Dr. Kiki Kristanto, S.H., M.H.
Dr. Rakhmat Baihaki, S.H., M.H.

PT MEDIA PENERBIT INDONESIA

BUKU REFERENSI

TINDAK PIDANA SIBER DI INDONESIA

REGULASI, TANTANGAN, DAN PENEGAKAN HUKUM

TINDAK PIDANA SIBER DI INDONESIA

REGULASI, TANTANGAN, DAN PENEGAKAN HUKUM

Dr. Kiki Kristanto, S.H., M.H.
Dr. Rakhmat Baihaki, S.H., M.H.

PT MEDIA PENERBIT INDONESIA

TINDAK PIDANA SIBER DI INDONESIA

REGULASI, TANTANGAN, DAN PENEGAKAN HUKUM

Ditulis oleh:

Dr. Kiki Kristanto, S.H., M.H.
Dr. Rakhmat Baihaki, S.H., M.H.

Hak Cipta dilindungi oleh undang-undang. Dilarang keras memperbanyak, menerjemahkan atau mengutip baik sebagian ataupun keseluruhan isi buku tanpa izin tertulis dari penerbit.

ISBN: 978-634-7184-75-7
IV + 203 hlm; 18,2 x 25,7 cm.
Cetakan I, Juni 2025

Desain Cover dan Tata Letak:
Melvin Mirsal

Diterbitkan, dicetak, dan didistribusikan oleh
PT Media Penerbit Indonesia
Royal Suite No. 6C, Jalan Sedap Malam IX, Sempakata
Kecamatan Medan Selayang, Kota Medan 20131
Telp: 081362150605
Email: ptmediapenerbitindonesia@gmail.com
Web: https://mediapenerbitindonesia.com
Anggota IKAPI No.088/SUT/2024

KATA PENGANTAR

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Namun, di balik berbagai kemudahan yang ditawarkan, teknologi juga membuka peluang munculnya tindak kejahatan baru yang memanfaatkan dunia maya atau siber sebagai medianya. Kejahatan siber atau *cyber crime* telah menjadi ancaman global yang menimbulkan kerugian material maupun immaterial, baik bagi individu, organisasi, maupun negara.

Buku referensi ini disusun untuk memberikan pemahaman menyeluruh mengenai tindak pidana siber di Indonesia, mulai dari aspek normatif regulasi yang berlaku, tantangan yang dihadapi dalam praktik, hingga strategi penegakan hukum yang efektif. Dengan pendekatan multidisipliner, buku referensi ini tidak hanya membahas peraturan perundang-undangan, tetapi juga menganalisis kasus-kasus nyata, praktik penegakan hukum, serta potensi perbaikan kebijakan ke depan.

Semoga buku referensi ini dapat menjadi referensi bagi mahasiswa, akademisi, peneliti, praktisi hukum, serta seluruh pihak yang memiliki perhatian terhadap isu-isu hukum di dunia digital.

Salam Hangat,

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **ii**
BAB I PENGANTAR TINDAK PIDANA SIBER **1**
A. Definisi dan Karakteristik Kejahatan Siber 2
B. Sejarah dan Perkembangan Kejahatan Siber 5
C. Klasifikasi Tindak Pidana Siber 8
D. Dampak Sosial, Ekonomi, dan Keamanan dari Kejahatan Siber 11

BAB II KERANGKA HUKUM TINDAK PIDANA SIBER DI INDONESIA **15**
A. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) 16
B. KUHP dan Relevansinya terhadap Kejahatan Siber 19
C. Regulasi Perlindungan Data Pribadi 22
D. Perbandingan Regulasi Siber Indonesia dengan Negara Lain 25

BAB III JENIS-JENIS KEJAHATAN SIBER **29**
A. *Cyber Fraud* (Penipuan Online, *Skimming*, *Phishing*) 29
B. *Cyber Terrorism* dan Keamanan Nasional 34
C. *Cyber Bullying* dan Kejahatan terhadap Privasi 38
D. Penyebaran *Hoaks*, *Hate Speech*, dan Ujaran Kebencian .. 45
E. Peretasan dan Serangan Siber terhadap Infrastruktur Negara 51
F. Perdagangan Ilegal di Dark Web 58

BAB IV PENEGAKAN HUKUM DALAM KASUS TINDAK PIDANA SIBER **65**
A. Peran Kepolisian dan Penyidik dalam Menangani Kejahatan Siber 66
B. Bukti Elektronik dalam Proses Pembuktian Hukum 72

C. Peran Badan Siber dan Sandi Negara (BSSN) dalam Keamanan Digital 76
D. Tantangan dalam Investigasi dan Penuntutan Tindak Pidana Siber 82

BAB V TEROBOSAN HUKUM DALAM PENANGANAN KEJAHATAN SIBER 89
A. Penguatan Regulasi dan Harmonisasi UU ITE..... 89
B. Pengembangan Teknologi Forensik Digital 96
C. Peran *Artificial Intelligence* dalam Deteksi Kejahatan Siber 102
D. Upaya Pencegahan Melalui Literasi Digital 108

BAB VI CYBERCRIME DALAM KONTEKS INTERNASIONAL 115
A. Perjanjian dan Kerjasama Internasional dalam Penanganan Kejahatan Siber..... 116
B. *Cybercrime* Convention (Budapest Convention) dan Implikasinya bagi Indonesia 122
C. Peran INTERPOL dan ASEAN dalam Penanggulangan Kejahatan Siber..... 127
D. Studi Kasus Kejahatan Siber di Berbagai Negara 132

BAB VII KEJAHATAN SIBER DAN PERLINDUNGAN KORBAN ...137
A. Hak-Hak Korban Kejahatan Siber 137
B. Perlindungan Data Pribadi dan Keamanan Digital..... 144
C. Mekanisme Pengaduan dan Bantuan Hukum bagi Korban 151
D. Peran Masyarakat dalam Pencegahan Kejahatan Siber ... 157

BAB VIII MASA DEPAN PENANGGULANGAN TINDAK PIDANA SIBER 165
A. Tantangan Hukum di Era *Artificial Intelligence* dan Big Data..... 165
B. Keamanan Siber dalam Transformasi Digital Indonesia . 168
C. Kebijakan Pencegahan Kejahatan Siber di Sektor Publik dan Swasta 173

D. Menuju Sistem Keamanan Digital yang Lebih Kuat dan Berkeadilan 178

DAFTAR PUSTAKA 185
GLOSARIUM.....193
INDEKS 197
BIOGRAFI PENULIS 201
SINOPSIS 203

BAB I
PENGANTAR TINDAK PIDANA SIBER

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, mulai dari cara berinteraksi sosial hingga sistem ekonomi dan pemerintahan. Namun, di balik manfaat yang ditawarkan oleh era digital, muncul pula tantangan serius berupa tindak pidana siber yang kian kompleks dan sulit dikendalikan. Kejahatan yang memanfaatkan jaringan internet sebagai sarana utamanya ini tidak lagi terbatas pada wilayah geografis tertentu, melainkan bersifat lintas negara, berskala global, dan sering kali melibatkan pelaku yang tidak mudah dilacak. Di Indonesia, kemunculan tindak pidana siber mulai menjadi perhatian serius sejak meningkatnya kasus penipuan daring, pencurian data pribadi, penyebaran *hoaks*, hingga peretasan situs-situs pemerintah. Kejahatan ini tidak hanya mengancam keamanan informasi individu dan lembaga, tetapi juga mengganggu stabilitas sosial, politik, dan ekonomi negara. Oleh karena itu, perlindungan hukum terhadap kejahatan siber menjadi suatu keharusan yang mendesak, tidak hanya melalui regulasi formal seperti undang-undang, tetapi juga melalui penguatan kapasitas lembaga penegak hukum dan peningkatan literasi digital masyarakat. Dalam konteks ini, penting untuk memahami secara mendalam karakteristik tindak pidana siber, tantangan yang dihadapi dalam penanggulangannya, serta bagaimana sistem hukum di Indonesia merespons ancaman ini secara efektif dan adaptif.

A. Definisi dan Karakteristik Kejahatan Siber

1. Definisi Kejahatan Siber menurut Perspektif Nasional dan Internasional

Perkembangan teknologi informasi dan komunikasi (TIK) secara signifikan telah mengubah wajah kejahatan konvensional menjadi bentuk-bentuk kejahatan baru yang dikenal sebagai *cybercrime* atau kejahatan siber. Kejahatan ini tidak hanya beroperasi dalam ruang digital tetapi juga berdampak nyata terhadap dunia nyata, termasuk sektor keuangan, pemerintahan, hingga kehidupan pribadi masyarakat. Oleh karena itu, pemahaman tentang definisi kejahatan siber menjadi landasan penting dalam menyusun kerangka hukum dan kebijakan penanggulangan yang efektif. Menurut Interpol (2022), kejahatan siber didefinisikan sebagai tindak kriminal yang dilakukan melalui jaringan komputer, internet, atau perangkat digital lainnya yang bertujuan untuk mencuri, menipu, merusak, atau mengganggu sistem informasi seseorang atau organisasi. Kejahatan ini mencakup berbagai jenis pelanggaran hukum, mulai dari penipuan daring (*online fraud*), peretasan (*hacking*), pencurian identitas digital, penyebaran *malware*, hingga serangan siber terhadap infrastruktur kritis.

Pada konteks internasional, Konvensi Budapest tentang Kejahatan Siber (2001) yang menjadi acuan hukum internasional pertama mengenai *cybercrime*, membagi tindak kejahatan siber ke dalam beberapa kategori: kejahatan terhadap kerahasiaan, integritas, dan ketersediaan data komputer atau sistem; kejahatan yang berkaitan dengan konten ilegal; dan kejahatan yang berkaitan dengan pelanggaran hak kekayaan intelektual dan penipuan. Meskipun Indonesia belum meratifikasi konvensi ini, prinsip-prinsipnya banyak digunakan sebagai rujukan dalam pembentukan regulasi nasional, seperti dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya dalam UU Nomor 19 Tahun 2016.

Di Indonesia, UU ITE secara eksplisit tidak menggunakan istilah "kejahatan siber", namun mengatur berbagai tindak pidana yang dilakukan melalui sistem elektronik dan/atau internet. Pasal-pasal dalam UU ITE mencakup pelanggaran terhadap integritas dan keamanan sistem elektronik, penghinaan atau pencemaran nama baik melalui media digital, penyebaran konten pornografi, perjudian daring, hingga ujaran

kebencian berbasis SARA. Menurut Barda Nawawi Arief (2012), kejahatan siber dapat dimaknai sebagai kejahatan yang berkaitan langsung dengan penggunaan teknologi informasi sebagai alat, sasaran, atau tempat berlangsungnya kejahatan tersebut.

Menurut Soedarto (2015), pengertian kejahatan harus terus mengalami pembaruan seiring dengan perkembangan masyarakat dan teknologi. Dalam hal ini, kejahatan siber merupakan manifestasi modern dari tindak pidana, yang sering kali melampaui batas yurisdiksi hukum nasional, sehingga menimbulkan tantangan tersendiri dalam aspek pembuktian, identifikasi pelaku, dan proses penegakan hukum. Oleh karena itu, pendekatan multidisiplin diperlukan dalam memahami definisi kejahatan siber, yang tidak hanya bersifat legalistik, tetapi juga melibatkan pendekatan teknologi, sosial, dan psikologis. Kejahatan siber pun sering kali bersifat tidak kasat mata (*invisible crime*) karena tidak menimbulkan kerusakan fisik secara langsung, namun dampaknya sangat merusak secara ekonomi dan psikologis. Oleh sebab itu, regulasi yang ada perlu secara tegas mendefinisikan ruang lingkup kejahatan ini agar tidak menimbulkan multitafsir dan ketidakpastian hukum di tengah masyarakat digital yang terus berkembang.

