Menkominfo Tekankan Pentingnya Perlindungan Data di ASEAN | Republika Online, (diakses pada 13 Februari 2021, 21.55 WIB).

[40] *Ibid.*

untreacable (anonim dan sulit ditelusuri), serta target-targetnya sangat rentan karena belum terlindungi dengan baik.[41]

Di bidang sosial budaya, teknologi digital membuat interaksi antar manusia menjadi lebih cepat, masif, dan lebih penetratif. Kondisi ini membawa masyarakat pada situasi ketidakteraturan arus informasi yang berimplikasi pada terjebaknya masyarakat pada fenomena *post truth* dengan adanya penyebaran hoaks dan ungkapan kebencian.[42]

Di bidang politik, di tengah perkembangan teknologi informasi yang bersamaan dengan peningkatan pengguna transaksi elektronik yang begitu pesatnya, urgensi untuk membentuk suatu aturan khusus mengenai perlindungan data pribadi di Indonesia semakin santer terdengar. Indonesia masih ketinggalan dibandingkan dengan negara-negara lain dalam hal regulasi dan penegakan aturan mengenai penyalahgunaan data pribadi. Beberapa aturan perundang-undangan yang disahkan oleh pemerintah telah memuat beberapa aspek terkait privasi dan perlindungan data pribadi di berbagai bidang. Namun, belum ada aturan khusus yang memuat mengenai perlindungan data pribadi secara terpadu yang kemudian dikaitkan dengan keamanan nasional.

d. Peluang dan Kendala

Khususnya dalam hal perlindungan data pribadi, yang menjadi kekuatan *(strengths)* yang dimiliki oleh pemerintah Indonesia, antara lain:

1) Pemerintah telah memiliki kesadaran akan pentingnya perlindungan data pribadi yang dibuktikan melalui pengesahan kebijakan sektoral dan perumusan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP).

---

[41] Teddy Mantoro, *Dinamika Perkembangan Teknologi Informasi (Siber) dan Ancaman yang Ditimbulkan*, Paparan disampaikan di LEMHANAS RI, pada 30 Maret 2022.

[42] Kepolisian Republik Indonesia, *Rencana Kerja Kepolisian Negara Republik Indonesia Tahun Anggaran 2022, Lampiran Keputusan Kapolri Nomor: Kep/1087/Vi/2021 Tanggal: 29 Juni 2021,* (Jakarta: Kepolisian Republik Indonesia, 2022), hlm. 2.

2) Adanya kebijakan sektoral berupa Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

3) Pemerintah telah memiliki lembaga yang lengkap mulai dari tingkat pusat sampai dengan tingkat daerah.

4) Adanya program percepatan aksesibilitas dan pemerataan jaringan di seluruh wilayah Indonesia.

Sedangkan yang menjadi kelemahan *(weakness)* adalah:

1) Belum disahkannya RUU PDP hingga saat ini.

2) Masih belum ada undang-undang yang terintegrasi dan secara khusus mengatur mengenai perlindungan data pribadi.

3) Belum adanya standar pengamanan data pribadi yang setara pada semua lembaga mulai dari pusat sampai ke daerah.

4) Infrastruktur teknologi di Indonesia belum memadai.

Sementara dari faktor eksternal, yang menjadi peluang *(opportunities)* antara lain:

1) Masyarakat digital Indonesia, badan usaha swasta, pers, dan *non-governmental organization* sudah memiliki kesadaran akan pentingnya perlindungan data pribadi dan telah muncul dukungan terhadap pengesahan undang-undang terkait.

2) Penyelenggara transaksi digital, khususnya badan usaha swasta telah mulai menciptakan sistem-sistem keamanan terhadap perlindungan data pribadi.

Sedangkan yang menjadi ancaman *(threat)* adalah:

1) Belum meratanya kesadaran digital dan tingkat literasi masyarakat Indonesia.

2) Masih marak aplikasi elektronik ilegal yang menghimpun data pribadi masyarakat.

3) Rendahnya tingkat kepercayaan publik terhadap pemerintah, khususnya dalam hal keamanan data pribadi.

4) Penduduk Indonesia yang tersebar di wilayah geografis yang sangat luas dengan infrastruktur yang belum merata.

BAB III
PEMBAHASAN

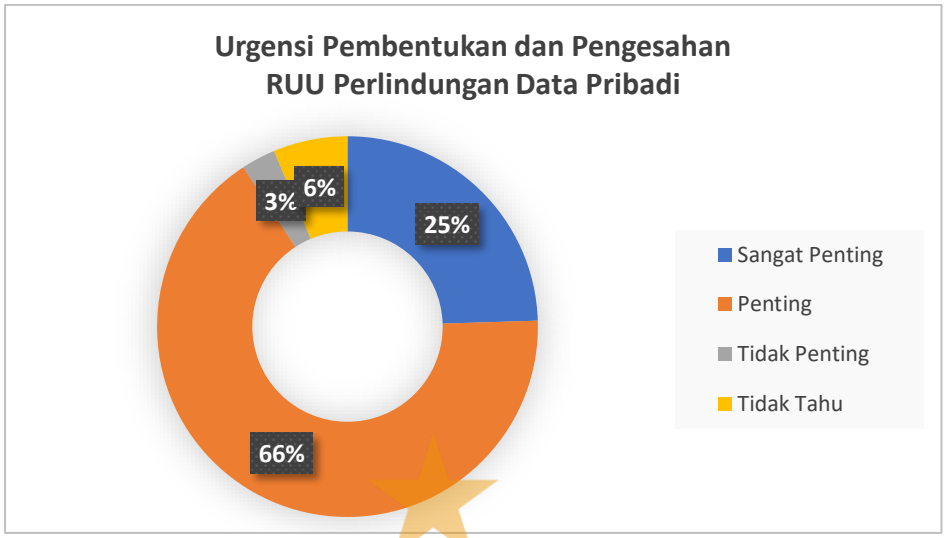
12. Umum

Setelah sebelumnya dijelaskan mengenai data dan fakta serta hal-hal yang berkaitan dengan fenomena kebocoran data pribadi, maka selanjutnya dalam bab ini akan dijabarkan hasil analisis data dan fakta berdasarkan teori yang digunakan, sehingga akan ditemukan faktor-faktor yang mempengaruhi terjadinya/munculnya permasalahan kebocoran data pribadi, sehingga dapat dirumuskan solusinya. Pembahasan pada bab ini meliputi 4 (empat) aspek dalam rumusan masalah, yang terdiri dari: (a) Penyusunan regulasi perlindungan data pribadi di ruang digital; (b) Persiapan infrastruktur perlindungan data pribadi di ruang digital; (c) Pembentukan kelembagaan khusus perlindungan data pribadi di ruang digital; serta (d) Sistem dan metode dalam upaya melindungi data pribadi di ruang digital.

13. Penyusunan Regulasi Perlindungan Data Pribadi di Ruang Digital

Pada tanggal 23 sampai dengan 27 Februari 2021, Litbang Kompas melakukan survei mengenai pentingnya/urgensi pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), menggunakan metode penelitian dengan mengumpulkan pendapat dari responden melalui panggilan telepon. Dari 1.007 (seribu tujuh) responden yang tersebar di 34 (tiga puluh empat) provinsi di Indonesia dengan usia minimal 17 (tujuh belas) tahun, hasil survei menunjukkan, bahwa sebanyak 90,8% (sembilan puluh koma delapan persen) responden berpendapat pengesahan RUU PDP sangat penting dan harus disahkan sesegera mungkin.[43]

[43] Marlinda Oktavia Erwanti, 2021, *Survei Kompas: 90,8% Responden Dorong RUU Perlindungan Data Pribadi Disahkan,* https://www.google.com/search?q=%2C+https%3A%2F%2Fnews.detik.com%2Fberita%2Fd-5493536%2Fsurvei-kompas-908-responden-dorong-ruu-perlindungan-data-pribadi-disahkan%2C&oq=%2C+https%3A%2F%2Fnews.detik.com%2Fberita%2Fd-5493536%2Fsurvei-kompas-908-responden-dorong-ruu-perlindungan-data-pribadi-disahkan%2C&aqs=chrome..69i57.906j0j9&sourceid=chrome&ie=UTF-8, (diakses pada 19 Maret 2022, pukul 22.17 WIB).



Gambar 4. Survei Urgensi Pembentukan RUU Perlindungan Data Pribadi
Sumber: Litbang Kompas, 2021

Berdasarkan data di atas dapat disimpulkan, bahwa kesadaran akan pentingnya Undang-Undang Perlindungan Data Pribadi sudah muncul dan tumbuh di tengah masyarakat indonesia. Pengaturan mengenai data pribadi dirasa sangat penting, karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman, dan keamanan data pribadi. Secara umum, pengaturan data pribadi adalah untuk mencari keseimbangan antara kebutuhan akan perlindungan data pribadi individu dengan kebutuhan pemerintah/negara dan pelaku industri digital (bisnis) untuk memperoleh dan memproses data pribadi dalam suatu keperluan yang wajar dan sah. Apabila keseimbangan ini terwujud, maka dapat meminimalisir ancaman nasional, baik itu yang berasal dari dalam maupun luar negeri.

Sebenarnya saat ini Indonesia sudah memiliki beberapa instrumen hukum yang mengatur mengenai perlindungan data pribadi, baik itu di level undang-undang maupun peraturan di bawahnya. Namun, semua perangkat aturan ini masih bersifat parsial dan terpisah-pisah, serta masih berorientasi pada kelembagaan. Di antaranya adalah:

a. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan (UU Perbankan). Pasal 40 menyebutkan, bahwa bank wajib merahasiakan keterangan mengenai penyimpan dan simpanan nasabah, kecuali dalam hal-hal tertentu.

Pengaturan tersebut mengisyaratkan, bahwa privasi nasabah tidak hanya berkenaan dengan data miliknya saja, tetapi juga data pribadi yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data pribadi. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena pada kenyataannya data pribadi nasabah di suatu bank tertentu sering sekali mengalami kebocoran kepada bank lainnya, sehingga bank lain tersebut memiliki akses untuk menghubungi nasabah dalam upaya menawarkan produk maupun jasa.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Pasal 42 ayat (1) mewajibkan penyelenggara jasa telekomunikasi untuk merahasiakan informasi pelanggan jasa telekomunikasi. Pengecualian terhadap kerahasiaan ini adalah untuk kepentingan proses peradilan pidana melalui permintaan tertulis Jaksa Agung atau Kepala Kepolisian serta penyidik. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena tidak berbeda dengan nasabah bank, data pribadi pengguna *provider* telekomunikasi sering kali bocor hingga *provider* telekomunikasi lain memiliki akses untuk menjangkau pengguna, baik melalui panggilan telepon maupun SMS *blast* dalam rangka menawarkan produk maupun jasa.

c. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Undang-Undang HAM). Pasal 29 ayat (1) mengakui hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya. Hak privasi sebagai bagian dari HAM yang dilindungi. Pasal 32 juga mengatur, bahwa kemerdekaan dan kerahasiaan dalam komunikasi melalui sarana elektronik dijamin kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan perundang-undangan yang berlaku. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena pada kenyataannya amanat dalam undang-undang ini belum sepenuhnya terimplementasikan, mengingat data pribadi warga negara masih belum terlindungi sebagaimana mestinya dan masih kerap disalahgunakan oleh pihak-pihak tertentu.

d. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan). Pasal 2 menjamin hak setiap orang untuk memperoleh perlindungan atas data pribadi, kepastian hukum atas kepemilikan dokumen, serta informasi mengenai data hasil pendaftaran penduduk dan pencatatan sipil atas dirinya dan/atau keluarganya. Dalam Pasal 2 huruf f disebutkan, bahwa penduduk berhak memperoleh ganti rugi dan pemulihan nama baik jika terjadi kesalahan dalam pendaftaran penduduk dan pencatatan sipil serta penyalahgunaan data pribadi oleh instansi pelaksana. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena pada kenyataannya amanat dalam undang-undang ini belum terimplementasikan sepenuhnya. Terlebih karena masyarakat Indonesia belum seluruhnya memiliki kesadaran akan pentingnya data pribadi, sehingga dalam beberapa kasus, korban memilih untuk diam dan tidak melaporkannya.

e. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE). Undang-Undang ITE mengatur mengenai perlindungan atas data pribadi dan hak privasi yang tertuang dalam Pasal 26 ayat (1) yang menyatakan, bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan, kecuali ditentukan lain oleh perundang-undangan. Pasal dalam undang-undang ini pada dasarnya dapat dijadikan sebagai pijakan, tetapi belum menjangkau secara menyeluruh terkait perlindungan data pribadi.

f. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Undang-Undang Keterbukaan Informasi Publik). Perlindungan data dan informasi publik yang dihimpun oleh badan publik

diatur dalam Pasal 6 ayat (3). Di antara informasi publik yang tidak dapat diberikan oleh badan publik, salah satunya adalah informasi yang berkaitan dengan hak-hak pribadi. Pasal dalam undang-undang ini merupakan modal bagi badan publik penghimpun data pribadi untuk menjaga dan tidak menyalahgunakan data pribadi warga. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena tidak mengatur secara lebih spesifik mengenai perlindungan data pribadi.

g. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Dalam Pasal 15 ayat (1) secara tegas disebutkan, bahwa penyelenggara sistem elektronik wajib untuk: (1) Menjaga rahasia, keutuhan, dan ketersediaan data pribadi yang dikelolanya; (2) Menjamin perolehan, penggunaan, dan pemanfaatan data pribadi berdasarkan persetujuan pemilik data kecuali ditentukan lain oleh perundang-undangan; serta (3) Menjamin penggunaan atau pengungkapan data berdasarkan persetujuan dari pemilik data dan sesuai dengan tujuan yang disampaikan kepada pemilik data pada saat perolehan data. Namun, undang-undang ini belum cukup efektif untuk menjamin perlindungan data pribadi, karena walaupun pasal dalam undang-undang ini dapat dikatakan cukup jelas, tetapi masih belum terimplementasikan sepenuhnya. Hal ini bisa saja disebabkan, karena di Indonesia belum ada undang-undang spesifik yang mengatur tentang perlindungan data pribadi beserta sanksi yang mengikutinya.

h. Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah (PBI No. 7/6/PBI/2005). PBI ini ditetapkan berdasarkan pertimbangan, bahwa transparansi terhadap penggunaan data pribadi yang disampaikan oleh nasabah kepada bank diperlukan untuk meningkatkan perlindungan terhadap hak-hak pribadi nasabah dalam berhubungan dengan bank.

Selain yang telah disebutkan di atas, masih terdapat beberapa peraturan-peraturan lainnya yang memuat ketentuan tentang pengaturan

perlindungan data pribadi. Namun, belum ada aturan selevel undang-undang yang dapat dijadikan sebagai payung hukum bagi masyarakat, pelaku bisnis, dan pemerintah dalam pengelolaan data pribadi masyarakat. Ditambah belum ada satu pun di antara peraturan tersebut yang mengatur secara tegas, bahwa perlindungan data pribadi merupakan suatu kepentingan negara yang berkaitan langsung terhadap keamanan nasional.

Sejak tahun 2019 Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) telah masuk dalam Program Legislasi Nasional (Prolegnas). Namun, hingga tahun 2021 pembahasan tentang RUU tersebut belum rampung. Hal ini perlu menjadi perhatian pemerintah dan Dewan Perwakilan Rakyat Republik Indonesia (DPR RI), karena hingga Desember 2021, dari sebanyak 317 (tiga ratus tujuh belas) Daftar Inventarisasi Masalah (DIM), pemerintah dan DPR baru menyelesaikan 43 (empat puluh tiga) DIM atau setara dengan 13% (tiga belas persen).[44]

Urgensi pembentukan UU PDP sangat dibutuhkan saat ini sebagai jaminan dan perlindungan hukum dalam pengelolaan keamanan data pribadi. Oleh karena itu diharapkan pemerintah sesegera mungkin merampungkan perumusan RUU PDP, karena RUU ini memiliki manfaat yang meliputi:

a. Menjadi kerangka regulasi yang lebih kuat dan komprehensif dalam memberikan perlindungan hak asasi manusia, khususnya terkait data pribadi.

b. Menjadi instrumen hukum kunci dalam pencegahan dan penanganan kasus pelanggaran data pribadi yang masih banyak terjadi dan menjadi tantangan bersama.

c. Mempercepat pembangunan ekosistem ekonomi digital dan meningkatkan iklim investasi yang aman dengan memberikan kepastian hukum bagi bisnis dan meningkatkan kepercayaan konsumen.

d. 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 oleh pengendali dan pemroses data pribadi.

---

[44] Danny Kobrata, 2022, *RUU Perlindungan Data Pribadi: Sebuah Penantian,* RUU Pelindungan Data Pribadi: Sebuah Penantian (hukumonline.com), (diakses pada 18 Maret 2022, pukul 17:32 WIB).

e. Menjadi instrumen hukum kunci dalam pencegahan dan penanganan kasus pelanggaran data pribadi yang masih banyak terjadi dan menjadi tantangan bersama.[45]

Dengan demikian, pemerintah perlu segera mengambil langkah kebijakan terkait perlindungan data pribadi, karena apabila data pribadi masyarakat dapat dilindungi sedemikian rupa, maka hak asasi manusia dalam aspek privasi dapat diseimbangkan dengan urgensi ekonomi yang tentunya berdampak positif terhadap penguatan keamanan nasional. Maka dari itu, tentunya dibutuhkan suatu perundang-undangan bersifat khusus yang dapat mengatur mengenai perlindungan data pribadi untuk memastikan data pribadi masyarakat dilindungi dengan baik oleh pemerintah. Dalam perkembangan ekonomi khususnya industri bisnis di bidang digital, adanya aturan khusus mengenai perlindungan data pribadi akan memperkuat posisi Indonesia sebagai kawasan ramah bisnis dan investasi yang terpercaya, sehingga dapat menstimulus industri digital bahkan industri pengolahan data untuk berkembang di Indonesia.

Undang-Undang Perlindungan Data Pribadi diharapkan mampu menjadi jawaban atas keluhan masyarakat dan solusi bagi permasalahan penyalahgunaan data pribadi yang terjadi saat ini. Supaya undang-undang ini dapat berlaku efektif, maka selain memenuhi syarat formil proses pembuatan perundang-undangan, di dalam pembahasan undang-undang ini pemerintah dan DPR harus memastikan, bahwa substansi yang akan diatur dapat mengawal kepentingan hak individu, konsumen, pelaku bisnis, dan pemerintah.

Ditinjau dari Teori Peran Pemerintah, menurut Henry J. Abraham, setidaknya terdapat 3 (tiga) peranan pemerintah, antara lain:

a. Mula-mula peranan pemerintah adalah sebagai penjaga keamanan dan ketertiban dalam perkembangan.

b. Selanjutnya timbul pengertian tentang *service state*, dimana peranan pemerintah merupakan abdi sosial dari keperluan-keperluan yang perlu diatur dalam masyarakat.

---

[45] Henry Subiakto, *Perlindungan Data Pribadi dan Tantangannya,* Pemaparan Staf Ahli Menteri Komunikasi dan Informatika, 2021, hlm. 34.

c. Kemudian terdapat peranan pemerintah sebagai *entrepreneur* atau pendorong inisiatif usaha pembaharuan dan pembangunan masyarakat. Pemerintah menjadi *'development agent'* atau unsur pendorong pembaharuan/pembangunan.

Merujuk pada Teori Peran Pemerintah menurut Henry J. Abraham, maka tahapan peranan pemerintah harus diawali orientasi untuk menjaga keamanan dan ketertiban dalam perkembangan kehidupan masyarakat, yaitu pemerintah secara proaktif mengeluarkan kebijakan-kebijakan yang cenderung bersifat represif, yakni kebijakan yang berfungsi untuk mengawasi pelanggaran sekaligus penerapan sanksi. Khususnya terkait perlindungan data pribadi, Indonesia bahkan belum memiliki peraturan perundang-undangan khusus/spesifik yang mengatur tentang perlindungan data pribadi beserta sanksi yang mengikutinya.

Tahap berikutnya adalah kebijakan pemerintah dalam pengertian *service state*, dimana pemerintah menyediakan infrastruktur fisik maupun sistem kelembagaan sebagai upaya perwujudan perlindungan data pribadi. Pada tahapan ini pemerintah harus melakukan usaha-usaha sebagai bentuk pengabdian dan tanggung jawab konstitusional dalam rangka memperkuat keamanan nasional.

Pada akhirnya, pembentukan UU PDP diharapkan mampu mencapai tujuan akhir perwujudan peran pemerintah sebagai *development agent* atau pendorong pembaharuan. Kebijakan perlindungan data pribadi yang dilakukan diharapkan dapat menimbulkan kesadaran inisiatif untuk melakukan usaha-usaha perlindungan data pribadi sebagai suatu sistem bagi seluruh masyarakat Indonesia, sekaligus kesadaran untuk menjaga dan memperkuat keamanan nasional.

Tidak hanya sampai di sana, pemerintah juga perlu melakukan kebijakan-kebijakan melalui program kerja untuk memastikan meratanya kesadaran akan pentingnya kerahasiaan data pribadi di tengah masyarakat. Hal ini dapat berupa sosialisasi sebagai upaya untuk menciptakan kondisi tertib penggunaan data pribadi oleh seluruh lapisan masyarakat (khususnya masyarakat digital), pemerintah, dan pelaku bisnis demi terwujudnya penguatan keamanan nasional. Selain itu pengetahuan seputar data pribadi

dapat dimasukkan sebagai bahan pembelajaran di sekolah-sekolah dalam wujud edukasi dini. Melalui undang-undang ini juga dapat dilakukan pembentukan lembaga khusus yang bersifat independen sebagai salah satu instrumen pelaksana UU PDP yang memiliki kewenangan pencegahan dan pengawasan pengelolaan data pribadi.

14. Persiapan Infrastruktur Perlindungan Data Pribadi di Ruang Digital

Setelah pembentukan perangkat hukum yakni Undang-Undang Perlindungan Data Pribadi, selanjutnya pemerintah harus memastikan undang-undang tersebut dapat diterima dan ditaati oleh kelompok sasaran, yakni masyarakat umum dan pelaku bisnis.

Menurut Soerjono Soekanto, efektif atau tidaknya suatu hukum ditentukan oleh 5 (lima) faktor, yang meliputi: (1) Faktor hukum itu sendiri (undang-undang); (2) Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum; (3) Faktor sarana atau fasilitas yang mendukung penegakan hukum; (4) Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan; serta (5) Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.[46]

Berdasarkan Peraturan Presiden Nomor 38 Tahun 2015 Tentang Kerja Sama Pemerintah dengan Badan Usaha Dalam Penyediaan Infrastruktur, infrastruktur didefinisikan sebagai fasilitas teknis, fisik, sistem, perangkat keras, dan perangkat lunak yang diperlukan untuk melakukan pelayanan kepada masyarakat dan mendukung jaringan struktur, agar pertumbuhan ekonomi dan sosial masyarakat dapat berjalan dengan baik.

Tidak dapat dipungkiri, bahwa infrastruktur perlindungan data pribadi di Indonesia, baik itu dari segi fasilitas secara fisik maupun non-fisik masih tergolong lemah. Penyebab utamanya karena belum ada payung hukum yang mengamanatkan pembuatan atau peningkatan infrastruktur. Dalam orientasi umum yang berkembang saat ini, perlindungan data pribadi masih

[46] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, (Jakarta: PT Raja Grafindo Persada), 2008, hlm. 8.

menitikberatkan pada pertanggungjawaban pemilik maupun pengguna informasi data pribadi tersebut.

