LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

JUDUL:

KEWASPADAAN NASIONAL TERHADAP KEJAHATAN DIGITAL GUNA MENINGKATKAN KETAHANAN NASIONAL

Oleh:

BONY JOHANNES SANGANADI SIRAIT, S.I.K., M.H.

KOMBES POL NRP 74040739

KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)

PROGRAM PENDIDIKAN REGULAR ANGKATAN (PPRA) LXIV

LEMHANNAS RI

TAHUN 2022

KATA PENGANTAR

Assalammualaikum Wr Wb, salam sejahtera bagi kita semua.

Dengan memanjatkan puji syukur kehadirat Allah Subhanahu Wata'ala serta atas segala rahmat dan karunia-Nya, penulis sebagai salah satu peserta Program Pendidikan Regular Angkatan (PPRA) LXIV telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan judul: "**KEWASPADAAN NASIONAL TERHADAP KEJAHATAN DIGITAL GUNA MENINGKATKAN KETAHANAN NASIONAL**".

Penentuan Tutor dan judul Taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor 122 Tahun 2022 tanggal 6 Juni 2022 tentang Pengangkatan Tutor Taskap kepada para peserta PPRA LXIV untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada Bapak Gubernur Lemhannas RI yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXIV di Lemhannas RI tahun 2022. Ucapan yang sama juga disampaikan kepada Pembimbing atau Tutor Taskap kami Mayjen TNI (Purn) Dr. I Putu Sastra Wingarta, S.IP., M.Sc dan Tim Penguji Taskap serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini.

Besar harapan saya agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya.

Semoga Allah Subhanahu Wata'ala senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada Negara dan bangsa Indonesia yang kita cintai dan kita banggakan.

Sekian dan terima kasih. Wassalamualaikum Warahmatullahi Wabarakatuh.

Jakarta, 10 Oktober 2022

Penulis

BONY JOHANNES SANGANADI SIRAIT, S.I.K., M.H.

KOMBES POL NRP 74040739

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

   Nama : Bony Johannes Sanganadi Sirait, S.I.K., M.H.

   Pangkat : Komisaris Besar Polisi

   Jabatan : Analis Kebijakkan Bidang Dalpers SSDM Polri

   Instansi : POLRI

   Alamat : Jl. Saturnus No. 9 Turangga, Bandung

   Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) ke LXIV 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, 10 Oktober 2022

BONY JOHANNES SANGANADI SIRAIT, S.I.K., M.H.

KOMBES POL NRP 74040739

LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

DAFTAR ISI

		Halaman
KATA PENGANTAR		i
PERNYATAAN KEASLIAN		iii
DAFTAR ISI		iv
TABEL		vi
DAFTAR GAMBAR		vii
BAB I.	**PENDAHULUAN**	
1.	Latar Belakang	1
2.	Rumusan Masalah	6
3	Maksud dan Tujuan	6
4.	Ruang Lingkup dan Sistematika	6
5.	Metode dan Pendekatan	8
6.	Pengertian	8
BAB II.	**TINJAUAN PUSTAKA**	
7.	Umum	10
8.	Paradigma Nasional	10
9.	Peraturan Perundang-undangan	12
10.	Kerangka Teoritis	13
11.	Data dan Fakta	16
12.	Lingkungan Strategis	20
BAB III.	**PEMBAHASAN**	
13.	Umum	26
14.	Anatomi Kejahatan Digital yang Terjadi Selama Ini	27
15.	Dampak kejahatan Digital terhadap Ketahanan Nasional	37

TANHANA DHARMMA MANGRVA

16. Penerapan Kewaspadaan Nasional Terhadap Kejahatan Digital Guna Meningkatkan Ketahanan Nasional…..……..……...…….. 48

BAB IV. PENUTUP

17. Simpulan 57
18. Rekomendasi 59

DAFTAR PUSTAKA

DAFTAR LAMPIRAN:

1. Alur Pikir
2. Daftar Riwayat Hidup

TABEL

TABEL 1 LAPORAN DATA KEJAHATAN DIGITAL YANG DITANGANI POLRI

TABEL 2 DATA STATISTIK LAPORAN DATA KEJAHATAN DIGITAL DI TIAP POLDA

DAFTAR GAMBAR

GAMBAR 1. KESADARAN TERHADAP PRIVASI DAN KEAMANAN DATA

GAMBAR 2. DATA PENGGUNA INTERNET DI INDONESIA

GAMBAR 3 LAPORAN KONTEN KASUS KEJAHATAN SIBER

GAMBAR 4 JUMLAH PENGGUNA INTERNET DAN MEDIA SOSIAL DI INDONESIA

TANHANA DHARMMA MANGRVA

BAB I
PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi telah banyak mempengaruhi peradaban manusia secara global. Berkembangnya adopsi teknologi digital membuat dunia menjadi tanpa batas (*borderless*) sehingga mengakibatkan terjadinya perubahan sosial bermasyarakat. Transformasi digital tidak hanya mengubah cara berkomunikasi dan mendapatkan informasi, namun telah mengubah dan memberi keanekaragaman manfaat dalam berbagai aspek kehidupan manusia. Masyarakat sudah mulai familiar dengan belanja daring, melakukan transaksi perbankan secara online melalui ponsel pintarnya, melakukan kegiatan belajar mengajar secara daring hingga memanfaatkan berbagai kemudahan pelayanan publik secara digital. Perkembangan dunia digital yang begitu cepat, terus berkembang dan menghadirkan teknologi *Internet of Things* di mana seseorang dapat dengan mudah terhubung dengan berbagai benda di sekitarnya secara online.

Era ini juga telah membuat manusia menjadi berkelimpahan data dan informasi, sehingga terkadang sulit membedakan antara yang bermanfaat dengan yang tidak bermanfaat, antara yang benar dan bohong, termasuk antara pujian dan penghinaan. Kemajuan teknologi digital sebetulnya membuat kehidupan menjadi semakin mudah, cepat dan efektif. Namun di sisi lain, kemajuan teknologi ini juga membawa serta potensi negatif yang merusak bahkan mampu menghancurkan tatanan kehidupan nasional.

Datangnya pandemi Covid-19 dua tahun lalu telah memaksa terjadinya percepatan transformasi digital di tengah masyakarat. Banyak masyarakat yang belum terbiasa menggunakan teknologi digital, dipaksa oleh keadaan untuk belajar cepat memanfaatkan teknologi digital secara lebih maksimal. Mulai dari guru, siswa, hingga orang tua murid, terpaksa harus cepat beradaptasi dengan cara belajar mengajar secara daring. Para petinggi perusahaan yang umumnya sudah berusia lanjut harus membiasakan diri untuk melakukan rapat daring dari rumah. Demikian pula para pedagang dan pelaku UMKM yang harus belajar memasarkan

produknya melalui internet. Maklum, pembatasan sosial yang dilakukan pemerintah untuk mengendalikan penyebaran Covid-19 membuat banyak pelaku UMKM harus menutup toko dan tempat usahanya.

Percepatan proses transformasi digital tersebut pada satu sisi bermanfaat bagi kehidupan masyarakat, namun pada sisi lain membuat masyarakat rentan menjadi korban kejahatan digital. Literasi teknologi digital yang terbatas membuat masyarakat belum mengerti betul cara melindungi diri dan memanfaatkan teknologi agar aman dari kejahatan digital. Berbagai bentuk kejahatan digital, seperti peretasan dan pencurian data, penyebaran kabar bohong dan kontek provokatif, pembajakan akun, penyebaran data rahasia pribadi secara ilegal di media sosial (*doxing*) hingga aksi perundungan siber marak terjadi di Indonesia.[1]

Berdasarkan data dari Kementerian Informasi dan Komunikasi, terjadi peningkatan laporan penyalahgunaan teknologi informasi melalui kanal situs resminya. Tidak kurang 5.000 pengaduan terkait penipuan daring (*fraud*) dilaporkan setiap minggunya. Angka tersebut jika dihitung sejak periode Maret 2020 hingga Oktober 2021 mencapai hampir 200.000 aduan. Data ini menunjukan bahwa angka kejahatan siber di Indonesia sudah dalam kategori tinggi dan berbahaya. Tidak mengherankan jika Kemenkominfo menyatakan bahwa Indonesia darurat kejahatan siber. Faktor peningkatan aktivitas belanja daring masyarakat selama masa pandemi diduga menjadi salah satu pemicu meningkatnya kejahatan siber. Menurut data dari Direktorat Tindak Pidana Siber (Ditipidsiber) Polri, ada sejumlah modus kejahatan yang kerap terjadi di Indonesia, mulai dari peratasan, penggantian laman web secara ilegal, pengelabuhan (*phishing*), penyalinan informasi (skimming) dan yang paling marak adalah rekayasa sosial (*social engineering*). Kejahatan ini memanfaatkan ketidaktahuan dan kelengahan masyarakat sehingga terperdaya untuk menyerahkan sejumlah data dan informasi sesitif seperti data nama, alamat nomor NIK, nomor ATM hingga PIN dan password

[1] https://www.kompas.id/baca/polhuk/2021/07/01/kapolri-ubah-pendekatan-penanganan-kejahatan-siber diakses pada tanggal 7 April 2022 pukul 23.00 WIB.

sehingga pelaku kejahatan bisa mengambil alih akses perbankan atau dompet digital korban.[2]

Tingginya kasus kejahatan digital, khususnya terkait dengan kejahatan penipuan, umumnya banyak dipengaruhi oleh lemahnya kesadaran dan kewaspadaan masyarakat untuk mengamankan data pribadinya. Hal tersebut setidaknya tercermin dalam survei yang dipublikasikan oleh Harian Kompas pada awal tahun 2022 ini. Berdasarkan data yang berhasil dihimpun oleh Litbang Harian Kompas, didapatkan fakta bahwa hampir setengah dari responden (46,5 persen) tidak menyadari atau tidak mengetahui jika aktivitas daringnya seperti dalam mengunjungi berbagai laman situs, aktivitas berbelanja online, hingga beragam aktivias media sosial menyimpan berbagai data penting. Literasi terkait pentingnya mengamankan data pribadi dalam aktivitas digital seseorang, menjadi pekerjaan rumah krusial dalam membangun kesadaran terhadap keamanan data. Ketidaktahuan ini menjadi cermin masih rendahnya kesadaran akan data memengaruhi kesadaran terhadap keamanan data. [3]

Jajak pendapat juga merekam, kejahatan siber yang berakar dari pencurian data pernah dialami 17,4 persen responden. Kelompok ini mengaku pernah jadi korban penipuan, yakni dengan cara pelaku menggunakan data pribadi mereka. Sementara sebagian kecil responden lain menyampaikan penipuan serupa terjadi pada kerabat dekat mereka. Potret ini menambah catatan buram kejahatan yang berakar dari lemahnya pengamanan data pribadi.

Hal ini mengambarkan bagaimana kesadaran dan pengetahuan masyarakat terhadap keamanan data pribadi sebagai bentuk kewaspadaan terhadap kejahatan digital masih sangat rendah. Tidak sedikit masyarakat yang belum memiliki pengetahuan yang memadai mengenai bagaimana langkah-langkah yang diperlukan untuk pengamanan data. Sebut saja seperti kebiasaan membaca ketentuan keamanan, mengganti kata sandi berkala, dan memeriksa kredibilitas layanan digital, hingga memasang

[2] https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber diakses pada tanggal 7 April 2022 pukul 23.00 WIB.
[3] https://www.kompas.id/baca/opini-publik/2022/02/06/membangun-perisai-keamanan-data diakses pada tanggal 7 April 2022 pukul 22.00 WIB.

aplikasi *antivirus* dan *antimalware* untuk mencegah terjadinya pencurian data.

Kondisi tersebut semestinya membuat pemerintah lebih tanggap dan sigap untuk megambil sejumlah langkah yang diperlukan. Selain berupaya secara lebih masif menyebarkan edukasi kepada masyarakat, pemerintah bisa segera merampungkan Rancangan Undang-Undang Perlindungan Data Pribadi. Bersama dengan revisi UU Informasi dan Transaksi Elektronik, pemerintah semestinya segera mempercepat pembahasan RUU Keamanan dan Ketahanan Siber, serta RUU Perlindungan Data Pribadi guna memperkuat payung hukum keamanan digital. Ketersediaan regulasi yang mengatur pengamanan data sudah sangat mendesak dilakukan agar dalam era transformasi digital di berbagai bidang saat ini, perlindungan kepada masyarakat terhadap kejahatan digital menjadi satu keniscayaan.

Kebocoran data pribadi masyarakat semestinya tidak lagi diremehkan, mengingat di era serba digital saat ini, beraneka informasi dan data telah menjadi komoditas tambang berharga yang bisa dieksploitasi dengan motif ekonomi, politik, hingga serangan ideologi negara yang dapat mengancam keamanan negara. Oleh sebab itu, negara didesak segera hadir melindungi hak privasi warganya.

Pada sisi lain, dalam kehidupan sosial politik Indonesia yang kini telah merambah ke dunia digital, ada ungkapan mengatakan bahwa gejolak politik dapat dimulai dari "jari tangan". Ungkapan ini menjadi pengganti dari ungkapan lama yang mengatakan "mulutmu, harimaumu". Sebuah ungkapan yang mengingatkan setiap anak bangsa untuk waspada terhadap gejolak politik yang bersumber dari internet, yang merupaan hasil permainan jari tangan yang bisa menjadi salah satu bentuk kejahatan digital saat digunakan untuk menghasilkan disinformasi yang menyesatkan dan tidak jelas basis kebenarannya, seperti konten hoak, berita palsu, hingga ujaran kebencian yang menghasilkan keterbelahan masyarakat. Fenomena tersebut perlu disikapi dengan konsep kewaspadaan nasional.

Kewaspadaan Nasional adalah sikap peduli terhadap nasionalisme yang menghasilkan kesiagaan nasional dalam menghadapi ancaman seperti yang diamanatkan dalam Undang-Undang Intelijen tentang ancaman.

Kesiagaan itu mengandung unsur-unsur diteksi dini, peringatan dini, tangkal awal, cegah awal dan taggap awal terhadap setiap ancaman yang dihadapi, termasuk ancaman yang berupa kejahatan digital, yang membawa dampak buruk bagi ketahannan nasional. Menurut Laboratorium Pengukuran Ketahanan Nasional (Labkurtannas) Lemhannas RI per Desember 2021, Indek Ketahanan Nasional Indonesia masih menunjukan hasil "Kurang Tangguh"[4]. Kondisi seperti itu, tidak jatuh dari langit begitu saja, namun kehadiran teknologi internet yang mewarnai era digital juga turut berkontribusi menjadi salah satu komponen yang melemahkan.

Perkembangan lingkungan strategis global, regional dan nasional yang kita hadapi sekarang ini menunjukkan fenomena yang mengarah kepada semakin maraknya kejahatan digital akibat "jari tangan" yang tidak dapat dikendalikan dengan baik dan benar, sehingga semakin marak kejahatan digital. Kemajuan teknologi komunikasi digital yang berbasis internet, tidak saja membawa manfaat bagi kehidupan, namun sekaligus membawa potensi kejahatan yang perlu diwaspadai. Terlebih kejahatan itu mengancam integrasi nasional yang berpotensi memporak porandakan kehidupan nasional.

Media sosial selain memberi banyak manfaat dalam kehidupan di era digital, namun juga sangat dominan kontribusinya dalam menciptakan keterbelahan masyarakat. Negara Amerika Serikat yang kerap dijadikan rujukan terhadap potret negara demokrasi yang baik pun, justru terjerembab dalam framing media yang memporakporandakan kehidupan demokrasinya. *Black Lives Matter* (BLM) yang diawali dengan pengunggahan video di media sosial oleh seorang warga masyarakatnya, telah mengundang demo besar-besaran di Amerika yang menghancurkan kehidupan sosial Amerika Serikat dan sekaligus memberi pengaruh terhadap ketidakterpilihan Trump masa kepemimpinan keduanya. Kejadian seperti ini banyak juga terjadi di dalam negeri kita, termasuk pemanfaatan media sosial untuk melakukan kampanye hitam. Atas dasar itu, maka dipandang perlu untuk mengangkat sebuah

[4] Labkurtannas Lemhannas RI per Desember 2021

tulisan berjudul Kewaspadaan Nasional Terhadap Kejahatan Digital Guna meningkatkan Ketahanan Nasional.

2. Rumusan masalah

Berdasarkan latar belakang dan uraian di atas, maka rumusan permasalahan dalam penulisan ini adalah **"Bagaimana kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional?"**

Dalam rangka memudahkan analisa dan pembahasan, rumusan permasalahan di atas dijabarkan ke beberapa pertanyan kajian dan persoalannya, sebagai berikut:

a. Bagaimana anatomi kejahatan digital yang terjadi selama ini?
b. Bagaimana dampak kejahatan digital terhadap ketahanan nasional?
c. Bagaimana konsep kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional?

3. Maksud dan Tujuan

a. **Maksud**. Penulisan taskap ini dibuat dengan maksud untuk memberikan gambaran dan analisis mengenai bagaimana pentingnya kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional.
b. **Tujuan**. Penulisan Taskap ini bertujuan untuk menyampaikan suatu gagasan dan konsep pemikiran sebagai masukan dan pertimbangan bagi para pengambil kebijakan yang berkepentingan terkait pentingnya menumbuhkan kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional.

4. Ruang Lingkup dan Sistematika

Ruang lingkup penulisan Taskap ini dibatasi pada anatomi kejahatan digital dan dampaknya terhadap ketahanan nasional, serta konsep kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional.

Uraian pembahasan dan analisa analisa terkait pokok-pokok pertanyaan kajian di dalam penulisan Taskap ini, kemudian disusun dengan sistematika atau tata urut penulisan sebagai berikut:

a. **BAB I: PENDAHULUAN**

Bab ini dijabarkan mengenai apa saja yang menjadi latar belakang permasalahan, maksud dan tujuan penulisan Taskap, batasan ruang lingkup, sistematika penulisan, metode dan pendekatan yang digunakan, hingga beberapa penjelasan pengertian terkait istilah yang digunakan dalam penulisan Taskap ini.

b. **BAB II: TINJAUAN PUSTAKA**

Dalam Bab ini dibahas tentang paradigma nasional, peraturan perundang-undangan yang menjadi landasan hukum, kerangka teoritis sebagai landasan pemikiran, data dan fakta yang menjelaskan kondisi saat ini dan paparan singkat mengenai perkembangan lingkungan strategis yang berpotensi mempengaruhi rumusan pemecahan persoalan berkaitan dengan kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional.

c. **BAB III: PEMBAHASAN**

Dalam Bab ini akan diuraikan setiap persoalan yang ada berkaitan dengan kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional. Pada Bab ini akan dibahas semua pertanyaan kajian yang telah disampaikan pada Bab I. Dimulai dari melihat anatomi kejahatan digital yang terjadi selama ini, dilanjutkan dengan mengenali dampak kejahatan digital terhadap ketahanan nasional. Pada akhinya merumuskan konsep kewaspadaan nasional yang coba ditawarkan dalam menghadapi kejahatan digital yang semakin marak terjadi guna meningkatkan ketahanan nasional.

d. **BAB IV: PENUTUP**

Bab ini berisi simpulan yang memaparkan hasil analisa yang menjawab rumusan masalah yang terjabar dalam pertanyaan kajian dan disertai beberapa saran untuk dapat digunakan sebagai bahan pertimbangan bagi para pengambil kebijakan.

5. **Metode dan Pendekatan**

a. **Metode.** Penulisan Taskap ini menggunakan metode kualitatif, yaitu deskriptif analisis. Proses pencarian, pengumpulan dan penelitian data selain menggunakan data primer yang dilakukan melalui wawancara dengan pihak-pihak terkait, juga didukung dengan teknik studi kepustakaan (*library research*).