2. Karakteristik Kejahatan Siber: Kompleksitas, Lintas Negara, dan Bukti Digital

Kejahatan siber memiliki karakteristik yang sangat berbeda dari kejahatan konvensional, terutama karena sifatnya yang tidak terikat ruang dan waktu. Karakteristik ini menjadi tantangan utama dalam proses pencegahan, penyelidikan, serta penegakan hukum. Menurut Wall (2007), kejahatan siber memiliki empat karakter utama, yaitu: (1) non-fisik, (2) bersifat lintas batas negara, (3) sulit dideteksi, dan (4) membutuhkan keahlian teknis khusus untuk mengungkapkannya.

a. Kejahatan siber bersifat non-fisik, artinya kejahatan ini tidak selalu menimbulkan kerusakan fisik secara langsung, melainkan menyerang aspek-aspek digital seperti data, sistem informasi, dan perangkat lunak. Contohnya adalah kasus pencurian data pribadi pengguna internet yang digunakan untuk kegiatan penipuan atau pemerasan. Kerugian dalam bentuk finansial bisa sangat besar, namun pelaku kejahatan tidak perlu melakukan kontak fisik dengan korban, cukup dengan menggunakan perangkat lunak dan jaringan internet.

b. Karakteristik lintas batas negara (*borderless crime*) merupakan ciri khas kejahatan siber yang paling menyulitkan penegakan hukum nasional. Seorang pelaku kejahatan di satu negara dapat melakukan serangan terhadap sistem informasi di negara lain tanpa harus berpindah tempat. Misalnya, pelaku yang berada di Rusia dapat meretas situs e-commerce di Indonesia dan mencuri informasi kartu kredit pengguna. Dalam situasi seperti ini, yurisdiksi nasional menjadi terbatas, dan dibutuhkan kerja sama internasional yang kuat untuk menindak pelaku. Hal ini diperkuat oleh pendapat Brenner (2010) yang menyatakan bahwa kejahatan siber menantang batas tradisional kedaulatan hukum karena pelaku, korban, dan sistem yang diserang bisa berada di tiga negara yang berbeda secara geografis.
c. Kejahatan siber cenderung sulit dideteksi dan dibuktikan. Serangan siber sering kali bersifat *stealthy* (diam-diam) dan baru disadari setelah kerusakan terjadi. Beberapa jenis *malware* bahkan dirancang untuk menyusup tanpa diketahui dan mengambil data dalam jangka panjang. Proses investigasi pun menjadi rumit karena pelaku sering menggunakan metode penyamaran seperti VPN, *proxy*, dan jaringan *dark web* untuk menyembunyikan identitasnya. Oleh karena itu, diperlukan alat digital forensik dan kemampuan teknis tinggi dalam proses penyelidikan kejahatan siber.
d. Bukti dalam kejahatan siber bersifat digital dan mudah dimanipulasi. Berbeda dengan bukti fisik, bukti digital seperti log data, email, atau *file* elektronik bisa dihapus, dimodifikasi, atau disembunyikan dengan mudah. Menurut Casey (2011), proses pengumpulan, penyimpanan, dan penyajian bukti digital harus dilakukan secara hati-hati dan sesuai prosedur agar dapat digunakan di pengadilan. Hal ini mencakup penggunaan teknik *chain of custody* yang ketat untuk menjaga integritas data.

Karakteristik lainnya adalah kecepatan penyebaran dampak. Sebuah virus komputer atau *ransomware* dapat menjangkiti ribuan sistem hanya dalam hitungan menit, sebagaimana terjadi dalam kasus *WannaCry ransomware* global tahun 2017 yang melumpuhkan rumah sakit, institusi pemerintahan, dan perusahaan di lebih dari 150 negara. Dalam kasus seperti ini, respons hukum dan teknis harus dilakukan secara cepat, terkoordinasi, dan berbasis pada sistem peringatan dini yang kuat. Di Indonesia, kejahatan siber juga menunjukkan

kecenderungan meningkat dari tahun ke tahun. Menurut data dari Badan Siber dan Sandi Negara (BSSN, 2023), terdapat lebih dari 400 juta serangan siber yang terdeteksi selama tahun 2022, sebagian besar berupa upaya pencurian data dan serangan terhadap sistem pemerintah. Hal ini menunjukkan urgensi penanganan kejahatan siber secara strategis dan menyeluruh.

B. Sejarah dan Perkembangan Kejahatan Siber

1. Awal Kemunculan Kejahatan Siber: Dari Eksperimen Teknologi hingga Ancaman Global

Perjalanan kejahatan siber dimulai sejak perkembangan teknologi komputer pertama kali digunakan secara luas, terutama pada tahun 1960-an hingga 1980-an. Pada masa itu, tindakan-tindakan yang kini tergolong sebagai kejahatan siber belum sepenuhnya dianggap sebagai tindak pidana, melainkan sering kali dilihat sebagai tindakan eksperimental oleh para teknisi atau peneliti komputer. Salah satu kasus awal yang kerap disebut sebagai tonggak lahirnya *cybercrime* adalah kasus "*phone phreaking*" yang dilakukan oleh John Draper (alias "*Captain Crunch*") pada awal 1970-an di Amerika Serikat. Draper menemukan bahwa peluit dari sereal *Cap'n Crunch* bisa menghasilkan frekuensi nada 2600 Hz yang digunakan oleh jaringan telepon AT&T untuk mengatur jalur sambungan panggilan. Temuannya ini digunakan untuk membuat panggilan jarak jauh secara gratis, sebuah tindakan yang kemudian diidentifikasi sebagai pelanggaran sistem komunikasi meskipun tidak menggunakan komputer (Sterling, 1992).

Memasuki era 1980-an, penggunaan komputer personal mulai meluas, dan diikuti pula dengan munculnya perangkat lunak berbahaya (*malware*) pertama. Salah satu *malware* paling terkenal dari periode ini adalah "*Brain Virus*" yang ditemukan di Pakistan pada tahun 1986 oleh dua bersaudara, Basit dan Amjad Farooq Alvi. Virus ini menyebar melalui disket dan menyerang sistem operasi MS-DOS. Meski tidak merusak, virus tersebut menunjukkan potensi komputer sebagai sarana penyebaran kejahatan digital secara global (Cluley, 2011). Sejak saat itu, kejahatan siber mulai berkembang menjadi bentuk kejahatan nyata yang memanfaatkan kerentanan teknologi informasi. Pada tahun 1986 juga disahkan *Computer Fraud and Abuse Act* (CFAA) di Amerika Serikat, sebagai respons terhadap meningkatnya akses ilegal ke sistem komputer

pemerintah dan militer. CFAA menjadi salah satu regulasi awal yang mengatur secara hukum kejahatan berbasis komputer, dan menjadi inspirasi bagi banyak negara lain, termasuk Indonesia, dalam membentuk regulasi siber nasional.

Ketika jaringan internet mulai berkembang pesat di awal 1990-an, cakupan kejahatan siber turut melebar. Aktivitas seperti pencurian identitas, peretasan situs web, penyebaran spam, dan pembobolan data mulai marak terjadi. Salah satu peretas terkenal di era ini adalah Kevin Mitnick, yang ditangkap pada 1995 setelah berhasil mengakses sistem komputer sejumlah perusahaan besar dan lembaga pemerintah AS. Mitnick tidak hanya mencuri data, tapi juga mengungkap betapa lemahnya sistem keamanan digital saat itu. Kasusnya menjadi perhatian global dan menunjukkan perlunya peningkatan hukum dan teknologi dalam menangani ancaman siber (Shimons, 1996).

Pada konteks Indonesia, kejahatan siber mulai muncul secara signifikan pada awal tahun 2000-an, ditandai dengan maraknya kasus penipuan melalui surat elektronik dan situs palsu (*phishing*). Pemerintah kemudian merespons dengan mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi payung hukum utama penindakan kejahatan siber di Indonesia. Undang-undang ini kemudian diperbarui melalui UU Nomor 19 Tahun 2016 untuk menyesuaikan dengan dinamika teknologi dan sosial yang berkembang sangat cepat.

2. Evolusi Kejahatan Siber: Dari Peretas Tunggal hingga Serangan Siber Negara

Memasuki abad ke-21, kejahatan siber telah mengalami transformasi besar. Bila pada awalnya pelaku kejahatan siber adalah individu atau kelompok kecil yang bertindak demi reputasi atau keuntungan pribadi, kini telah berkembang menjadi kelompok terorganisir dengan dukungan logistik, finansial, dan kadang kala politik. Organisasi kejahatan siber modern memiliki struktur seperti korporasi, dengan pembagian tugas yang jelas seperti pengembang *malware*, operator jaringan botnet, ahli pencucian uang digital, dan pemasaran di dark web. Salah satu karakter transformasi yang mencolok adalah meningkatnya insiden *ransomware*. Serangan *ransomware* seperti WannaCry (2017) dan NotPetya (2017) menjadi bukti nyata bahwa kejahatan siber tidak hanya menargetkan individu tetapi juga

infrastruktur penting negara seperti rumah sakit, bank, pelabuhan, dan sistem pemerintahan. Menurut laporan Europol (2019), WannaCry menyerang lebih dari 200.000 komputer di 150 negara hanya dalam beberapa hari, menimbulkan kerugian miliaran dolar dan menunjukkan bagaimana kejahatan siber bisa melumpuhkan sektor vital global dalam waktu singkat.

Muncul pula kejahatan berbasis pencurian data dalam skala besar, seperti kebocoran data pengguna Facebook (Cambridge Analytica, 2018) dan peretasan Equifax (2017) yang mengungkap data pribadi lebih dari 147 juta warga AS. Kejahatan ini menunjukkan bahwa data menjadi komoditas utama dalam ekonomi digital, dan pencurian data bukan hanya ancaman bagi individu, melainkan juga bagi proses demokrasi dan keamanan nasional. Pada dekade terakhir, muncul pula tren baru yaitu serangan siber yang diduga melibatkan aktor negara (*state-sponsored cyberattacks*). Contoh nyata adalah kasus Stuxnet (2010), sebuah worm canggih yang menyerang sistem industri di Iran dan secara khusus dirancang untuk merusak sentrifugal uranium. Serangan ini diduga dilakukan oleh kerjasama antara AS dan Israel sebagai bentuk sabotase terhadap program nuklir Iran (Zetter, 2014). Serangan semacam ini menunjukkan bagaimana dunia maya telah menjadi medan baru peperangan modern, tempat negara-negara adikuasa bertarung secara diam-diam dengan teknologi.

Di Indonesia, evolusi kejahatan siber juga terlihat dari meningkatnya kompleksitas serangan terhadap sistem pemerintah, pendidikan, dan sektor swasta. Menurut laporan Badan Siber dan Sandi Negara (BSSN, 2023), sepanjang tahun 2022 saja terdapat lebih dari 400 juta serangan siber yang terdeteksi di Indonesia, termasuk serangan DDoS (*Distributed Denial of Service*), *malware*, dan pencurian kredensial akun. Salah satu insiden terbesar terjadi pada 2021 ketika situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan mengalami kebocoran data yang melibatkan lebih dari 279 juta data penduduk Indonesia.

Perkembangan kejahatan siber juga ditandai dengan masuknya unsur ideologis dan sosial. Kelompok ekstremis dan teroris kini menggunakan media digital untuk menyebarkan propaganda, merekrut anggota baru, hingga menggalang dana melalui metode cryptocurrency. Dalam hal ini, kejahatan siber tidak lagi murni bersifat kriminal ekonomi, tetapi juga bersinggungan dengan isu-isu keamanan nasional

dan internasional. *United Nations Office on Drugs and Crime* (UNODC, 2020) mencatat bahwa kejahatan siber telah menjadi ancaman lintas sektor yang memerlukan kerja sama multinasional dalam penanganannya.

Seiring dengan semakin berkembangnya teknologi seperti kecerdasan buatan, *Internet of Things* (IoT), dan komputasi awan, potensi eksploitasi untuk kejahatan siber pun meningkat. Ke depan, diperkirakan bahwa serangan akan semakin menyasar sektor-sektor sensitif seperti kendaraan otonom, perangkat kesehatan digital, dan sistem energi berbasis jaringan pintar. Oleh sebab itu, perlindungan terhadap ekosistem digital harus menjadi prioritas bersama antara pemerintah, sektor swasta, dan masyarakat global.

C. Klasifikasi Tindak Pidana Siber

1. Klasifikasi Berdasarkan Objek dan Motif Kejahatan Siber

Kejahatan siber dapat diklasifikasikan berdasarkan objek yang disasar serta motif dari pelaku. Berdasarkan pendekatan ini, *The Council of Europe Convention on Cybercrime* (Budapest Convention, 2001) mengelompokkan kejahatan siber ke dalam tiga kategori utama: kejahatan terhadap sistem komputer, kejahatan terhadap data komputer, dan kejahatan yang menggunakan komputer sebagai alat untuk melakukan tindak pidana lainnya. Pendekatan klasifikasi ini banyak digunakan dalam berbagai sistem hukum internasional maupun nasional karena sifatnya yang komprehensif dan adaptif terhadap dinamika teknologi informasi. Kejahatan terhadap sistem komputer adalah bentuk pelanggaran yang bertujuan merusak, mengganggu, atau mengakses sistem komputer secara tidak sah. Contoh kejahatan dalam kategori ini termasuk *hacking*, DDoS (*Distributed Denial of Service*) attack, dan pembuatan virus atau *malware* yang menargetkan sistem operasional. Di Indonesia, tindakan ini diatur dalam UU ITE Pasal 30 ayat (1), (2), dan (3) yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain dapat dikenai sanksi pidana (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016).