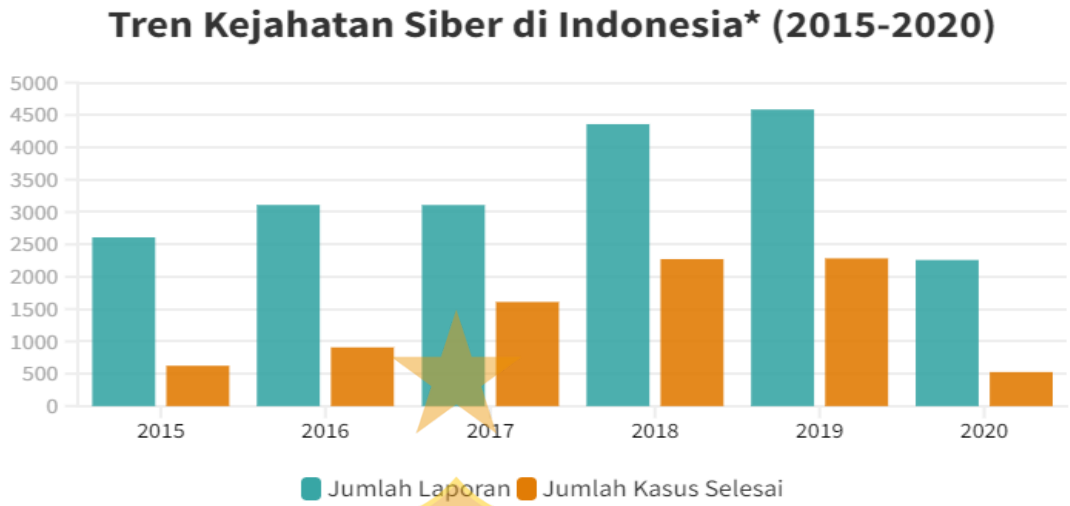
Sebagaimana tertuang dalam Pasal 32 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, pihak pemilik data pribadi harus bertanggung jawab atas data yang diberikan, yaitu benar dan sesuai dengan data pribadinya sendiri, bukan memberikan data pribadi orang lain. Sedangkan tanggung jawab dari pemegang data pribadi adalah melindungi data pribadi milik orang lain, serta bertanggung jawab terhadap pengamanan dan perlindungan sarana dan prasarana sistem elektronik.

Hal ini tidak bisa dikatakan salah, mengingat penjagaan informasi pribadi adalah kewajiban masing-masing pihak secara bersama-sama. Namun, hal ini tentu harus didukung dengan adanya suatu jaminan sistem keamanan yang diberikan oleh pemerintah kepada masyarakat. Jaminan keamanan ini tidak hanya terbatas pada data-data di dalam situs-situs pemerintahan, tetapi juga penjaminan terhadap data-data pribadi yang dihimpun oleh para pelaku industri digital, termasuk pelaku transaksi elektronik. Penjaminan ini dapat mencakup perizinan dan pengawasan terhadap pelaku penghimpun data pribadi.

Selain masih berorientasi parsial dan kelembagaan, perlindungan data pribadi di Indonesia saat ini juga masih bersifat represif (menitikberatkan pada tindakan penghukuman setelah terjadi serangan siber). Kepolisian Republik Indonesia (Polri) yang dalam hal ini sebagai penegak hukum terhadap serangan siber juga telah mentransformasikan diri untuk dapat menangani kasus-kasus serangan siber. Misalnya melalui pembentukan situs berdomain patrolisiber.id oleh Direktorat Tindak Pidana Siber (Dirtippidsiber Bareskrim Polri) yang dikhususkan untuk mengatasi kejahatan siber. Melalui situs tersebut, masyarakat dapat lebih mudah melaporkan adanya suatu tindak kejahatan siber *(cyber crime)* yang terjadi.

Dilansir dari situs patrolisiber.id, sepanjang tahun 2015- 2020 kejahatan siber di Indonesia cenderung meningkat walaupun sempat mengalami penurunan di tahun 2020. Perbandingan antara jumlah kasus yang dapat diselesaikan masih berada di bawah 50% (lima puluh persen) dari total jumlah

laporan yang dilaporkan oleh sub-bagian Pembinaan Operasi Direktorat Reserse Kriminal Khusus seluruh kepolisian daerah.



Gambar 5. Tren Kejahatan Siber di Indonesia
Sumber: patrolisiber.id

Dalam usaha-usaha preventif (pencegahan), di Indonesia sendiri pemerintah semakin memberikan perhatian dengan masalah keamanan data pribadi. Indonesia melalui Badan Standardisasi Nasional (BSN) telah mengakui SNI ISO/IEC 27001:2013. ISO 27001 adalah spesifikasi untuk membuat ISMS *(Information Security Management System)* atau Sistem Manajemen Keamanan Informasi (SMKI), yaitu istilah yang muncul dari SNI ISO/IEC 27001:2013 yang diadopsi dari ISO/IEC 27001:2013 yang merujuk pada suatu sistem manajemen yang berhubungan dengan keamanan informasi.[47] Namun, sertifikasi tersebut masih bersifat suka rela (tidak wajib) bagi pelaku industri digital, sehingga standarisasi mengenai keamanan pengelolaan data pribadi belum merata bagi seluruh *platform* digital, termasuk bagi lembaga-lembaga pemerintah.

Menurut Farouk Muhammad (Saat itu menjabat sebagai Gubernur PTIK) dari kalangan Polri, bahwa keamanan negara merupakan satu bidang keamanan, yaitu adanya upaya untuk menjamin keamanan negara sebagai suatu entitas. Walau saling terkait, tetapi keamanan negara berada pada domain yang berbeda dengan keamanan umum. Keamanan negara

[47] Muhammad Bahrudin, Firmansyah, *Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001,* Jurnal Media Pustakawan, Volume 25, Nomor 1, (2018), Perpustakaan Nasional Republik Indonesia, hlm. 49.

menyangkut eksistensi/kelangsungan hidup dan ketenteraman individu/kelompok orang (pada umumnya) yang hidup dalam suatu negara. Oleh sebab itu menurut Farouk Muhammad, ancaman terhadap keamanan negara belum tentu merupakan gangguan terhadap keamanan manusia/kelompok/masyarakat.[48]

Pendapat tersebut sangat sesuai dengan kondisi perkembangan perlindungan data pribadi di Indonesia saat ini. Keamanan negara dalam hal ini pencurian data pribadi secara masif, baik itu melalui serangan yang berasal dari luar negeri maupun dari dalam negeri sering kali tidak secara langsung menimbulkan gangguan ketertiban/keamanan suatu kelompok atau masyarakat. Serangan terhadap data pribadi pada umumnya dilakukan secara senyap dalam waktu yang tidak terduga-duga, sehingga reaksi atas perbuatan tersebut cenderung terlambat. Padahal, ancaman yang muncul akibat pencurian data tersebut sangat serius dan dapat membahayakan keamanan nasional. Untuk itu, infrastruktur pendukung sebagai upaya prefentif (pencegahan) sangat diperlukan.

Jika merujuk pada pandangan Soerjono Soekanto mengenai patokan efektivitas elemen-elemen dari suatu prasarana, maka tidak mungkin penegakan hukum (dalam hal ini perlindungan data pribadi) akan berjalan dengan baik apabila tidak didukung oleh infrastruktur yang memadai. Infrastruktur tersebut mencakup Sumber Daya Manusia (SDM) yang kompeten (berpendidikan dan terampil), organisasi kelembagaan yang terstruktur, anggaran yang cukup, peralatan yang memadai, dan faktor pendukung lainnya. Oleh sebab itu, dituntut peningkatan peran pemerintah dalam hal menjamin terpenuhinya infrastruktur tersebut.

Selain itu dibutuhkan juga koordinasi yang baik antar lembaga negara yang memiliki keterkaitan terhadap pengelolaan data digital, seperti halnya Kepolisian Negara Republik Indonesia (Polri), Tentara Nasional Indonesia (TNI), Badan Intelijen Negara (BIN), hingga Kementerian Komunikasi dan Informatika (Kemkominfo). Koordinasi yang dimaksud adalah adanya pembagian tugas yang jelas antara lembaga negara, sehingga tidak terjadi

[48] Farouk Muhammad, *Polri Dalam Sistem Pertahanan dan Keamanan*, Makalah Seminar IODAS, 25 Agustus 2008, Jakarta, hlm. 2-3.

tumpang tindih wewenang antara lembaga yang satu dengan lembaga lainnya. Hal ini bertujuan untuk menghindari adanya lembaga negara yang merasa paling berwenang dan *super power*, sehingga berpotensi menimbulkan *abuse of power* dan benturan kepentingan antar lembaga negara.

Sebagai salah satu upaya mempersiapkan infrastruktur perlindungan data pribadi, Kemkominfo menerapkan kebijakan PSE (Penyelenggara Sistem Elektronik), dimana setiap *platform* digital yang masuk atau digunakan oleh masyarakat Indonesia harus mendaftarkan diri. Kebijakan ini bertujuan agar Menkominfo dapat mengawasi dan memantau arus lalu lintas informasi dan data yang tersebar di ruang digital melalui *platform-platform* tersebut. Hal ini sempat menjadi perhatian publik baru-baru ini, karena Menkominfo memblokir situs *Paypal* (dompet elektronik) dan juga beberapa *game online*, karena *platform-platform* tersebut belum mendaftarkan diri di PSE hingga tenggat waktu yang telah ditentukan. Ironisnya, kebijakan ini justru disambut kemarahan oleh masyarakat hingga melakukan aksi unjuk rasa yang meminta agar blokiran platform atau situs tersebut kembali dibuka. Hal ini menjadi bukti betapa masih tingginya tingkat ketidakpercayaan *(distrust)* masyarakat terhadap kemampuan pemerintah untuk melindungi data pribadi warganya. Hal ini perlu mendapat perhatian khusus dari para pemangku kebijakan.

Dalam pemaparannya, Dr Pratama Persadha menggambarkan secara sederhana bagaimana peran dari beberapa lembaga negara dalam penguatan kemampuan siber, yang digambarkan dalam diagram berikut:[49]

Gambar 6. Koordinasi Lembaga Negara Dalam Hal Penguatan Kemampuan Siber
Sumber: Pemaparan Lembaga Riset Siber Indonesia

Infrastruktur berikutnya yang sangat penting adalah infrastruktur di bidang teknologi. Dalam usaha membentuk infrastruktur pengamanan data

[49] *Ibid.*

pribadi, Indonesia tentu tidak bisa bergantung pada teknologi perangkat lunak *(software)* dari luar negeri apalagi perlindungan data pribadi di dunia digital erat kaitannya dengan penguatan keamanan nasional. Oleh sebab itu, pemerintah Indonesia harus mulai mempersiapkan SDM-SDM yang ahli menciptakan sistem untuk menghadapi risiko keamanan digital. Dibutuhkan peran dan kolaborasi antara pemerintah dan pelaku Industri dengan perguruan tinggi maupun sekolah vokasi untuk menciptakan SDM-SDM unggul yang dapat mengatasi persoalan *cyber security* ke depannya. Apabila seluruh elemen infrastruktur tersebut telah memenuhi standar dan memadai, maka upaya perlindungan data pribadi dapat dilakukan secara optimal, sehingga penguatan keamanan nasional dapat terwujud.

15. Pembentukan Kelembagaan Khusus Untuk Perlindungan Data Pribadi di Ruang Digital

Banyaknya pertukaran informasi di ruang digital membuat isu perlindungan data pribadi menjadi salah satu poin penting dalam kaitannya dengan keamanan nasional. Oleh sebab itu, dibutuhkan adanya suatu undang-undang mengenai perlindungan data pribadi untuk dapat menciptakan suatu sistem administrasi pemerintahan yang efisien dan efektif dalam memberikan pelayanan bagi masyarakat, sehingga iklim bisnis dan penegakan hukum menjadi semakin baik.

Dikarenakan belum adanya payung hukum yang menaungi keamanan data pribadi di Indonesia, maka dibuatlah suatu Rancangan Undang-Undang Perlindungan Data Pribadi yang apabila disahkan dan dinyatakan berlaku kelak, dapat dijadikan sebagai payung hukum dalam mengatur tata kelola data, sehingga pergerakan, perpindahan, dan penggunaan data pribadi tetap menghormati hak privasi dari sang pemilik data.

Salah satu hal yang masih menjadi pembahasan dalam RUU PDP adalah terkait dengan pembentukan lembaga yang berfungsi sebagai regulator, pengawas, dan pengendali *(independent regulatory body)*. Dalam salah satu pemaparannya, Prof Dr. Henry Subiakto selaku Staf Ahli

Menkominfo RI menyatakan, bahwa lembaga perlindungan data pribadi setidaknya harus memiliki tugas dan fungsi yang terdiri dari:[50]

a. *Regulatory*, yaitu membuat regulasi dan kebijakan, dimana keputusannya bersifat mengikat.

b. *Surveillance*, yaitu pengawasan dan penegakan hukum.

c. *Evaluasi compliance,* yaitu penyelesaian sengketa dan penegakan hukum.

d. *Cooperation*, yaitu kerja sama dengan institusi lain, baik dalam skala nasional maupun internasional.

e. *Development,* yaitu pengembangan ekosistem.

f. *Promotion,* yaitu promosi, sosialisasi, dan edukasi kepada publik.