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

6. Pengertian

Guna menghindari terjadinya perbedaan penafsiran mengenai penggunaan satu istilah dan guna lebih menyatukan persepsi pada pembahasan selanjutnya, maka dalam Taskap ini dijelaskan beberapa pengertian yang digunakan sebagai berikut:

a. Anatomi, adalah uraian atau penjelasan yang mendalam mengenai sesuatu.[5]

b. *Fraud*, adalah merupakan satu jenis kejahatan berupa tindakan penipuan atau kecurangan yang sengaja dilakukan seseorang, sekelompok orang atau sebuah perusahaan dalam rangka memperoleh keuntungan bagi diri sendiri.[6]

c. Implementasi. Yang dimaksud dengan implementasi adalah pelaksanaan atau penerapan[7]

d. Kejahatan digital, atau juga dikenal dengan kejahatan siber (*cyber crime*) merupakan istilah yang mengacu pada kejahatan dengan menggunakan komputer, baik sebagai alat, sasaran maupun tempat

[5] https://kbbi.web.id/anatomi diakses pada tanggal
[6] https://www.ekrut.com/media/fraud-adalah diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.
[7] https://kbbi.web.id/implementasi diakses pada tanggal 19 Juni 2022 pukul 13.00 WIB.

terjadinya kejahatan. Kejahatan siber juga dapat diartikan sebagai segala bentuk tindakan ilegal yang dilakukan melalui jaringan komputer atau internet untuk memperoleh keuntungan pribadi dan merugikan pihak lain.[8]

e. **Kewaspadaan nasional,** adalah suatu kualitas kesiapan dan kesiagaan yang dimiliki oleh bangsa Indonesia untuk mampu mendeteksi, mengantisipasi sejak dini, dan melakukan aksi pencegahan berbagai bentuk dan sifat potensi ancaman terhadap NKRI.[9]

f. ***Phishing*,** adalah bentuk penipuan atau pengelabuhan yang umumnya memiliki ciri dilakukan melalui percobaan untuk mendapatkan informasi sensitif/pribadi seperti kata sandi, kode OTP atau data kartu kredit dengan menyamar sebagai seseorang yang terpercaya dalam sebuah komunikasi elektronik seperti surat elektronik atau pesang singkat.[10]

g. ***Skimming*,** adalah aktivitas penggandaan informasi atau pencurian data yang terdapat dalam pita magnetik.[11] Teknik ini umumnya digunakan penjahat untuk membobol rekening melalui penggandaan kartu ATM.

h. ***social engineering*,** atau dalam bahasa Indonesia disebut rekayasa sosial, merupakan suatu teknik manipulasi yang memanfaatkan kesalahan manusia guna memperoleh akses pada informasi pribadi dan data-data berharga lainnya.[12]

---

[8] https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/ diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.
[9] Tim Pokja Bahan Ajar Padnas. 2022. Materi Pokok Bidang Studi Kewaspadaan Nasional. Jakarta: Lemhannas RI.
[10] Huda, Miftahul. 2020. Keamanan Informasi. Surabaya: CV. Garuda Mas Sejahtera.
[11] Ibrahim dan Sirait. 2018. Kejahatan Transfer Dana: Evolusi dan Modus Kejahatan Melalui Sarana Lembaga Keuangan Bank. Jakarta: Sinar Grafika.
[12] https://glints.com/id/lowongan/social-engineering/#.Ypbub8NBzb0 diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.

BAB II
TINJAUAN PUSTAKA

7. Umum

Transformasi digital telah mempengaruhi seluruh aspek kehidupan masyarakat. Kehadirannya diikuti dengan meningkatnya berbagai jenis kejahatan digital, tidak terkecuali peretasan, penipuan, pencurian data pribadi, hingga penyebaran kabar bohong. Minimnya kewaspadaan masyarakat membuat jumlah korban dan kerugian materiil yang ditimbulkan oleh kejahatan digital terus meningkat.

Sebelum dapat menganalisa apa yang menjadi pokok persoalan terkait implementasi kewaspadaan nasional terhadap kejahatan digital terlebih dahulu perlu disajikan tentang paradigma nasional dan berbagai regulasi perundang-undangan yang selama ini menjadi landasan hukum, faktor lingkungan strategis yang berpengaruh hingga sejumlah teori yang dapat menjadi landasan dalam pemecahan persoalan.

8. Paradigma Nasional

a. Pancasila Sebagai Landasan Idiil

Pancasila merupakan sumber dari segala sumber hukum dan sumber tertib hukum negara Republik Indonesia. Sebagai dasar negara, fungsi Pancasila dalam tinjauan sosiologis memiliki arti sebagai pengatur hidup kemasyarakatan. Sedangkan dalam tinjauan etis filosofis memiliki arti sebagai pengatur tingkah laku serta cara-cara mencari kebenaran.[13]

Hal tersebut dituangkan sebagai bagian dari tugas negara untuk melindungi para warga negaranya agar dapat menjalankan kewajiban, hak, serta pengembangan dirinya secara tertib dan aman. Selanjutnya, pemerintahan memiliki kewenangan untuk mengatur penyelenggaraan kehidupan bangsa dan negara berdasarkan hukum yang telah ditetapkan. Pembangunan hukum yang berkeadilan tersebut bukan hanya sekedar membatasi, mengikat warga mengikuti aturan yang ketat

[13] Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Empat Konsensus Dasar Bangsa. Jakarta: Lemhannas RI.

tapi harus lebih mengarahkan warga untuk lebih dan semakin sejahtera serta merasakan keadilan dalam hidup bermasyarakat. Keberadaaan hukum juga berfungsi untuk memberikan perlindungan bagi seluruh warga negara Indonesia, termasuk dari ancaman kejahatan digital yang kini semakin marak terjadi.

b. UUD NRI Tahun 1945 Sebagai Landasan Konstitusi

UUD NRI tahun 1945 merupakan hukum dasar yang menjadi acuan utama bangsa Indonesia dalam menyelenggarakan kehidupan berbangsa, bernegara dan bermasyarakat. Para pendiri bangsa telah mengikrarkan dengan tegas bahwa Indonesia adalah negara hukum. Oleh sebab itu, segala permasalahan dalam kehidupan berbangsa dan bernegara harus diselesaikan melalui jalur hukum dan hukum dasarnya adalah UUD NRI tahun 1945.[14]

Berdasarkan kepada pokok-pokok pikiran tersebut, maka segala bentuk kejahatan digital harus diproses secara hukum sesuai dengan aturan perundang-undangan yang berlaku. Apabila saat ini ada sejumlah kekosongan hukum, maka menjadi kewajiban pemerintah untuk membentuk payung hukum yang baru atau pun melakukan perbaikan terhadap regulasi yang sudah ada dengan tetap mengacu pada UUD NRI tahun 1945 sebagai hukum dasarnya. Ketersediaan payung hukum dibutuhkan sebagai landasan hukum bagi aparat penegak hukum termasuk kepolisian RI untuk menindak segala bentuk kejahatan digital di Indonesia sebagai bagian dari implementasi kewaspadaan nasional.

c. Wawasan Nusantara Sebagai Landasan Visional

Wawasan Nusantara sebagai landasan visional mengandung arti cara pandang bangsa Indonesia terhadap diri dan lingkungannya dengan berlandaskan konstelasi geografis Indonesia yang berfungsi menumbuhkan nasionalisme.[15] Hakikat Wawasan Nusantara tersebut

[14] Ibid
[15] Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Wawasan Nusantara. Jakarta: Lemhannas RI.

menciptakan cara pandang bangsa Indonesia yang salah satunya mencangkup perwujudan kepulauan Nusantara sebagai satu kesatuan pertahanan keamanan. Hal ini ketika dikontekstualisasikan dalam mewujudkan implementasi kewaspadaan nasional terhadap kejahatan digital di Indonesia memberikan titik temu bahwa upaya tersebut harus menjadi tanggung jawab seluruh seluruh komponen bangsa sebagai satu kesatuan pertahanan keamanan.

d. Ketahanan Nasional Sebagai Landasan Konsepsional

Ketahanan nasional adalah kondisi dinamis bangsa yang berisi keuletan dan ketangguhan dalam menghimpun dan mengembangkan segala potensi (sumber daya) yang ada menjadi kekuatan nasional yang berisi keuletan dan ketangguhan untuk menghadapi dan mengatasi segala tantangan, hambatan, ancaman dan gangguan, baik yang datang dari luar maupun dari dalam negeri yang dapat membahayakan kelangsungan hidup negara Indonesia dalam mencapai tujuan nasional.[16]

Semakin meningkatnya kejahatan digital yang terjadi di Indonesia merupakan satu ancaman aktual yang harus menjadi perhatian seluruh komponen bangsa. Kerugian yang disebabkan oleh jenis kejahatan ini semakin lama semakin besar sehingga dapat mempengaruhi ketangguhan ketahanan nasional Indonesia. Oleh sebab itulah dibutuhkan upaya untuk mengembangkan keuletan dan ketangguhan untuk mengatasi ancaman kejahatan digital tersebut dengan mengembangkan kewaspadaan nasional.

9. Peraturan Perundang-undangan

a. Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dalam Pasal 3 dijelaskan Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum,

[16] Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Ketahanan Nasional. Jakarta: Lemhannas RI.

manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Hal ini menunjukan bahwa penggunaan teknologi informasi dan transaksi elektronik apapun bentuknya yang dilakukan di wilayah NKRI akan selalu terikat oleh hukum perundang-undangan yang berlaku di Indonesia.

b. Undang-Undang RI Nomor 17 Tahun 2011 tentang Intelijen Negara

Pada Pasl 4 dijelaskan bahwa intelijen negara memiliki peran untuk melakukan upaya, kegiatan pekerjaan dan tindakan deteksi dini dan peringatan dini guna pencegahan, penangkalan dan penanggulangan terhadap hakekat ancaman yang mungkin muncul dan mengancam kepentingan serta keamanan nasional.

c. Undang-Undang RI Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentag Informasi dan Transaksi Elektronik

Pasal 40 ayat (2) dengan tegas menyatakan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

Hal ini memberikan payung hukum bahwa menjadi kewajiban pemerintah, termasuk aparat penegak hukum untuk melindungi masyarakat dari berbagai bentuk penyalahgunaan teknologi informasi dan transaksi elektronik (kejahatan digital).

10. Kerangka Teoritis

a. Teori Angsa Hitam dan Gajah Hitam

Teori Angsa Hitam (*black swan*) dan teori Gajah Hitam (*black elephants*) menggambarkan satu risiko dalam dua perspektif. Angsa Hitam dan Gajah Hitam keduanya menggambarkan peristiwa bahaya dengan dampak tinggi, paparan tinggi, dan kerentanan tinggi tetapi dilihat dari dua sudut pandang yang berbeda. Angsa hitam (Taleb, 2007)

menggambarkan ancaman tidak terduga, akibat terlalu fokus pada hal yang diketahui dan tidak mempertimbangkan pada hal yang tidak diketahuinya. Akibatnya orang yang tidak mengetahui adanya ancaman tersebut berpotensi menderita kerugian yang paling besar, jika ancaman dari angsa hitam menjadi kenyataan. Sementara teori Gajah Hitam (Sweidan, 2014) merupakan persilangan dari teori Angsa Hitam dengan teori Gajah di dalam ruangan yang pada intinya menggambarkan ancaman besar yang sudah diketahui oleh semua orang namun banyak yang mengabaikannya. Angsa Hitam dapat menjadi Gajah Hitam, keduanya berpotensi menimbulkan dampak bencana. Penggunaan teori ini berkaitan dengan kelanjutan dari Teori *Chaos* dan kompleksitas milik Edward Lorenz (1975). Kesemua teori ini berkaitan dengan peringatan untuk menjaga keamanan nasional dari ancaman nyata maupun potensial yang dihadapi dalam kehidupan nasional.[17] Teori-teori ini sejalan dengan konsep Ketahanan Nasional maupun Konsep Kewaspadaan Nasional yang menjadi Bidang Studi Inti di Lemhannas RI.

b. Teori Literasi Digital

Menurut Bawden (2001) literasi digital didefinisikan sebagai kemampuan menggunakan teknologi dan informasi dari piranti digital secara efektif dan efisien dalam berbagai konteks, seperti akademik, karier, dan kehidupan. Literasi digital lebih banyak dikaitkan dengan keterampilan teknis mengakses, merangkai, memahami, dan menyebarluaskan informasi, (Kemendikbud, 2017:7).[18]

Literasi digital menjadi sebuah pengetahuan dan kecakapan dalam menggunakan media digital, termasuk alat komunikasi modern atau jaringan internet dalam menemukan, mengerjakan, mengevaluasi, menggunakan informasi, membuat informasi dan memanfaatkannya secara bijak, cerdas, tepat dan tentunya patuh hukum dan aturan dalam rangka membina komunikasi dan interaksi positif dalam kehidupan

[17] Margaretha Hanita, 2019, Pemikiran-Pemikiran Stratejik Intelijen, UI Publishing, Jakarta
[18] https://eprints.umm.ac.id/51432/3/BAB%20II.pdf diakses pada tanggal 12 Mei 2022 pukul 20.00 WIB

sehari-hari. Literasi digital juga merupakan kemampuan dalam menggunakan teknologi informasi dan komunikasi untuk mengkomunikasikan informasi secara kognitif dan teknikal.[19] Teori ini menjadi landasan bagaimana pentingnya mengerti, memahami dan menguasai teknologi digital dan karakteristiknya, karena tanpa pengetahuan yang mendalam, seseorang tidak pernah mengerti bahaya apa saja yang mengancam ketika mereka menggunakan teknologi.

c. Teori *Security Awarness*

Security Awareness adalah pengetahuan yang dimiliki oleh seseorang terkait pengetahuan dan praktik keamanan yang baik dan pentingnya melindngi data pribadi ataupun kelompok saat menggunakan internet (Edwards, 2015). Saat seseorang memiliki kesadaran keamanan, maka dia akan melindungi data dan informasi yang mereka miliki saat terhubung dengan internet. Akan muncul kesadaran untuk mempertimbangkan dan menentukan informasi pribadi apa saja yang akan dibagikan di internet sehingga tidak menimbulkan ancaman dan kerugian bagi dirinya saat ini maupun dikemudian hari.[20]

d. Konsep Kewaspadaan Nasional

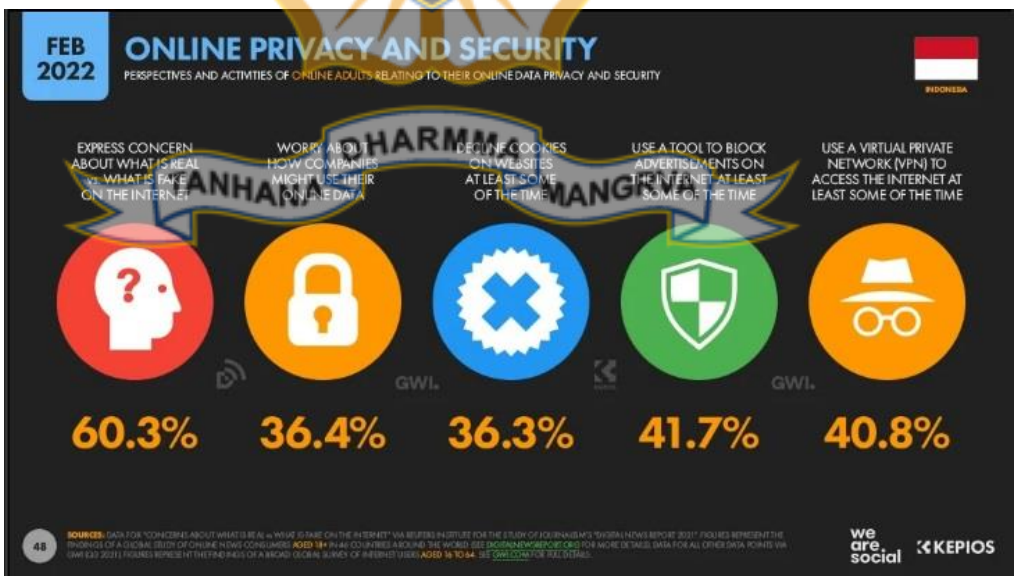
Kewaspadaan Nasional (Padnas) dipandang sebagai suatu kualitas kesiapan dan kesiagaan yang dimiliki oleh bangsa untuk mampu mendeteksi, mengantisipasi sejak dini, dan melakukan aksi pencegahan berbagai bentuk dan sifat potensi ancaman terhadap NKRI. Padnas merupakan bentuk manifestasi kepedulian dan tanggung jawab setiap warga negara atas keselamatan dan keutuhan bangsa.[21] Oleh sebab itu dalam tataran operasional dalam konteks mewaspadai kejahatan digital, kewaspadaan nasional bukan lagi menjadi tanggung jawab Polri, Badan Siber dan Sandi Negara (BSSN) atau Kemenkominfo, namun juga

[19] Suherdi, dkk. 2021. Peran Literasi Digital di masa Pandemik. Deli Serdang: Cattleya Darmaya Fortuna
[20] https://repository.usd.ac.id/37599/2/162114041_full.pdf diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.
[21] Tim Pokja Bahan Ajar BS. Padnas, 2022, Modul Bidang Studi Kewaspadaan Nasional, Lemhannas, Jakarta

menjadi tanggung jawab setiap warga negara Indonesia untuk ikut berperan aktif. Salah satunya dengan meningkatkan usaha untuk memproteksi diri dari potensi menjadi korban kejahatan digital.

11. Data dan Fakta

Menurut data dari We Are Social, kesadaran pengguna internet di Indonesia dalam menjaga privasi dan keamanan data masih tergolong rendah. Hal ini tergambar dari data statistik yang menunjukan hanya 36,4 persen pengguna internet mengkhawatirkan bagaimana pihak ketiga akan menggunakan data onlinennya. Demikian halnya dengan masyarakat yang dengan sadar setidaknya sesekali menolak permintaan cookies (pengambilan data) dari aktivitas pengguna saat mengunjungi satu situs web yang hanya tercatat sebesar 36,3 persen. Data yang menunjukan jumlah masyarakat yang memasang aplikasi untuk memblok iklan di internet juga hanya berjumlah 41,7 persen. Beruntung bahwa ada 60,3 persen masyarakat yang memulai sadar untuk tidak mudah percaya dan memilih mencari tahu suatu informasi yang diterimanya di internat suatu kebenaran atau termasuk berita palsu.[22]



Sumber: wearesocial.com

Gambar 1. Kesadaran Terhadap Privasi dan Keamanan Data

[22] https://datareportal.com/reports/digital-2022-indonesia diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB

Pakar keamanan siber dari lembaga nirlaba Communication & Information System Security Research Center (CISSReC) Pratama Persadha mengungkap jika kejahatan siber pada tahun 2022 berpotensi untuk lebih tinggi dibandingkan tahun-tahun sebelumnya. Ancaman pencurian data dan *ransomware* masih akan mendominasi kejahatan digital yang terjadi di Indonesia. Tingginya permintaan data dalam jumlah besar menjadi pendorong maraknya kejahatan terkait dengan data.[23]

Dengan jumlah pengguna internet yang cukup tinggi hingga di atas 200 juta, pemerintah Indonesia dianggap belum serius dalam mengantisipasi dan mengatasi kejahatan siber hingga kini. Ini terbukti dengan RUU Perlindungan Data Pribadi yang tidak kunjung selesai dibahas dan disahkan sekalipun sudah masuk dalam pembahasan sejak tahun 2020 lalu. Selama ini aparat penegak hukum tidak bisa berbuat banyak dalam menghadapi beragam kebocoran data karena belum memiliki instrumen hukum yang dengan jelas mengaturnya. Saat ini Indonesia baru memiliki Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang menjadi satu-satunya regulasi yang mengatur mengenai kejahatan digital/siber, sementara modus dan jenis kejahatan digital terus berkembang sehingga muncul adanya kekosongan regulasi terkait sejumlah jenis kejahatan yang baru.[24]

Dari jumlah kasus kejahatan digital yang terjadi di Indonesia, jika dipetakan berdasarkan wilayah, didapatkan data bahwa DKI Jakarta menjadi daerah yang paling rawan tindak kejahatan digital. Kemudian disusul provinsi Sumatra Utara dan Jawa Timur. Jumlah ini mengalami penurunan sekitar 32 persen jika dibandingkan dengan tahun sebelumnya yang mencapai 4790 kasus. Dari jumlah tersebut kejahatan terkait pencemaran nama baik menjadi jenis kejahatan digital yang paling banyak dilaporkan masyarakat dengan jumlah kasus 1.136 kasus, disusul kasus penipuan sebanyak 864 kasus dan pornografi sebanyak 321 kasus.