Kejahatan terhadap data komputer merujuk pada tindakan yang melibatkan manipulasi, pencurian, atau penghancuran data digital. Contohnya termasuk pencurian data pribadi, modifikasi data tanpa izin,

serta penyebaran informasi palsu (*fake news*) yang dapat memicu keresahan sosial. Data menjadi aset utama dalam dunia digital, dan serangan terhadap data sangat berdampak, baik dari sisi finansial maupun reputasi institusi. Menurut laporan IBM (2023), kerugian rata-rata akibat kebocoran data mencapai USD 4,45 juta per insiden secara global, dengan sektor kesehatan dan keuangan sebagai yang paling rentan. Kategori ketiga adalah kejahatan konvensional yang dimediasi atau difasilitasi oleh teknologi komputer, seperti penipuan daring *(online fraud*), perdagangan ilegal (misalnya, narkoba atau senjata melalui dark web), pelecehan seksual daring, dan ujaran kebencian. Di Indonesia, kasus penipuan online mendominasi laporan kejahatan siber kepada kepolisian. Menurut Bareskrim Polri (2023), lebih dari 70% dari total laporan kejahatan siber sepanjang tahun 2022 berkaitan dengan modus penipuan melalui e-commerce, investasi bodong digital, dan *phishing*.

Klasifikasi juga dapat dilakukan berdasarkan motif pelaku. Motif ekonomi merupakan yang paling dominan, di mana pelaku termotivasi untuk mendapatkan keuntungan finansial melalui pencurian data kartu kredit, pemerasan siber (*cyber extortion*), atau perdagangan ilegal. Motif politik dan ideologis juga muncul dalam bentuk hacktivism, yaitu kegiatan peretasan untuk menyuarakan isu tertentu atau menentang institusi negara. Sementara itu, motif personal meliputi dendam, balas sakit hati, atau pelecehan daring yang umumnya dilakukan oleh individu terhadap individu lainnya. Maka dari itu, pemahaman tentang klasifikasi berdasarkan objek dan motif penting dalam upaya penegakan hukum serta penetapan strategi mitigasi. Klasifikasi ini tidak hanya membantu aparat penegak hukum dalam proses pembuktian pidana, tetapi juga membantu sektor publik dan swasta dalam memetakan risiko digital dan menyusun sistem pengamanan berbasis prioritas.

2. Klasifikasi Berdasarkan Metode dan Teknik Serangan Siber

Kejahatan siber juga diklasifikasikan menurut metode dan teknik yang digunakan oleh pelaku. Perkembangan teknologi telah menghasilkan berbagai teknik serangan digital yang semakin kompleks dan sulit dilacak. Menurut laporan Verizon (2023), metode kejahatan siber saat ini meliputi *phishing*, *malware*, *social engineering, credential stuffing,* hingga *advanced persistent threat* (APT). Setiap metode ini memiliki karakteristik teknis dan dampak yang berbeda terhadap korban. *Phishing* adalah metode paling umum yang dilakukan dengan

mengirimkan email atau pesan palsu seolah-olah berasal dari pihak terpercaya untuk mengelabui korban agar memberikan informasi sensitif. Teknik ini sangat efektif karena memanfaatkan kelemahan manusia (*human error*). Menurut Proofpoint (2022), lebih dari 83% perusahaan global mengalami serangan *phishing* dalam kurun waktu setahun terakhir, dan 60% di antaranya berdampak pada pencurian data karyawan.

Malware, atau perangkat lunak berbahaya, mencakup virus, worm, spyware, *ransomware*, dan trojan. *Ransomware* menjadi metode yang paling banyak menimbulkan kerugian ekonomi dalam beberapa tahun terakhir. Pelaku mengenkripsi data korban dan meminta tebusan untuk mengembalikan aksesnya. Serangan *ransomware* LockBit dan Conti banyak menargetkan institusi pendidikan dan kesehatan di Asia Tenggara, termasuk Indonesia (Interpol, 2023). *Social engineering* adalah metode manipulasi psikologis yang membuat korban dengan sukarela memberikan informasi atau akses ke sistem. Teknik ini digunakan dalam berbagai bentuk, seperti *pretexting, baiting*, dan *quid pro quo*. Kejahatan ini sulit dideteksi karena tidak selalu melibatkan kode program atau perangkat keras.

Credential stuffing adalah teknik otomatisasi untuk mencoba kombinasi username dan password yang bocor dari situs tertentu dan menggunakannya di situs lain. Teknik ini sangat efektif karena banyak pengguna memakai kata sandi yang sama di berbagai platform. Oleh karena itu, perusahaan kini menerapkan sistem autentikasi ganda (*two-factor authentication*) untuk mencegah akses ilegal semacam ini. APT atau *Advanced Persistent Threat* merupakan metode kejahatan siber tingkat tinggi yang umumnya dilakukan oleh aktor negara atau organisasi kriminal besar. APT biasanya berlangsung dalam jangka waktu lama dan menyasar target strategis seperti lembaga pemerintah, perusahaan teknologi, atau lembaga pertahanan. Teknik ini mencakup kombinasi berbagai metode serangan termasuk spear *phishing*, exploit kits, hingga backdoor implants. Serangan APT terkenal yang melibatkan Indonesia adalah serangan terhadap sistem e-government dan data pemilu yang dikaitkan dengan aktor luar negeri (APNIC, 2022).

D. Dampak Sosial, Ekonomi, dan Keamanan dari Kejahatan Siber

1. Dampak Sosial dan Psikologis Kejahatan Siber terhadap Masyarakat

Kejahatan siber tidak hanya menimbulkan kerugian material, tetapi juga berdampak luas terhadap struktur sosial, psikologi individu, dan tatanan interaksi masyarakat. Dalam dunia digital yang semakin terkoneksi, kejahatan seperti perundungan siber (*cyberbullying*), penyebaran *hoaks*, pencemaran nama baik daring, dan pelecehan seksual digital telah memperluas spektrum ancaman sosial secara signifikan. Menurut penelitian Livingstone dan Smith (2014), korban perundungan siber cenderung mengalami depresi, kecemasan, hingga trauma jangka panjang, terutama di kalangan remaja. Bentuk intimidasi ini seringkali bersifat anonim dan berlangsung terus-menerus, membuat korbannya kesulitan mencari perlindungan.

Penyebaran informasi palsu atau *hoaks* menjadi masalah sosial serius di era digital. Di Indonesia, isu ini sangat relevan, khususnya pada masa pemilu atau krisis kesehatan seperti pandemi COVID-19. Menurut laporan Masyarakat Anti Fitnah Indonesia (MAFINDO, 2022), jumlah *hoaks* yang beredar selama tahun 2021 mencapai lebih dari 2.000 kasus, sebagian besar tersebar melalui media sosial dan aplikasi pesan instan. Penyebaran *hoaks* dapat menurunkan kepercayaan masyarakat terhadap institusi negara, memicu kepanikan, serta merusak integrasi sosial.

Dampak sosial lainnya mencakup pelanggaran privasi, di mana data pribadi seseorang diekspos atau disalahgunakan oleh pihak tidak bertanggung jawab. Fenomena *doxing*, yaitu membocorkan informasi pribadi di ruang publik daring, telah menjadi bentuk kejahatan yang menghancurkan reputasi dan keselamatan korban. Selain itu, pelecehan seksual digital, seperti pengiriman gambar tak senonoh tanpa persetujuan atau penyebaran konten intim, juga memberikan dampak psikologis mendalam. Menurut UN Women (2020), hampir 40% perempuan pengguna internet mengalami kekerasan berbasis gender secara daring.

Fenomena kejahatan siber juga menciptakan ketimpangan digital dan ketidakadilan sosial. Kelompok rentan seperti anak-anak, perempuan, penyandang disabilitas, dan masyarakat di daerah terpencil sering kali menjadi korban karena keterbatasan akses terhadap literasi digital dan teknologi pelindung. Hal ini memperbesar jurang digital dan memperparah eksklusi sosial. Oleh karena itu, penanggulangan

kejahatan siber harus memperhatikan perspektif sosial yang inklusif dan berbasis hak asasi manusia.

Dampak sosial dari kejahatan siber tidak hanya menimpa individu, tetapi juga mempengaruhi kohesi sosial dan kualitas hidup masyarakat. Kepercayaan publik terhadap ruang digital menjadi terganggu, dan partisipasi masyarakat dalam platform digital dapat menurun apabila tidak ada jaminan perlindungan yang memadai. Situasi ini mengharuskan adanya sinergi antara pemerintah, masyarakat sipil, dan sektor swasta dalam membangun ekosistem digital yang aman dan berkeadilan.

2. Dampak Ekonomi dan Keamanan Nasional dari Kejahatan Siber

Dari sisi ekonomi, kejahatan siber telah menyebabkan kerugian finansial yang sangat besar baik bagi individu, perusahaan, maupun negara. Menurut laporan *Cybersecurity Ventures* (2023), kerugian global akibat kejahatan siber diperkirakan mencapai USD 8 triliun pada tahun 2023 dan diproyeksikan akan meningkat menjadi USD 10,5 triliun pada 2025. Bentuk kerugian ini mencakup pencurian data keuangan, gangguan operasional, biaya pemulihan sistem, serta kerugian reputasi bisnis. Di Indonesia, Otoritas Jasa Keuangan (OJK, 2022) mencatat bahwa sektor perbankan mengalami peningkatan insiden fraud digital sebesar 37% dibanding tahun sebelumnya. Kejahatan seperti *ransomware* menimbulkan kerugian berlapis, mulai dari tebusan yang dibayarkan, kehilangan data bisnis, hingga penghentian operasional layanan. Dalam kasus serangan *ransomware* WannaCry (2017) dan REvil (2021), banyak perusahaan besar dan lembaga publik harus menutup layanan untuk sementara waktu, yang berdampak langsung pada pendapatan dan kepercayaan pelanggan. Serangan semacam ini membuktikan bahwa ekonomi digital yang terintegrasi tinggi juga membawa risiko sistemik yang signifikan.

Ekonomi digital yang terganggu oleh kejahatan siber juga mempengaruhi iklim investasi. Investor cenderung berhati-hati dalam menanamkan modal di negara yang belum memiliki sistem perlindungan siber yang kuat. Hal ini dapat memperlambat pertumbuhan sektor teknologi dan menghambat inovasi. Selain itu, kejahatan seperti pencurian kekayaan intelektual dan spionase industri menyebabkan kerugian tidak langsung yang besar terhadap potensi kompetitif

perusahaan dan negara. Dampak kejahatan siber terhadap keamanan nasional juga sangat krusial. Serangan terhadap infrastruktur kritis seperti sistem listrik, transportasi, telekomunikasi, dan layanan kesehatan dapat melumpuhkan operasional negara. Dalam konteks ini, kejahatan siber tidak lagi hanya dianggap sebagai tindak kriminal biasa, tetapi telah berkembang menjadi ancaman strategis. Menurut laporan World Economic Forum (2023), serangan siber terhadap infrastruktur publik merupakan salah satu risiko utama global dalam dekade ini.

Serangan yang melibatkan aktor negara, seperti dalam kasus APT (*Advanced Persistent Threat*), menunjukkan bahwa siber telah menjadi medan baru dalam konflik geopolitik. Negara-negara seperti Amerika Serikat, Rusia, Tiongkok, dan Korea Utara telah dikaitkan dengan serangkaian serangan siber lintas batas yang menyasar sistem pemerintahan, data sensitif, dan opini publik negara lain. Dalam konteks Indonesia, serangan terhadap data pemilih dan situs kementerian menunjukkan bahwa negara ini juga menjadi target dalam peta ancaman global. Kejahatan siber juga melemahkan keamanan sosial-politik. Manipulasi media sosial oleh bot dan algoritma untuk menyebarkan disinformasi dapat memengaruhi opini publik dan bahkan hasil pemilu. Menurut Oxford Internet Institute (2022), lebih dari 80 negara mengalami manipulasi informasi politik secara daring, baik oleh aktor domestik maupun asing. Hal ini menjadi tantangan besar bagi demokrasi digital dan integritas sistem pemilu di banyak negara.