Dalam pemaparan Lembaga Riset Siber Indonesia yang berjudul "Kewaspadaan Nasional Terhadap Perkembangan Siber dan Ancamannya" disebutkan, bahwa setidaknya lembaga khusus yang dibentuk harus merupakan organisasi atau tim yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan siber. Tim khusus dibentuk dengan tujuan untuk melakukan penyelidikan komprehensif dan melindungi sistem atau data atas insiden keamanan siber yang terjadi pada organisasi.

Tim yang dinamakan dengan CSIRT *(Computer Security Incident Response Team)* ini setidaknya memiliki fungsi:

a. *Defense*: Melindungi infrastruktur kritis.

b. *Monitoring*: Menganalisis anomali dengan berbagai pola terdefinisi dan pola tidak terdefinisi (disebut sebagai *vulnerability database*).

c. *Intercepting*: Mengumpulkan konten spesifik atau disebut *targeted content.*

d. *Surveillance*: Mengamati dan menganalisis aktivitas yang dicurigai dan informasi yang berubah dalam sistem.

e. *Mitigating*: Mengendalikan kerusakan serta menjaga ketersediaan dan kemampuan layanan tersebut.

f. *Remediation*: Membuat solusi untuk mencegah kegiatan yang berulang-ulang dan mempengaruhi sistem.

---

[50] *Ibid.*

g. *Offensive*: Pencegahan/perlawanan dengan menyerang balik seperti *Cyber Army* dan kemampuan untuk menembus sistem keamanan.[51]

Dalam hal mewujudkan sistem perlindungan data pribadi, peranan pemerintah sangat signifikan dan vital. Pemerintah adalah lembaga yang dibentuk melalui konsensus bersama suatu negara melalui pembentukan konstitusi guna mewujudkan cita-cita masyarakat suatu bangsa, serta membuat dan melaksanakan keputusan untuk mencapai cita-cita tersebut. Perbedaan yang jelas antara pemerintah dengan lembaga lain terletak pada konteks inter-relasi sosial. Pemerintah memiliki legitimasi kekuasaan yang bersifat memaksa, yang disebut Huges sebagai *"the power of coercion,"* sedangkan lembaga lain memiliki pola inter-relasi yang bersifat sukarela *(voluntary).* "Kekuasaan yang bersifat memaksa" itu timbul dari legitimasi undang-undang yang dimiliki oleh pemerintah untuk bertindak atas nama negara dalam konteks menjaga dan menjamin kepentingan sosial dalam proses pencapaian tujuan.[52]

Pemikiran dari Irving Swerdlow menyebutkan *involvement* atau campur tangan pemerintah dalam proses perkembangan kegiatan masyarakat dapat dilakukan dengan 5 (lima) macam cara, yang terdiri dari:

a. Operasi langsung *(operation)*: Pemerintah menjalankan sendiri kegiatan-kegiatan tertentu.

b. Pengendalian langsung *(direct control):* Penggunaan perizinan, lisensi (untuk kredit, kegiatan ekonomi lain), penjatahan, dan lain sebagainya. Dilakukan oleh badan-badan pemerintahan yang telah atau berusaha menjadi *'action ladem'* (yang berwenang dalam berbagai perizinan, alokasi, tarif, dan lain sebagainya).

c. Pengendalian tidak langsung *(indirect control):* Memberikan pengaturan dan syarat-syarat tertentu.

d. Pemengaruhan langsung *(direct influence):* Melakukan persuasi dan nasihat misalnya supaya golongan masyarakat tertentu dapat turut menggabungkan diri dalam koperasi atau program tertentu.

---

[51] Pratama Persadha, *Op.Cit.*

[52] Budi Setiyono, *Pemerintahan dan Manajemen Sektor Publik*, (Jakarta: CAPS), 2014, hlm. 11-12.

e. Pemengaruhan tidak langsung *(indirect influence):* Merupakan bentuk *involvement* yang paling ringan, misalnya hanya memberikan informasi, penyuluhan, dan pembinaan untuk dapat menerima hal-hal yang baru *(promoting a receptive attitude toward innovation).*

Sistem Perlindungan siber oleh suatu lembaga diharapkan dapat menjalankan fungsi regulasi (dalam rangka pengendalian langsung maupun tidak langsung), riset (operasi langsung), sosialisasi dan pengawasan yang mencakup praktik teknologi informasi yang adil dan independen, sehingga lebih jauh melibatkan perluasan kekuatan sektor bisnis, pemerintahan, dan kepentingan hak asasi pribadi. Mengingat hal ini berkaitan erat dengan penguatan sistem keamanan nasional, maka harus pula memegang peran koordinasi dengan lembaga pertahanan dan keamanan nasional seperti Polri dan TNI, maupun lembaga pemerintah maupun lembaga bentukan lainnya.

Supaya dapat memenuhi tujuan besar dalam melindungi data pribadi guna memperkuat keamanan nasional, maka harus dibentuk suatu lembaga/komisi perlindungan data pribadi yang berdiri secara independen, karena harus berdiri di tengah-tengah antara kepentingan pemerintah, masyarakat umum, dan industri bisnis. Apabila kepentingan ini bisa diakomodir dengan tingkat kepercayaan kelembagaan yang tinggi dari masyarakat, maka penguatan keamanan nasional akan dapat terwujud.

Secara khusus, sistem pengawasan dan perlindungan siber oleh suatu lembaga diharapkan dapat menjalankan fungsi regulasi (dalam rangka pengendalian langsung), riset (operasi langsung), sosialisasi, dan pengawasan yang mencakup praktik teknologi informasi yang adil dan independen, sehingga lebih jauh melibatkan perluasan kekuatan sektor bisnis, pemerintahan, dan kepentingan hak asasi pribadi. Mengingat hal ini berkaitan erat dengan penguatan sistem keamanan nasional, maka harus pula memegang peran koordinasi dengan lembaga pertahanan dan keamanan nasional seperti Polri dan TNI.

Lembaga Perlindungan Data Pribadi akan lebih efektif jika bersifat independen, bukan di bawah Menkominfo, tetapi bertanggung jawab langsung kepada presiden sebagaimana badan-badan independen yang sudah ada, seperti Ombudsman, Komisi Pemberantasan Korupsi (KPK), Badan

Pengawas Pemilu (Bawaslu), Komisi Pengawas Persaingan Usaha (KPPU), maupun Komisi Nasional Hak Asasi Manusia (Komnas HAM) yang kedudukannya bersifat independen. Hal ini bertujuan untuk mencegah terjadinya benturan kepentingan antar lembaga sekaligus untuk meningkatkan fungsi melalui efektivitas kerja lembaga.

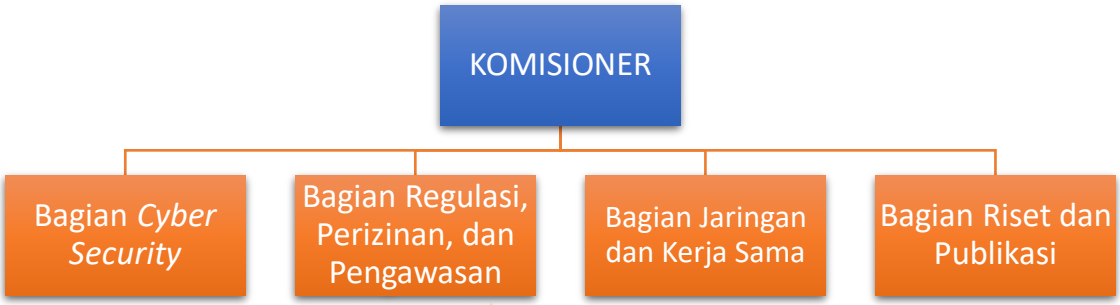
Lembaga Perlindungan Data Pribadi tidak perlu menjangkau hingga ranah penegakan hukum, karena sudah ada Kepolisian Republik Indonesia (Polri) yang berwenang melakukan hal tersebut. Lembaga Perlindungan Data Pribadi dalam fungsi pengawasan nantinya dapat berwenang untuk pelaporan dan koordinasi dengan penegak hukum lainnya. Hal ini dimaksudkan untuk meminimalisir risiko terjadinya tumpang tindih *(over lapping)* kewenangan antar penegak hukum yang tentunya dapat berdampak pada terganggunya sistem penegakan hukum, sehingga berpotensi menimbulkan ketidakpercayaan *(distrust)* yang lebih besar dari masyarakat terhadap pemerintah.

Kebijakan yang diambil oleh Lembaga Perlindungan Data Pribadi harus menjadikan derajat kepatuhan hukum masyarakat sebagai salah satu parameter tentang efektivitas hukum tersebut (Undang-Undang Perlindungan Data Pribadi) diberlakukan. Kepatuhan masyarakat dapat dimotivasi oleh berbagai penyebab, baik yang ditimbulkan oleh kondisi internal maupun eksternal. Perlu juga diingat, bahwa secara umum, masyarakat Indonesia memiliki kecenderungan yang besar untuk mengasosiasikan dan bahkan mengidentifikasi hukum dengan petugas (dalam hal ini penegak hukum sebagai pribadi), sehingga baik buruknya hukum senantiasa dikaitkan dengan pola perilaku oknum-oknum penegak hukum.[53]

Lebih lanjut lagi, dalam hal ini penulis berpendapat, bahwa dalam pelaksanaan tugasnya, tim khusus atau Lembaga Perlindungan Data Pribadi setidaknya harus memenuhi 4 (empat) fungsi yang dijalankan oleh 4 (empat) bagian organisasi, dengan pimpinan lembaga (Komisioner) yang harus mewakili unsur masyarakat, pemerintah, dan pelaku industri bisnis. Secara sederhana penulis merancang model struktur berikut:

[53] Soerjono Soekanto, *Op. Cit.,* hlm. 84.

Model Struktur Lembaga Perlindungan Data Pribadi di Indonesia



Gambar 7. Model Struktur Lembaga Perlindungan Data Pribadi di Indonesia

Dalam melaksanakan fungsinya, secara umum Lembaga Perlindungan Data Pribadi setidak-tidaknya harus memiliki unsur yang terdiri dari:

a. Komisioner

1) **Wewenang:**

Memimpin lembaga, mengatur arah kebijakan dan pelaksanaan tugas lembaga, serta mewakili organisasi ke luar dan ke dalam. Anggota komisi dipilih mewakili unsur masyarakat, pelaku industri bisnis digital, dan pemerintah.

2) **Tugas:**

a) Pelaksanaan kode etik; pengawasan internal melalui mekanisme dewan audit; serta fungsi, tugas, dan wewenang pengawasan untuk sektor industri dan pemerintahan.

b) Mewakili organisasi ke dalam maupun ke luar.

c) Memegang peranan penyelesaian sengketa pengelolaan informasi data pribadi melalui sidang komisi.

b. Bagian *Cyber Security*

1) **Wewenang:**

Mengurus segala sesuatu yang berkaitan dengan teknologi komputasi dan jaringan untuk kebutuhan perlindungan data pribadi.

2) **Tugas:**

a) Peningkatan infrastruktur berupa perangkat keras *(hardware),* perangkat lunak *(software),* jaringan, dan perangkat keamanan yang kinerjanya harus dipertahankan dan ditingkatkan.

b) Pelaksanaan tugas yang mencakup *critical infrastructure* (infrastruktur kritis), *application security* (keamanan aplikasi), *network security* (keamanan jaringan), *cloud security* (keamanan penyimpanan), dan lain sebagainya yang bertujuan untuk mencegah dan menghindari (preventif) serangan terhadap pelaku pengelolaan data pribadi.

c) Mendukung usaha pemulihan pasca terjadi kebocoran data pribadi secara teknis komputasi, termasuk di dalamnya pemblokiran akses, pemulihan data, dan lain sebagainya.

c. Bagian Regulasi, Perizinan, dan Pengawasan

1) **Wewenang:**

Menerbitkan regulasi tentang perlindungan data pribadi (peraturan pelaksana yang lebih rendah daripada undang- undang) dan perizinan, serta melakukan pengawasan terhadap lembaga pemerintah dan pelaku Industri bisnis yang melakukan pengelolaan data pribadi.