[23] https://www.tagar.id/pencurian-data-diperkirakan-meningkat-tahun-2022 diakses pada tanggal 10 Juni 2022 pukul 21.00 WIB
[24] Ibid.

NO	JENIS KEJAHATAN	2019			2020			2021		
		CT	CC	%	CT	CC	%	CT	CC	%
1	BERITA BOHONG / BERITA PALSU	97	69	71,13%	197	75	38,07%	83	80	96,39%
2	PORNOGRAFI	364	144	39,56%	404	184	45,54%	321	205	63,86%
3	PERJUDIAN	35	20	57,14%	82	69	84,15%	54	48	88,89%
4	PENCEMARAN NAMA BAIK	1333	597	44,79%	1794	403	22,46%	1136	707	62,24%
5	PEMERASAN	132	58	43,94%	37	22	59,46%	33	14	42,42%
6	PENIPUAN	1617	966	59,74%	1319	268	20,32%	864	350	40,51%
7	UJARAN KEBENCIAN / SARA	247	88	35,63%	223	56	25,11%	115	72	62,61%
8	PENGANCAMAN	92	33	35,87%	135	36	26,67%	131	54	41,22%
9	AKSES ILEGAL	248	91	36,69%	303	90	29,70%	311	132	42,44%
10	PENCURIAN DATA / IDENTITAS	143	75	52,45%	47	19	40,43%	32	17	53,13%
11	PERETASAN SISTEM ELEKTRONIK	148	82	55,41%	39	7	17,95%	15	4	26,67%
12	INTERSEPSI ILEGAL	3	3	100,00%	29	4	13,79%	5	2	40,00%
13	PENGUBAHAN TAMPILAN SITUS	4	2	50,00%	10	4	40,00%	5	1	20,00%
14	GANGGUAN SISTEM / DDOS	9	3	33,33%	8	0	0,00%	4	4	100,00%
15	MANIPULASI DATA	114	51	44,74%	163	46	28,22%	161	90	55,90%
TOTAL		4586	2282	49,76%	4790	1283	26,78%	3270	1780	54,43%

Sumber: Bareskrim Polri

Tabel 1. Laporan Data Kejahatan Digital yang Ditangani Polri

Berdasarkan data Anev Bareskrim Polri, selama tahun 2021, jumlah kasus kejahatan digital yang ditangani oleh Polri sebanyak 3.270 kasus. Jumlah ini mengalami penurunan sekitar 32 persen jika dibandingkan dengan tahun sebelumnya yang mencapai 4790 kasus. Dari jumlah tersebut kejahatan terkait pencemaran nama baik menjadi jenis kejahatan digital yang paling banyak dilaporkan masyarakat dengan jumlah kasus 1.136 kasus, disusul kasus penipuan sebanyak 864 kasus dan pornografi 321 kasus.

Dari jumlah kasus kejahatan digital yang terjadi di Indonesia, jika dipetakan berdasarkan wilayah, didapatkan data bahwa DKI Jakarta menjadi daerah yang paling rawan tindak kejahatan digital, Kemudian disusul provinsi Sumatra Utara dan Jawa Timur. Jumlah ini mengalami penurunan sekitar 32 persen jika dibandingkan dengan tahun sebelumnya yang mencapai 4790 kasus. Dari jumlah tersebut kejahatan terkait pencemaran nama baik menjadi jenis kejahatan digital yang paling banyak dilaporkan masyarakat

dengan jumlah kasus 1.136 kasus, disusul kasus penipuan sebanyak 864 kasus dan pornografi sebanyak 321 kasus.

NO	NAMA SATKER	2021		
		CT	CC	%
1	ACEH	51	42	82,35%
2	SUMUT	620	289	46,61%
3	SUMBAR	20	30	150,00%
4	SUMSEL	74	31	41,89%
5	KEPRI	32	23	71,88%
6	LAMPUNG	27	8	29,63%
7	JAMBI	36	33	91,67%
8	RIAU	38	2	5,26%
9	BENGKULU	14	9	64,29%
10	BABEL	1	1	100,00%
11	PMJ	807	428	53,04%
12	JABAR	285	68	23,86%
13	BANTEN	27	30	111,11%
14	JATENG	23	48	208,70%
15	JATIM	290	212	73,10%
16	DIY	22	2	9,09%
17	BALI	21	27	128,57%
18	NTT	44	53	120,45%
19	NTB	52	24	46,15%
20	KALTARA	13	7	53,85%
21	KALSEL	38	34	89,47%
22	KALBAR	55	39	70,91%
23	KALTENG	14	5	35,71%
24	KALTIM	26	15	57,69%
25	SULBAR	27	20	74,07%
26	SULSEL	20	0	0,00%
27	SULTENG	116	77	66,38%
28	SULTRA	25	0	0,00%
29	SULUT	93	54	58,06%
30	GORONTALO	53	11	20,75%
31	MALUKU	37	20	54,05%
32	MALUT	27	12	44,44%
33	PAPUA	73	29	39,73%
34	PAPUA BARAT	22	15	68,18%
35	DITTIPIDSIBER	147	82	55,78%
TOTAL		3270	1780	54,43%

Sumber: Bareskrim Polri

Tabel 1. Data Statistik Laporan Data Kejahatan Digital di Tiap Polda

12. Lingkungan Strategis

a. Faktor Global

Kejahatan siber merupakan satu bentuk kejahatan yang menjadi perhatian dunia internasional. Setiap negara tidak luput dari ancaman kejahatan siber yang terus berkembang. Internet Crime Complaint Center (IC3) mengungkapkan bahwa pada tahun 2021 total kerugian yang diakibatkan oleh kejahatan siber yang dilaporkan masyarakat Amerika Serikat mencapai US$ 6,9 miliar atau sekitar Rp 100 triliun. Angka kerugian tersebut rata-rata naik 51,7 persen setiap tahunnya dalam lima tahun terakhir. [25]

Data yang lebih mencengangkan diungkap oleh Dana Moneter Internasional (IMF). Menurut lembaga keuangan dunia ini estimasi total kerugian yang dialami oleh sektor perbankan di dunia akibat serangan siber setiap tahunnya mencapai US$ 100 miliar atau setara Rp 1.450 triliun. Sektor keuangan menjadi sektor kedua yang paling banyak diincar oleh para penjahat siber setelah sektor pemerintahan.[26] Kondisi ini harus menggugah kesadaran semua pihak bagaimana pentingnya untuk meningkatkan keamanan digital di semua sektor.

b. Faktor Regional

Indonesia harus belajar banyak dari negeri jiran Malaysia. Hal ini karena menurut data yang dirilis oleh *e-Governance Academy Foundation*, Malaysia menjadi negara yang memiliki tingkat keamanan siber terbaik di Asia Tenggara pada tahun 2021. Negara ini memiliki skor indeks keamanan siber sebesar 79,22 poin. Skor ini mengalahkan negara Singapura berada di urutan kedua dengan skor sebesar 71,43 poin. Disusul Thailand, Filipina dan Brunei Darusalam. Sedangkan Indonesia jauh tertinggal beradai di urutan keenam dengan skor sebesar 38,96 poin.[27]

---

[25] https://databoks.katadata.co.id/datapublish/2022/05/09/kerugian-akibat-kejahatan-siber-capai-us69-miliar-pada-2021 diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.
[26] https://money.kompas.com/read/2021/10/26/173828526/imbas-kejahatan-cyber-bank-bank-dunia-merugi-rp-1420-triliun-per-tahun diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.
[27] https://dataindonesia.id/digital/detail/malaysia-miliki-keamanan-siber-terbaik-di-asean diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.

Pencapain ini harus menjadi bahan evaluasi pemerintah agar Indonesia bisa memiliki keamanan siber yang lebih baik. Hal ini penting karena menurut Internasional Business Machinse Corporation (IBM), terungkap bahwa Asia menjadi wilayah yang mengalami serangan siber terbanyak di dunia selama tahun 2021. Jenis kejahatan ransomware dan phising masih menjadi ancaman yang paling mengemuka selama satu tahun tersebut.[28]

c. Faktor Nasional

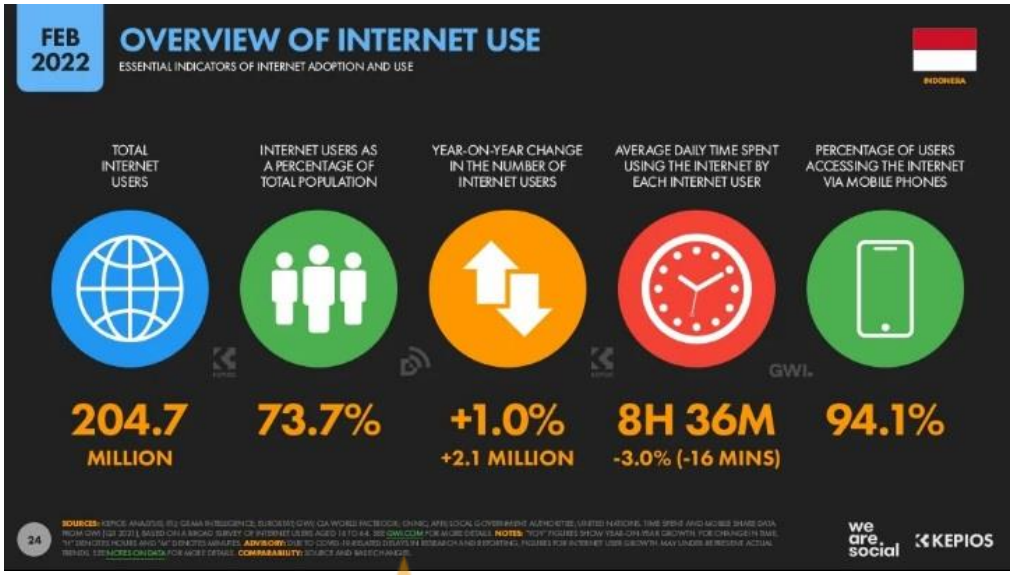
1) Demografi

Menurut data dari We Are Social, jumlah pengguna internet di Indonesia pada Februari 2022 telah mencapai 204,7 juta. Ini berarti ada 73,7 persen dari populasi Indonesia yang telah menggunakan internet. Sedangkan jumlah pengguna aktif media sosial di Indonesia mencapai 191,4 juta orang atai 68,9 persen dari total penduduk Indonesia. Jumlah itu telah meningkat 12,35% dibandingkan pada tahun sebelumnya yang sebanyak 170 juta orang. Rata-rata masyarakat Indonesia menghabiskan waktunya selama delapan jam 36 menit untuk berselancar di internet, dan tiga jam 17 menit untuk bersosial media. Tiga kegiatan yang sering dilakukan masyarakat Indonesia menghabisakan waktunya di internet adalah untuk mencari informasi, mencari ide dan inspirasi baru dan untuk berhubungan dengan sahabat dan keluarga.[29]

Penetrasi pengguna internet di Indonesia yang terus meningkat ditandai dengan semakin banyaknya penduduk Indonesia yang menjadi pengguna internet ini perlu memiliki kesadaran terhadap keamanan digital agar aktivitas digitalnya, aman dari ancaman kejahatan siber. Generasi muda Indonesia yang cenderung memiliki literasi digital yang mumpuni semestinya bisa menyebarkan kesadaran keamanan digital kepada generasi lainnya.

---

[28] https://ekbis.sindonews.com/read/708377/178/duh-asia-jadi-wilayah-terbesar-ancaman-serangan-siber-1646885026 diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.
[29] https://datareportal.com/reports/digital-2022-indonesia diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB



Sumber: wearesocial.com

Gambar 2. Data Pengguna Internet di Indonesia

2) Politik.

Rasa aman masyarakat dalam berinternet saat ini dinilai sangat mengkhawatirkan. Pencurian data pribadi hingga data korporasi, tidak sedikit yang terjadi yang kemudian dijual ke pasar gelap. Selain itu, data kependudukan yang dikelola pemerintah bekerja sama dengan pihak ketiga berisiko disalahgunakan. Situasi Indonesia yang semakin darurat kejahatan siber kurang mendapatkan perhatian serius terutama oleh para pembuat regulasi di negeri ini.

Buktinya DPR dan pemerintah tidak juga segera menyelesaikan pembahasan dan mengesahkan RUU Keamanan dan Ketahanan Siber dan RUU Perlindungan Data Pribadi (PDP) yang sudah dibahas sejak tahun 2020 lalu. Kekosongan regulasi untuk melindungi sejumlah kejahatan digital jika terus dibiarkan akan mengganggu kebijakan pemerintah yang sedang giat berupaya mempercepat transformasi digital di berbagai bidang.

Indonesia menjadi satu-satunya negara anggota G20 yang belum memiliki UU PDP. Mencermati hal tersebut, DPR berupaya untuk mempercepat dan menyelesaikan pembahasan RUU PDP sebelum acara G20 berlangsung di Bali bulan November 2022.

Rencana ini membawa angin segar bagi penguatan keamanan digital di Indonesia.[30]

3) Ekonomi.

Nilai transaksi perdagangan digital Indonesia pada tahun 2021 mencapai Rp401,25 triliun dengan volume transaksi sebesar 1,73 miliar. Angka tersebut mendorong potensi ekonomi digital di Indonesia sebagai yang paling besar di Asia Tenggara. Pada tahun 2021 nilai ekonomi digital Indonesia telah mencapai angka sekitar USD70 miliar dan diperkirakan masih sangat mungkin untuk tumbuh hingga mencapai USD146 miliar pada tahun 2025.[31] Perkembangan ekonomi digital Indonesia yang berkembang dengan pesat sejak pandemi Covid-19 tentu berpotensi menjadi sasaran kejahatan siber jika para pelaku usaha dan masyarakat tidak meningkatkan kewaspadaannya. Oleh sebab itu sudah menjadi tanggung jawab pemerintah untuk melindungi dan mewujudkan satu ekosistem digital yang aman di Indonesia, agar ekonomi digital Indonesia dapat terus tumbuh dan berkembang di masa yang akan datang.

4) Sosial Budaya

Pandemi Covid-19 turut mendorong terjadinya percepatan transformasi digital yang tidak hanya terjadi di sektor komunikasi dan ekonomi, namun merambah ke semua sektor kehidupan masyarakat. Sejak pandemi Covid-19 di mana pemerintah memberlakukan pembatasan sosial berskala besar, membuat banyak aktivitas masyarakat beralih ke dunia digital. Berbagai kegiatan dilakukan serba daring, mulai dari sekolah secara daring, rapat daring, berbelanja daring, dan banyak aktifitas lain yang semua dilakukan serba daring.

[30] https://www.kompas.id/baca/polhuk/2022/05/23/pembahasan-ruu-pdp-dilanjutkan diakses pada tanggal 12 Juni 2022 pukul 22.00 WIB.
[31] https://www.kemenkeu.go.id/publikasi/berita/nilai-ekonomi-digital-indonesia-usd70-miliar-tertinggi-di-asia-tenggara/

Pandemi telah memaksa masyarakat untuk bisa belajar menyesuaikan diri dengan berbagai keterbatasan yang ada dengan mengoptimalkan pemanfaatan teknologi. Tua muda hingga anak-anak dituntut untuk segera menguasai semua yang kini serba digital. Kondisi ini pada satu sisi menjadi satu lompatan kemajuan yang luar biasa bagi bangsa Indonesia, di mana adopsi dan transformasi digital bisa berlangsung cepat. Namun proses belajar cepat masyarakat ini memunculkan resiko, mereka bisa kapan saja menjadi korban kejahatan digital. Hal ini karena tidak sedikit masyarakat yang tidak memiliki literasi yang mencukupi mengenai potensi kejahatan digital dan bagaimana cara untuk mencegahnya.

5) Pertahanan dan Keamanan.

Indonesia sudah memiliki sejumlah lembaga yang berwenang untuk membangun dan mengembangkan keamanan digital/siber di Indonesia. Pemerintah pada tahun 2017 telah membentuk Badan Siber dan Sandi Negara (BSSN) yang bertugas menjadi *leading sector* dalam melaksanakan keamanan siber secara nasional dengan memanfaatkan dan mengembangkan semua unsur dan potensi yang ada. Institusi Polri telah memiliki Direktorat Tindak Pidana Siber yang berada di bawah Bareskrim Polri. Selain itu, ada Kementerian Komunikasi dan Informasi juga turut aktif membantu mewujudkan ekosistem keamanan siber di tanah air.

Keberadaan lembaga kementerian di atas telah berperan dalam membangun kewaspadaan terhadap potensi ancaman kejahatan siber secara nasional. Apa yang diperlukan kini hanyalah mengoptimalkan potensi yang ada sehingga mampu membangun postur pertahanan dan keamanan siber yang kuat.

d. Peluang dan Kendala

1) Peluang

a) Literasi digital generasi muda umumnya cukup memadai sehingga bisa dioptimalkan untuk memberikan edukasi dan

pendampingan baik pada generasi yang lebih tua maupun generasi yang lebih muda.

b) Potensi ekonomi digital Indonesia cukup besar sehingga memberikan tanggung jawab kepada negara untuk memberikan ekosistem yang aman.

c) Indonesia memiliki lembaga dan institusi yang secara khusus mengurusi keamanan digital/siber.

2) Kendala

a) Banyak masyarakat Indonesia yang memiliki kesadaran dan pengetahuan mengenai keamanan digital/siber yang minim

b) Masih adanya kekosongan regulasi terkait dengan keamanan dan pertahanan siber.

c) Tren ancaman keamanan digital dunia akan semakin canggih dan berpotensi menimbulkan kerugian finansial semakin besar.

TANHANA DHARMMA MANGRVA

BAB III
PEMBAHASAN

13. Umum

Pembatasan sosial berskala besar yang diterapkan pemerintah guna mengendalikan penyebaran Covid-19 di tengah masyarakat telah mendorong percepatan transformasi digital dalam kehidupan masyarakat. Berbagai pembatasan yang ada, membuat masyarakat melakukan berbagai penyiasatan agar aktivitas keseharian masih bisa dikerjakan sekalipun secara fisik mereka ada di rumah masing-masing. Salah satu yang utama adalah dengan memanfaatkan teknologi digital.

Pada masa pandemi lalu, masyarakat betul-betul dipaksa oleh keadaan untuk bisa memanfaatkan teknologi digital guna menopang berbagai aspek kehidupan. Anak sekolah dan kuliah harus melanjutkan proses belajar mengajar jarak jauh secara daring. Anak ditantang untuk belajar secara mandiri dan mengekplorasi internet sebagai sumber ilmu dan referensi. Orang tua yang sebagian dikenal gagap dengan teknologi, dipaksa ikut belajar menggunakan internet dan sejumlah aplikasi pembelajaran daring guna menggantikan peran guru mendampingi belajar anak di rumah. Para pekerja kantoran dipaksa bekerja secara *remote*, melakukan berbagai rapat dari rumah. Kegiatan belanja kebutuhan sehari-hari yang biasanya dilakukan dengan mengunjungi pusat perbelanjaan, digantikan dengan melakukan belanja daring di sejumlah situs *e-commerce*. Demikian halnya dengan masyarakat yang membutuhkan layanan kesehatan namun takut untuk datang ke rumah sakit, mereka mulai membiasakan diri menggunakan layanan *telemedicine* untuk berkonsultasi daring dengan dokter. Sementara guna memenuhi kebutuhan makan sehari-hari, tidak sedikit masyarakat yang memanfaatkan aplikasi pesan-antar makanan dari ponsel pintarnya.