BAB II
KERANGKA HUKUM TINDAK PIDANA SIBER DI INDONESIA

Untuk menghadapi eskalasi kejahatan siber yang semakin kompleks dan transnasional, keberadaan kerangka hukum yang kuat dan adaptif menjadi suatu kebutuhan mutlak di Indonesia. Dunia digital yang terus berkembang memunculkan berbagai bentuk kejahatan baru yang tidak selalu dapat dijangkau oleh norma-norma hukum konvensional, sehingga menuntut negara untuk merumuskan instrumen hukum yang tidak hanya bersifat represif tetapi juga preventif dan responsif terhadap dinamika teknologi informasi. Indonesia telah mengadopsi beberapa regulasi penting dalam rangka menangani kejahatan siber, terutama melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui UU Nomor 19 Tahun 2016, serta regulasi sektoral lainnya yang terkait dengan perlindungan data pribadi, transaksi elektronik, dan keamanan siber nasional. Namun, meskipun berbagai regulasi telah tersedia, implementasi dan harmonisasi antar-institusi penegak hukum serta kesiapan infrastruktur digital nasional masih menghadapi berbagai tantangan signifikan. Penegakan hukum terhadap pelaku kejahatan siber seringkali terkendala oleh kurangnya kapasitas sumber daya manusia, lemahnya koordinasi lintas lembaga, serta belum optimalnya kerjasama internasional dalam rangka menghadapi serangan siber lintas batas negara. Oleh karena itu, kerangka hukum di bidang ini perlu terus diperbarui, disosialisasikan secara luas, dan ditopang oleh sistem peradilan yang adaptif terhadap realitas digital.

A. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

1. Latar Belakang dan Tujuan Pembentukan UU ITE

Kemunculan teknologi informasi dan komunikasi digital telah membawa perubahan besar dalam cara masyarakat berinteraksi, bertransaksi, dan mengakses informasi. Perubahan ini menimbulkan kebutuhan mendesak bagi negara untuk menghadirkan regulasi yang dapat mengakomodasi fenomena hukum baru di dunia maya. Sebagai respons terhadap dinamika tersebut, Indonesia memberlakukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. UU ITE menjadi tonggak utama dalam pengaturan aktivitas di ruang digital, termasuk dalam mengatur tindak pidana siber dan memberikan dasar hukum terhadap bukti elektronik.

UU ITE dirancang untuk memberikan kepastian hukum bagi pelaku dan pengguna teknologi informasi. Menurut Sinta Dewi (2019), UU ini lahir untuk menciptakan sistem informasi dan transaksi elektronik yang aman, andal, dan bertanggung jawab. Salah satu tujuan utamanya adalah melindungi masyarakat dari penyalahgunaan teknologi, baik dalam bentuk penipuan daring, pencemaran nama baik, hingga pelanggaran hak cipta secara digital. Dalam Pasal 3 UU ITE, ditegaskan bahwa teknologi informasi harus digunakan untuk menciptakan ketertiban, keadilan, dan manfaat sosial.

Pentingnya UU ITE juga tampak dari upaya negara untuk menjadikan ruang digital sebagai ruang publik yang tertib hukum. Hal ini mencerminkan filosofi bahwa meskipun aktivitas digital bersifat maya, dampaknya sangat nyata dalam kehidupan sosial, ekonomi, dan bahkan politik. UU ITE mencakup berbagai aspek penting, mulai dari pengakuan terhadap dokumen elektronik sebagai alat bukti sah di pengadilan (Pasal 5 dan 6), pengaturan tanda tangan elektronik (Pasal 11), perlindungan terhadap data pribadi, hingga kriminalisasi konten dan aktivitas ilegal di internet.

Pada praktiknya, UU ITE menuai banyak kritik, terutama karena beberapa pasalnya dinilai multitafsir dan berpotensi mengekang kebebasan berekspresi. Pasal 27 ayat (3) tentang pencemaran nama baik serta Pasal 28 ayat (2) tentang penyebaran kebencian seringkali dijadikan dasar pelaporan terhadap kritik yang dilontarkan di media sosial. Menurut laporan SAFEnet (2021), banyak aktivis, jurnalis, dan warga

biasa dilaporkan atau dipidana dengan menggunakan pasal-pasal ini, menimbulkan kekhawatiran terhadap potensi penyalahgunaan hukum. Oleh karena itu, pada tahun 2016, pemerintah merevisi UU ITE melalui UU Nomor 19 Tahun 2016. Revisi ini bertujuan untuk memperjelas rumusan delik dan mengurangi potensi kriminalisasi berlebihan. Salah satu perubahan penting adalah pengurangan ancaman pidana dalam beberapa pasal dan penguatan mekanisme pelaporan serta klarifikasi digital. Namun demikian, substansi pasal yang dianggap problematik tetap dipertahankan, meskipun sudah disertai dengan penjelasan tambahan.

Pada konteks internasional, UU ITE juga menjadi instrumen penting untuk mendukung komitmen Indonesia dalam penanggulangan kejahatan siber lintas batas. Meskipun Indonesia belum menjadi pihak dalam Konvensi Budapest tentang *Cybercrime*, UU ITE telah mengadopsi prinsip-prinsip penting terkait penindakan terhadap pelaku kejahatan siber, perlindungan terhadap sistem elektronik, dan upaya internasional dalam memerangi serangan digital. Dengan demikian, UU ITE merupakan instrumen hukum yang penting sekaligus kompleks. Ia menjadi pondasi bagi pengaturan aktivitas digital di Indonesia, tetapi juga membutuhkan pengawasan dan evaluasi berkelanjutan agar tetap sejalan dengan prinsip-prinsip demokrasi, keadilan, dan hak asasi manusia.

2. Substansi Pengaturan dan Tantangan Implementasi UU ITE

Secara substansi, UU ITE mencakup dua hal utama, yaitu pengaturan aktivitas elektronik yang sah serta larangan terhadap berbagai bentuk kejahatan siber. UU ini terdiri dari 54 pasal yang terbagi ke dalam beberapa bagian, termasuk ketentuan umum, prinsip-prinsip pemanfaatan teknologi informasi, tanda tangan digital, penyelenggaraan sistem elektronik, transaksi elektronik, serta ketentuan pidana. Salah satu aspek penting adalah pengakuan legal terhadap dokumen elektronik dan tanda tangan digital. Hal ini memberikan legitimasi terhadap transaksi daring yang sah, sehingga mendorong pertumbuhan ekonomi digital. Pengaturan ini sangat relevan dalam konteks e-commerce, e-government, dan berbagai bentuk layanan digital lain yang berkembang pesat. Menurut Nugroho dan Utami (2020), pengakuan terhadap transaksi elektronik melalui UU ITE mempercepat integrasi sistem digital ke dalam sektor-sektor publik dan swasta di Indonesia.

Ketentuan pidana dalam UU ITE mengatur berbagai bentuk kejahatan siber, seperti pencemaran nama baik, pengancaman, penipuan daring, akses ilegal terhadap sistem elektronik, penyadapan ilegal, distribusi konten pornografi, serta penyebaran kebencian berbasis SARA. Pasal 30 sampai Pasal 37 secara spesifik mengatur perbuatan yang menyerang integritas, ketersediaan, dan kerahasiaan sistem elektronik. Sedangkan Pasal 27 sampai 29 mengatur konten bermuatan ilegal dan delik konten. Meskipun secara normatif UU ITE memuat berbagai perlindungan penting, implementasinya di lapangan tidak selalu berjalan optimal. Salah satu tantangan utama adalah keterbatasan kapasitas aparat penegak hukum dalam memahami karakteristik kejahatan digital yang terus berkembang. Menurut Suryanto (2021), banyak kasus kejahatan siber yang tidak tertangani secara efektif karena minimnya pelatihan teknis dan forensik digital di kepolisian dan kejaksaan.

Penggunaan pasal-pasal tertentu secara selektif atau represif menjadi sorotan publik. Pasal 27 ayat (3) tentang penghinaan atau pencemaran nama baik seringkali digunakan untuk melaporkan konten kritik terhadap pejabat atau institusi negara. Ini memunculkan kekhawatiran akan pelanggaran terhadap hak kebebasan berpendapat yang dijamin dalam UUD 1945 dan instrumen HAM internasional. Laporan Komnas HAM (2022) menunjukkan bahwa lebih dari separuh aduan masyarakat tentang pembatasan kebebasan berekspresi berakar dari penerapan UU ITE. Tantangan lainnya adalah keterbatasan koordinasi antarinstansi. Dalam menindak kejahatan siber, diperlukan sinergi antara Kominfo, BSSN, Kepolisian, Kejaksaan, dan lembaga peradilan. Namun, tumpang tindih kewenangan dan tidak adanya pusat komando nasional yang solid menyebabkan proses penindakan seringkali lambat dan tidak konsisten. Menurut Putri dan Nugraha (2021), Indonesia perlu membentuk lembaga khusus penegakan hukum siber yang bersifat terpadu dan independen.

Terdapat pula tantangan dari sisi regulasi yang tidak selalu responsif terhadap perkembangan teknologi. Misalnya, UU ITE belum secara eksplisit mengatur tentang perlindungan data pribadi secara komprehensif (sebelum UU PDP disahkan pada 2022), pengawasan terhadap algoritma platform digital, serta pengaturan *artificial intelligence* (AI) dalam konteks siber. Hal ini menyebabkan ruang kosong hukum (*legal vacuum*) yang rawan dimanfaatkan oleh pelaku

kejahatan siber. Sebagai tanggapan terhadap dinamika tersebut, pemerintah membentuk Tim Revisi UU ITE dan melakukan uji publik terhadap substansi pasal-pasal yang dianggap bermasalah. Namun, proses revisi berjalan lambat dan tidak sepenuhnya mengakomodasi tuntutan masyarakat sipil. Beberapa usulan seperti penghapusan delik aduan untuk pencemaran nama baik atau penguatan mediasi digital belum terealisasi secara penuh.

B. KUHP dan Relevansinya terhadap Kejahatan Siber

1. Evolusi KUHP dan Keterbatasannya dalam Mengakomodasi Kejahatan Siber

Kitab Undang-Undang Hukum Pidana (KUHP) merupakan produk hukum kolonial Belanda yang telah digunakan sejak diberlakukannya Wetboek van Strafrecht voor Nederlandsch-Indië pada tahun 1918, dan tetap diadopsi setelah kemerdekaan Indonesia dengan beberapa penyesuaian. Sejak awal, KUHP dirancang untuk mengatur tindak pidana konvensional, seperti pencurian, penganiayaan, pembunuhan, dan kejahatan terhadap keamanan negara. Namun, seiring dengan perkembangan teknologi informasi, muncul jenis-jenis kejahatan baru yang tidak lagi terbatas pada ruang fisik, melainkan terjadi di dunia digital atau siber. Hal ini menimbulkan tantangan besar bagi sistem hukum pidana Indonesia yang masih mendasarkan banyak aspek penegakan hukumnya pada KUHP yang usang.

Menurut Andi Hamzah (2001), KUHP merupakan sistem hukum pidana yang "usang" dalam arti tidak relevan untuk menangani dinamika kejahatan modern, terutama kejahatan yang bersifat lintas batas, terdesentralisasi, dan anonim seperti halnya tindak pidana siber. KUHP klasik tidak mengenal konsep-konsep hukum seperti akses ilegal terhadap sistem elektronik, perusakan data, penyadapan digital, atau distribusi konten terlarang di internet. Sebagai contoh, tindak pidana pencurian dalam Pasal 362 KUHP hanya mengatur perbuatan mengambil barang yang bersifat fisik, sementara dalam dunia siber, pencurian dapat terjadi dalam bentuk pencurian data, identitas, atau aset digital.

Situasi ini mendorong perlunya perangkat hukum baru yang mampu melengkapi atau bahkan menggantikan peran KUHP dalam konteks kejahatan digital. Meskipun begitu, KUHP masih tetap memiliki

relevansi dalam penegakan hukum siber, terutama dalam kasus-kasus yang masih berkaitan dengan bentuk kejahatan tradisional tetapi dilakukan melalui media digital. Sebagai contoh, tindak pidana penipuan daring dapat dikenakan Pasal 378 KUHP tentang penipuan, sementara ujaran kebencian atau fitnah secara daring dapat dikenakan Pasal 310 atau 311 KUHP. Ini menunjukkan bahwa beberapa pasal dalam KUHP masih dapat diinterpretasikan untuk menjerat pelaku kejahatan siber, meskipun cakupan dan kerangka pasalnya tidak dirancang secara spesifik untuk ranah digital.