2) **Tugas:**

a) Menerbitkan perizinan sebagai syarat operasional suatu aplikasi/*platform* pelaku transaksi elektronik yang menghimpun data pribadi.

b) Menetapkan standar operasional atau produk-produk regulasi lainnya yang menjadi pedoman bagi aplikasi/*platform* pengelola informasi data pribadi.

c) Melakukan tindakan pengawasan yang meliputi audit teknologi informasi dan manajemen sistem keamanan informasi yang dimiliki oleh *platform* penghimpun data pribadi, termasuk pemberian sanksi administratif seperti pencabutan izin.

d) Secara aktif melakukan kerja sama dengan Polri sebagai penegak hukum untuk menindak secara pidana pencurian data pribadi dan serangan siber lainnya.

d. Bagian Jaringan dan Kerja sama

1) **Wewenang:**

Melakukan sosialisasi peningkatan literasi digital, khususnya perlindungan data pribadi kepada masyarakat dan menjalin kerja sama dengan lembaga-lembaga terkait, baik itu yang berada di dalam negeri maupun di luar negeri untuk menciptakan keamanan perlindungan data pribadi di Indonesia.

2) **Tugas:**

a) Melakukan pemetaan lembaga-lembaga yang terkait dengan pengelolaan informasi data pribadi.

b) Melakukan penjajakan strategis dan menjalin kerja sama dengan lembaga-lembaga yang terkait dengan perlindungan data pribadi di dalam maupun luar negeri, baik itu swasta, swadaya masyarakat, maupun lembaga pemerintahan.

c) Secara aktif melakukan sosialisasi atau strategi komunikasi lainnya dengan tujuan untuk meningkatkan literasi digital dan kesadaran masyarakat akan pentingnya perlindungan data pribadi.

d) Secara aktif melakukan kerja sama dengan Badan Intelijen Negara (BIN), Polri, TNI, maupun lembaga terkait lainnya untuk mengantisipasi serangan siber dengan tujuan *spionase* atau tujuan lain yang mengancam keamanan nasional.

e. Bagian Riset dan Pengembangan

1) **Wewenang:**

Melakukan riset dan penelitian yang bertujuan untuk pengembangan perlindungan data pribadi, baik itu mencakup pengembangan kualitas SDM, jaringan teknologi, dan infrastruktur lainnya.

2) **Tugas:**

a) Melakukan pemetaan dan membentuk *big data* terkait badan atau *platform* digital yang melakukan penghimpunan informasi data pribadi.

b) Aktif melakukan penelitian dalam hal pengembangan teknologi untuk menciptakan atau meningkatkan infrastruktur perlindungan data pribadi.

c) Melakukan usaha-usaha peningkatan kualitas SDM melalui kerja sama dengan institut/universitas dan sekolah vokasi.

Pada dasarnya tidak ada bentuk lembaga yang secara mutlak ideal dalam pelaksanaan undang-undang perlindungan data pribadi dalam suatu negara. Peran lembaga perlindungan data pribadi akan sangat dipengaruhi oleh kemandirian, ketidakberpihakan, dan efektivitas dalam bertugas. Efektivitas dalam bertugas menjadi titik tolak, karena jangan sampai kehadiran lembaga perlindungan data pribadi justru menjadi mengganggu iklim bisnis, khususnya dalam hal perizinan bagi para pelaku transaksi elektronik atau penghimpun informasi data pribadi lainnya. Lembaga Perlindungan Data Pribadi harus mampu mengakomodir kepentingan negara (dalam hal ini pemerintah), hak asasi individu masyarakat, dan pelaku industri bisnis digital.

16. Sistem dan Metode Dalam Upaya Melindungi Data Pribadi di Ruang Digital

Dalam hal menjawab pentingnya membangun sistem dan metode dalam upaya melindungi data pribadi di ruang digital, maka sudah semestinya perlu menelusuri dan memahami apa yang dimaksud dengan data pribadi dan sejarah perlindungannya. Entitas yang dilindungi dalam mekanisme perlindungan data pribadi adalah 'orang perorangan' *(natural person)* dan bukan 'badan hukum' *(legal person)*. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau yang disebut juga dengan *the right to private life*. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian, orang perorangan adalah pemilik utama dari hak perlindungan data pribadi.[54]

Konsep perlindungan data mengisyaratkan, bahwa individu memiliki hak untuk menentukan apakah mereka akan atau bersedia membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Lebih jauh, perlindungan data juga berhubungan dengan konsep hak

[54] Naskah Akademik RUU Perlindungan Data Pribadi, *Loc. Cit.*

privasi. Hak privasi telah berkembang, sehingga dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.[55]

Pandangan tentang privasi pertama kali ditulis oleh Warren dan Brandheis di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul "*The Right to Privacy*" atau dapat diartikan sebagai "hak untuk tidak diganggu." Dalam jurnal tersebut, Warren dan Brandheis berpendapat, bahwa dengan adanya perkembangan dan kemajuan teknologi, maka timbul suatu kesadaran masyarakat akan adanya hak seseorang untuk menikmati hidup.[56] Dengan demikian dapat dikatakan, bahwa hak privasi adalah hak seseorang untuk berdaulat atas hidupnya sendiri, termasuk untuk menikmati kehidupan dengan terbebas dari gangguan maupun ikut campur dari pihak lain dan hak kebebasan memilih untuk berkenan membagikan kehidupan pribadinya kepada pihak lain atau tidak.

Hak privasi adalah salah satu hak yang melekat pada diri setiap orang dan merupakan martabat yang harus dilindungi. Data pribadi dimaknai sebagai data-data yang berkenaan dengan ciri seseorang, seperti nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[57] Data pribadi merupakan hal yang bersifat privat dan sensitif yang dimiliki oleh setiap orang. Di dalam data pribadi terdapat hak yang harus dilindungi, agar tidak terjadi penyalahgunaan terhadap informasi yang terkandung di dalamnya.

Salah satu bahaya penyalahgunaan data pribadi yang diunggah ke internet adalah kebocoran data yang dapat menimbulkan kejahatan-kejahatan baru, baik itu *cyber crime* (kejahatan dunia maya) maupun kejahatan konvensional seperti perampokan, penipuan, pemerasan, pencemaran nama baik, dan lain sebagainya.

---

[55] *Human Rights Committee General Comment No. 16 (1988*) *on the Right to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation* (art. 17) sebagaimana dikutip dalam Naskah Akademik RUU Perlindungan Data Pribadi, 2019, *Op. Cit.,* hlm.2.

[56] Latumahina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal Gema Aktualita, Volume 3, Nomor 2, (2014), hlm. 14-25.

[57] Mahira, *et.all*, *Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept,* Jurnal Legislatif, Volume 3, Nomor 2, (2020), hlm. 287-302.

Kebocoran data secara masif pada dasarnya dapat dikategorikan sebagai ancaman siber yang mengarah pada kejahatan siber *(cyber crime)*. Secara umum, ancaman siber dibagi menjadi 2 (dua) golongan, yakni ancaman siber yang tidak disengaja dan ancaman siber yang disengaja. Salah satu contoh ancaman siber yang tidak disengaja adalah ketika memperbarui perangkat lunak atau pengelolaan prosedur yang tidak sengaja merusak sistem, sedangkan ancaman siber yang disengaja terdiri atas 2 (dua) jenis, yaitu serangan tertuju (serangan yang terjadi ketika suatu kelompok atau individu secara spesifik menyerang suatu aset siber) dan serangan tidak tertuju (objek serangan yang tidak ditetapkan atau serangan acak).[58]

Sepanjang tahun 2022, Badan Siber dan Sandi Negara mencatat serangan siber yang masuk ke Indonesia mencapai 1,6 (satu koma enam) miliar serangan dalam bentuk *malware, trojan activity* (aktivitas trojan), dan *information gathering* (pengumpulan informasi untuk mencari celah keamanan).[59]

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mencatat, bahwa dalam kurun waktu Januari hingga Desember 2021, terdapat sebanyak 19.529 (sembilan belas ribu lima ratus dua puluh sembilan) laporan kasus kejahatan siber, yang terdiri dari pengancaman, penipuan, pemerasan, *fake news,* dan pornografi. Sementara berdasarkan laporan Kementerian Kominfo, sepanjang Januari-Desember 2021 terdapat sebanyak 2.036 (dua ribu tiga puluh enam) aduan berupa berita bohong *(hoax)*.[60]

Pakar keamanan siber dari lembaga CISSReC menjelaskan, bahwa ancaman siber pada tahun 2022 tidak akan jauh berbeda seperti tahun 2021, yakni pencurian data dan *ransomware*. Dengan kata lain, pencurian data pribadi masih akan menjadi tren di tahun 2022. Hal ini diduga, karena data

---

[58] *Ibid.*

[59] CNN Indonesia, 2021, *888 Juta Serangan Siber Sepanjang 2021,* https://www.cnnindonesia.com/nasional/20210913131225-12-693494/bssn-ada-888-juta-serangan-siber-sepanjang-2021, (diakses pada 27 Februari 2022, pukul 15.49 WIB).

[60] Databoks.katadata.co.id, 2020, *Daftar Kejahatan Siber yang Paling Banyak Dilaporkan ke Polisi*, https://databoks.katadata.co.id/datapublish/2020/09/08/daftar-kejahatan-siber-yang-paling-banyak-dilaporkan-ke-polisi, (diakses pada 29 Januari 2022, pukul 16.04 WIB).

dalam jumlah masif semakin dibutuhkan oleh banyak pihak, baik untuk kegiatan legal maupun ilegal.[61]

Semakin terintegrasinya pusat-pusat data maupun infrastruktur penting, baik yang bersifat fisik maupun non-fisik ke dalam jaringan teknologi, selain memberikan kemudahan akses dan kontrol, juga menempatkannya pada risiko keamanan baru. Risiko tersebut di antaranya bersumber dari adanya ancaman intrusi yang dilancarkan dari dunia maya yang mampu menembus sistem jaringan keamanan data dan informasi terhadap pusat dan infrastruktur penting.[62]

Potensi pelanggaran privasi atas data pribadi secara *online* yang marak terjadi adalah pengumpulan data pribadi secara masal *(digital dossier),* pemasaran langsung *(direct selling*), dan kegiatan komputasi awan *(cloud computing). Digital dossier* merupakan suatu pengumpulan data pribadi seseorang dalam jumlah banyak dengan menggunakan teknologi digital. Praktik ini telah dimulai sejak tahun 1970 oleh pemerintah terutama di negara-negara Eropa dan Amerika Serikat. Kini pihak swasta juga menjadi pelaku *digital dossier* dengan menggunakan teknologi internet.[63]

Pemasaran langsung *(direct selling)* adalah praktik yang dilakukan oleh para penjual untuk memasarkan barang dengan cara pemasaran langsung. Dengan berkembangnya cara pemasaran tersebut, maka berkembang pula industri bank data yang bertujuan khusus untuk mengumpulkan informasi konsumen dan data-data tersebut akan dijual kepada perusahaan-perusahaan yang melakukan praktik *direct selling.* Praktik *direct selling* sendiri telah cukup marak terjadi di Indonesia, terutama dalam industri keuangan, khususnya dalam pengelolaan kartu kredit dan asuransi.[64] Dalam hal ini dapat disimpulkan, bahwa informasi pribadi konsumen telah diperjualbelikan melalui agen-agen tanpa sepengetahuan dan izin dari pemilik informasi/data.

---

[61] Liberty Jemadu, 2021, *Ancaman Siber di 2022 Masih Didominasi Pencurian Data dan Ransomware,* https://www.suara.com/tekno/2021/12/24/184819/ancaman-siber-di-2022-masih-didominasi-pencurian-data-dan-ransomware, (diakses pada 27 Februari, pukul 16.02 WIB).

[62] Dwi Rezki Sri Astarini, *et al, Siber Intelijen Untuk Keamanan Nasional*, Jurnal Renaissance, Volume 6, Nomor 01, (Mei, 2021), hlm. 24.

[63] Daniel J. Solove, *The Digital Person, Technology and Privacy in the Information Age, West Group Publication*, (New York: New York University Press, 2004), hlm. 13-17.

[64] Naskah Akademik RUU Perlindungan Data Pribadi, *Op. Cit.,* hlm.5.