Kecepatan masyarakat Indonesia dalam beradaptasi dengan penggunaan teknologi digital di satu sisi menjadi satu keunggulan dan modal kuat bangsa Indonesia dalam melanjutkan pembangunan nasional memasuki Revolusi Industri 4.0. Namun di sisi lain, percepatan transformasi

digital yang disertai dengan minimnya literasi terkait keamanan digital menjadikan masyarakat rentan menjadi korban kejahatan digital.

14. Anatomi Kejahatan Digital yang Terjadi Selama Ini

Akselerasi dalam mengadopsi teknologi oleh masyarakat selama masa pandemi Covid-19 memang tergolong cepat. Kondisi di era Pandemi Covid-19 turut berperan sebagai faktor pendorong yang menuntut percepatan arus digitalisasi untuk masuk pada seluruh aspek kehidupan sehari-hari. Pemerintah membatasi kegiatan dan operasi bisnis secara langsung, dan mendorong orang untuk bekerja dari rumah sebanyak mungkin, sehingga hampir semua aktifitas mengalami lompatan untuk mempercepat proses menuju transformasi digital. Menurut penelitian yang dilakukan oleh Mckinsey menunjukkan adanya peningkatan kemampuan mengadopsi perubahan digital 20-25 kali lebih cepat dari yang mereka harapkan.[32]

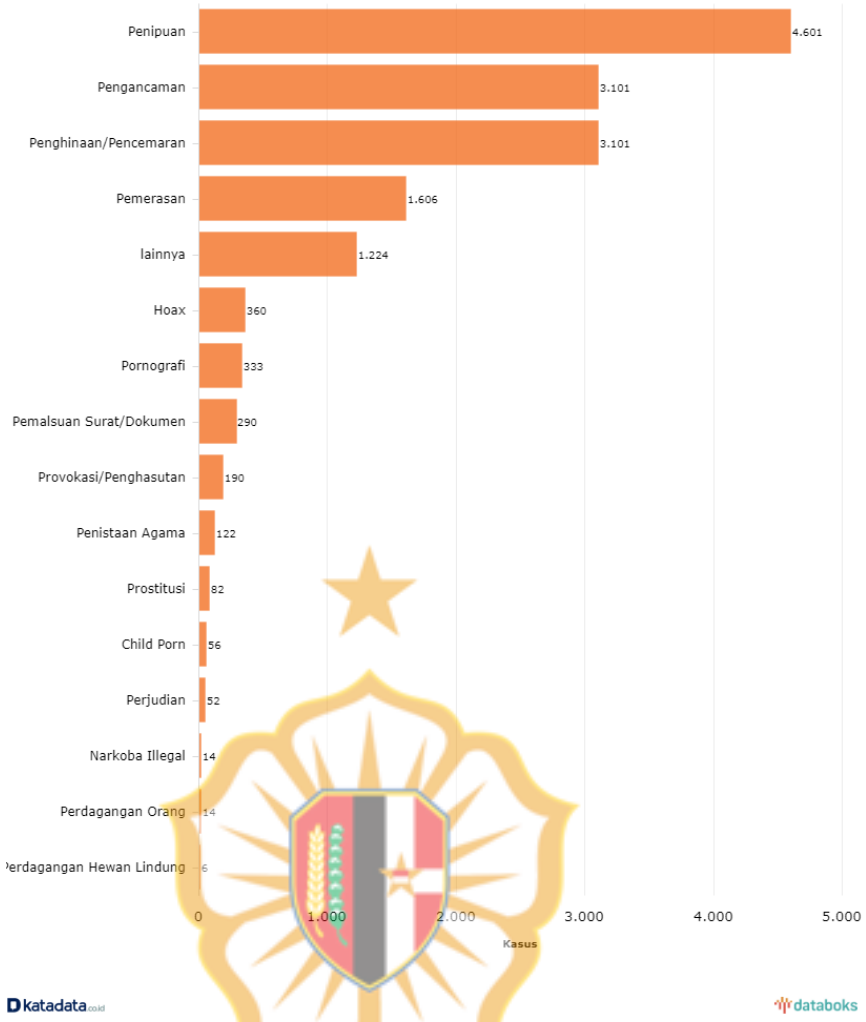
Permasalahan muncul ketika proses percepatan transformasi digital terjadi di tengah masyarakat cenderung tidak sempurna. Tranformasi digital tidak hanya sekedar menuntut masyarakat untuk tahu cara menggunakan dan memanfaatkan teknologi digital. Akan tetapi lebih dari itu, masyarakat semestinya memiliki pengetahuan mengenai berbagai konsekuensi termasuk pentingnya masyarakat juga memahami potensi bahaya kejahatan digital, modus operandinya dan bagaimana upaya preventif yang harus dimiliki dan dibangun masyarakat agar tidak menjadi korban kejahatan dalam aktivitasnya menggunakan teknologi digital.

Berdasarkan data patrolisiber.id seperti dikutip oleh katadata.co.id, sepanjang bulan Januari hingga September 2021 terdapat 15.152 pengaduan kejahatan siber dengan total kerugian mencapai Rp 3,88 triliun. Jenis kejahatan penipuan menjadi kasus yang paling mendominasi, disusul kasus pengancaman, pencemaran nama baik dan pemerasan.[33]

---

[32] https://www.mckinsey.com/featured-insights/coronavirus-leading-through-the-crisis/charting-the-path-to-the-next-normal/a-pandemic-digital-silver-lining-companies-digitized-many-activities-20-to-25-times-faster-during-covid-19 diakses pada tanggal 29 Juli 2022 pukul 20.00 WIB.

[33] https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.



Sumber: katadata.co.id

Gambar 3 Laporan Konten Kasus Kejahatan Siber

Ada beberapa jenis kejahatan digital yang terjadi di Indonesia dalam kurun beberapa tahun terakhir, baik jenis kejahatan baru maupun jenis kejahatan lama yang memiliki modus operandi yang baru. Beberapa jenis kejahatan digital yang terjadi di Indonesia. antara lain:

a. Peretasan (*hacking*)

   Peretasan adalah teknik yang dilakukan oleh orang untuk masuk dan menguasai suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan keamanan dengan maksud untuk mendapatkan hak akses atas data dan sistem. Kejahatan ini merupakan bentuk pelanggaran Pasal 30 UU ITE.

b. Intersepsi ilegal

Penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain. Kejahatan *malware*, sebuah perangkat lunak yang dibuat untuk menyusup pada sistem komputer dan melakukan penyadapan untuk mencuri data dan aktivitas pengguna komputer merupakan bentuk intersepsi ilegal. Kejahatan ini merupakan bentuk pelanggaran Pasal 31 ayat (1) dan ayat (2) UU ITE.

c. *Deface*

Bentuk kejahatan peretasan yang dilakukan dengan mengganti visual dari sebuah halaman web dengan teknik mengganti atau menyisipkan file pada server, teknik ini dapat dilakukan karena terdapat lubang pada sistem keamanan yang ada di dalam sebuah aplikasi atau *website*. Kejahatan ini merupakan bentuk pelanggaran Pasal 32 UU ITE.

d. *Phishing*

Kejahatan digital yang bertujuan mencuri informasi dan data pribadi sensitif mulai dari nama, tanggal lahir, alamat, e-mail, nomor HP, hingga nomor rekening, nomor ATM, hingga nama ibu kandung, dan OTP yang jika berhasil didapatkan oleh orang yang tidak bertanggung jawab bisa menguras rekening dan isi dompet digital korban. Cara kerja *phishing* terus berkembang, dan kini banyak menggunakan metode *social engineering* untuk mengelabuhi korban dengan memainkan emosi dan pikiran korban sehingga tanpa sadar menyerahkan data-data yang diminta penipu. Kejahatan ini merupakan bentuk pelanggaran Pasal 28 ayat (1) UU ITE.

e. Pemalsuan Data

Kejahatan *data forgery* merupakan tindakan memalsukan data dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database. Kejahatan ini merupakan bentuk pelanggaran Pasal 35 UU ITE

f. *Hoax*

Pembuatan dan penyebaran informasi yang sesungguhnya tidak benar, tetapi dibuat seolah-olah benar. Tujuan dari berita bohong adalah membuat masyarakat merasa tidak aman, tidak nyaman, dan kebingungan. Kejahatan ini merupakan bentuk pelanggaan Pasal 28 Ayat (1) UU ITE

g. *Skimming*

Kejahatan *Skimming* yakni kejahatan pencurian data kartu debit atau kartu kredit untuk menarik dana di rekening melalui penggandaan kartu. Kejahatan ini merupakan bentuk pelanggaran Pasal 46 UU ITE

h. *Ransomware*

Ransomware adalah tipe *malware* yang ketika berhasil masuk dan menyusup ke sistem komputer korban akan berusaha mengenkripsi dan mengunci file tersebut, untuk meminta tebusan. Kejahatan ini merupakan bentuk pelanggaran UU ITE Pasal 27 Ayat 4 UU ITE.

i. Serangan DDoS

Distributed Denial of Service (DDoS) merupakan bentuk kejahatan dengan membuat lalu lintas *server* berjalan dengan beban berat hingga tidak bisa menampung koneksi dan membuat sistem tidak bisa diakses. Teknik penyerangan DDoS biasanya dilaksanakan dengan banyak cara, seperti virus dan kumpulan bot yang disisipkan pada *malware* dan lainnya. Kejahatan ini merupakan bentuk pelanggaran Pasal 30 ayat (1) UU ITE.

j. Ujaran Kebencian

Bentuk kejahatan berupa konten yang mengandung kebencian, menyerang dan berkobar-kobar guna menimbulkan dampak tertentu, baik secara langsung maupun tidak langsung menginspirasi orang lain untuk membenci seseorang atau satu institusi. Kejahatan ini merupakan bentuk pelanggaran Pasal 28 ayat (2) UU ITE.

k. Konten Pornografi

Bentuk konten di internet berupa gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, video, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat. Kejahatan ini merupakan bentuk pelanggaran Pasal 27 ayat (1) UU ITE.

l. Carding

Bentuk kejahatan pencurian data informasi kartu kredit milik orang lain. Data tersebut kemudian digunakan oleh pelaku untuk melakukan transaksi *online* atau mencairkan saldo limit kartu ke rekening mereka. Kejahatan ini merupakan bentuk pelanggaran Pasal 32 UU ITE.

m. Cyber espionage

Kejahatan yang memanfaatkan internet untuk mmasuk ke sistem atau jaringan komputer secara ilegal guna memata-matai target tertentu. Kejahatan ini bisa saja terjadi karena alasan ekonomi, politik, hingga menyangkut keamanan negera karena bisa mencuri data dan dokumen penting yang tersimpan dalam komputer pejabat negara. Kejahatan ini merupakan bentuk pelanggaran Pasal 30 UU ITE.

TANHANA DHARMA MANGRVA

Berbagai tindak kejahatan digital di atas masih menjadi ancaman aktual bagi bangsa Indonesia. Sejumlah faktor menjadi penyebab dan pemicu kian maraknya kejahatan digital di negeri ini, yaitu:

a. Kesalahan Pengguna

Faktor manusia menjadi faktor yang paling banyak dijadikan pintu masuk penjahat digital. Sering kali, perilaku *sembrono* seseorang, tanpa sadar memberikan akses masuk bagi penjahat digital untuk mengambil alih sistem, akun dan aplikasi yang bisa mendatangkan kerugian finansial. Hal ini acapkali terjadi karena rendahnya literasi digital masyarakat.

b. Kerentanan Sistem

Sistem operasi pada sebuah komputer sering kali memiliki lubang keamanan yang baru disadari ketika sistem operasi tersebut sudah diedarkan secara luas ke tengah masyarakat. Oleh sebab itu, tidak jarang penyedia sistem operasi menyediakan update untuk menutup lubang keamanan tersebut. Persoalannya, tidak semua paham dan melakukannya.

c. Sistem Keamanan Digital Masih Rapuh

Setiap jaringan yang terhubung dengan internet membutuhkan tambahan pengamanan seperti antivirus, antimalware dan firewall untuk meningkatkan ketangguhan dalam menahan serangan siber dan upaya peretasan. Saat ini infrastruktur dan sistem keamanan siber di Indonesia masih cenderung lemah. Hal tersebut terlihat dari maraknya aksi peretasan dan serangan siber yang terjadi.

d. Kesiapan Regulasi dan Belum Optimalnya Penegakan Hukum

Perlu diakui bahwa hingga kini masih ada sejumlah kejahatan digital yang belum diatur sanksinya oleh regulasi. Kekosongan hukum menjadi pemicu tumbuh suburnya kejahatan digital di Indonesia. Selain itu, belum optimalnya penegakan hukum terkait kejahatan siber yang ditandai dengan rendahnya tingkat penyelesaian kasus kejahatan digital/siber di Indonesia turut berpengaruh.

15. Dampak Kejahatan Digital Terhadap Ketahanan Nasional

Selama ini banyak kalangan masyarakat tidak memiliki pengetahuan yang memadai terhadap potensi dan konsekuensi bahaya yang ditimbulkan dari aktivitas penggunaan teknologi digitalnya. Akibatnya, karena ketidaktahuan masyarakat tersebut, banyak di antaranya menjadi korban kejahatan digital. Hal ini menunjukan bagaimana pentingnya kemampuan literasi digital bagi masyarakat, khususnya berkaitan dengan pengetahuan mengenai kejahatan digital dan kemampuan untuk melakukan pencegahannya.

Literasi digital merupakan "*survival skill in the digital era*", demikian diungkapkan oleh Eshet-Alkalai (2004). Pernyataan ini menunjukan bagaimana pentingnya seseorang yang saat ini hidup di lingkungan digital memiliki literasi yang mumpuni. Literasi digital bukan hanya sekedar kemampuan untuk memanfaatkan perangkat lunak atau mengoperasikan perangkat digital, namun juga mencangkup banyak variasi dari kemampuan motorik, kognitif, emosional hingga sosiologis yang kompleks, yang dibutuhkan pengguna agar dapat berfungsi secara efektif di lingkungan digital (eshet, 2004).[34]

Literasi digital menjadi sebuah pengetahuan dan kecakapan dalam menggunakan media digital, termasuk alat komunikasi modern atau jaringan internet dalam menemukan, mengerjakan, mengevaluasi, menggunakan informasi, membuat informasi dan memanfaatkannya secara bijak, cerdas, tepat dan tentunya patuh hukum dan aturan dalam rangka membina komunikasi dan interaksi positif dalam kehidupan sehari-hari. Literasi digital juga merupakan kemampuan dalam menggunakan teknologi informasi dan komunikasi untuk mengkomunikasikan informasi secara kognitif dan teknikal.[35]

Menurut Martin (2006), literasi digital meliputi kemampuan yang kompleks, yang tidak hanya merujuk pada ketrampilan teknis menggunaikan media, namun juga kemampuan dalam memproses sumber-sumber digital. Luasnya cakupan kemampuan yang ada dalam literasi digital mengintegrasikan berbagai literasi dan keahlian lainnya. Sementara jaringan Pegiat Literasi Digital (Japelidi) mengurai kompetensi literasi digital terdiri dari kompetensi fungsional yang merupakan kemampuan dalam mengakses, menyeleksi, memahami, mendistribusikan dan memproduksi informasi melalui perangkat digital, serta kompetensi kritis meliputi kemampuan dalam menganalisis, menverifikasi, mengevaluasi, berpartisipasi dan berkolaborasi (Adiputra, dkk, 2019).[36]

---

[34] Rahayu, dkk. 2021. Perempuan dan Literasi Digital: Antara Problem, Hambatan dan Arah Pemberdayaan. Yogyakarta: UGM Press.
[35] Suherdi, dkk. 2021. Peran Literasi Digital di masa Pandemik. Deli Serdang: Cattleya Darmaya Fortuna
[36] Rahayu, dkk. 2021. Perempuan dan Literasi Digital: Antara Problem, Hambatan dan Arah Pemberdayaan. Yogyakarta: UGM Press.

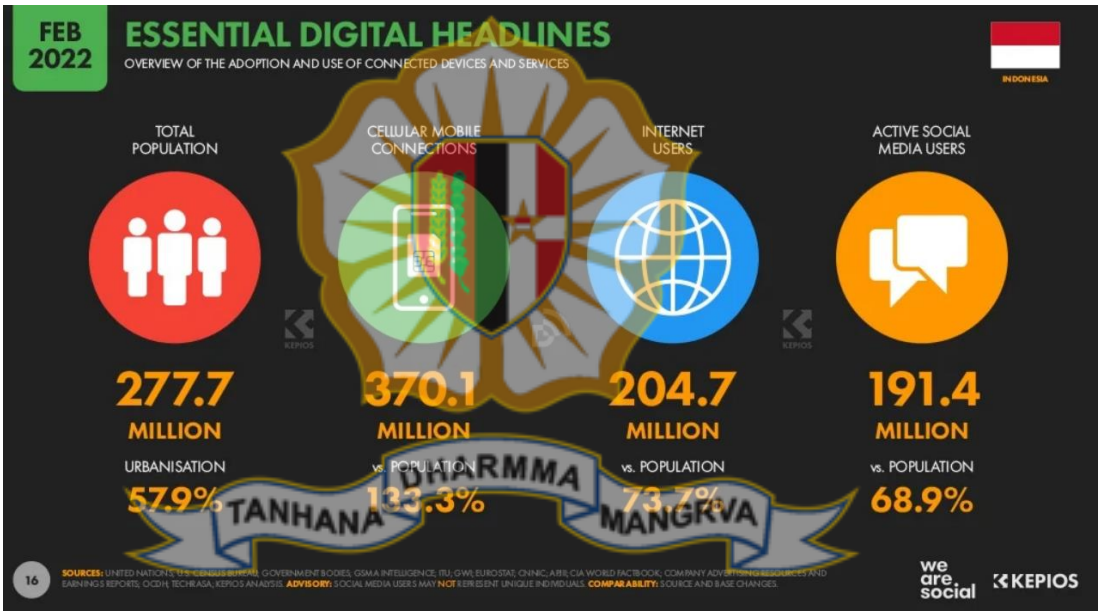
Literasi digital tidak hanya sekedar merupakan kemampuan untuk memahami dan menguasai teknologi digital ataupun terkait dengan kemampuan seseorang berpikir kritis dan selalu berupaya untuk melakukan validasi terhadap kebenaran dari informasi yang diterimanya dari media digital. Akan tetapi, lebih dari itu, literasi digital juga perlu dimaknai sebagai kemampuan seseorang mengetahui konsekuensi dari penggunaan teknologi digital, termasuk mengerti dan memahami kerawanan teknologi digital terhadap beragam kejahatan yang modusnya terus berkembang, serta mengetahui cara dan metode mengamankan diri dan mencegah agar tidak menjadi korban kejahatan digital/siber.

Tidak bisa dipungkiri bahwa selama ini kampanye dan sosialisasi terkait dengan bahaya kejahatan digital, berikut cara dan metode untuk mencegah dan memproteksi diri dari kejahatan digital sangat minim. Jika pun sudah dilakukan, upaya pemerintah, aparat penegak hukum dan *stakeholder* terkait lainnya untuk mengedukasi masyarakat untuk meningkatkan kewaspadaan terhadap kejahatan digital masih jauh dari optimal. Akibatnya sebagian besar masyarakat belum memiliki *security awareness* dan tidak mengetahui bagaimana cara "menjaga diri" saat menggunakan teknologi digital khususnya terkait dengan dunia siber.