Penggunaan KUHP terhadap kejahatan siber juga menghadapi tantangan interpretasi hukum dan pembuktian. Bukti elektronik yang menjadi inti dalam perkara siber tidak diatur secara rinci dalam KUHP, yang menyebabkan aparat penegak hukum seringkali harus mengacu pada UU ITE untuk memperkuat dakwaan. Selain itu, KUHP tidak memberikan pedoman tentang jurisdiksi lintas batas yang sering terjadi dalam kejahatan siber, seperti peretasan dari luar negeri, sehingga menyulitkan proses hukum yang membutuhkan kerjasama internasional. Oleh karena itu, KUHP lama dianggap tidak memadai dalam menjawab kebutuhan zaman, dan menjadi salah satu alasan utama reformasi hukum pidana nasional. Reformasi tersebut terwujud dalam pengesahan KUHP Nasional melalui Undang-Undang Nomor 1 Tahun 2023, yang menggantikan KUHP lama. KUHP baru ini mencerminkan kesadaran pemerintah untuk memperbarui sistem hukum pidana secara komprehensif dan relevan terhadap kondisi sosial-teknologis masyarakat modern. Meskipun demikian, apakah KUHP baru ini cukup responsif terhadap kejahatan siber masih menjadi bahan diskusi di kalangan akademisi dan praktisi hukum.

2. Cakupan KUHP Baru (UU No. 1 Tahun 2023) dalam Konteks Kejahatan Siber

KUHP Nasional yang disahkan melalui UU No. 1 Tahun 2023 mulai berlaku secara efektif pada tahun 2026 setelah masa transisi. Dalam dokumen resmi penjelasan undang-undang, pemerintah menyatakan bahwa KUHP baru dirancang untuk lebih adaptif terhadap perkembangan kejahatan modern, termasuk kejahatan yang terjadi di ruang digital. Meskipun secara eksplisit tidak mengatur secara mendetail seluruh bentuk kejahatan siber, KUHP baru ini mengadopsi beberapa pasal yang dapat digunakan untuk menjerat pelaku kejahatan siber

berdasarkan asas analogi dan relevansi konteks. Salah satu contoh bentuk adaptasi adalah pengaturan terhadap penyebaran informasi bohong, ujaran kebencian, serta perbuatan yang dapat mengganggu ketertiban umum melalui media apa pun, termasuk media elektronik. Pasal 263 KUHP baru mengatur pidana terhadap orang yang menyebarkan berita bohong yang menimbulkan keonaran di masyarakat. Pasal ini dapat diterapkan untuk menindak pelaku penyebar *hoaks* di media sosial yang memicu keresahan publik. Sementara itu, Pasal 412 dan 413 mengatur tentang penghinaan terhadap pemerintah atau lembaga negara, yang juga bisa dilakukan melalui sarana elektronik.

KUHP baru juga mengatur mengenai perlindungan terhadap hak privasi. Pasal-pasal mengenai perbuatan meretas atau menyadap komunikasi orang lain dapat dianggap melanggar norma privasi dan dapat dijerat dengan pasal-pasal dalam KUHP baru yang mengatur tindakan tanpa hak terhadap data atau komunikasi pribadi. Meskipun tidak disebut secara eksplisit sebagai kejahatan siber, norma ini memiliki irisan langsung dengan tindak pidana seperti *hacking*, *doxing*, atau *phising*. Namun, sejumlah kalangan menilai bahwa KUHP baru belum cukup komprehensif dalam menjawab tantangan kejahatan siber yang bersifat sangat teknis dan terus berubah. Menurut Widodo Ekatjahjana (2023), KUHP nasional belum secara rinci mengatur kejahatan terhadap sistem informasi, serangan *malware*, sabotase digital, serta kejahatan siber yang terorganisir dan lintas batas. Hal ini mengindikasikan bahwa UU ITE dan regulasi sektoral lainnya masih sangat dibutuhkan untuk mengisi kekosongan hukum yang tidak dicakup oleh KUHP.

Kendati demikian, integrasi KUHP dengan peraturan perundang-undangan lain seperti UU ITE, UU PDP (Perlindungan Data Pribadi), dan peraturan-peraturan dari BSSN (Badan Siber dan Sandi Negara) diharapkan dapat menciptakan sistem hukum yang lebih terintegrasi dan responsif terhadap kejahatan digital. Ke depannya, revisi dan penguatan substansi hukum pidana dalam KUHP juga masih dimungkinkan melalui mekanisme perubahan undang-undang atau pengaturan teknis dalam bentuk peraturan pemerintah dan peraturan pelaksana lainnya.

C. Regulasi Perlindungan Data Pribadi

1. Latar Belakang dan Kebutuhan Perlindungan Data Pribadi di Era Digital

Perkembangan teknologi informasi telah membawa perubahan besar dalam cara manusia berinteraksi, bekerja, dan mengakses layanan publik maupun privat. Dalam proses digitalisasi tersebut, data pribadi menjadi komoditas yang sangat berharga karena dapat digunakan untuk berbagai keperluan, mulai dari pemasaran, pengambilan keputusan bisnis, hingga pelayanan publik. Namun, meningkatnya pemrosesan dan pertukaran data pribadi juga diiringi oleh meningkatnya risiko pelanggaran privasi, penyalahgunaan data, dan kebocoran informasi yang bersifat sensitif. Dalam konteks inilah, perlindungan data pribadi menjadi isu hukum yang sangat penting, baik secara nasional maupun global.

Di Indonesia, perlindungan data pribadi sebelumnya diatur secara parsial dalam beberapa peraturan sektoral seperti UU ITE No. 11 Tahun 2008 dan perubahannya (UU No. 19 Tahun 2016), Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), serta Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Namun regulasi-regulasi tersebut dinilai belum cukup kuat, karena tidak memiliki kekuatan hukum setara undang-undang, serta belum menjangkau aspek perlindungan menyeluruh seperti hak subjek data, mekanisme pengaduan, dan sanksi yang tegas bagi pelanggar.

Kesadaran akan lemahnya perlindungan hukum terhadap data pribadi diperkuat oleh berbagai kasus kebocoran data yang mencuat ke publik, seperti kebocoran data pelanggan Tokopedia (2020), BPJS Kesehatan (2021), dan e-commerce lainnya, yang menunjukkan betapa rentannya sistem elektronik di Indonesia. Menurut laporan Data Protection Asia (2022), lebih dari 70% perusahaan di Indonesia pernah mengalami insiden pelanggaran data, dan sebagian besar belum memiliki kebijakan perlindungan data yang memadai. Di sisi lain, masyarakat juga masih memiliki kesadaran yang rendah tentang hak-haknya atas data pribadi.

Melihat kebutuhan tersebut, pemerintah dan DPR akhirnya mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menjadi tonggak penting

dalam pembangunan sistem perlindungan privasi digital di Indonesia. UU PDP disusun dengan merujuk pada standar global, seperti *General Data Protection Regulation* (GDPR) milik Uni Eropa, dan memberikan payung hukum yang lebih sistematis dan tegas dalam melindungi data pribadi warga negara Indonesia.

2. Substansi UU PDP dan Implikasinya terhadap Penanggulangan Kejahatan Siber

Undang-Undang No. 27 Tahun 2022 mendefinisikan data pribadi sebagai data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik. UU ini membagi data pribadi menjadi dua kategori: data pribadi umum (seperti nama, jenis kelamin, kewarganegaraan, dll.) dan data pribadi spesifik (seperti data biometrik, data kesehatan, informasi keuangan, pandangan politik, dan data genetika). Pembagian ini penting untuk menentukan tingkat perlindungan dan perlakuan hukum yang lebih ketat terhadap data sensitif.

Salah satu aspek penting dalam UU PDP adalah penetapan hak-hak subjek data, termasuk hak untuk mendapatkan informasi, hak untuk mengakses dan memperbaiki data, hak untuk menghapus data, serta hak untuk menarik persetujuan pemrosesan data. Selain itu, pengendali dan prosesor data diwajibkan untuk menerapkan prinsip perlindungan data seperti keabsahan pemrosesan, pembatasan tujuan, akurasi, dan akuntabilitas. Kewajiban ini diperkuat dengan ancaman sanksi administratif, pidana, dan perdata terhadap pelanggaran.

Dari sisi penegakan hukum, UU PDP mengatur pembentukan Otoritas Pelindung Data Pribadi, sebuah lembaga independen yang memiliki kewenangan untuk mengawasi kepatuhan, melakukan pemeriksaan, menangani pengaduan, serta menjatuhkan sanksi administratif. Hal ini merupakan terobosan penting karena sebelumnya tidak ada lembaga khusus yang berperan sebagai regulator perlindungan data. Selain itu, UU ini memberikan dasar hukum yang kuat bagi aparat penegak hukum, khususnya dalam menangani kejahatan siber yang berkaitan dengan penyalahgunaan data pribadi seperti pencurian identitas, *doxing*, *phising*, dan penipuan berbasis data korban.

Pasal 67 hingga Pasal 73 UU PDP mengatur sanksi pidana terhadap pelaku penyalahgunaan data pribadi, dengan ancaman pidana penjara maksimal 5 tahun dan denda maksimal Rp5 miliar. Misalnya, Pasal 67 menyebutkan bahwa setiap orang yang dengan sengaja memperoleh atau mengumpulkan data pribadi yang bukan miliknya secara melawan hukum dapat dipidana. Demikian pula, Pasal 69 mengatur pidana bagi pihak yang memproses data tanpa hak atau melanggar prinsip perlindungan data. Regulasi ini memperjelas ruang lingkup kejahatan siber berbasis data pribadi yang selama ini belum dijangkau secara efektif oleh KUHP maupun UU ITE.

Implementasi UU PDP masih menghadapi tantangan besar, terutama dari sisi kesiapan institusi, literasi digital masyarakat, dan infrastruktur keamanan data di sektor publik dan swasta. Menurut Simorangkir (2023), banyak institusi, khususnya UMKM dan layanan publik, belum memiliki sistem perlindungan data yang sesuai standar, bahkan belum memiliki petugas perlindungan data (*Data Protection Officer*/DPO) sebagaimana diwajibkan oleh UU. Di sisi lain, masyarakat juga belum sepenuhnya menyadari pentingnya menjaga privasi dan belum kritis dalam memberikan persetujuan pemrosesan data di berbagai platform digital.

Keberhasilan UU PDP dalam melindungi data pribadi dan menanggulangi kejahatan siber akan sangat bergantung pada sinergi antarlembaga, konsistensi penegakan hukum, serta kampanye literasi digital secara masif. Penerapan teknologi seperti enkripsi, manajemen identitas digital, dan sistem audit keamanan juga perlu diperkuat untuk mendukung implementasi regulasi ini secara teknis. Sebagai tambahan, UU PDP membuka peluang kerjasama internasional dalam pengelolaan dan perlindungan data lintas batas (*cross-border data transfer*). Pasal 56 mengatur bahwa transfer data ke luar negeri hanya dapat dilakukan ke negara yang memiliki tingkat perlindungan data yang setara atau berdasarkan perjanjian antarnegara. Ini penting karena banyak layanan digital dan penyimpanan data yang bersifat global. Maka, regulasi ini sekaligus mengokohkan posisi Indonesia dalam diplomasi digital global, serta memberikan kerangka hukum yang lebih kuat dalam menangani kasus kejahatan siber berskala internasional.

D. Perbandingan Regulasi Siber Indonesia dengan Negara Lain

Perbandingan Regulasi Siber Indonesia dengan Negara Lain yang membahas bagaimana Indonesia mengatur kejahatan siber dan perlindungan data pribadi dibandingkan dengan negara-negara lain yang memiliki regulasi serupa. Uraian ini dibagi dalam dua poin pembahasan utama dan dilengkapi dengan referensi yang valid.

1. Regulasi Siber Indonesia dan Perbandingannya dengan Negara-negara Eropa

Indonesia telah mengalami kemajuan yang signifikan dalam hal regulasi terkait dengan tindak pidana siber, terutama dengan diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini memberikan kerangka hukum yang lebih komprehensif untuk perlindungan data pribadi dan penyalahgunaannya dalam ranah digital, mengacu pada standar internasional seperti *General Data Protection Regulation* (GDPR) milik Uni Eropa. Meskipun demikian, terdapat perbedaan penting dalam penerapan dan pengawasan antara Indonesia dan negara-negara Eropa.

GDPR yang diberlakukan pada Mei 2018 di Uni Eropa adalah regulasi yang paling ketat di dunia mengenai perlindungan data pribadi. Regulasi ini menekankan pada hak-hak individu terhadap data pribadinya, termasuk hak untuk diberitahu tentang pengumpulan data, hak untuk mengakses data pribadi, hak untuk menghapus data (*right to be forgotten*), dan hak untuk menolak pemrosesan data yang berisiko bagi privasi individu. GDPR juga membebankan kewajiban kepada perusahaan dan organisasi untuk memastikan bahwa data pribadi diproses secara sah dan transparan. Selain itu, GDPR memberikan kewenangan kepada *European Data Protection Board* (EDPB) untuk memastikan kepatuhan terhadap regulasi ini dan menangani pelanggaran melalui sanksi yang sangat tinggi (hingga 4% dari total pendapatan global tahunan).