Sementara komputasi awan (*cloud computing*) adalah gabungan antara pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan penyimpanan). Saat ini beberapa perusahaan teknologi informasi dan komunikasi terkemuka telah mengeluarkan aplikasi yang menyediakan ruang penyimpanan data pengguna, seperti *Evernote, Dropbox, Google Drive, Sky Drive, Scribd, iCloud,* dan lain sebagainya. Perkembangan pemanfaatan teknologi tersebut menimbulkan potensi pelanggaran serius. Contoh pelanggaran terbaru adalah bobolnya data pengguna *iCloud* (komputasi awan yang disediakan oleh *Apple*) yang kemudian menyebar di beberapa media massa. Kasus ini mendapat banyak perhatian publik, karena pemilik data merupakan beberapa selebritis terkenal Hollywood, seperti Jennifer Lawrence, Jenny McCarthy, Rihanna, Kate Upton, Mary Elizabeth Winstead, Kristen Dunst, Ariana Grande, dan Victoria Justice.[65]

Dengan melihat semua ancaman dan potensi pelanggaran yang telah dijelaskan di atas, maka dapat dikatakan, bahwa permasalahan perlindungan data pribadi tidak hanya menjadi kepentingan privasi secara murni, tetapi kebutuhan akan perlindungan data pribadi individu sebagai konsumen atau pelaku bisnis juga menjadi konsentrasi penting, mengingat data tersebut memiliki nilai tinggi untuk kepentingan bisnis sementara pengumpulan serta pengolahannya menjadi kian mudah dengan perkembangan teknologi informasi komunikasi. Terutama di era analisis *big data* saat ini dimana data pribadi menjadi sangat berharga bagi kepentingan bisnis, karena mengandung data yang dapat menginformasikan hal-hal yang dapat mempengaruhi pasar.

Selain itu, pengumpulan dan pengolahan data secara makro berpotensi menimbulkan ancaman lebih serius yang dapat mengganggu stabilitas keamanan nasional. Terlebih jika dalam muatan data tersebut terhimpun juga data-data yang bersifat sensitif, seperti informasi menyangkut etnis, agama

---

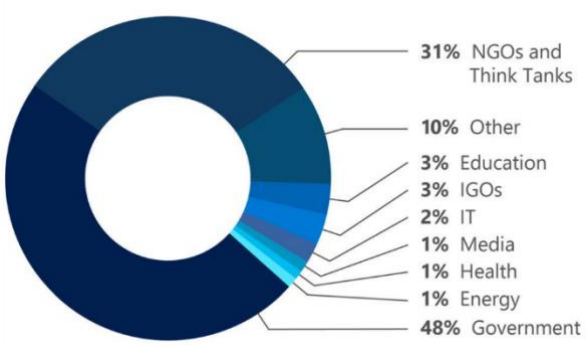
[65] Reska K Nistanto, 2014, *iCloud Dibobol, Foto Artis Hollywood Beredar,* https://tekno.kompas.com/read/2014/09/01/09591567/iCloud.Dibobol.Foto.Sensual.Jennifer.Lawrence.Beredar, (diakses pada 7 Maret 2022, pukul 09:30 WIB).

dan kepercayaan, pilihan politik, keanggotaan organisasi, riwayat kesehatan fisik maupun mental, dan bahkan kecenderungan seksual seseorang.

Pintu ancaman terhadap keamanan nasional menjadi terbuka dan sangat mudah dimasuki apabila terjadi penyalahgunaan terhadap data-data pribadi (terlebih data bersifat sensitif) masyarakat secara kolektif. Misalnya data mengenai pilihan politik dapat dimanfaatkan untuk melakukan penggiringan opini di masyarakat dengan tujuan untuk mengganggu stabilitas politik, informasi mengenai etnis dan agama dapat dimanfaatkan untuk menyerang dan melakukan diskriminasi terhadap etnis maupun agama tertentu, atau tindakan-tindakan lain yang berujung pada konflik dan perpecahan. Belum lagi kerentanan data-data di situs-situs pemerintahan yang berisiko diretas oleh peretas *(hacker)* untuk melakukan kegiatan spionase (*cyber spionase*) internasional, yang tentunya akan mengancam keamanan dan pertahanan nasional. Saat ini serangan/perang dunia maya *(cyber attack/cyber warfare)* dianggap sebagai media yang sangat ampuh untuk mengguncang stabilitas keamanan suatu negara atau bangsa, karena memiliki karakteristik yang murah, mudah dijalankan, dan efektif dalam mencapai hasil yang diharapkan dibandingkan dengan perang secara konvensional.

Berdasarkan laporan *Microsoft* yang dirilis pada Oktober 2021, secara global target spionase siber saat ini adalah meliputi: (1) Sektor pemerintahan sebesar 48% (empat puluh delapan persen); (2) Lembaga Swadaya Masyarakat (LSM) dan lembaga penelitian sebesar 31% (tiga puluh satu persen); (3) Sektor pendidikan sebesar 3% (tiga persen); (4) Sektor organisasi lingkungan sebesar 3% (tiga persen); (5) Sektor Informasi dan Teknologi (IT) sebesar 2% (dua persen); (6) Sektor media sebesar 1% (satu persen); (7) Sektor kesehatan sebesar 1% (satu persen); (8) Sektor energi sebesar 1% (satu persen); dan (9) Sektor lainnya sebesar 10% (sepuluh persen).[66]

[66] Microsoft.com, 2021, *Microsoft Digital Defense Report,* https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report, (diakses pada 7 Maret 2022, pukul 14:00 WIB).



Gambar 8. Target Operasi Spionase Siber Global (Juli 2020- Juni 2021)
Sumber: Microsof Digital Defense Report 2021

Fakta spionase siber (*cyber espionage)* mulai memainkan peran penting dalam peperangan modern dapat terlihat dalam serangan siber *(cyber attack)* yang dilakukan oleh Rusia terhadap Estonia pada tahun 2007 dan Georgia pada tahun 2008. Kedua negara tersebut diserang dengan metode *DDoS (Distributed Denial of Service) attack* yang berakibat pada lumpuhnya layanan publik dan terputusnya saluran komunikasi di seluruh negara tersebut. Ini adalah kali pertama *cyber espionage* dipergunakan untuk melancarkan serangan (perang) konvensional. Bahkan Rusia juga menggunakan taktik ini pada serangannya terhadap Ukraina, dimana Rusia sudah terlebih dahulu menyerang sistem komunikasi telepon *mobile* milik Ukraina sebelum melancarkan serangan secara konvensional.[67]

Berdasarkan uraian di atas dapat disimpulkan, bahwa perlindungan data pribadi memiliki posisi penting dan krusial, karena dampak yang dapat ditimbulkannya cukup fatal. Oleh sebab itu, sudah seharusnya pemerintah mengambil peranan penting dan sesegera mungkin merumuskan regulasi dan kebijakan terkait perlindungan data pribadi di ruang digital guna menjaga stabilitas keamanan nasional.

Seiring perkembangannya, keamanan nasional yang dikenal saat ini berkonsep keamanan yang berpusat pada orang/masyarakat *(people centered security*), dari yang semula mengusung konsep keamanan berpusat pada negara *(state centered security).* Berdasarkan teori ini, orientasi kebijakan keamanan nasional harus berpusat kepada orang/masyarakat yang meluas *(people centered security),* termasuk perlindungan data pribadi. Data

[67] Sri Sutanto, 2017, *Cyber Espionage (Spionase Siber) dan Dampaknya di Era Siber,* https://porosnews.com/2017/10/05/cyber-espionage-spionase-siber-dan-dampaknya-di-era-siber/, (diakses pada 8 Maret 2022, pukul 08:00 WIB).

pribadi yang dimiliki oleh setiap orang adalah bagian dari hak privasi yang di era digital saat ini juga memiliki fungsi ekonomis.

Merujuk pada pendapat Berry Buzan, bahwa keamanan tidak semata berfokus pada sudut pandang negara *(state security)* secara sempit dimana jika kebutuhan pokok masyarakat terpenuhi dan rakyat dianggap sejahtera, maka secara otomatis akan tercipta keamanan. Lebih luas daripada itu, perwujudan keamanan nasional mengacu pada pandangan, bahwa keamanan nasional di negara demokrasi harus mencakup keamanan negara *(state security),* keamanan masyarakat *(public security),* dan keamanan manusia *(human/people security)*. Melindungi data pribadi berarti melindungi banyak aspek kehidupan masyarakat, sehingga orientasi kebijakan yang disusun harus berpusat pada kepentingan orang/masyarakat yang apabila diwujudkan secara benar akan secara otomatis melindungi kepentingan keamanan nasional. Perlindungan data pribadi warga negara sebagai bagian dari usaha mewujudkan keamanan nasional mutlak menjadi tanggung jawab bersama antara pemerintah, unsur swasta, dan masyarakat.

Dalam mewujudkan keberhasilan suatu implementasi kebijakan, maka suatu kebijakan harus mengacu pada aturan yang menjadi panduan pelaksanaan kebijakan tersebut, yang dalam tatanan kenegaraan Indonesia adalah Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan peraturan perundang-undangan terkait di bawahnya. Selain itu berhasil tidaknya suatu kebijakan dapat dilihat dari dampak yang diperoleh masyarakat dan adanya perubahan yang terjadi di tengah masyarakat, khususnya setelah memperoleh kebijakan. Merujuk pada hal tersebut, maka dalam hal ini pemerintah harus memperhatikan variable *content of policy* (isi kebijakan), termasuk di dalamnya pembentukan lembaga dan instrumen hukum berupa undang-undang; dan *context of implementation* (lingkungan implementasi kebijakan), dimana pemerintah harus memperhatikan pula tingkat kepatuhan dan responsivitas dari kelompok sasaran, yang dalam hal ini adalah masyarakat digital Indonesia.

Dalam hal pengimplementasian, adapun sistem dan metode yang harus dilakukan sebagai bentuk upaya dalam melindungi data pribadi di ruang digital

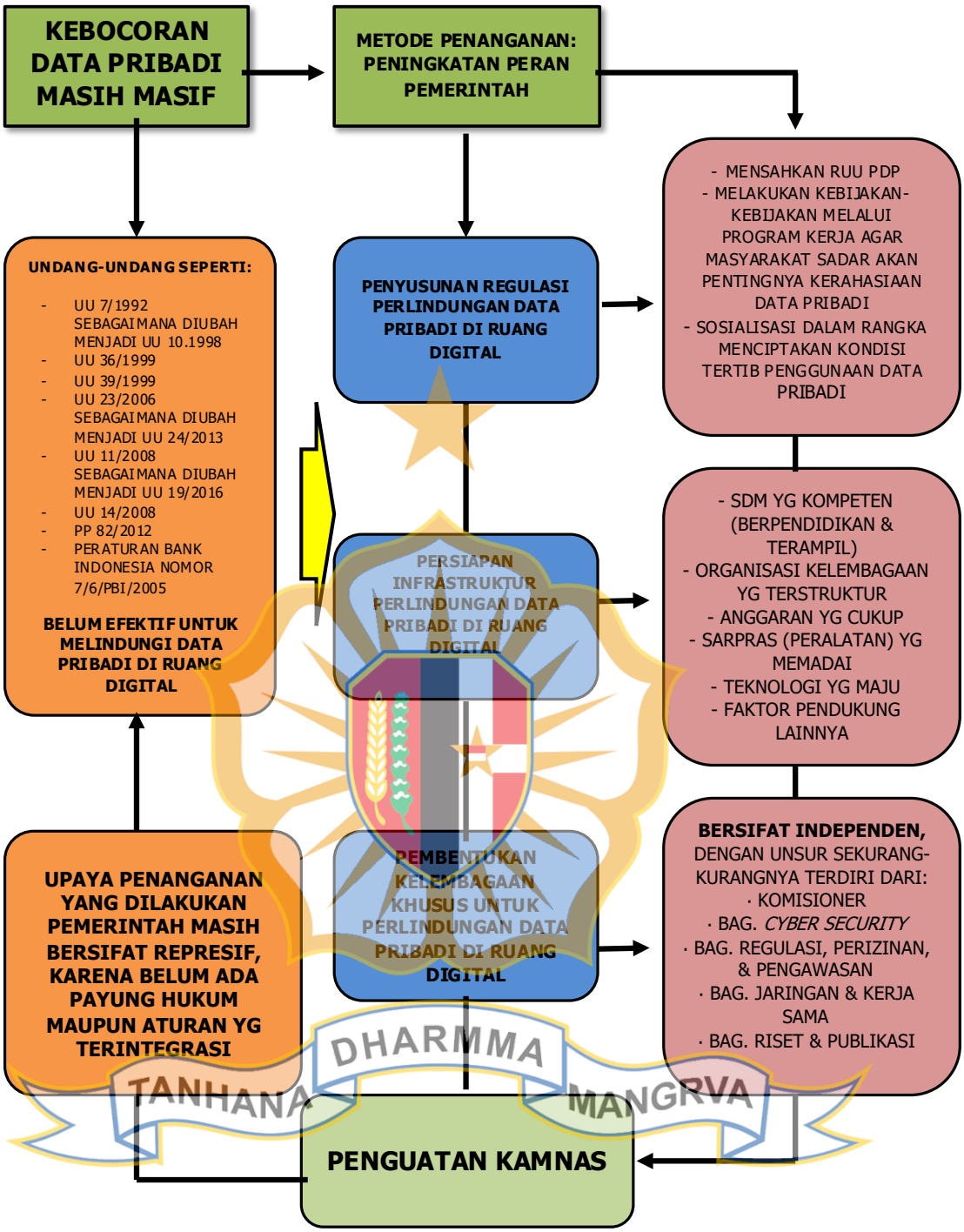
guna memperkuat keamanan nasional adalah melalui 3 (tiga) upaya yang telah dijabarkan sebelumnya, yang terdiri dari:

a. Menyusun regulasi perlindungan data pribadi di ruang digital, yang dilakukan dengan cara segera mengesahkan Undang-Undang Perlindungan Data Pribadi, agar dapat menjadi payung hukum terkait perlindungan data pribadi di ruang digital.