Security Awareness adalah pengetahuan yang dimiliki oleh seseorang terkait pengetahuan dan praktik keamanan yang baik dan pentingnya melindngi data pribadi ataupun kelompok saat menggunakan internet (Edwards, 2015). Saat seseorang memiliki kesadaran keamanan, maka dia akan melindungi data dan informasi yang mereka miliki saat terhubung dengan internet. Akan muncul kesadaran untuk mempertimbangkan dan menentukan informasi pribadi apa saja yang akan dibagikan di internet sehingga tidak menimbulkan ancaman dan kerugian bagi dirinya saat ini maupun dikemudian hari.

Menurut data dari We Are Social, jumlah pengguna internet di Indonesia pada Februari 2022 telah mencapai 204,7 juta. Ini berarti ada 73,7 persen dari populasi Indonesia yang telah menggunakan internet. Sedangkan jumlah pengguna aktif media sosial di Indonesia mencapai 191,4 juta orang atai 68,9 persen dari total penduduk Indonesia. Rata-rata

masyarakat Indonesia menghabiskan waktunya selama delapan jam 36 menit untuk berselancar di internet, dan tiga jam 17 menit untuk bersosial media. Tiga kegiatan yang sering dilakukan masyarakat Indonesia menghabisakan waktunya di internet adalah untuk mencari informasi, mencari ide dan inspirasi baru dan untuk berhubungan dengan sahabat dan keluarga.[37] Penetrasi pengguna internet di Indonesia terus meningkat menandakan proses transformasi digital di negeri ini masih terus berjalan dengan pesat. Banyaknya penduduk Indonesia yang menjadi pengguna internet ini akan menjadi sasaran empuk penjahat siber jika tidak ada upaya untuk meningkatkan kesadaran terhadap keamanan digital agar aktivitas digitalnya, aman dari ancaman kejahatan siber.



Sumber: wearesocial.com

Gambar 4. Jumlah Pengguna Internet dan Media Sosial di Indonesia

Berdasarkan data Kementerian Komunikasi dan Informatika, Indonesia mengalami darurat kejahatan siber. Sejak terjadi akselerasi digital yang semakin cepat pasca pandemi Covid-19, beragam modus kejahatan siber terus berkembang pesat. Setiap minggu sedikitnya terdapat 5.000 laporan pengaduan tindakan penipuan (*fraud*) masuk ke *website* pengaduan

[37] https://datareportal.com/reports/digital-2022-indonesia diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB

yang dimiliki Kemenkominfo. Data tersebut jika dikalkulasikan sejak Maret 2020 hingga akhir tahun 2021 membuat kejahatan penipuan daring yang dilaporkan masyarakat mencapai sekitar 200.000 laporan. Kebanyakan didominasi oleh kasus *fraud* di media Whatsapp dan Instagram.[38]

Social engineering merupakan suatu cara yang dilakukan oleh penjahat siber untuk mengelabui atau memanipulasi psikologi korban dengan cara memengaruhi pikiran bawah sadar korban menggunakan berbagai cara dan media yang persuasif, dengan cara membuat korban senang atau panik sehingga korban tanpa sadar akan menjawab atau mengikuti instruksi pelaku. Dari sini pelaku kejahatan bisa mendapatkan berbagai informasi data pribadi atau akses yang diinginkan. Modus ini menjadi sangat berbahaya karena tanpa disadari korban memberikan data pribadi yang bisa digunakan untuk meretas dan mencuri semua uang korban baik yang disimpan dalam dompet digital maupun dana tabungan korban yang tersimpan di bank. Sejumlah data pribadi yang menjadi sasaran penjahat mulai dari user name dan password aplikasi, PIN, MPIN, kode *One Time Password* (OTP), nomor kartu ATM atau kartu kredit atau debit, nomor CVV/CVC hingga nama ibu kandung.[39]

Aksi tipu-tipu dan pencurian data tersebut tidak hanya menyasar pada masyarakat biasa tapi juga merambah pada pelaku usaha UMKM yang sejak pandemi Covid-19 mulai berlomba melakukan transformasi digital dan mulai beralih untuk menggarap pangsa pasar digital. Salah satu yang aktual adalah maraknya aksi penipuan terhadap pelaku usaha mitra GoFood, aplikasi layanan pesan-antar makanan yang mengincar rekening korban. Para pelaku usaha yang baru saja mendaftar menjadi mitra GoFood, banyak kemudian dihubungi oleh penjahat siber melalui e-mail maupun pesan WhatsApp yang mengatasnamakan pihak GoFood, dan meminta sejumlah data atau bahkan uang dengan dalih sebagai bagian dari proses aktivasi keanggotaan. Ketidaktahuan pelaku usaha yang sedang berupaya merintis usaha secara digital, yang sebagian belum sepenuhnya melek digital,

[38] https://www.wartaekonomi.co.id/read367315/gegara-tranformasi-digital-indonesia-darurat-kejahatan-siber diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.
[39] https://www.cnbcindonesia.com/tech/20220621062955-37-348746/mengenal-social-engineering-dan-4-modus-bobol-rekening diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

membuat tidak sedikit dari mereka terjebak dan menjadi korban penjahat siber.[40]

Peristiwa ini memprihatinkan sekaligus ironi, karena ketika pemerintah melalui Kementerian Koperasi dan UKM sedang giat mendorong transformasi digital pada pelaku UMKM, yang dikampanyekan bisa menjadi sarana UMKM bisa melebarkan pangsa pasar dan bisa membuat usahanya segera naik kelas, justru harus mengalami kerugian finansial ketika sedang mencoba menjalankan proses transformasi digital. Pada sisi lain, kemampuan penjahat digital mengetahui data siapa saja yang baru mendaftar menjadi mitra GoFood menguak adanya dugaan kebocoran data digital pihak GoFood sekalipun dugaan tersebut beberapa kali telah dibantah oleh perusahaan.

Berdasarkan data internal Gojek menunjukkan pada Maret hingga Agustus 2020 saja ada lebih dari 250.000 pedagang (merchant) menjadi mitra GoFood. Dari jumlah tersebut, hasil riset dari Lembaga Demografi Fakultas Ekonomi dan Bisnis Universitas Indonesia menyebutkan, 94 persen pedagang yang baru bergabung ke GoFood merupakan usaha mikro, kecil, dan menengah (UMKM) berskala mikro dan 43 persen adalah pebisnis pemula.[41]

BSSN mencatat sepanjang 2020 terjadi anomali trafik terhadap Indonesia berjumlah 495.337.202. Anomali trafik tertinggi terjadi pada 10 Desember 2020 dengan jumlah 7,3 juta anomali. Pada 2019, anomali trafik tercatat 228.277.875. Dari total anomali trafik tersebut, 37 persen adalah aktivitas yang terkait dengan perangkat lunak berbahaya berjenis *trojan*. Berbeda dengan virus, *trojan* bersifat tidak terlihat dan sering kali menyerupai program atau *file* yang wajar, tetapi didesain khusus untuk berbagai tujuan, seperti pencurian data. Biasanya *malware* yang menginfeksi perangkat elektronik pengguna bertujuan untuk mencuri informasi pribadi, seperti

[40] https://katadata.co.id/desysetyowati/digital/5eb1268ec4a86/marak-penipuan-mitra-gofood-gojek-data-rekening-jadi-incaran diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.
[41] https://www.liputan6.com/tekno/read/4359908/selama-pandemi-covid-19-gofood-punya-lebih-dari-250-ribu-merchant-baru diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

rekaman penelusuran hingga informasi finansial. Selain itu terdapat pula *malware* yang dibuat untuk mencuri kata kunci (*password*). [42]

Aktivitas peretasan data di Indonesia memang cenderung semakin marak dalam tiga tahun terakhir. Miliaran data pribadi masyarakat berhasil digondol pencuri digital hingga diperjualbelikan di sejumlah forum *darkweb*. Menurut data Badan Siber dan Sandi Negara (BSSN) pada tahun 2021 di Indonesia terjadi 5.574 kasus peretasan dan 1,6 miliar serangan siber. Aktivitas *malware* atau perangkat lunak berbahaya mendominasi serangan, yakni mencapai 62,27 persen. Ada tiga sektor yang banyak menjadi korban peretasan yaitu situs pendidikan tinggi, swasta hingga pemerintah daerah.[43]

Dalam beberapa bulan terakhir aksi peretasan yang dilakukan oleh *hacker* berjuluk Bjorka cukup menyita perhatian publik. Pasalnya, beberapa kali sang hacker diduga telah membobol sejumlah dokumen dan data secara ilegal milik lembaga pemerintah Indonesia. Selain mengklaim berhasil mencuri 105 juta data kependudukan dari server Komisi Pemilihan Umum (KPU) pada 6 September 2022 lalu, Bjorka juga diklaim telah membobol 1,3 miliar data registrasi SIM card, mempublikasikan surat yang bersifat rahasia untuk Presiden Jokowi pada periode 2019-2021, termasuk surat yang berasal dari Badan Intelijen Negara (BIN). Seakan menantang pemerintah untuk menangkapnya, Bjorka bahkan mempublikasikan data pribadi milik pejabat, di antaranya menteri Komunikasi dan Informatika.

Sebelum meretas server KPU, Bjorka memang sudah dikenal sebagai pembobol data pribadi. Pada April 2020 Bjorka telah berhasil menggondol data jutaan pengguna Tokopedia berukuran 11 GB. Selain itu pada Agustus 2022 juga diklaim telah meretas dan mencuri 26 juta pelanggan IndiHome yang berisi nama lengkap, email, Nomor Induk Kependudukan (NIK) dan jenis kelamin.[44] Serangkaian kasus ini hingga kini masih belum berhasil diungkap oleh Kepolisian RI.

---

[42] https://www.kompas.id/baca/polhuk/2021/03/01/pandemi-covid-19-ancaman-siber-meningkat/ diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

[43] https://www.kompas.id/baca/polhuk/2022/01/20/sebanyak-5574-kasus-peretasan-terjadi-di-2021 diakses pada tanggal 18 September 2022 pukul 21.30 WIB

[44] https://grafis.tempo.co/read/3087/sosok-bjorka-peretas-yang-mengacak-acak-sistem-data-indonesia diakses pada tanggal 18 September 2022 pukul 21.30 WIB

Kasus kebocoran data yang terjadi pada Tokopedia tersebut, bukan pertama kali. Pada Maret 2019, kebocoran data serupa terjadi pada perusahaan e-dagang lain yaitu Bukalapak. Dalam pemberitaan sebelumnya, peretas Gnosticplayers yang diduga beroperasi dari Pakistan dikabarkan menjual 13 juta data akun pengguna dari Bukalapak. Meski kemudian pendiri Bukalapak, Achmad Zaky, mengklaim peretasan oleh Gnosticplayers tidak berhasil mendapatkan data-data penting mitra dan pengguna Bukalapak.[45]

Kebocoran data juga pernah terjadi di laman Lazada dan Traveloka. Sementara di lingkungan pemerintahan, pencurian data juga pernah terjadi terhadap 2,3 juta data pemilih dari *server* Komisi pemilihan Umum, serta 1,3 juta pengguna aplikasi *Electronic Health Alert Card* (eHAC) dari Kementerian Kesehatan diduga telah bocor. Kasus dugaan kebocoran 279 juta data peserta BPJS kesehatan juga pernah diberitakan pada bulan Mei 2021 lalu.[46]

Menurut Pratama Pesadha, *chairman* lembaga riset siber Indonesia *Communication & Information System Security Research Center* (CISSReC) Pratama Persadha kebocoran data dari sejumlah situs di tanah air yang ditawarkan di pasar gelap di internet, jika disatukan bisa menjadi sangat berbahaya karena penjahat siber tidak hanya sekedar bisa mengantongi nama, alamat e-mail dan nomor ponsel aktif saja, tapi juga data nomor KTP dan KK. Serangkaian data tersebut bisa disalahgunakan untuk melakukan pinjaman online jika pelaku mahir mengelola data.[47]

Persoalannya, hingga kini belum ada regulasi yang menghukum korporasi ataupun lembaga pemerintah yang dianggap lalai sehingga membuat data masyarakat yang tersimpan di dalam server mereka dicuri dan diambil secara ilegal oleh penjahat siber. Semestinya ada sanksi hukum yang bisa menjerat korporasi/lembaga atau setidaknya penanggung jawab penyedia layanan yang menyimpan data pribadi masyarakat. Terlebih, peretasan dan aktivitas ancaman siber sendiri tidak selalu berorientasi

[45] https://www.kompas.id/baca/ekonomi/2020/05/03/peretasan-data-pengguna-rawan-berlanjut-menjadi-kejahatan-siber
[46] https://www.liputan6.com/bisnis/read/4563758/279-data-bpjs-kesehatan-bocor-dpr-ketahanan-siber-indonesia-lemah diakses pada tanggal 2 Agustus 2022 pukul 21.30 WIB.
[47] https://cyberthreat.id/read/6779/Pakar-Jika-Data-Tokopedia-Bukalapak-Dikombinasikan-dengan-Data-KPU-yang-Bocor-Ini-Berbahaya diakses pada tanggal 2 Agustus 2022 pukul 21.30 WIB.

ekonomi. Sejumlah aktivitas spionase juga tidak jarang dilakukan pada level negara. Mereka biasanya mengintai berbagai macam hal, seperti rencana strategi dan kebijakan negara, hingga ditemukan profiling pejabat negara. Seperti halnya pada pertengahan September 2021, media asing mengabarkan bahwa 10 jaringan internal lembaga negara, termasuk Badan Intelijen Negara, telah diretas. Pelakunya dikabarkan merupakan sekelompok peretas dari China dengan identitas Mustang Panda yang dikenal kerap melakukan aksi spionase dan menargetkan negara-negara di Asia Tenggara. Kondisi ini memperlihatkan bagaimana kejahatan digital semakin mempengaruhi ketangguhan ketahanan nasional Indonesia.

Berdasarkan data Kementerian Komunikasi dan Informatika, Indonesia mengalami darurat kejahatan siber. Sejak terjadi akselerasi digital yang semakin cepat pasca pandemi Covid-19, beragam modus kejahatan siber terus berkembang pesat. Setiap minggu sedikitnya terdapat 5.000 laporan pengaduan tindakan penipuan (*fraud*) masuk ke *website* pengaduan yang dimiliki Kemenkominfo. Data tersebut jika dikalkulasikan sejak Maret 2020 hingga akhir tahun 2021 membuat kejahatan penipuan daring yang dilaporkan masyarakat mencapai sekitar 200.000 laporan. Kebanyakan didominasi oleh kasus *fraud* di media Whatsapp dan Instagram.[48]

BSSN mencatat sepanjang 2020 terjadi anomali trafik terhadap Indonesia berjumlah 495.337.202. Anomali trafik tertinggi terjadi pada 10 Desember 2020 dengan jumlah 7,3 juta anomali. Pada 2019, anomali trafik tercatat 228.277.875. Dari total anomali trafik tersebut, 37 persen adalah aktivitas yang terkait dengan perangkat lunak berbahaya berjenis *trojan*. Berbeda dengan virus, *trojan* bersifat tidak terlihat dan sering kali menyerupai program atau *file* yang wajar, tetapi didesain khusus untuk berbagai tujuan, seperti pencurian data. Biasanya *malware* yang menginfeksi perangkat elektronik pengguna bertujuan untuk mencuri informasi pribadi, seperti rekaman penelusuran hingga informasi finansial. Selain itu terdapat pula *malware* yang dibuat untuk mencuri kata kunci (*password*).[49]

---

[48] https://www.wartaekonomi.co.id/read367315/gegara-tranformasi-digital-indonesia-darurat-kejahatan-siber diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.
[49] https://www.kompas.id/baca/polhuk/2021/03/01/pandemi-covid-19-ancaman-siber-meningkat/ diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

Kejahatan siber merupakan satu bentuk kejahatan yang menjadi perhatian dunia internasional. Setiap negara tidak luput dari ancaman kejahatan siber yang terus berkembang. Berdasarkan data Anev Bareskrim Polri, selama tahun 2021, jumlah kasus kejahatan digital yang ditangani oleh Polri sebanyak 3.270 kasus. Jumlah ini mengalami penurunan sekitar 32 persen jika dibandingkan dengan tahun sebelumnya yang mencapai 4790 kasus. Kejahatan terkait pencemaran nama baik menjadi jenis kejahatan digital paling dominan. Dari jumlah tersebut kejahatan terkait pencemaran nama baik menjadi jenis kejahatan digital yang paling banyak dilaporkan masyarakat dengan jumlah kasus 1.136 kasus, disusul kasus penipuan sebanyak 864 kasus dan pornografi sebanyak 321 kasus.

Pencurian data pribadi hingga data korporasi yang semakin meningkat akhir-akhir ini mempengaruhi rasa aman masyarakat dalam berinternet. Terlebih tidak sedikit kebocoran data pribadi tersebut yang kemudian dijual ke pasar gelap. Selain itu, data kependudukan yang dikelola pemerintah bekerja sama dengan pihak ketiga berisiko disalahgunakan. Situasi Indonesia yang semakin darurat kejahatan siber kurang mendapatkan perhatian serius terutama oleh para pembuat regulasi di negeri ini. Buktinya DPR dan pemerintah tidak juga segera menyelesaikan pembahasan dan mengesahkan RUU Keamanan dan Ketahanan Siber dan RUU Perlindungan Data Pribadi (PDP) yang sudah dibahas sejak tahun 2020 lalu. Kekosongan regulasi untuk melindungi sejumlah kejahatan digital jika terus dibiarkan akan mengganggu kebijakan pemerintah yang sedang giat berupaya mempercepat transformasi digital di berbagai bidang. Indonesia menjadi satu-satunya negara anggota G20 yang belum memiliki UU PDP.

Keberadaan UU PDP diharapkan mengisi kekosongan regulasi berkaitan dengan perlindungan terhadap penyalahgunaan data pribadi masyarakat. Salah satunya terkait dengan kejahatan *doxing* yang kini semakin marak terjadi di media sosial. *Doxing* atau pengumpulan data pribadi seseorang untuk disebar dengan narasi tertentu, berpotensi menjadi sarana untuk membungkam daya kritis. Dari sejumlah kasus, perempuan berada dalam posisi yang cenderung lebih rentan sebagai korban.

Selain menggunakan data pribadi tanpa hak, modus yang juga dipergunakan adalah data tersebut ditampilkan di sejumlah aplikasi yang ada sangkut pautnya dengan kegiatan prostitusi daring. Hal ini membuat para korban menerima ribuan pesan setiap harinya yang terkait dengan praktik prostitusi. Sekalipun dialami warga biasa, *doxing* tidak bisa dianggap sebagai perundungan yang lebih cenderung berupaya merendahkan martabat. Pasalnya, ada tujuan yang hendak dicapai *doxing*, yakni menghentikan perjuangan atau advokasi yang dilakukan korban. Selama ini banyak korban *doxing* kerap kali takut melapor ke pihak berwajib. Korban juga trauma tatkala harus mengulangi ingatan mengenai peristiwanya.[50] Guna menghadapi doxing sebagai dimensi kejahatan baru, Rancangan Undang-Undang tentang Perlindungan Data Pribadi perlu segera dibahas dan disahkan.