Berbeda dengan GDPR, regulasi di Indonesia, meskipun memiliki dasar hukum yang lebih kuat dengan hadirnya UU PDP, belum sepenuhnya dapat menyamai ketatnya standar yang diterapkan oleh negara-negara Eropa. Salah satu kekurangan yang dihadapi Indonesia adalah belum adanya lembaga independen yang benar-benar kuat dan memiliki wewenang penuh untuk menangani pelanggaran data pribadi.

Di Eropa, lembaga-lembaga pengawas seperti *Information Commissioner's Office* (ICO) di Inggris atau *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI) di Jerman memiliki otoritas yang sangat kuat untuk menindak pelanggar regulasi, sementara di Indonesia, meskipun telah ada Otoritas Pelindung Data Pribadi, lembaga ini masih dalam tahap penguatan dan pembentukan.

Pada pemrosesan data lintas batas, GDPR sangat ketat dengan peraturan mengenai transfer data ke luar Uni Eropa hanya dapat dilakukan ke negara yang memiliki tingkat perlindungan data yang setara. Sementara itu, meskipun Indonesia juga mengatur hal serupa dalam UU PDP Pasal 56, regulasi ini masih menghadapi tantangan dalam implementasinya, terutama dalam hal kesepakatan internasional dan pengawasan terhadap perusahaan asing yang beroperasi di Indonesia.

2. Perbandingan dengan Negara-negara Asia Tenggara

Di tingkat Asia Tenggara, negara-negara seperti Singapura, Malaysia, dan Thailand juga telah mengembangkan regulasi yang relevan untuk mengatasi tantangan yang muncul akibat perkembangan teknologi dan ancaman kejahatan siber. Singapura, misalnya, memiliki *Personal Data Protection Act* (PDPA) yang mulai diberlakukan pada 2014. PDPA Singapura sangat mirip dengan GDPR dalam hal memberikan hak-hak kepada individu terkait data pribadinya. Salah satu fitur kunci dari PDPA adalah kewajiban bagi organisasi untuk memperoleh persetujuan eksplisit sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi. Sanksi untuk pelanggaran juga cukup tegas, dengan denda mencapai SGD 1 juta.

Meskipun regulasi di Singapura sangat progresif, Indonesia lebih fokus pada pendekatan yang lebih terintegrasi dengan sektor teknologi lokal. UU PDP Indonesia tidak hanya mengatur aspek perlindungan data pribadi, tetapi juga memberikan perlindungan terhadap aspek lainnya seperti kebocoran data dan penyalahgunaan data dalam sistem digital yang lebih luas. Hal ini mencerminkan bahwa Indonesia cenderung menghadapi tantangan yang lebih kompleks dalam hal infrastruktur keamanan siber dan literasi digital masyarakatnya, yang memerlukan perhatian lebih dibandingkan dengan negara-negara lain seperti Singapura.

Malaysia juga memiliki regulasi terkait perlindungan data pribadi, yakni *Personal Data Protection Act* 2010 (PDPA), yang

dirancang untuk melindungi hak-hak individu terhadap data pribadinya yang diproses oleh organisasi. PDPA Malaysia mirip dengan undang-undang di Singapura, tetapi terdapat beberapa perbedaan dalam hal penerapan dan pengawasan. Malaysia memiliki *Personal Data Protection Commissioner* (PDPC) yang bertanggung jawab untuk memastikan kepatuhan terhadap PDPA, sementara Indonesia baru membentuk Otoritas Pelindung Data Pribadi yang hingga kini masih mengembangkan kapasitas dan wewenangnya.

Thailand memiliki *Personal Data Protection Act* (PDPA) yang baru diterapkan pada 2022, lebih lambat dibandingkan dengan negara-negara lain di Asia Tenggara. Namun, Thailand juga mencatatkan perkembangan yang signifikan dengan membentuk *Office of the Personal Data Protection Committee* yang memiliki tugas serupa dengan lembaga pengawas di negara lain. Meskipun regulasinya sudah diberlakukan, tantangan utama yang dihadapi Thailand adalah penerapan yang kurang merata, khususnya dalam sektor publik dan UMKM, yang menjadi tantangan juga bagi Indonesia.

Secara umum, meskipun UU PDP Indonesia telah menempatkan Indonesia dalam jalur yang tepat untuk meningkatkan perlindungan data pribadi, tantangan dalam hal infrastruktur, kesadaran hukum masyarakat, dan kapasitas lembaga pengawas masih menjadi hambatan yang perlu diatasi. Di sisi lain, negara-negara Asia Tenggara lainnya, meskipun sudah memiliki regulasi yang sebanding, juga menghadapi tantangan yang serupa dalam hal implementasi dan penegakan hukum. Oleh karena itu, pengembangan dan penerapan regulasi perlindungan data pribadi di Indonesia memerlukan kerjasama antara pemerintah, sektor swasta, dan masyarakat untuk memastikan bahwa regulasi ini dapat efektif mengatasi kejahatan siber dan melindungi privasi digital warga negara.

BAB III
JENIS-JENIS KEJAHATAN SIBER

Kejahatan siber merupakan bentuk tindak pidana yang memanfaatkan teknologi informasi dan komunikasi untuk melakukan pelanggaran terhadap hukum, sering kali berhubungan dengan sistem komputer dan jaringan digital. Seiring dengan pesatnya perkembangan teknologi digital, kejahatan siber semakin kompleks dan beragam, mencakup berbagai tindakan yang merugikan individu, organisasi, bahkan negara. Berbagai jenis kejahatan siber, mulai dari pencurian data pribadi, penipuan daring, hingga serangan terhadap infrastruktur kritikal, menuntut perhatian serius baik dari sisi regulasi hukum maupun teknologi. Kejahatan siber tidak hanya mencakup pelanggaran terhadap privasi dan data pribadi, tetapi juga dapat berdampak pada ekonomi, keamanan, dan stabilitas sosial. Misalnya, serangan *ransomware* yang mengunci data perusahaan hingga meminta tebusan atau penipuan berbasis *phishing* yang merugikan korban secara finansial. Karena sifatnya yang terdesentralisasi dan lintas batas negara, kejahatan siber menjadi tantangan besar bagi penegakan hukum yang memerlukan kerja sama internasional. Oleh karena itu, penting untuk memahami berbagai jenis kejahatan siber, baik yang melibatkan individu maupun kelompok, untuk merumuskan langkah-langkah pencegahan yang lebih efektif dan menciptakan sistem yang lebih aman di dunia maya.

A. *Cyber Fraud* (Penipuan Online, *Skimming*, *Phishing*)

1. Pengertian dan Jenis-jenis *Cyber Fraud*

Cyber fraud merujuk pada segala bentuk penipuan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya internet, untuk melakukan kejahatan yang merugikan pihak lain, baik individu maupun organisasi. Penipuan online ini dapat dilakukan dalam berbagai bentuk, dengan tujuan utama untuk memperoleh keuntungan finansial atau informasi pribadi dengan cara

yang tidak sah. Salah satu bentuk *cyber fraud* yang umum terjadi adalah *phishing*, di mana pelaku mencoba untuk memperoleh data sensitif seperti nomor kartu kredit, informasi login, atau data pribadi lainnya dengan cara yang menipu. *Phishing* dapat dilakukan melalui email, pesan instan, atau bahkan situs web palsu yang meniru situs resmi.

Skimming juga merupakan jenis *cyber fraud* yang semakin banyak terjadi. *Skimming* adalah teknik di mana pelaku menyalin informasi kartu kredit atau debit menggunakan perangkat khusus, kemudian menggunakan data tersebut untuk melakukan transaksi ilegal. Biasanya, *skimming* ini terjadi di mesin ATM atau perangkat POS (*Point of Sale*) yang tidak terlindungi dengan baik. Meskipun perangkat keras yang digunakan untuk *skimming* sering kali kecil dan tidak terlihat, dampaknya terhadap korban sangat besar, karena dapat kehilangan akses ke rekening bank atau bahkan seluruh tabungannya. Penipuan online yang terjadi di dunia maya ini sangat beragam, namun sering kali melibatkan manipulasi psikologis dan kecanggihan teknologi untuk menipu korban. Berdasarkan data dari Symantec (2019), lebih dari 1,5 juta kasus penipuan online terjadi setiap tahun di seluruh dunia, yang menunjukkan betapa besarnya ancaman yang dihadapi oleh pengguna internet saat ini. Hal ini menandakan pentingnya kesadaran dan perlindungan yang lebih baik terhadap ancaman-ancaman siber semacam ini.

Salah satu contoh serangan *phishing* yang cukup terkenal adalah *phishing* melalui email yang mengatasnamakan bank atau lembaga keuangan lain. Pelaku mengirimkan email yang tampak seperti pemberitahuan resmi dari bank, meminta penerima untuk mengklik link dan memasukkan informasi akunnya. Dalam beberapa kasus, pelaku dapat menyamar sebagai organisasi yang memiliki kredibilitas tinggi untuk meyakinkan korban agar memberikan informasi pribadi. Selain itu, jenis *cyber fraud* lainnya yang merugikan banyak pengguna internet adalah penipuan berbasis transaksi e-commerce. Dengan semakin berkembangnya platform perdagangan online, penipuan semacam ini dapat berupa penjualan barang palsu, barang yang tidak pernah dikirimkan, atau barang yang tidak sesuai dengan deskripsi yang diberikan. Misalnya, seorang konsumen dapat membeli barang melalui situs web yang tampaknya resmi, namun setelah pembayaran dilakukan, barang yang dijanjikan tidak pernah sampai.

2. Dampak dan Upaya Penanggulangan *Cyber Fraud*

Cyber fraud atau penipuan online adalah salah satu bentuk kejahatan siber yang semakin marak seiring dengan perkembangan pesat teknologi informasi dan komunikasi. Kejahatan ini melibatkan berbagai metode yang digunakan oleh pelaku untuk menipu korban dan memperoleh keuntungan secara tidak sah, seperti *phishing*, *skimming*, dan penipuan e-commerce. Dampak dari *cyber fraud* tidak hanya dirasakan oleh individu sebagai korban, tetapi juga memiliki implikasi yang lebih luas, terutama bagi dunia digital dan ekonomi. Di Indonesia, dengan penetrasi internet yang terus berkembang, potensi terjadinya *cyber fraud* semakin besar, sehingga upaya penanggulangan yang efektif sangat diperlukan. Penipuan online dapat merusak kepercayaan masyarakat terhadap transaksi digital dan e-commerce, yang kini menjadi bagian penting dari kehidupan sehari-hari.

Pada beberapa tahun terakhir, data menunjukkan bahwa kerugian akibat *cyber fraud* semakin meningkat. Menurut laporan dari *Federal Trade Commission* (FTC) pada tahun 2020, kerugian akibat penipuan online di Amerika Serikat mencapai lebih dari $1,9 miliar, dengan *phishing* sebagai salah satu metode utama yang digunakan pelaku untuk mencuri informasi pribadi dan finansial korban. Di Indonesia, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melaporkan bahwa sekitar 20% pengguna internet Indonesia pernah menjadi korban penipuan online, yang mencakup berbagai bentuk penipuan seperti pembelian barang palsu, penipuan investasi, dan pencurian data pribadi melalui metode *phishing*. Angka ini menunjukkan besarnya ancaman yang dihadapi masyarakat, yang tidak hanya berdampak pada korban secara finansial, tetapi juga merusak integritas dan kepercayaan terhadap platform digital.

Dampak sosial dari *cyber fraud* juga signifikan. Masyarakat yang telah menjadi korban penipuan online sering kali merasa dirugikan dan kehilangan rasa aman dalam melakukan transaksi digital. Kepercayaan publik terhadap sistem e-commerce dan perbankan digital dapat menurun, yang pada akhirnya dapat mempengaruhi pertumbuhan sektor ekonomi digital di Indonesia. Hal ini menjadi tantangan besar bagi industri yang bergantung pada transaksi digital, karena kepercayaan konsumen adalah faktor kunci untuk kelangsungan dan pertumbuhan bisnis di dunia maya. Meskipun sebagian besar pelaku *cyber fraud* dapat menghindari deteksi melalui anonimitas yang disediakan oleh internet,

dampak jangka panjang terhadap ekonomi digital sangat besar, sehingga diperlukan upaya yang lebih intensif untuk mengurangi risiko ini.