b. Mempersiapkan infrastruktur perlindungan data pribadi di ruang digital, yang dilakukan dengan cara mempersiapkan Sumber Daya Manusia (SDM) yang berpendidikan dan terampil (kompeten), mempersiapkan organisasi kelembagaan yang terstruktur, mempersiapkan anggaran yang cukup, menyediakan peralatan yang dibutuhkan, memasukkan tentang pentingnya data pribadi di dalam kurikulum pendidikan sebagai bentuk edukasi sejak dini, dan mempersiapkan faktor-faktor pendukung lainnya.

c. Membentuk kelembagaan khusus untuk perlindungan data pribadi di ruang digital, yang dilakukan dengan cara membentuk suatu Lembaga Perlindungan Data Pribadi yang berdiri secara independen, karena harus berdiri di tengah-tengah antara kepentingan pemerintah, masyarakat umum, dan industri bisnis. Lembaga tersebut setidak-tidaknya harus memiliki unsur yang terdiri dari: (1) Komisioner; (2) Bagian *Cyber Security*; (3) Bagian Regulasi, Perizinan, dan Pengawasan; (4) Bagian Jaringan dan Kerja Sama; serta (5) Bagian Riset dan Pengembangan.

Secara garis besar, upaya Peningkatan Peran Pemerintah Dalam Perlindungan Data Pribadi di Ruang Digital Guna Memperkuat Keamanan Nasional digambarkan dalam *flow chart* berikut:



Gambar 9. Sistem dan Metode Dalam Upaya Melindungi Data Pribadi di Ruang Digital

BAB IV
PENUTUP

17. Simpulan

Berdasarkan uraian pada bab pembahasan sebelumnya, maka diperoleh beberapa simpulan, yakni sebagai berikut:

a. Temuan pada kajian pertama menunjukkan, bahwa kesadaran akan pentingnya Undang-Undang Perlindungan Data Pribadi sudah muncul dan tumbuh di tengah masyarakat. Pengaturan mengenai data pribadi sangat penting, karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman, dan keamanan data pribadi. Saat ini Indonesia sudah memiliki beberapa instrumen hukum yang mengatur mengenai perlindungan data pribadi, baik itu di level undang-undang maupun peraturan di bawahnya. Namun, semua perangkat aturan ini masih bersifat parsial dan terpisah-pisah serta masih berorientasi pada kelembagaan. Maka sebagai jawaban atas kajian pertama, RUU PDP yang sebenarnya sudah masuk Prolegnas dan dibahas sejak tahun 2019 perlu segera disahkan menjadi undang-undang yang dapat digunakan sebagai payung hukum dalam rangka menjamin regulasi mengenai perlindungan data pribadi.

b. Temuan pada kajian kedua menunjukkan, bahwa infrastruktur perlindungan data pribadi di Indonesia dari segi fasilitas secara fisik maupun non-fisik masih tergolong lemah. Penegakan hukum perlindungan data pribadi juga masih berorientasi represif, sedangkan dari sisi preventif pemerintah telah mengakui sertifikasi SNI ISO 27001:2013, tetapi masih bersifat suka rela. Saat ini, pemerintah Republik Indonesia melalui Kementerian Komunikasi dan Informatika (KOMINFO) telah mengembangkan penyediaan Pusat Data Nasional Sementara (PDNS) untuk mempercepat konsolidasi pusat data instansi dan konsolidasi *database* nasional. Maka sebagai jawaban atas kajian kedua, dibutuhkan usaha yang masif dari pemerintah untuk melakukan peningkatan infrastruktur perlindungan data pribadi dengan

mengkonsolidasikan seluruh lembaga dan mengoptimalkan seluruh sumber daya yang ada.

c. Temuan pada kajian ketiga menunjukkan, bahwa pembentukan kelembagaan khusus dalam penanganan perlindungan data pribadi di ruang digital sangat perlu dilakukan. Pada intinya tidak ada bentuk lembaga yang secara mutlak ideal dalam pelaksanaan undang-undang perlindungan data pribadi pada suatu negara. Maka sebagai jawaban atas kajian ketiga, pemerintah perlu membentuk Lembaga Perlindungan Data Pribadi yang secara umum setidak-tidaknya harus memiliki unsur/bagian: (1) Komisioner; (2) Bagian *Cyber Security*; (3) Bagian Regulasi, Wewenang, dan Pengawasan; (4) Bagian Jaringan dan Kerja Sama; serta (5) Bagian Riset dan Pengembangan. Lembaga tersebut harus mampu mengakomodir kepentingan negara, hak asasi individu masyarakat, dan pelaku industri bisnis digital. Apabila kebijakan pemerintah ini terwujud dengan baik, maka keamanan nasional dapat terjamin.

d. Temuan pada kajian keempat menunjukkan, bahwa data pribadi individu menjadi konsentrasi penting, karena informasi yang terkandung dalam data pribadi adalah hak atas privasi individu, dan saat ini memiliki nilai tinggi sebagai data untuk kepentingan bisnis. Temuan pada kajian keempat adalah, bahwa dibutuhkan sistem dan metode sebagai bentuk upaya melindungi data pribadi di ruang digital, yang dilakukan dengan cara: (1) Menyusun regulasi perlindungan data pribadi di ruang digital; (2) Menyiapkan infrastruktur perlindungan data pribadi di ruang digital; serta (3) Membentuk kelembagaan khusus untuk perlindungan data pribadi di ruang digital.

18. Rekomendasi

Adapun rekomendasi yang dikemukakan, terdiri dari:

a. Presiden bersama-sama dengan Dewan Perwakilan Rakyat (DPR) harus mengambil peran dalam menciptakan iklim digital yang aman terhadap perlindungan data pribadi dengan membentuk regulasi (Undang-Undang Perlindungan Data Pribadi), serta melakukan

kebijakan hukum dengan mencabut atau mengubah aturan-aturan yang tumpang tindih dan tidak sesuai dengan perkembangan zaman (mewujudkan efektivitas hukum).

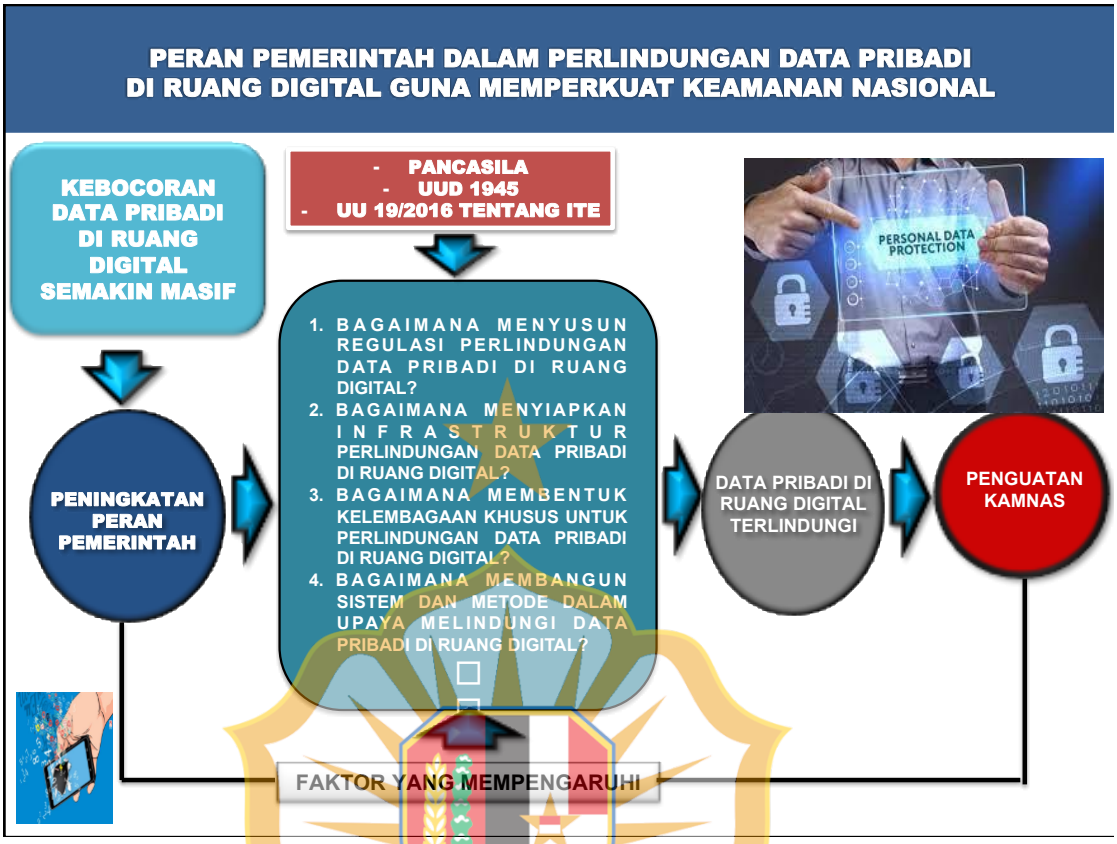
b. Presiden bersama-sama dengan Dewan Perwakilan Rakyat (DPR) membentuk suatu lembaga independen sebagai pelaksana Undang-Undang Perlindungan Data Pribadi yang bertugas untuk melakukan fungsi pelaksanaan, regulasi, dan pengawasan terhadap pelaku penghimpun data pribadi.

c. Kementerian Komunikasi dan Informatika (KOMINFO) bekerja sama dengan Badan Intelijen Negara (BIN), Tentara Nasional Indonesia (TNI), dan Polri perlu membuat suatu rancangan besar mengenai perlindungan data pribadi di Indonesia dalam kaitannya dengan keamanan nasional, yang mencakup pada rancangan pengembangan infrastruktur, termasuk Sumber Daya Manusia (SDM).

d. Kementerian/Lembaga seperti KOMINFO, Otoritas Jasa Keuangan (OJK), Bank Indonesia, dan lain sebagainya melalui kebijakannya harus melakukan kerja sama yang baik dan strategis antara sektor pemerintahan (pusat sampai dengan daerah), pelaku industri bisnis digital, masyarakat Indonesia, dan luar negeri untuk menjamin keamanan data pribadi, agar tercipta iklim dunia digital yang ramah terhadap perlindungan hak asasi dan kegiatan bisnis, sehingga stabilitas keamanan nasional dapat senantiasa terjaga.

e. Penegak hukum (Polri, Kejaksaan, Kehakiman, dan Advokat) perlu mengusahakan sebuah proses peradilan pidana yang ideal dan menjamin kepastian, keadilan, dan kemanfaatan hukum dalam penegakan undang-undang perlindungan data pribadi. Hal ini sangat berkaitan erat dengan perlunya pengesahan RUU PDP menjadi undang-undang. Jika undang-undang tersebut telah disahkan, maka para penegak hukum dapat merumuskan Standar Operasional Prosedur (SOP) sesuai dengan perundang-undangan dalam penindakan dan penegakan hukum terkait perlindungan data pribadi.