Urgensi pengesahan RUU PDP juga menjadi penting untuk mengikat komitmen penyedia layanan digital untuk benar-benar menjaga data-data yang mereka kumpulkan dari masyarakat agar tidak mengalami kebocoran. Para penyedia layanan digital baik yang dikelola pemerintah maupun swasta sudah semestinya memiliki kewajiban dan tanggung jawab untuk menjaga data yang mereka simpan dari upaya peretasan dan pencurian data oleh para penjahat siber. Komitmen tersebut semestinya diatur secara ketat, disertai dengan sanksi hukuman, bisa berupa pidana maupun denda besar, jika terbukti melakukan keteledoran.

Pada sisi lain, arah pembangunan sistem keamanan siber korporasi di Indonesia selama ini dinilai sudah berada di jalur yang tepat. Hanya tidak diimbangi dengan infrastruktur keamanan yang mumpuni. Teknologi keamanan siber yang digunakan oleh sejumlah korporasi maupun pemerintah dinilai masih tertinggal. Hal ini perlu menjadi perhatian mengingat volume serangan siber kian meningkat. Hasil studi firma keamanan siber Amerika Serikat, Palo Alto Networks, terhadap 100 pemimpin perusahaan di empat negara anggota ASEAN, yaitu Indonesia, Filipina, Thailand, dan Singapura, pada Februari 2020 menunjukan sebanyak 84 persen perusahaan Indonesia memiliki kecenderungan untuk mengalami

[50] https://www.kompas.id/baca/ilmu-pengetahuan-teknologi/2020/02/18/doxing-secara-terstruktur-terjadi diakses pada tanggal 29 Agustus 2022 pukul 21.00 WIB

peningkatan anggaran keamanan siber pada 2020. Hal ini menunjukkan bahwa keamanan siber mulai disadari sebagai domain yang penting.

Dalam studi tersebut ditemukan bahwa perkembangan ancaman yang muncul menjadi pendorong utama peningkatan anggaran keamanan siber tersebut. Meskipun berada di jalur yang tepat, kondisi eksisting keamanan siber menjadi hal yang patut dikhawatirkan. Sebanyak 44 persen responden menyatakan tidak percaya diri dengan sistem keamanan siber yang dimiliki perusahaannya. Secara umum, tingkat kepercayaan keamanan siber di Indonesia cenderung rendah (52 persen).

Pada sisi teknologi, mayoritas perusahaan Indonesia masih menggunakan sistem keamanan yang tertinggal (legacy), seperti penggunaan perangkat lunak *antivirus* ataupun *antimalware*. Sebanyak 76 persen perusahaan menganggap *antivirus* sebagai solusi keamanan siber. Di sisi lain, infrastruktur baru, seperti *firewall* generasi baru (*next gen firewall*), baru diadopsi 51 persen perusahaan Indonesia. Hal ini berbeda dengan negara yang tingkat kepercayaan keamanan sibernya lebih tinggi seperti Singapura (75 persen) yang tingkat implementasi solusi berbasis komputasi awan, seperti SD-WAN (*software defined wide-area network*), lebih tinggi.[51]

Hasil kajian Palo Alto Network seharusnya menjadi peringatan bagi Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang ditunjuk negara untuk menyinergikan dan mengonsolidasikan semua unsur keamanan siber bahwa infrastruktur dan ekosistem digital di Indonesia belum relatif aman dan mampu menghadapi ancaman kejahatanan siber. Hal ini menunjukan bahwa masih ada pekerjaan rumah kewaspadaan nasional yang perlu untuk terus dibenahi terkait teknologi dan infrastruktur keamanan siber di Indonesia.

Pada sisi lain keberadaan Undang-Undang Informasi dan Transaksi Elektronik (ITE) sejak diundangkan pada tahun 2008 hingga kemudian disempurnakan melalui UU nomor 19 tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang ITE dinilai banyak pihak masih mengalami banyak kekurangan. Selain tidak mengatur semua jenis kejahatan siber, UU

[51] https://www.kompas.id/baca/gaya-hidup/2020/07/15/palo-alto-keamanan-siber-indonesia-ke-arah-yang-tepat diakses pada 2 Agustus 2022 pukul 22.15 WIB.

ini banyak menerima kritik dari masyarakat karena memiliki sejumlah pasal karet di dalamnya. Akibatnya, bukannya memberikan rasa aman kepada masyarakat, UU ITE yang ada saat ini berpotensi digunakan untuk mengkriminalisasi masyarakat. Terbukti kerentanan tersebut menimpa sejumlah kalangan, seperti jurnalis, aktivis antikorupsi, aktivis lingkungan, minoritas jender, dan minoritas agama. Mereka diserang secara digital dan fisik, mengalami *doxing* (tindakan melacak identitas seseorang dari dunia maya), ditangkap, dituntut dengan hukum internet hanya karena menyatakan kritik di media sosial. Pasal 27 terkait pencemaran nama baik dan Pasal 28 terkait berita yang menebarkan kebencian dalam UU ITE dinilai mudah membungkam mereka yang bersuara kritis khususnya di media sosial atau internet.

Sejumlah kasus yang menurut masyarakat merupakan bentuk kriminalisasi antara lain, kasus yang dialami aktivis sekaligus pengurus nasional Aliansi Jurnalis Independen (AJI), Dandhy Dwi Laksono, September 2019. Ia ditangkap di rumahnya oleh petugas Polda Metro Jaya dengan tuduhan melanggar Pasal 28 Ayat (2) serta Pasal 45 A Ayat (2) UU ITE dan/atau Pasal 14 dan Pasal 15 Kitab Undang-undang Hukum Pidana karena alasan unggahan di media sosial Twitter mengenai Papua yang menimbulkan rasa kebencian.

Selain itu, ada juga kasus yang dialami Baiq Nuril, salah seorang guru honorer di Mataram, NTB, yang malah dikriminalisasi dengan UU ITE karena menyebarkan bukti terkait pelecehan seksual yang dialaminya. Ia akhirnya mendapat amnesti dari Presiden Joko Widodo setelah dipidana dengan hukuman penjara 6 bulan dan denda Rp 500 juta. Kasusnya pun sudah berjalan hingga tingkat Mahkamah Agung ketika itu. Menurut direktur Asosiasi Lembaga Penelitian, Pendidikan, dan Penerangan Ekonomi dan Sosial Wijayanto mengatakan, UU ITE juga kerap dijadikan sebagai senjata bagi setiap orang yang memiliki perbedaan pandangan politik satu sama lain. UU ITE juga kerap dijadikan alat untuk melemahkan kelompok yang kritis terhadap pemerintah.[52]

[52] https://www.kompas.id/baca/utama/2019/12/21/jumlah-kasus-kriminalisasi-uu-ite-meningkat/ diakses pada tanggal 1 Agustus 2022 pukul 21.30 WIB.

Pemerintah pada bulan Juni 2021 sebenarnya telah mengeluarkan Surat Keputusan Bersama (SKB) Pedoman Kriteria Implementasi UU Informasi dan Transaksi Elektronik (ITE) yang ditandatangani oleh Menteri Komunikasi dan Informatika RI, Kapolri, dan Jaksa Agung. SKB ini dibuat sebagai pedoman bagi aparat penegak hukum terkait sejumlah pasal UU ITE yang dinilai banyak pihak menimbulkan multitafsir, yaitu Pasal 27, Pasal 28, Pasal 29 dan Pasal 36. Dengan adanya SKB tersebut diharapkan pelaksanaan penegakan hukum terkait sejumlah pasal karet menjadi lebih kaku dan fokus sehingga bisa memberikan kepastian hukum, sembari menunggu pembahasan mengenai revisi terbatas UU ITE selesai dibahas oleh DPR.[53]

Sebelumnya keluarnya SKB UU ITE, Kapolri pada tanggal 22 Februari 2021 mengeluarkan Surat Edaran Kepala Kepolisian Negara RI Nomor 2 Tahun 2021 tentang Kesadaran Budaya Beretika untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat, dan Produktif. Dalam surat edaran tersebut Polri memilih untuk mengedepankan pendekatan edukatif jika menemukan indikasi ujaran kebencian di dunia maya. Penyidik Polri juga diberikan pembekalan pemahaman untuk tidak serta merta melakukan penegakan hukum jika mendapati laporan terkait UU ITE. Melalui pendekatan edukasi dan persuasif, diharapkan nantinya tidak terjadi lagi dugaan kriminalisasi terhadap orang atau pihak yang dilaporkan ke polisi. Keluarnya SE Kapolri tersebut tidak bisa dilepaskan dari banyaknya masyarakat yang saling melaporkan ujaran kebencian sebagai buntut polarisasi politik yang diakibatkan penggunaan politik identitas pada Pilpres 2019.

Bersamaan dengan keluarnya SE Kaplori, Polri membentuk polisi virtual. Program ini merupakan bentuk baru penegakan hukum di dunia siber. Dengan pendekatan Polisi Virtual, Polri akan lebih dahulu memberikan peringatan kepada masyarakat jika menemukan ada hal yang dilakukan masyarakat berisiko terhadap pelanggaran hukum. Hal ini menjadi wajah

[53] https://www.kominfo.go.id/content/detail/35229/skb-pedoman-implementasi-uu-ite-ditandatangani-menko-polhukam-berharap-beri-perlindungan-pada-masyarakat/0/berita diakses pada tanggal 1 Agustus 2022 pukul 21.30 WIB.

baru pendekatan Polri dalam melakukan penegakan hukum dalam penggunaan ruang digital yang tetap beretika. Namun demikian, langkah pengawasan dan preventif oleh Polri dirasa tidak akan optimal jika tidak dibarengi dengan penguatan literasi digital.

Munculnya tren menjadikan Indonesia sebagai basis kejahatan siber internasional oleh warga negara asing juga semestinya dapat diantisipasi sejak dini oleh pemerintah. Selama ini ada dugaan sejumlah warga negara asing memanfaatkan kelemahan pada sistem keimigrasian dan keterbasan aparat keamanan dalam melakukan pengawasan warga asing selama berada di Indonesia untuk menjalankan kejahatan siber internasional yang terorganisir. Terlebih karakter kejahatan siber yang bisa dilakukan dari mana saja tanpa dibatasi oleh batasan geografi, di mana pelakunya dengan mudah bisa menyembunyikan identitasnya (*anonymous*).

Berdasarkan data dari Bareskrim sepanjang 2018-2021, WNA pelaku penipuan siber yang terungkap berasal dari beberapa negara, mulai dari Nigeria (8 kasus), Gambia (1 kasus), Kongo (1 kasus), Ukraina (1 kasus), hingga China. Kejahatan siber yang dilakukan WNA di Indonesia terjadi secara terorganisasi. Misalnya, dalam modus *business e-mail compromise* (BEC) atau penipuan menggunakan surel palsu dengan mengatasnamakan sebuah perusahaan. Perusahaan yang sengaja dibuat secara fiktif itu nantinya merekayasa skenario agar calon korban, yang juga menyasar pada korban korporasi, untuk mengirimkan sejumlah uang ke nomor rekening yang mereka berikan. Para pelaku beraksi dalam sebuah kelompok yang dibagi atas beberapa peran, mulai dari pembuat perusahaan, pembuat nomor rekening bank, hingga mereka yang menarik uang hasil penipuan.

Begitu juga dengan modus *fraudulent wire transfer* atau rekayasa transfer dana untuk memeras korban. Modus itu dilakukan dengan mempelajari terlebih dahulu latar belakang korban yang disasar, yakni orang awam dengan literasi keuangan rendah. Kemudian pelaku membagi peran, umumnya menyamar sebagai penegak hukum untuk mengelabui korban dengan cara mengancam akan memproses hukum korban, karena telah menerima uang hasil kejahatan.

Pada 2021 lalu Polri juga telah menangkap sejumlah WNA China yang melakukan penipuan investasi. Mereka membuat situs penjualan mata uang kripto palsu dan menawarkan mata uang kripto dengan harga jual kembali yang jauh di atas harga pasaran sehingga akan menguntungkan pembeli. Untuk meyakinkan pembeli, para penipu juga membuat akun media sosial yang dilengkapi dengan berbagai testimoni fiktif. Kejahatan siber oleh WNA umumnya dilakukan dari wilayah perkotaan. Para pelaku umumnya menyewa ruko hingga rumah di kawasan elit untuk dijadikan tempat tinggal dan markas operasi. Mereka juga berupaya membaur, bahkan menikah dengan warga setempat untuk menghilangkan kecurigaan.

Menurut Teuku Rezasyah, pengajar Program Studi Hubungan Internasional Universitas Padjadjaran Bandung, keberadan warga asing yang melakukan tindak kejahatan siber di wilayah hukum Indonesia terjadi lemahnya sistem keimigrasian dan kapasitas aparat keamanan di Indonesia dalam mendeteksi aktivitas WNA di Indonesia. Pelaku kejahatan bisa dengan mudah masuk dan mendapatkan izin tinggal karena sistem keimigrasian hanya mengandalkan data yang mereka serahkan saat mengajukan permohonan visa. Saat mereka menunjukkan curriculum vitae yang baik, terlebih membawa sejumlah dana untuk berlibur, umumnya pihak imigrasi akan mudah memberikan visa. Sementara, setelah WNA masuk ke wilayah Indonesia, umumnya sulit bagi aparat untuk mengetahui keberadaan dan aktivitas mereka. Kapasitas surveilans aparat masih terbatas. Oleh sebab itulah menjadi penting meningkatkan kesadaran intelijen atau intelligence awareness, baik pada aparat maupun masyarakat.[54]

Intelijen adalah kepintaran untuk memanfaatkan informasi untuk tujuan pengambilan keputusan. Teori ini berkaitan dengan teori angsa hitam (*black swan*) dan teori gajah hitam (*black elephants*) untuk keamanan nasional. Teori ini menggambarkan satu risiko dalam dua perspektif. Angsa Hitam dan Gajah Hitam keduanya menggambarkan peristiwa bahaya dengan dampak tinggi, paparan tinggi, dan kerentanan tinggi tetapi dilihat dari dua sudut pandang yang berbeda. Dengan pengetahuan tetapi tanpa pengakuan,

[54] https://www.kompas.id/baca/polhuk/2022/06/15/mencegah-indonesia-jadi-surga-kejahatan-warga-negara-asing

Angsa Hitam menjadi Gajah Hitam. Keduanya berpotensi menimbulkan dampak bencana. Penggunaan teori ini berkaitan dengan kelanjutan dari Teori *Chaos* dan kompleksitas milik Edward Lorenz (1975). Kesemua teori ini berkaitan dengan peringatan untuk menjaga keamanan nasional dari ancaman nyata maupun potensial yang dihadapi dalam kehidupan nasional.[55]

Diperlukan pendidikan yang lebih intens dan spesifik untuk aparat, baik yang berasal dari kepolisian, keimigrasian, maupun Badan Intelijen Negara (BIN) untuk meningkatkan kemampuannya dalam melihat peragai dan aktivitas WNA yang mencurigakan di Indonesia. Aparat keamanan dan intelijen perlu memahami alur dan logika kejahatan kerah putih yang kerap dilakukan WNA. Dengan begitu, pergerakan orang, surat-menyurat, sandi, dan keuangan yang dilakukan bisa dibaca dan ditelusuri.

Pada sisi lain, jika melihat data Anev Bareksrim Polri. Selama tiga tahun ke belakang, tingkat penyelesaian kasus-kasus kejahatan siber tergolong rendah. Pada tahun 2019, dari 4.586 kasus yang diterima Polri hanya 2.282 kasus (49,76 persen) yang berhasil diselesaikan. Jumlah tersebut menurun tajam pada tahun 2020, di mana dari 4.790 kasus, hanya 1.283 kasus (26,78 persen) yang berhasil dituntaskan. Sementara pada tahun 2021, dari 3.270 kasus kejahatan siber, terdapat 1.780 kasus (54,43 persen) berhasil diselesaikan. Kompleksitas kasus, sulitnya mendapatkan dan mengamankan barang bukti, keterbatasan SDM dan anggaran menjadi sejumlah persoalan yang harus dihadapi kepolisian saat ini.

Berdasarkan paparan di atas, rendahnya literasi digital masyarakat banyak mempengaruhi kesadaran masyarakat untuk membangun kesigapan dalam menghadapi ancaman kejahatan digital Akibat tidak sedikit masyarakat yang menjadi korban kejahatan digital di Indonesia. Pada sisi lain, pemerintah dinilai belum optimal dalam menjalankan berbagai kewenangan dan tanggung jawabnya dalam membangun kewaspadaan nasional terhadap ancaman kejahatan digital yang kini terus menggerus ketangguhan ketahanan nasional.

[55] Margaretha Hanita, 2019, Pemikiran-Pemikiran Stratejik Intelijen, UI Publishing, Jakarta

16. Penerapan Kewaspadaan Nasional Terhadap Kejahatan Digital Guna Meningkatkan Ketahanan Nasional

Kesadaran bahwa nilai ekonomi digital Indonesia merupakan paling besar di Asia Tenggara, semestinya menjadi cambuk bagi seluruh *stakeholder* untuk bersama-sama memperkuat keamanan siber Indonesia. Menurut data yang dirilis oleh *e-Governance Academy Foundation*, Malaysia menjadi negara yang memiliki tingkat keamanan siber terbaik di Asia Tenggara pada tahun 2021. Negara ini memiliki skor indeks keamanan siber sebesar 79,22 poin. Skor ini mengalahkan negara Singapura berada di urutan kedua dengan skor sebesar 71,43 poin. Disusul Thailand, Filipina dan Brunei Darusalam. Sedangkan Indonesia jauh tertinggal berada di urutan keenam dengan skor sebesar 38,96 poin.[56]

Sebagai negara ekonomi digital terbesar di ASEAN, sudah semestinya Indonesia memiliki dukungan keamanan digital yang terbaik pula. Hal tersebut bisa diwujudkan jika kewaspadaan nasional terhadap kejahatan digital sudah terbangun kuat di semua lapisan masyarakat. Kewaspadaan Nasional (Padnas) dapat diartikan sebagai suatu kualitas kesiapan dan kesiagaan yang dimiliki oleh bangsa untuk mampu mendeteksi, mengantisipasi sejak dini, dan melakukan aksi pencegahan berbagai bentuk dan sifat potensi ancaman terhadap NKRI.[57]

Kewaspadaan nasional harus bertolak dari keyakinan ideologis dan nasionalisme yang kukuh serta perlu didukung oleh usaha-usaha pemantauan sejak dini dan terus-menerus terhadap berbagai implikasi dari situasi serta kondisi yang berkembang baik di dalam maupun di luar negeri. Dalam tataran operasional, kewaspadaan nasional digunakan untuk menciptakan suatu sistem deteksi dan peringatan dini (*early warning system*). Sistem tersebut diwujudkan melalui serangkaian upaya cegah dini, tangkal dini dan tanggap dini dalam menghadapi ancaman.

---

[56] https://dataindonesia.id/digital/detail/malaysia-miliki-keamanan-siber-terbaik-di-asean diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.
[57] Tim Pokja Bahan Ajar BS. Padnas, 2022, Modul Bidang Studi Kewaspadaan Nasional, Lemhannas, Jakarta

a. Cegah Dini

Berkaitan dengan ancaman kejahatan digital, maka sejumlah upaya yang bisa dilakukan untuk melakukan upaya cegah dini dapat dimulai dengan memetakan jenis kejahatan dan perkembangan modus operandi dari kejahatan digital yang berpotensi marak terjadi di Indonesia. Hal ini membutuhkan sinergitas dari BSSN, institusi intelijen (BIN), Polri dan Kemenkominfo guna mengumpulkan data kejahatan digital baik yang terjadi di dalam negeri maupun di luar negeri. Pemetaan ini penting untuk mengetahui modus operandi hingga seberapa besar bahaya dan potensi kerugian yang bisa terjadi. Dari data tersebut bisa dianalisa upaya apa yang bisa dilakukan untuk mencegah dan memproteksi agar kejahatan digital tersebut tidak berdampak luas di masyarakat. Saat semua kejahatan sudah terpetakan, maka menjadi kewajiban Kemenkominfo bekerja sama dengan media untuk menyebarkan informasi tersebut kepada masyarakat dengan tujuan agar masyarakat memiliki pengetahuan adanya potensi ancaman dan bagaimana mengantisipasinya.