Upaya penanggulangan *cyber fraud* di Indonesia melibatkan peran aktif berbagai pihak, baik pemerintah, sektor swasta, maupun masyarakat. Pemerintah Indonesia telah mengeluarkan berbagai regulasi yang bertujuan untuk menanggulangi tindak pidana siber, termasuk *cyber fraud*. Salah satu regulasi utama adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur berbagai bentuk tindak pidana yang dilakukan melalui media elektronik, termasuk penipuan online. UU ITE memberikan dasar hukum yang jelas bagi penegak hukum untuk menangani kasus-kasus *cyber fraud*, meskipun implementasinya masih menghadapi tantangan dalam hal penegakan hukum dan koordinasi antar lembaga. Meskipun demikian, UU ITE telah menjadi landasan penting dalam pemberantasan kejahatan siber di Indonesia dan memberikan perlindungan kepada korban yang dirugikan.

Sektor swasta juga memiliki peran yang sangat penting dalam mengatasi *cyber fraud*. Banyak perusahaan teknologi, terutama yang bergerak di sektor e-commerce dan perbankan digital, telah mengembangkan dan menerapkan berbagai teknologi untuk melindungi data pengguna dan mencegah penipuan online. Salah satu teknologi yang sangat efektif dalam hal ini adalah autentikasi dua faktor (2FA). Autentikasi dua faktor memberikan lapisan tambahan keamanan di luar penggunaan password, sehingga meskipun password pengguna berhasil dicuri, pelaku tidak dapat mengakses akun tanpa kode verifikasi tambahan yang dikirimkan ke perangkat pengguna. Teknologi ini sudah banyak diterapkan oleh platform e-commerce besar dan penyedia layanan perbankan digital untuk memberikan jaminan bahwa transaksi yang dilakukan aman dan terlindungi.

Teknologi enkripsi juga berperan penting dalam menjaga keamanan data pengguna. Enkripsi adalah proses mengubah data yang dapat dibaca menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dengan enkripsi, meskipun data berhasil dicegat selama transmisi, informasi yang diperoleh oleh pelaku tidak dapat digunakan karena telah diubah menjadi bentuk yang tidak bisa dipahami. Banyak platform digital yang kini mengadopsi enkripsi tingkat tinggi untuk melindungi transaksi dan komunikasi antara pengguna dan penyedia layanan. Teknologi ini membantu mengurangi potensi

kerugian yang diakibatkan oleh serangan siber yang bertujuan untuk mencuri informasi pribadi dan finansial pengguna.

Teknologi saja tidak cukup untuk menanggulangi *cyber fraud* secara efektif. Kesadaran dan edukasi masyarakat menjadi faktor penting dalam mencegah kejahatan ini. Banyak korban penipuan online yang disebabkan oleh kelalaian atau kurangnya pengetahuan dalam mengenali tanda-tanda penipuan. Oleh karena itu, pemerintah dan sektor swasta harus bekerja sama dalam mengedukasi masyarakat tentang cara-cara melindungi data pribadinya dan mengenali potensi ancaman siber. Kampanye literasi digital yang menjelaskan pentingnya pengamanan data pribadi dan memberikan panduan tentang cara menghindari penipuan online sangat penting untuk membangun kesadaran dan memberikan perlindungan kepada masyarakat.

Beberapa lembaga pemerintah dan swasta telah memulai inisiatif untuk meningkatkan literasi digital, seperti mengadakan seminar, pelatihan, dan sosialisasi mengenai cara mengenali penipuan online. Masyarakat juga disarankan untuk lebih berhati-hati dalam memasukkan informasi pribadinya di situs web, memeriksa alamat situs untuk memastikan keasliannya, dan tidak mengklik tautan dari email yang mencurigakan atau tidak dikenal. Selain itu, pengguna juga harus menghindari berbagi informasi pribadi secara sembarangan, terutama di media sosial atau platform yang tidak dapat dipertanggungjawabkan.

Penerapan kebijakan yang ketat oleh platform e-commerce dan penyedia layanan digital juga sangat penting dalam pencegahan *cyber fraud*. Banyak platform e-commerce yang kini menerapkan kebijakan untuk memverifikasi identitas pedagang atau penjual sebelum dapat berjualan di platformnya. Selain itu, platform-platform ini juga sering menyediakan sistem untuk melaporkan penjual yang terlibat dalam aktivitas penipuan, sehingga konsumen dapat melindungi dirinya sendiri dan sesama pengguna dari penipuan. Sistem pembayaran yang aman juga menjadi bagian integral dari upaya pencegahan penipuan online, dengan menyediakan perlindungan bagi konsumen dalam transaksi yang mencurigakan.

B. *Cyber Terrorism* dan Keamanan Nasional

1. Pengertian dan Ciri-ciri *Cyber Terrorism*

Cyber terrorism adalah bentuk serangan siber yang dirancang dengan tujuan untuk menyebabkan ketakutan, kerusakan besar, atau gangguan pada infrastruktur vital sebuah negara. Serangan semacam ini memiliki karakteristik yang sangat berbeda dengan kejahatan siber biasa, yang sering kali berfokus pada keuntungan pribadi atau finansial. *Cyber terrorism* biasanya dilakukan dengan motif politik atau ideologis yang berkaitan dengan tujuan untuk mengubah keadaan sosial, politik, atau ekonomi melalui penggunaan teknologi. Biasanya, serangan ini berfokus pada menghancurkan atau merusak sistem yang mendukung infrastruktur negara, yang pada gilirannya dapat menyebabkan dampak yang luas pada kehidupan sehari-hari masyarakat. Infrastruktur yang menjadi sasaran serangan ini meliputi sektor-sektor vital seperti sistem energi, keuangan, komunikasi, serta layanan publik lainnya yang sangat penting bagi kelangsungan hidup negara.

Salah satu contoh yang paling terkenal dalam sejarah *cyber terrorism* adalah serangan Stuxnet pada tahun 2010. Serangan ini dirancang untuk merusak fasilitas nuklir Iran dengan cara yang sangat canggih, memanfaatkan kelemahan perangkat lunak yang digunakan dalam sistem pengendalian industri. Stuxnet bukan hanya sekadar virus atau *malware* biasa, tetapi merupakan sebuah senjata siber yang dirancang untuk merusak secara fisik peralatan industri yang digunakan dalam pengolahan uranium di Iran. Serangan ini menonjolkan betapa besar potensi kerusakan yang dapat diakibatkan oleh *cyber terrorism*, yang tidak hanya merusak data atau sistem komputer, tetapi juga dapat memengaruhi infrastruktur fisik yang vital bagi negara. Dalam hal ini, serangan cyber dapat memiliki dampak langsung yang setara dengan serangan fisik terhadap fasilitas strategis negara.

Salah satu ciri khas dari *cyber terrorism* adalah tujuannya untuk menciptakan ketakutan. Serangan yang dilakukan tidak hanya bertujuan untuk menghancurkan atau merusak infrastruktur vital, tetapi juga untuk menimbulkan ketegangan sosial atau politik. Ketika serangan siber berhasil merusak sistem yang mendukung kelangsungan hidup negara atau merusak kepercayaan publik terhadap pemerintah, maka dampaknya bisa jauh lebih besar daripada sekadar kerugian material. Ketakutan yang ditimbulkan oleh serangan semacam ini bisa

menciptakan ketidakstabilan sosial yang bisa dimanfaatkan oleh kelompok atau individu dengan agenda tertentu. Selain itu, *cyber terrorism* juga sering kali digunakan sebagai sarana untuk menyebarkan informasi yang salah atau berbahaya guna memanipulasi opini publik dan menciptakan ketegangan yang lebih besar di masyarakat.

Cyber terrorism sering kali dilakukan dengan menggunakan teknologi yang canggih, yang membuatnya semakin sulit untuk dideteksi atau dilawan. Pelaku kejahatan ini sering kali memanfaatkan kelemahan dalam sistem komputer dan perangkat lunak yang digunakan oleh negara atau perusahaan. Karena sifatnya yang sangat terdesentralisasi dan sering kali sulit dilacak, pelaku *cyber terrorism* dapat dengan mudah menyusup ke dalam jaringan yang sangat aman dan merusak sistem dari dalam tanpa menimbulkan gejolak fisik yang terlihat. Dalam banyak kasus, serangan ini juga dapat dilakukan oleh aktor negara atau kelompok teroris yang memiliki kemampuan teknis tinggi dan sumber daya yang memadai. Ini berarti bahwa *cyber terrorism* bukan hanya merupakan ancaman bagi individu atau perusahaan, tetapi juga bagi keamanan nasional dan global.

Dampak dari *cyber terrorism* tidak hanya terbatas pada kerusakan fisik atau gangguan terhadap infrastruktur. Kejahatan ini juga dapat menimbulkan kerugian ekonomi yang sangat besar. Ketika sebuah negara atau perusahaan menjadi korban serangan siber yang besar, biaya pemulihan dan perbaikan bisa sangat tinggi. Misalnya, kerusakan yang terjadi pada sistem energi atau transportasi dapat menyebabkan gangguan yang luas pada perekonomian negara, karena infrastruktur ini mendukung hampir semua aspek kehidupan ekonomi. Selain itu, kerusakan pada data sensitif yang digunakan oleh pemerintah dan perusahaan dapat mengarah pada kebocoran informasi yang sangat merugikan, baik secara finansial maupun reputasi. Kerugian ekonomi yang diakibatkan oleh *cyber terrorism* bisa sangat luas, termasuk biaya untuk memperbaiki kerusakan sistem, mengganti perangkat keras, serta mengembalikan kepercayaan masyarakat terhadap sistem yang telah diserang.

Di tingkat global, *cyber terrorism* menjadi ancaman yang semakin besar karena kemampuannya untuk menembus perbatasan negara dengan mudah. Dengan menggunakan internet, pelaku serangan tidak perlu berada di negara yang menjadi sasaran serangan untuk dapat melakukan aksinya. Hal ini membuat *cyber terrorism* jauh lebih sulit

untuk dikendalikan, terutama ketika pelaku berasal dari negara yang tidak dapat dijangkau oleh hukum internasional atau memiliki kepentingan politik yang berbeda. Keberadaan jaringan komputer global yang saling terhubung membuat dunia maya menjadi medan yang sangat kompleks dan rentan terhadap ancaman seperti *cyber terrorism*. Keberhasilan serangan siber di satu negara bisa berdampak langsung pada negara lain yang bergantung pada sistem yang sama atau yang terhubung melalui jaringan global. Ini menjadikan *cyber terrorism* sebagai ancaman yang lebih besar daripada kejahatan siber konvensional yang terlokalisasi pada satu wilayah tertentu.

Menurut laporan dari *United Nations Office on Drugs and Crime* (UNODC) pada 2019, lebih dari 50 negara di dunia mengalami insiden yang diduga terkait dengan *cyber terrorism*, yang menunjukkan tingkat ancaman global yang sangat tinggi. Kejahatan ini memiliki potensi untuk menyebabkan ketidakstabilan di tingkat internasional, mengingat dampaknya yang luas dan kemampuannya untuk merusak negara tanpa melibatkan kekerasan fisik. Dalam konteks ini, kolaborasi internasional sangat penting untuk mengatasi ancaman ini. Negara-negara di seluruh dunia harus bekerja sama untuk mengembangkan kebijakan yang lebih baik dalam mencegah dan menangani *cyber terrorism*, serta memperkuat sistem keamanan siber untuk melindungi infrastruktur vital dari serangan. Pendekatan yang lebih kolaboratif ini sangat diperlukan untuk mengurangi risiko serangan siber yang dapat menimbulkan kerusakan besar bagi negara dan masyarakat.

Salah satu tantangan utama dalam mengatasi *cyber terrorism* adalah adanya kesenjangan dalam kesiapan teknis dan kebijakan antara negara-negara di seluruh dunia. Beberapa negara mungkin memiliki infrastruktur teknologi yang lebih maju dan sistem keamanan yang lebih kuat, sementara negara lain mungkin masih mengalami kesulitan dalam mengembangkan kemampuan untuk mendeteksi dan melawan serangan siber. Oleh karena itu, penting bagi negara-negara dengan kemampuan teknis yang lebih baik untuk berbagi pengetahuan dan sumber daya dengan negara-negara yang lebih rentan terhadap ancaman ini. Kerja sama internasional dalam hal ini tidak hanya mencakup pertukaran informasi dan teknologi, tetapi juga mencakup penyusunan perjanjian internasional yang dapat mengatur penanganan *cyber terrorism* secara lebih efektif. Upaya bersama ini dapat membantu menciptakan sistem

global yang lebih aman dan lebih tangguh terhadap ancaman yang berkembang di dunia maya.