ALUR PIKIR



Gambar 10. Alur Pikir

DAFTAR RIWAYAT HIDUP

BIODATA

1.	Nama Lengkap	:	H. M. Sabilul Alif, S.H., S.I.K., M.Si
2.	Tempat, tanggal lahir	:	Gresik, 27 Juni 1975
3.	Jenis Kelamin	:	Laki-Laki
4.	Status Pernikahan	:	Kawin
5.	Alamat Rumah	:	Jl. Gayungsari II, No. 73, Gayungan, Surabaya, Jawa Timur
6.	Nomor telepon/ HP	:	08112629696
7.	E-mail	:	sabilul.alif9696@gmail.com
8.	Golongan Darah	:	B
9.	Agama	:	Islam
10.	Suku	:	Jawa

KARIR

1.	Pekerjaan	:	Polri
2.	Instansi	:	SSDM Polri
3.	Alamat	:	Jl. Trunojoyo, No. 3, Kebayoran Baru, Jakarta Selatan
4.	No. Telepon	:	
5.	NRP	:	
6.	Jabatan	:	Pamen SSDM Polri (Ajudan Wakil Presiden RI)
7.	Pangkat/ Golongan	:	Komisaris Besar Polisi

KELUARGA

1.	Pasangan	:	Nur Aja Putri
2.	Anak	:	Nisa Elysia Alif
			Farrel Daffani Aladamy

PENGHARGAAN

Pin Emas Kapolri	:	2020

KEPANGKATAN

IPDA	:	1996
IPTU	:	2001
AKP	:	2003
KOMPOL	:	2008
AKBP	:	2012
Kombes Pol	:	2018

DAFTAR PUSTAKA

Buku

----- *Naskah Akademik RUU Perlindungan Data Pribadi.* 2019. Jakarta.

Kepolisian Republik Indonesia. 2022. *Rencana Kerja Kepolisian Negara Republik Indonesia Tahun Anggaran 2022, Lampiran Keputusan Kapolri Nomor: Kep/1087/Vi/2021 Tanggal: 29 Juni 2021.* Jakarta: Kepolisian Republik Indonesia.

Rosadi, Sinta Dewi. 2009. *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional.* Bandung: Widya Padjajaran.

Solove, Daniel J. 2021. *The Digital Person, Technology and Privacy in the Information Age.* (New York: West Group Publication, New York University Press.

Tim Pokja. 2022. *Bahan Ajar Bidang Studi Hubungan Internasional.* Jakarta: Lembaga Ketahanan Nasional Republik Indonesia.

Makalah/Jurnal

Anggoro, Kusnanto. *Keamanan Nasional, Pertahanan Negara, dan Ketertiban Umum,* Makalah Pembanding Seminar Pembangunan Hukum Nasional VIII, (Juli 2003), Departemen Kehakiman dan HAM RI.

Astarini, Dwi Rezki Sri, *et al*. 2021. *Siber Intelijen Untuk Keamanan Nasional*. Jurnal Renaissance, Volume 6, Nomor 01. Mei.

Bahrudin, Muhammad dan Firmansyah. 2018. *Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001.* Jurnal Media Pustakawan, Volume 25, Nomor 1, Perpustakaan Nasional Republik Indonesia.

Chik, Warren B. 2013. *The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy.* Computer Law and Security Review, Volume 5.

Djafar, Wahyudi. 2019. *Hukum Perlindungan Data Pribadi di Indonesia.* Makalah disampaikan sebagai materi dalam kuliah umum Tantangan Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, Yogyakarta.

Kusumoningtyas, Anggi, *et.all.* 2020. *Dilema Hak Perlindungan Data Pribadi dan Pengawasan Siber: Tantangan di Masa Depan*. Jurnal Legislasi Indonesia, Volume 17, Nomor 2, Sekolah Kajian Stratejik dan Global, Universitas Indonesia. Juni.

Latumahina. 2014. *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Jurnal Gema Aktualita, Volume 3, Nomor 2.

Mahira, *et.all*. 2020. *Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept.* Jurnal Legislatif, Volume 3, Nomor 2.

Mantoro, Teddy. 2022. *Dinamika Perkembangan Teknologi Informasi (Siber) dan Ancaman yang Ditimbulkan.* Pemaparan di LEMHANAS.

Muhammad, Farouk. 2008. *Polri Dalam Sistem Pertahanan dan Keamanan*. Makalah Seminar IODAS. Jakarta.

Persadha, Pratama. 2022. *Kewaspadaan Nasional Terhadap Perkembangan Siber dan Ancamannya.* Pemaparan sebagai *Chairman* Lembaga Riset Keamanan Ciber CISSReC.

Sidratahta, Mukhtar. 2009. *Pemberantasan Terorisme di Indonesia dan Dampaknya Terhadap Keamanan Nasional.* Makalah Seminar Sehari, Departemen Ilmu Hubungan Internasional, Universitas Hasanuddin.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232. Tambahan Lembaran Negara Republik Indonesia Nomor 5475.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61. Tambahan Lembaran Negara Republik Indonesia Nomor 4846.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185. Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

Peraturan Presiden Nomor 38 tahun 2015 Tentang Kerja Sama Pemerintah dengan Badan Usaha Dalam Penyediaan Infrastruktur.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 103.

Lampiran Keputusan Kapolri Nomor: Kep/1087/Vi/2021 Tanggal: 29 Juni 2021 tentang Rencana Kerja Kepolisian Negara Republik Indonesia Tahun Anggaran 2022.

***Website*/Internet**

Ahmad, Kemas. 2021. *Media Sosial 2021: 170 Juta dari 274,9 Juta Jiwa Adalah Pengguna Media Sosial,* https://www.kompasiana.com/kemasahmadadnan6029/608a22fa8ede480b3e5165a3/media-sosial-2021-170-juta-dari-274-9-juta-jiwa-adalah-pengguna-media-sosial, (diakses pada 13 Februari 2022, pukul 21.18 WIB).

Ayuwuragil, Kustin. 2018. *Kominfo Akui 'Pencurian' NIK dan KK Saat Registrasi Kartu SIM,* https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim, (diakses pada 15 Februari 2022, pukul 17:00).

Burhan, Fahmi Ahmad. 2022. *Ahli IT: Data Bocor Bank Indonesia Berasal dari 200 Komputer,* https://katadata.co.id/desysetyowati/digital/61ee713f52c6d/ahli-it-data-bocor-bank-indonesia-berasal-dari-lebih-200-komputer, (diakses pada 29 Januari 2022, pukul 14.02 WIB).

Caesar Akbar. 2021. *6 Kasus Kebocoran Data Pribadi di Indonesia,* https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia, (diakses pada 29 Januari 2022, pukul 15.18 WIB).

CNN Indonesia. 2020. *Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank,* https://www.cnnindonesia.com/nasional/20200205211241-12-472073/ pembobolan-rekening-ilham-bintang-data-dijual-orang-bank, (diakses pada 15 Februari 2022, pukul 17:22).

CNN Indonesia. 2021. *888 Juta Serangan Siber Sepanjang 2021,* https://www.cnnindonesia.com/nasional/20210913131225-12-693494/bssn-ada-888-juta-serangan-siber-sepanjang-2021, (diakses pada 27 Februari 2022, pukul 15.49 WIB).

Dandi. 2022. *Kebocoran Data Situs Pemerintah,* Kebocoran Data Situs Pemerintah (republika.co.id, (diakses pada 13 Februari 2022, pukul 21.29 WIB).

Databoks.katadata.co.id. 2020. *Daftar Kejahatan Siber yang Paling Banyak Dilaporkan ke Polisi*, https://databoks.katadata.co.id/datapublish/2020/09/08/daftar-kejahatan-siber-yang-paling-banyak-dilaporkan-ke-polisi, (diakses pada 29 Januari 2022, pukul 16.04 WIB).

Dukcapil.kemendagri.go.id. 2022. *273 Juta Penduduk Indonesia Terupdate Versi Kemendagri,* https://dukcapil.kemendagri.go.id/berita/baca/1032/273-juta-penduduk-indonesia-terupdate-versi-kemendagri#:~:text=Jakarta%20%2D%20Kemendagri%20melalui%20Direktorat%20Jenderal,Indonesia%20adalah%20273.879.750%20jiwa, (diakses pada 28 Mei 2022, pukul 12.06 WIB).

Erwanti, Marlinda Oktavia. 2021. *Survei Kompas: 90,8% Responden Dorong RUU Perlindungan Data Pribadi Disahkan,* https://news.detik.com/berita/d-5493536/survei-kompas-908-responden-dorong-ruu-perlindungan-data-pribadi-disahkan, (diakses pada 19 Maret 2022).

Ikhsan, M. 2021. *279 Juta Data Penduduk RI Diduga Bocor dan Dijual di Forum,* https://www.cnnindonesia.com/teknologi/20210520140736-185-644759/279-juta-data-penduduk-ri-diduga-bocor-dan-dijual-di-forum, (diakses pada 29 Januari 2022, pukul 15.12 WIB).

Jatimiko, Leo Dwi. 2021. *Microsoft: Serangan SIber, Lahan Bisnis Baru buat Peretas,* https://teknologi.bisnis.com/read/20211124/84/1470012/waduh-microsoft-serangan-siber-lahan-bisnis-baru-buat-peretas, (diakses pada 18 Maret 2022 pukul 18:30WIB).

Jayani, Dwi Hadya. 2021. *Pencurian Data Pribadi Makin Marak Kala Pandemi,* https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi, (diakses pada 29 Januari 2022, pukul 16.27 WIB).

Jemadu, Liberty. 2021. *Ancaman Siber di 2022 Masih Didominasi Pencurian Data dan Ransomware,* https://www.suara.com/tekno/2021/12/24/184819/ancaman-siber-di-2022-masih-didominasi-pencurian-data-dan-ransomware, (diakses pada 27 Februari, pukul 16.02 WIB).

Kobrata, Danny. 2022. *RUU Perlindungan Data Pribadi: Sebuah Penantian,* RUU Pelindungan Data Pribadi: Sebuah Penantian (hukumonline.com), (diakses pada 18 Maret 2022 pukul 17:32 WIB).

Kominfo.go.id. *Memastikan Data Pribadi Aman,* https://www.kominfo.go.id/content/detail/37332/memastikan-data-pribadi-aman/0/artikel, (diakses pada 29 Januari 2022, pukul 17.02 WIB).

Kusnandar, Viva Budy. 2021. *Pengguna Internet Indonesia Peringat Ke-3 Terbanyak di Asia,* https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia#:~:text=Berdasarkan%20data%20internetworldstats%2C%20pengguna%20internet,pengguna%20internet%20terbanyak%20di%20Asia, (diakses pada 29 Januari 2022, pukul 13.30 WIB).

Lidwina, Andrea. 2021. *Kebocoran Data Pribadi yang Terus Berulang,* Kebocoran Data Pribadi yang Terus Berulang - Infografik Katadata.co.id, (diakses pada 13 Februari 2022, pukul 21.07 WIB).

Microsoft.com. 2021. *Microsoft Digital Defense Report,* https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report, (diakses pada 7 Maret 2022, pukul 14:00 WIB).

Mursid, Fauziah. 2021. *Menkominfo Tekankan Pentingnya Perlindungan Data di ASEAN,* Menkominfo Tekankan Pentingnya Pelindungan Data di ASEAN | Republika Online, (diakses pada 13 Februari 2021, 21.55 WIB).

Nistanto, Reska K. 2014. *iCloud Dibobol, Foto Artis Hollywood Beredar,* https://tekno.kompas.com/read/2014/09/01/09591567/iCloud.Dibobol.Foto.Sensual.Jennifer.Lawrence.Beredar, (diakses pada 7 Maret 2022 pada pukul 09:30 WIB).

Susi. 2019*. Memahami Konsep Keamanan,* https://tribratanews.kepri.polri.go.id/2019/07/17/memahami-konsep-keamanan-3/, (diakses pada 6 Mei 2022, pukul 19:00 WIB).

Sutanto, Sri. 2017. *Cyber Espionage (Spionase Siber) dan Dampaknya di Era Siber,* https://porosnews.com/2017/10/05/cyber-espionage-spionase-siber-dan-dampaknya-di-era-siber/, (diakses pada 8 Maret 2022, pukul 08:00 WIB).

Wareza, Monica. 2021. *Ini Serius! Serangan Siber Bikin Bank-Bank RI Rugi Rp246M,* https://www.cnbcindonesia.com/market/20211026131120-17-286621/ini-serius-serangan-siber-bikin-bank-bank-ri-rugi-rp-246-m, (diakses pada 29 Januari 2022, pukul 14.25 WIB).