Upaya cegah dini lain adalah melakukan intervensi untuk memperkuat literasi digital masyarakat. Hal ini penting karena akan menjadi modal dasar dalam mengembangkan kewaspadaan nasional secara lebih holistik yang melibatkan seluruh komponen bangsa. Seperti telah dijelaskan sebelumnya, saat ini sebagian besar masyarakat tidak memiliki bekal literasi digital yang memadai sehingga mereka tidak memiliki pengetahuan yang cukup terhadap kejahatan digital yang sewaktu-waktu bisa mengancam dirinya. Mayoritas pengguna teknologi di Indonesia masih berada pada tingkat dasar dan menengah dalam pengusaan kemampuan dan pengetahuan mengenai teknologi digital. Artinya, masih banyak yang belum kompeten untuk aktif memperbarui diri dengan informasi keamanan digital dan penipuan. Selama ini banyak dari masyarakat yang tahu menggunakan teknologi digital dan daring tapi tidak mengerti bagaimana cara melindungi diri dari ancaman kejahatan digital.

Fakta empiris di lapangan selama ini menunjukkan bahwa banyak hal negatif dan kejahatan digital yang mengiringi perkembangan teknologi informatika di Indonesia. Semakin meningkatnya kasus pornografi, penipuan,

penyebaran berita hoaks, perjudian online, eksploitasi seksual pada anak, perundungan, ujaran kebencian bahkan radikalisme berbasis digital kerap mengancam persatuan dan kesatuan bangsa. Semua terjadi karena para pelaku yang memanfaatkan ruang digital belum memiliki kecakapan dan pemahaman sepenuhnya mengenai bagaimana seharusnya memanfaatkan internet dengan bijak dan benar.

Upaya untuk memperkuat literasi digital masyarakat semestinya dilakukan sejak dini dengan memasukan literasi digital ke dalam kurikulum pendidikan nasional. Jika saat ini pelajaran teknologi informatika dan komunikasi hanya mencakup kompetensi teknis, maka ke depannya, pelajaran ini harus menyertakan aspek literasi digital. Pelajaran tersebut perlu diberikan mulai dari siswa SD sampai SMA. Dalam pelajaran tersebut selain diberikan pengetahuan mengenai ragam ancaman kejahatan digital dan bagaimana modus operandinya, mereka juga perlu diajarkan memiliki kemampuan cara mengamankan diri agar tidak menjadi korban kejahatan digital. Para siswa diajarkan untuk berpikir kritis dan tidak begitu saja mudah percaya terhadap informasi dan berita yang mereka baca di media sosial. Hal ini penting agar generasi muda tidak terjebak ikut menyebarkan berita dan informasi hoax yang ada di media sosial.

Orang tua yang sudah memberikan fasilitas ponsel pintar kepada anak-anaknya perlu memberikan pengawasan dan edukasi mengenai beragam kejahatan yang ada dunia maya. Anak-anak perlu diajarkan untuk melapor kepada orang tuanya jika ada orang yang tidak dikenal menghubungi mereka baik melalui telepon maupun berbagai kanal media sosial. Sebab bagi anak-anak, media sosial hingga game online bisa menjadi pintu masuk para predator. Demikian pula sebaliknya, generasi milenial yang cenderung memiliki kemampuan dan literasi digital yang lebih baik, bisa memandu dan mengajarkan pengetahuan mengenai keamanan digital kepada orang tua yang kebetulan gaptek, sehingga mereka mengetahui apa saja yang harus dihindari dan dijaga agar tidak menjadi korban kejahatan digital. Dalam hal ini peran keluarga bisa saling melengkapi dan menjaga satu dengan yang lain agar tidak ada anggota keluarga yang karena ketidaktahuannya menjadi korban kejahatan siber.

Edukasi tentang keamanan digital juga diajarkan kepada para pelaku usaha UMKM sebelum menjalankan transformasi digital terhadap usaha miliknya. Sebab, kejahatan digital yang berbasis manipulasi psikologis (social engineering) bisa menjadi ancaman yang membuat mereka mengalami kerugian finansial. Tipe manipulasi psikologis ini tidak memanfaatkan kerentanan sistem namun memanfaatkan kelengahan dan kelemahan kompetensi digital si pengguna teknologi. Dengan semakin banyaknya pelaku usaha yang bermigrasi ke online, maka para pelaku manipulasi psikis ini pun mengincar merek.

Para pelaku usaha perlu diajarkan untuk memiliki kewaspadaan untuk mengamankan data pribadinya. Mereka perlu mengerti apa konsekuensi yang bisa menimpanya jika sembarangan memberikan informasi dan data pribadi kepada orang yang tidak dikenal yang menghubunginya. Edukasi terkait dengan literasi keamanan digital kepada pelaku UMKM ini tidak hanya menjadi tanggung jawab pemerintah, namun juga para penyedia layanan e-dagang yang akan digunakan oleh para pelaku usaha.

Selain orangtua, guru juga merupakan sosok dan figur yang sangat dibutuhkan dalam membantu menyukseskan program Literasi Digital Nasional, mengingat selama ini guru bisa dikatakan merupakan orangtua kedua bagi anak. Dalam memberikan materi pelajaran, guru perlu menyisipkan materi mengenai bagaimana pemanfaatan internet yang baik dan benar serta memberikan gambaran mengenai dampak negatif yang ditimbulkan akibat penyalahgunaan internet. Dengan demikian, diharapkan anak akan semakin bijak dalam mengoperasikan perangkat elektronik dan memanfaatkan perkembangan teknologi internet untuk berbagai kegiatan yang bersifat positif.

Lembaga swadaya masyarakat dan penggiat literasi digital bisa menjalin sinergi dengan pemerintah untuk lebih intens membuat beragam pelatihan baik daring maupun luring kepada masyarakat. Berbagai kampanye agar masyarakat terus meningkatkan literasi digitalnya perlu lebih masif digaungkan. Sementara peran media massa sangat penting dalam menggiring dan membentuk opini publik terkait pentingnya kemampuan literasi digital masyarakat perlu terus ditingkatkan. Masyarakat perlu

disadarkan bahwa pemberitaan mengenai kejahatan digital yang marak terjadi lebih dominan disebabkan karena kemampuan literasi digital masyarakat yang rendah.

Kecakapan agar aman bermedia digital masih perlu diperhatikan. Adapun kesadaran mengatur siapa yang dapat melihat unggahan, menonaktifkan opsi posisi geografis/GPS, membuat password yang aman, hingga mengidentifikasi e-mail yang berisi spam/virus/malware masih banyak yang tidak pernah melakukan dan tidak tahu. Kalaupun pernah melakukan, itu dilakukan dengan bantuan orang lain. Selain itu, kemampuan mengidentifikasi hoaks harus lebih ditingkatkan agar masyarakat tidak mudah terpengaruh oleh berita palsu di media sosial. Aspek pengetahuan terhadap keamanan digital dan etika digital juga perlu terus dikembangkan agar masyarakat mengerti konsekuensi dan tanggung jawab dalam memanfaatkan teknologi digital. Indonesia bisa mencontoh keberhasilan praktik literasi digital negara maju, seperti Australia, Kanada, Finlandia, Swedia, dan Denmark. Negara tersebut mengajarkan literasi digital berbasis kemampuan berpikir kritis kepada masyarakatnya sejak dini. Hasilnya, negara itu memiliki daya tahan tinggi menangkal disinformasi dan tercatat memiliki demokrasi berkualitas.[58]

b. Tangkal Dini

Langkah selanjutnya adalah melakukan upaya tangkal dini. Langkah ini merupakan upaya menangkal terjadinya kejahatan digital di Indonesia. Langkah ini diawali dengan upaya BSSN untuk merancang dan membangun infrasktruktur dan teknologi keamanan digital yang lebih kuat. Hal ini penting agar eksosistem digital Indonesia tidak rentan oleh serangan siber atau mudah ditembus dan disusupi virus atau malware. Dalam hal ini BSSN semestinya tidak hanya bertanggung jawab untuk memastikan infrastruktur dan teknologi keamanan yang dimiliki oleh seluruh lembaga pemerintahan cukup memadai untuk menangkal serangan dan kejahatan siber, tapi BSSN

[58] https://www.kompas.id/baca/polhuk/2020/01/22/literasi-digital-bakal-masuk-ruang-kelas/ diakses pada tanggal 10 Agustus 2022 pukul 23.00 WIB.

juga dapat memberikan pendampingan dan pembinaan terhadap korporasi swasta di Indonesia agar mampu mengembangkan standar teknologi keamanan yang sama tangguhnya. Ini artinya pemerintah perlu merumuskan satu standar keamanan siber nasional yang berlaku untuk semua. Standar akan terus ditinjau dan diperbaiki seiring dengan ditemukannya teknologi keamanan siber yang baru dan/atau seiring dengan ditemukan jenis ancaman kejahatan digital baru.

Penguatan upaya tangkal dini juga dapat diwujudkan dengan memperbaiki dan menyempurnakan regulasi. Oleh sebab itu pemerintah perlu segera merumuskan revisi undang-undang Informasi dan Transaksi Elektronik (ITE). Perbaikan signifikan perlu dilakukan dengan memperbaiki redaksional hukum terhadap bunyi pasal-pasal yang selama ini mengandung pengertian yang multitafsir sehingga bisa disalahgunakan sebagai sarana melakukan kriminalisasi kepada mereka yang berpikir kritis. Selain itu, cakupan UU ITE perlu diperluas dengan menambahkan sejumlah aturan dan sanksi terhadap berbagai kejahatan digital yang belum diatur sebelumnya, misal terkait dengan kasus prostitusi online, penyebaran konten radikalisme dan terorisme hingga kejahatan *doxing*.

Selain melakukan revisi terhadap UU ITE, upaya memperkuat regulasi dilakukan dengan mendorong segera diselesaikannya pembahasan dan disahkannya RUU Perlindungan Data Pribadi dan RUU Keamanan dan Ketahanan Siber. Kedua regulasi ini diperlukan untuk mengisi kekosongan regulasi terkait dengan keamanan dan ketahanan siber di Indonesia. Hal ini membutuhkan kesepahaman dan komitmen kuat antara pemerintah dan DPR untuk menyelesaikan RUU yang sudah beberapa kali masuk dalam prolegnas.

Bentuk upaya tangkal dini lain yang bisa dilakukan sebagai bagian dari kewaspadaan nasional adalah pengawasan ketat hingga pencekalan terhadap masuknya pelaku-pelaku kejahatan digital asing ke Indonesia. Seperti sudah disinggung sebelumnya, kondisi pengamanan terhadap WNA yang masuk ke Indonesia sering disalahgunakan para pelaku kejahatan siber terorganisir untuk menjadikan Indonesia sebagai basis operasional mereka. Hal ini perlu upaya pencegahan dengan meningkatkan hubungan bilateral

dan multilateral dengan berbagai negara sahabat sehingga antarnegara bisa berbagi informasi mengenai identitas pelaku kejahatan digital di negaranya. Informasi ini berguna bagi intelijen dan imigrasi untuk melakukan tindakan diperlukan terhadap masuknya WNA pelaku kejahatan siber ke Indonesia.

c. Tanggap Dini

Selain memperkuat upaya cegah dini dan tangkal dini, implementasi kewaspadaan nasional juga dilakukan dengan memperkuat upaya tanggap dini. Langkah ini penting untuk bisa segera meredam dan mengatasi kejahatan digital yang sudah terlanjur terjadi agar dampak kerugian bisa dihilangkan atau setidaknya diminimalkan, sementara pelakunya bisa segera ditindak dan diproses sesuai hukum yang berlaku.

Salah satu upaya yang termasuk dalam area tanggap dini adalah program BSSN untuk membentuk Computer Security Incident Response Team (CSIRT). Tim bentukan BSSN rencanakan akan ditempatkan di setiap lembaga kementerian dan pemerintah daerah sebagai satu tim reaksi cepat yang bertanggung jawab menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber. Keberadaan CSIRT diharapkan bisa membendung serangan siber baik dalam bentuk *malware*, *trojan*, *denial of services* atau aktivitas lain yang berpotensi mengganggu ketersediaan layanan. Pembentukan 121 CSIRT inilah yang didorong untuk bisa dipercepat guna meningkatkan ketangguhan bangsa Indonesia dalam menghadapi serangan siber dan kejahatan digital.

Hal lain yang perlu diperkuat adalah kesiapan aparat penegak hukum untuk mencari dan menindak pelaku kejahatan digital, serta kemampuan untuk meminimalkan dampak kejahatan digital yang terjadi. Hal ini membutuhkan tidak hanya peningkatan anggaran dan penambahan personil Polri pada Direktorat Tindak Pidana Siber Bareskrim Polri, tetapi juga perlu penguatan kapasitas dan kompetensi SDM agar mampu meningkatkan kualitas penanganan kejahatan digital di Indonesia dengan meningkatkan angka penyelesaian kasus-kasus kejahatan siber di Indonesia sehingga penegakan hukum terhadap kejahatan siber/digital semakin baik dan mampu memberikan efek jera terhadap pelaku kejahatan siber.

Sementara dari sisi partisipasi masyarakat, upaya tanggap dini bisa dilakukan dengan melaporkan segera jika masyarakat mengetahui atau menjadi korban kejahatan digital sehingga aparat penegak hukum bisa cepat merespon mengingat kecepatan masyarakat melapor berperan besar bagi polri untuk bisa mengamankan barang bukti kejahatan dan melakukan pelacakan terhadap pelaku kejahatan.

Harapannya melalui implementasi kewaspadaan nasional terhadap kejahatan digital yang diwujudkan melalui penguatan upaya cegah dini, tangkal dini dan tanggap dini kejahatan digital, kasus kejahatan digital di Indonesia bisa ditekan sehingga ketangguhan ketahanan nasional bisa tetap tangguh.

TANHANA DHARMMA MANGRVA

BAB IV
PENUTUP

17. Simpulan

Datangnya pandemi Covid-19 telah mendorong terjadinya percepatan proses transformasi digital di tengah masyarakat Indonesia. Situasi ini pada satu sisi menghadirkan beragam manfaat bagi kehidupan masyarakat, namun pada sisi lain membuat masyarakat rentan menjadi korban kejahatan digital. Penyebabnya, literasi teknologi digital yang terbatas membuat masyarakat belum mengerti betul cara melindungi diri dan memanfaatkan teknologi agar aman dari kejahatan digital.

Dilihat dari anatomi kejahatan digital yang ada selama ini, terdapat sedikitnya tiga belas jenis kejahatan digital yang marak terjadi di Indonesia, mulai dari peretasan dan pencurian data, penipuan daring (*phishing*), penyebaran kabar bohong dan konten ujaran kebencian, pembajakan akun, hingga kegiatan mata-mata menggunakan teknologi digital marak terjadi di Indonesia. Hal tersebut disebabkan oleh sejumlah faktor, mulai dari kesalahan pengguna akibat minimnya literasi digital masyarakat, kerentanan sistem, infrastruktur dan sistem keamanan siber yang masih rapuh, masih adanya kekosongan regulasi, hingga belum optimalnya penegakan hukum terhadap kasus-kasus kejahatan digital di Indonesia.

Kondisi tersebut mengakibatkan kondisi di mana perkembangan ancaman kejahatan digital, sudah mempengaruhi ketangguhan ketahanan nasional Indonesia. Fenomena tersebut dapat dilihat dari semakin banyaknya masyarakat yang korban kejahatan digital karena ketidaktahuan mereka. Kejahatan peretasan dan pencurian data yang telah berhasil membawa miliaran data pribadi masyarakat dan menjualnya ke forum *darkweb*. Kedaulatan dan wibawa negara pun mulai dipertaruhkan ketika data intelijen dan komunikasi kepada presiden yang sifatnya sangat rahasia bisa dibajak *hacker*. Sementara kekosongan regulasi membuat penyedia layanan elektronik baik dari institusi pemerintah maupun swasta yang terbukti tidak mampu menjaga data pribadi masyarakat yang dikelolanya tidak diberikan sanksi hukum. Demikian pula, rendahnya angka penyelesaian

kasuskejahatan digital memperlihatkan belum optimalnya penegakan hukum di Indonesia. Tidak mengherankan jika kemudian Indonesia dijadikan wilayah operasi organisasi kejahatan internasional.

Kondisi di atas menggambarkan bagaimana urgensi membangun kewaspadaan nasional terhadap kejahatan digital guna memperkuat ketahanan nasional Indonesia. Kewaspadaan nasional (Padnas) penting dibangun atas dasar nasionalisme yang dibangun dari rasa peduli dan tanggung jawab seorang warga negara terhadap kelangsungan hidup bermasyarakat, berbangsa dan bernegara dari potensi ancaman. Padnas menjadi suatu bentuk kesiapsiagaan yang dimiliki suatu bangsa guna mendeteksi, mengantisipasi sejak dini, dan melakukan serangkaian aksi pencegahan terhadap munculnya potensi ancaman.

Konsep kewaspadaan nasional terhadap kejahatan digital tersebut diwujudkan melalui adanya sistem deteksi dini, yang meliputi upaya cegah dini, tangkal dini dan tanggap dini terhadap munculnya ancaman kejahatan digital. Upaya cegah dini terhadap kejahatan digital bisa dimulai dengan memetakan perkembangan modus dan jenis kejahatan digital yang berpotensi marak terjadi di Indonesia, membangun infrastruktur dan teknologi keamanan digital nasional yang lebih kuat, memberikan pendampingan dan standarisasi nasional teknologi keamanan yang digunakan oleh korporasi swasta di Indonesia, hingga yang paling penting adalah meningkatkan literasi digital masyarakat khususnya berkaitan dengan keamanan digital. Upaya tangkal dini dapat diwujudkan melalui kesiapan regulasi perundang-undangan di Indonesia dalam menghadapi berbagai bentuk kejahatan digital. Sedangkan upaya tanggap dini diwujudkan melalui kemampuan untuk meminimalkan dampak kejahatan digital dan kesiapan aparat penegak hukum untuk mencari dan menindak pelaku kejahatan digital.

Kewaspadaan nasional terhadap ancaman kejahatan digital tersebut akan lebih optimal jika sistem deteksi dan peringatan dini tersebut merupakan hasil dari kerja bersama. Pelibatan semua potensi bangsa tersebut diyakini akan lebih efektif untuk mengantisipasi dan mengatasi

ancaman kejahatan digital sehingga tidak mempengaruhi ketahanan nasional Indonesia.

18. Rekomendasi

Berdasarkan paparan di atas, sejumlah rekomendasi konkrit yang dapat disampaikan kepada pihak-pihak terkait berhubungan dengan implementasi kewaspadaan nasional terhadap kejahatan digital guna meningkatkan ketahanan nasional, antara lain:

a. Upaya untuk memperkuat cegah dini, dilakukan melalui:
   1) Kemendikbud memasukan materi mengenai literasi digital, termasuk di dalamnya berkaitan dengan literasi keamanan digital dalam kurikulum pendidikan formal di Indonesia secara berjenjang mulai dari tingkat sekolah dasar.
   2) Kemenkominfo melakukan kampanye secara masif di berbagai media termasuk media sosial mengenai bahaya ancaman kejahatan digital guna meningkatkan *awareness* masyarakat terhadap ancaman kejahatan digital yang semakin marak terjadi.
   3) Kemenkominfo bersama BSSN dapat menyusun dan mempublikasikan tutorial bagaimana membangun kewaspadaan nasional terhadap kejahatan digital melalui sejumlah upaya untuk mengamankan diri agar tidak menjadi korban kejahatan digital.
   4) Kemenkominfo, BSSN, Polri dan difasilitasi Kemenlu perlu meningkatkan kerja sama dengan negara-negara sahabat baik dalam bentuk bilateral maupun multilateral, guna bersama-sama memerangi kejahatan digital yang dilakukan oleh organisasi internasional yang melibatkan pelaku dan tempat kejadian perkara lintas negara.

b. Upaya untuk memperkuat tangkal dini, dilakukan melalui:
   1) Kemenkominfo bersama Kemenkumham dan BSSN menyiapkan draft revisi perbaikan terhadap UU Informasi dan Transaksi Elektronik untuk memperbaiki redaksional hukum sejumlah pasal karet yang multitafsir serta melengkapi dengan sejumlah pasal tambahan yang mengatur sanksi hukum terkait berbagai jenis

kejahatan digital yang selama ini belum diatur oleh undang-undang.

2) Kemenkominfo bersama Kemenkumham bersama DPR dapat segera menyelesaikan pembahasan RUU Perlindungan Data Pribadi dan segera mengesahkannya sebagai undang-undang untuk memperkuat aturan mengenai perlindungan data di Indonesia.

3) BSSN dapat membuat peta jalan bagaimana membangun infrastruktur keamanan siber di Indonesia yang kuat dan merancang satu standar teknologi keamanan nasional yang harus dimiliki oleh setiap institusi pemerintah dan korporasi di Indonesia sehingga sistem dan data-data digital yang dimilikinya tidak mudah dibobol oleh para penjahat siber.

c. Upaya untuk memperkuat tanggap dini, dilakukan melalui:

1) Kemenkominfo segera menyelesaikan target pembentukan 121 CSIRT yang ditempatkan di berbagai lembaga/kementerian dan pemerintahan daerah guna menjadi tim reaksi cepat dalam menghadapi insiden dan serangan siber.

2) BSSN bersama Polri dapat membentuk tim teknis untuk melakukan audit dan digital foresic pada setiap insiden dugaan peretasan untuk mengkonfirmasi apakah benar telah terjadi peretasan dan mencari titik lemah keamanan yang menjadi pintu masuk *hacker* untuk dilakukan perbaikan.

3) Polri dapat meningkatkan anggaran, jumlah personil dan kapasitas SDM yang ada di Direktorat Tindak Pidana Siber Bareskrim Polri sehingga mampu meningkatkan angka penyelesaian kasus-kasus kejahatan siber di Indonesia sehingga penegakan hukum terhadap kejahatan siber/digital semakin baik dan mampu memberikan efek jera terhadap pelaku kejahatan siber.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang RI Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentag Informasi dan Transaksi Elektronik

Buku-Buku

Huda, Miftahul. 2020. Keamanan Informasi. Surabaya: CV. Garuda Mas Sejahtera.

Ibrahim dan Sirait. 2018. Kejahatan Transfer Dana: Evolusi dan Modus Kejahatan Melalui Sarana Lembaga Keuangan Bank. Jakarta: Sinar Grafika.

Kurnia, Novi. 2019. Literasi Digital Keluarga: teori dan praktik Pendampingan Orangtua terhadap Anak dalam berinternet. Yogyakarta: Gajah mada University Press.

Margaretha Hanita, 2019, Pemikiran-Pemikiran Stratejik Intelijen, UI Publishing, Jakarta

Rahayu, dkk. 2021. Perempuan dan Literasi Digital: Antara Problem, Hambatan dan Arah Pemberdayaan. Yogyakarta: UGM Press.

Suherdi, dkk. 2021. Peran Literasi Digital di masa Pandemik. Deli Serdang: Cattleya Darmaya Fortuna

Tim Pokja Bahan Ajar Padnas. 2022. Materi Pokok Bidang Studi Kewaspadaan Nasional. Jakarta: Lemhannas RI.

Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Empat Konsensus Dasar Bangsa. Jakarta: Lemhannas RI.

Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Ketahanan Nasional. Jakarta: Lemhannas RI.

Tim Pokja Lemhannas RI. 2022. Modul Bidang Studi Wawasan Nusantara. Jakarta: Lemhannas RI.

Yurizal. 2018. Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia. Malang: Media Nusa Creative

Jurnal

Ahmadian dan Sabri. 2021. Teknik Penyerangan Phising pada Social Engineering Menggunakan Set dan Pencegahannya. Jurnal Djtechno Journal of Information Technology Research, Vol.2, Nomor 1, Juli 2021, Hal.13-20.

Aswandi, Muchsin dan Sultan. 2020. Perlindungan Data dan Informasi pribadi Melalui Indonesian Data Protection System (IDPS). Jurnal Legislatif, Volume 3 Nomor 2, Juni 2020, Hal. 167-190.

Huwaidi dan Destya. 2021. Mencegah Serangan Rekayasa Sosial dengan Human Firewall. Justin Jurnal Sistem dan Teknologi Informasi, Volume 10, Nomor 1, Januari 2022, Hal.107-112

Kusumoningtyas dan Puspitasari. 2020. Dilema Hak Perlindungan Data pribadi dan Pengawasan Siber: Tantangan di Masa Depan. Jurnal LEGISLASI INDONESIA Vol 17, No. 2 - Juni 2020, Hal.234-250

Rumlus dan Hartadi. 2020. Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. Jurnal HAM, Volume 11, Nomor 2, Agustus 2020, Hal. 285-299.

Situmeang. 2021. Penyalahgunaan Data Pribadi Sebagai Bentuk kejahatan Sempurna Dalam Perspektif Hukum Siber. Jurnal Sasi, Volume 27Nomor 1, Januari-Maret 2021, Hal.38-52

Website

http://repository.lppm.unila.ac.id/34746/1/full%20paper%20artikel%20IICIS%202021..pdf diakses pada tanggal 14 Mei 2022 pukul 22.00 WIB.

https://cyberthreat.id/read/6779/Pakar-Jika-Data-Tokopedia-Bukalapak-Dikombinasikan-dengan-Data-KPU-yang-Bocor-Ini-Berbahaya diakses pada tanggal 2 Agustus 2022 pukul 21.30 WIB.

https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://dataindonesia.id/digital/detail/malaysia-miliki-keamanan-siber-terbaik-di-asean diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.

https://datareportal.com/reports/digital-2022-indonesia diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB

https://ekbis.sindonews.com/read/708377/178/duh-asia-jadi-wilayah-terbesar-ancaman-serangan-siber-1646885026 diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.

https://eprints.umm.ac.id/51432/3/BAB%20II.pdf diakses pada tanggal 12 Mei 2022 pukul 20.00 WIB

https://glints.com/id/lowongan/social-engineering/#.Ypbub8NBzb0 diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.

https://inet.detik.com/security/d-6227093/indeks-keamanan-siber-ri-ke-24-di-tingkat-global-ke-3-di-asean diakses pada tanggal 11 Agustus 2022 pukul 18.00 WIB.

https://katadata.co.id/desysetyowati/digital/5eb1268ec4a86/marak-penipuan-mitra-gofood-gojek-data-rekening-jadi-incaran diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://money.kompas.com/read/2021/10/26/173828526/imbas-kejahatan-cyber-bank-bank-dunia-merugi-rp-1420-triliun-per-tahun diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.

https://nasional.kompas.com/read/2022/08/22/15281161/bin-bantah-data-agen-intelijen-bocor diakses pada tanggal 29 Agustus 2022 pukul 21.30 WIB.

https://raharja.ac.id/2020/04/29/apa-itu-cyber-crime/ diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.

https://repository.usd.ac.id/37599/2/162114041_full.pdf diakses pada tanggal 12 Juni 2022 pukul 21.00 WIB.

https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber diakses pada tanggal 7 April 2022 pukul 23.00 WIB.

https://www.cnbcindonesia.com/tech/20220621062955-37-348746/mengenal-social-engineering-dan-4-modus-bobol-rekening diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://www.ekrut.com/media/fraud-adalah diakses pada tanggal 30 Mei 2022 pukul 20.00 WIB.

https://www.kemenkeu.go.id/publikasi/berita/nilai-ekonomi-digital-indonesia-usd70-miliar-tertinggi-di-asia-tenggara/ diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://www.kominfo.go.id/content/detail/35229/skb-pedoman-implementasi-uu-ite-ditandatangani-menko-polhukam-berharap-beri-perlindungan-pada-masyarakat/0/berita diakses pada tanggal 1 Agustus 2022 pukul 21.30 WIB.

https://www.kompas.id/baca/gaya-hidup/2020/07/15/palo-alto-keamanan-siber-indonesia-ke-arah-yang-tepat diakses pada 2 Agustus 2022 pukul 22.15 WIB.

https://www.kompas.id/baca/ilmu-pengetahuan-teknologi/2020/02/18/doxing-secara-terstruktur-terjadi diakses pada tanggal 29 Agustus 2022 pukul 21.00 WIB

https://www.kompas.id/baca/ilmu-pengetahuan-teknologi/2020/11/30/bisa-menggunakan-teknologi-saja-tak-cukup/ diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB

https://www.kompas.id/baca/opini/2022/07/10/rantai-keamanan-data-topang-transformasi-digital diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://www.kompas.id/baca/opini-publik/2022/02/06/membangun-perisai-keamanan-data diakses pada tanggal 7 April 2022 pukul 22.00 WIB.

https://www.kompas.id/baca/polhuk/2020/01/22/literasi-digital-bakal-masuk-ruang-kelas/ diakses pada tanggal 10 Agustus 2022 pukul 23.00 WIB.

https://www.kompas.id/baca/polhuk/2021/07/01/kapolri-ubah-pendekatan-penanganan-kejahatan-siber diakses pada tanggal 7 April 2022 pukul 23.00 WIB.

https://www.kompas.id/baca/polhuk/2022/06/15/mencegah-indonesia-jadi-surga-kejahatan-warga-negara-asing

https://www.kompas.id/baca/utama/2019/12/21/jumlah-kasus-kriminalisasi-uu-ite-meningkat/ diakses pada tanggal 1 Agustus 2022 pukul 21.30 WIB.

https://www.liputan6.com/bisnis/read/4563758/279-data-bpjs-kesehatan-bocor-dpr-ketahanan-siber-indonesia-lemah diakses pada tanggal 2 Agustus 2022 pukul 21.30 WIB.

https://www.liputan6.com/tekno/read/4359908/selama-pandemi-covid-19-gofood-punya-lebih-dari-250-ribu-merchant-baru diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

https://www.mckinsey.com/featured-insights/coronavirus-leading-through-the-crisis/charting-the-path-to-the-next-normal/a-pandemic-digital-silver-lining-

companies-digitized-many-activities-20-to-25-times-faster-during-covid-19 diakses pada tanggal 29 Juli 2022 pukul 20.00 WIB.

https://www.tagar.id/pencurian-data-diperkirakan-meningkat-tahun-2022 diakses pada tanggal 10 Juni 2022 pukul 21.00 WIB

https://www.wartaekonomi.co.id/read367315/gegara-tranformasi-digital-indonesia-darurat-kejahatan-siber diakses pada tanggal 1 Agustus 2022 pukul 21.00 WIB.

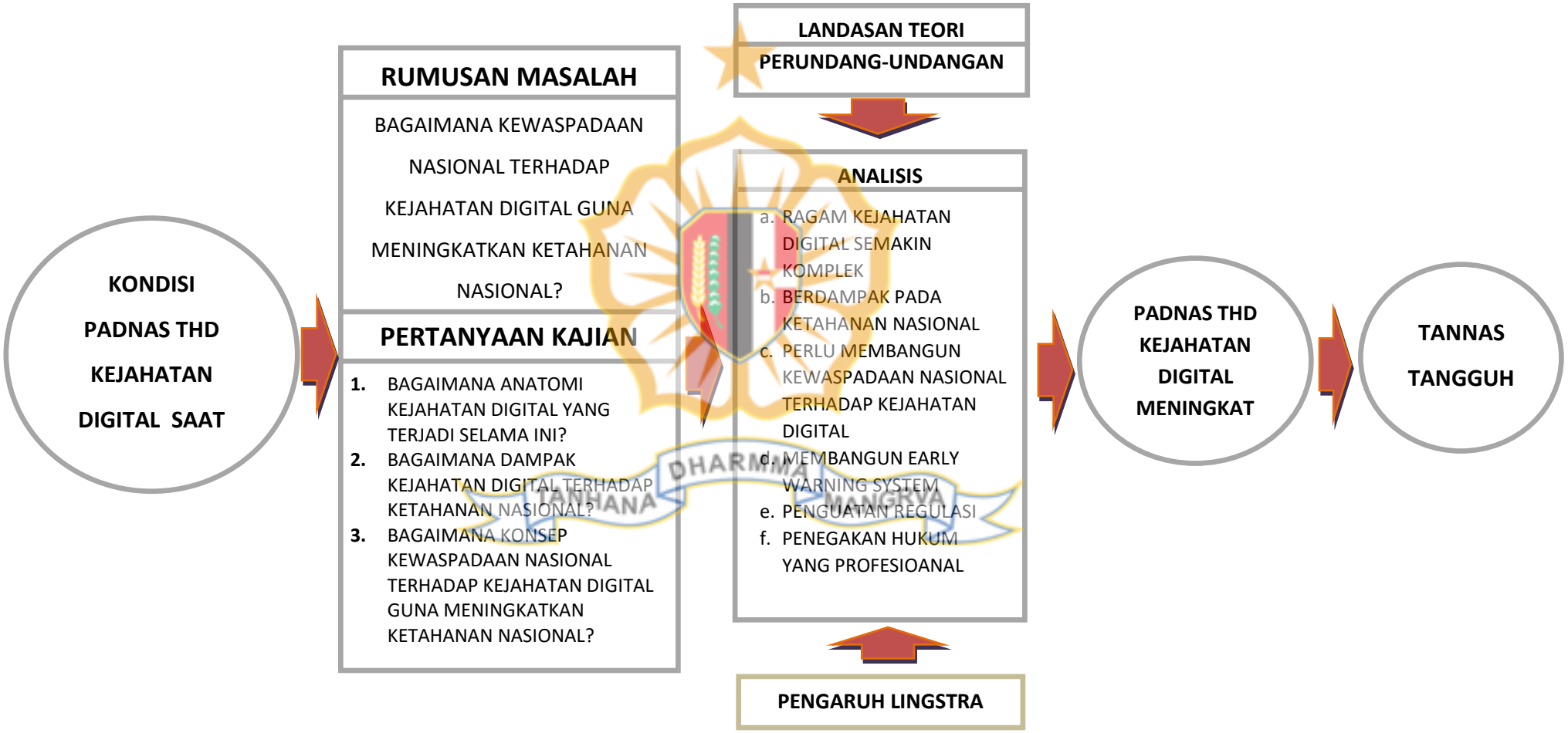
TANHANA DHARMMA MANGRVA

LAMPIRAN

ALUR PIKIR

KEWASPADAAN NASIONAL TERHADAP KEJAHATAN DIGITAL GUNA MENINGKATKAN KETAHANAN NASIONAL

`



LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA

RIWAYAT HIDUP PESERTA PPRA LXIV

A. Data Pribadi

Nama	: Bony Johannes Sanganadi Sirait S.I.K., M.H.
Pangkat	: Kombes Pol
Tempat/Tgl Lahir	: Bandung,14 April 1973
Jabatan	: Analis Kebijakkan Bidang Dalpers SSDM Polri
Instansi	: Mabes Polri
Agama	: Kristen
Alamat Email	: Bonysirait2@gmail.com

B. Pendidikan Umum

1. SD : 1986
2. SMP : 1989
3. SMA : 1992
4. S-2 : 2018

C. Pendidikan Polri

1. AKABRI : 1996
2. PTIK : 2007
3. SESPIMMEN : 2012

D. Pendidikan Kejuruan Kepolisian

1. KIBI PAJA AKPOL : 1996
2. PENDIDIKAN PERWIRA PERTAMA DASAR RESKRIM: 1997
3. JUR LAN PA SERSE UM : 2001
4. INTERNATIONAL LAW ENFORCEMENT ACADEMY BANGKOK, THAILAND : 2004
5. INTERNATIONAL LAW ENFORCEMENT ACADEMY BANGKOK, THAILAND : 2010
6. KURSUS JABATAN KAPOLRES : 2014

E. Pengalaman Jabatan

1. DANKI I SISWA DIKTUK BA SPN SAMPALI POLDA SUMUT POLRI : 06-08-1997
2. KANIT SERSEINTEL POLSEKTA MEDAN TIMUR POLTABES MEDAN POLDA SUMUT POLRI : 04-03-1998
3. KAPOLSEK TEBING TINGGI POLRES DELI SERDANG POLDA SUMUT POLRI : 09-07-1998
4. KASUBNIT SAT SERSE POLTABES MEDAN POLDA SUMUT POLRI : 22-01-1999
5. KANIT SAT SERSE POLTABES MEDAN POLDA SUMUT POLRI : 22-01-2000
6. KASAT SERSE POLRES SIMANUNGUNG POLDA SUMUT POLRI : 22-01-2001
7. KAPOLSEK PATUMBAK POLRESTABES MEDAN POLDA SUMUT (IIIB1) : 01-10-2001
8. WAKA SAT RESKRIM POLTABES MEDAN POLDA SUMUT POLRI : 22-01-2004
9. KATIM PENETRASI SUBDEN PENINDAK DEN 88 AT DIT RESKRIM POLDA SUMUT POLRI : 22-01-1005
10. KATIM NEGOSIATOR DEN 88 AT DIT RESKRIM POLDA SUMUT POLRI : 03-08-2005
11. PAMA PTIK (DLM RANGKA DIK PTIK) POLRI : 03-05-2007
12. PAMA POLDA MALUKU : 19-12-2007
13. KASI RENOPS SUBDIT BINOPS DIT POLAIR POLDA MALUKU POLRI : 11-02-2008
14. KASI BINGAKUM SUBDIT BINOPS DIT POLAIR POLDA MALUKU POLRI : 04-08-2008
15. WAKAPOLRES KEPULAUAN ARU POLDA MALUKU (IIIB1) : 30-09-2009
16. KANIT SUBDIT 1 DITRESKRIMUM POLDA MALUKU (IIIB2) : 29-10-2010
17. KASUBBAGMUTJAB BAGBINKAR ROSDM POLDA MALUKU (IIIB2) : 21-04-2011
18. KABAGBINKAR ROSDM POLDA MALUKU (IIIA1) : 28-11-2011
19. KASATROLDA DITPOLAIR POLDA MALUKU (IIIA2) : 09-04-2012
20. PAMEN LEMDIKLAT POLRI : 21-11-2012
21. KABAGBINSIS PUSDIK RESKRIM LEMDIKLAT POLRI (IIIA2) : 04-12-2012
22. KAPOLRES MANDAILING NATAL POLDA SUMUT (IIIA2) : 30-10-2014
23. KAPOLRES TAPANULI TENGAH POLDA SUMUT (IIIA2) : 02-04-2015
24. KABAGDALPERS ROSDM POLDA SUMUT (IIIA1) : 28-04-2016
25. KABAGBINKAR ROSDM POLDA SUMUT (IIIA1) : 18-04-2017

TANHANA DHARMMA MANGRVA

26. ASSESOR UTAMA POLRI
(BAGPENKOMPETEN ROBINKAR) (IIB3) : 21-12-2018
27. KARO SDM POLDA BALI (IIB2) : 03-02-2020

F. Data Keluarga

1. Nama Istri : Tety Luciana Purba
2. Nama Anak : Johna Samuel Oktosana Sirait
3. Nama Anak : Joshua Barachel Novalino Sirait

Jakarta, 10 Oktober 2022

BONY JOHANNES SANGANADI SIRAIT, S.I.K., M.H.
KOMBES POL NRP 74040739

TANHANA DHARMMA MANGRVA