Di Indonesia, meskipun ancaman *cyber terrorism* belum sebesar di beberapa negara maju, kesadaran akan pentingnya keamanan siber terus berkembang. Pemerintah Indonesia telah mulai mengimplementasikan berbagai kebijakan yang berkaitan dengan perlindungan infrastruktur kritis dan keamanan digital. Salah satu langkah yang diambil adalah melalui pembentukan Badan Siber dan Sandi Negara (BSSN), yang bertugas untuk mengelola keamanan siber di Indonesia, termasuk melindungi infrastruktur kritis dan menangani ancaman *cyber terrorism*. Selain itu, pemerintah juga telah mengeluarkan kebijakan yang mempromosikan peningkatan kesadaran akan ancaman siber dan pentingnya perlindungan data pribadi di kalangan masyarakat. Meski demikian, masih ada banyak pekerjaan yang harus dilakukan untuk memastikan bahwa Indonesia dapat menghadapi ancaman *cyber terrorism* dengan cara yang efektif, baik dari segi teknis maupun kebijakan.

2. Dampak *Cyber Terrorism* terhadap Keamanan Nasional

Dampak dari *cyber terrorism* sangat luas dan bisa mencakup banyak aspek kehidupan suatu negara, baik dari segi keamanan fisik, ekonomi, maupun sosial. Salah satu dampak paling signifikan adalah terhadap keamanan nasional itu sendiri, karena serangan siber bisa merusak sektor-sektor yang sangat vital, seperti energi, transportasi, perbankan, dan komunikasi. Jika sistem energi atau transportasi penting terganggu, hal ini dapat menimbulkan kekacauan sosial, gangguan ekonomi, atau bahkan ancaman terhadap nyawa manusia. Sebagai contoh, serangan terhadap sistem kelistrikan negara dapat menyebabkan pemadaman listrik yang meluas, mengganggu rumah sakit, sistem komunikasi darurat, dan distribusi barang-barang vital seperti makanan dan obat-obatan.

Cyber terrorism dapat mempengaruhi kedaulatan negara. Misalnya, serangan yang menargetkan lembaga pemerintah, seperti sistem administrasi publik atau lembaga pemilihan umum, dapat mengubah hasil pemilu atau menggoyahkan kepercayaan masyarakat terhadap pemerintah. Ancaman terhadap infrastruktur kritis seperti banking system juga bisa menyebabkan kerugian finansial yang sangat besar dan mempengaruhi stabilitas ekonomi negara. Dalam beberapa

kasus, serangan siber terhadap sektor keuangan dapat menyebabkan kehilangan data finansial yang tidak dapat dipulihkan, merusak kepercayaan investor, dan memicu krisis ekonomi.

Cyber terrorism juga bisa menciptakan gangguan sosial yang sangat luas, dengan menyebarkan informasi yang salah (*disinformation*) untuk menambah ketegangan atau konflik sosial. Misalnya, serangan terhadap media sosial atau platform berita dapat digunakan untuk menyebarkan *hoaks* atau propaganda yang berpotensi merusak tatanan sosial dan memperburuk ketegangan antar kelompok masyarakat.

Salah satu contoh terbaru yang menunjukkan dampak *cyber terrorism* terhadap stabilitas nasional adalah serangan terhadap Saudi Aramco pada tahun 2012. Kelompok yang dikenal dengan nama Cutting Sword of Justice melancarkan serangan terhadap perusahaan minyak terbesar di dunia, menghancurkan lebih dari 30.000 komputer dan merusak infrastruktur vital. Serangan tersebut menyebabkan gangguan besar dalam produksi minyak dan merugikan perekonomian negara. Ini adalah contoh nyata bagaimana *cyber terrorism* dapat mempengaruhi perekonomian dan keamanan energi nasional secara langsung.

Upaya untuk melindungi negara dari *cyber terrorism* memerlukan pendekatan yang melibatkan kerja sama internasional, penguatan kebijakan dan regulasi di tingkat nasional, serta pengembangan teknologi pertahanan siber yang lebih maju. Negara-negara di seluruh dunia semakin menyadari pentingnya meningkatkan ketahanan sibernya, dengan beberapa negara seperti Amerika Serikat, Israel, dan Rusia mengembangkan unit-unit khusus untuk menangani ancaman ini. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) adalah lembaga yang bertanggung jawab untuk meningkatkan keamanan siber negara, namun tantangan besar tetap ada, terutama terkait dengan koordinasi antara sektor publik dan swasta serta kesiapan infrastruktur negara untuk menghadapi ancaman ini.

C. *Cyber Bullying* dan Kejahatan terhadap Privasi

1. Pengertian dan Bentuk-bentuk *Cyber Bullying*

Cyber bullying adalah fenomena yang semakin meluas di era digital ini, di mana interaksi antar individu sebagian besar terjadi melalui media sosial, aplikasi pesan instan, dan berbagai platform daring lainnya. Berbeda dengan bullying tradisional yang terjadi dalam kehidupan nyata

dan lebih sering melibatkan kontak fisik atau tatap muka, *cyber bullying* terjadi di dunia maya dan sering kali tidak terdeteksi oleh orang lain di sekitar korban. Pelaku *cyber bullying* dapat menyembunyikan identitasnya di balik anonimitas internet, yang memberinya kebebasan untuk melakukan intimidasi tanpa takut dikenali atau dihukum. Karena itu, dampak dari *cyber bullying* bisa lebih mendalam dan sering kali lebih sulit untuk diatasi, karena korban merasa terisolasi dan tidak memiliki dukungan sosial yang cukup untuk melawan pelaku.

Bentuk-bentuk *cyber bullying* sangat beragam dan dapat muncul dalam berbagai cara. Salah satu yang paling umum adalah penghinaan verbal, di mana pelaku menyebarkan kata-kata kasar atau menghina korban melalui pesan pribadi atau komentar di media sosial. Penghinaan ini sering kali berfokus pada penampilan fisik, status sosial, atau aspek pribadi lainnya yang sangat sensitif bagi korban. Selain itu, penyebaran gosip atau informasi pribadi yang bersifat merugikan juga sering terjadi dalam kasus *cyber bullying*. Dalam beberapa kasus, pelaku akan dengan sengaja menyebarkan informasi pribadi korban, seperti foto atau video yang memalukan, yang dapat merusak reputasi korban secara permanen. Hal ini dapat sangat merugikan korban, terutama jika informasi tersebut tersebar luas dan menjadi konsumsi publik di dunia maya.

Salah satu bentuk *cyber bullying* yang sangat berbahaya adalah doxxing, yaitu tindakan mempublikasikan informasi pribadi korban di internet tanpa izin. Informasi yang dipublikasikan bisa berupa alamat rumah, nomor telepon, email, dan bahkan tempat kerja korban. Tujuan dari doxxing adalah untuk merusak kehidupan pribadi korban dan membuatnya merasa terancam atau tidak aman. Doxxing dapat berdampak besar pada korban, tidak hanya karena kerugian sosial dan emosional, tetapi juga karena risiko fisik yang ditimbulkan. Ketika informasi pribadi seseorang tersebar di internet, menjadi lebih rentan terhadap ancaman atau kekerasan dari pihak yang tidak bertanggung jawab. Hal ini bisa menyebabkan korban merasa sangat cemas dan takut akan keselamatan dirinya dan orang-orang yang dicintai.

Fenomena *cyberstalking* juga menjadi salah satu bentuk *cyber bullying* yang sangat mengganggu. *Cyberstalking* terjadi ketika pelaku secara terus-menerus mengawasi atau mengintimidasi korban melalui dunia maya. Pelaku menggunakan berbagai informasi yang diperoleh dari internet untuk mengancam atau menakut-nakuti korban, sering kali dengan tujuan untuk mengontrol atau menguasai kehidupan korban.

Dalam beberapa kasus, pelaku *cyberstalking* dapat menghubungi korban secara terus-menerus melalui pesan elektronik atau media sosial, mengirimkan ancaman atau membuat korban merasa terjebak dalam situasi yang sangat menegangkan. *Cyberstalking* dapat sangat merusak mental korban dan menyebabkannya merasa terperangkap dalam siklus ketakutan yang sulit untuk dihentikan.

Fenomena *cyber bullying* tidak hanya terbatas pada satu kelompok usia tertentu. Namun, anak-anak dan remaja adalah kelompok yang paling rentan terhadap dampak negatif dari perilaku ini. Menurut laporan dari Pew Research Center pada tahun 2020, lebih dari 59% remaja di Amerika Serikat mengaku pernah menjadi korban *cyber bullying*. Selain itu, lebih dari 40% darinya juga mengakui bahwa pernah menjadi pelaku *cyber bullying*. Angka-angka ini menunjukkan bahwa *cyber bullying* bukan hanya masalah yang dialami oleh segelintir orang, tetapi merupakan masalah sosial yang melibatkan sebagian besar populasi, terutama di kalangan remaja yang lebih sering menggunakan internet dan media sosial untuk berinteraksi dengan teman-teman.

Dampak dari *cyber bullying* terhadap korban tidak hanya bersifat psikologis, tetapi juga dapat mempengaruhi banyak aspek kehidupan. Korban *cyber bullying* sering kali mengalami gangguan emosional yang serius, seperti kecemasan, depresi, dan perasaan terisolasi, mungkin merasa tidak punya tempat untuk berkeluh kesah atau mencari dukungan, karena serangan yang diterima terjadi di dunia maya dan sering kali tidak terlihat oleh orang lain. Hal ini dapat mengarah pada penurunan harga diri, perasaan tidak aman, dan bahkan krisis identitas. Selain itu, efek psikologis dari *cyber bullying* dapat berlanjut dalam jangka panjang, mempengaruhi kehidupan korban bahkan setelah serangan berakhir. Banyak korban yang mengalami kesulitan dalam menjalani hubungan sosial atau prestasi akademik, karena dampak emosional dari bullying yang dialami.

Pada beberapa kasus, dampak dari *cyber bullying* bahkan dapat mengarah pada tindakan yang lebih ekstrem, seperti bunuh diri. Korban yang merasa tidak ada jalan keluar dari penderitaan yang dialami, atau merasa bahwa tidak bisa lagi menghadapi penghinaan yang terus-menerus, mungkin merasa bahwa kematian adalah satu-satunya cara untuk mengakhiri rasa sakitnya. Ini adalah salah satu akibat yang paling tragis dari *cyber bullying*, yang menunjukkan betapa seriusnya masalah ini. Meskipun tidak semua korban *cyber bullying* akan sampai pada titik

ini, namun peningkatan angka bunuh diri yang terkait dengan *cyber bullying* menjadi peringatan yang sangat penting bagi masyarakat dan pihak berwenang untuk lebih memperhatikan isu ini.

Cyber bullying bukan hanya merugikan korban secara emosional, tetapi juga dapat memiliki dampak jangka panjang pada kesehatan fisik. Stres yang diakibatkan oleh bullying dapat menyebabkan masalah kesehatan seperti gangguan tidur, penurunan sistem kekebalan tubuh, atau bahkan penyakit jantung pada beberapa individu. Selain itu, korban *cyber bullying* mungkin mengalami gangguan makan, seperti anoreksia atau bulimia, sebagai bentuk upaya untuk mengontrol tubuhnya sebagai respons terhadap tekanan emosional yang dialami. Hal ini menunjukkan bahwa dampak dari *cyber bullying* tidak hanya terbatas pada masalah psikologis, tetapi juga dapat memengaruhi kesejahteraan fisik korban.

Pencegahan dan penanggulangan *cyber bullying* sangat penting dilakukan, baik oleh individu, keluarga, sekolah, maupun pemerintah. Salah satu langkah yang dapat diambil adalah dengan meningkatkan kesadaran akan masalah ini melalui pendidikan dan kampanye publik. Anak-anak dan remaja perlu diajarkan tentang bahaya *cyber bullying* dan cara menghindarinya, serta bagaimana melaporkan kejadian bullying yang dialami kepada pihak yang berwenang. Selain itu, penting bagi orang tua untuk terlibat dalam kehidupan digital anak-anak, dengan cara memantau aktivitas online dan memberikan dukungan emosional ketika menghadapi perundungan. Program-program pencegahan yang melibatkan pihak sekolah dan komunitas juga bisa sangat efektif dalam menciptakan lingkungan yang lebih aman bagi anak-anak dan remaja.

Penting juga untuk memastikan adanya mekanisme penanggulangan yang efektif bagi korban *cyber bullying*. Pemerintah dan perusahaan teknologi harus bekerja sama untuk menyediakan alat yang memungkinkan korban untuk melaporkan perundungan yang terjadi secara online, serta memastikan bahwa pelaku diidentifikasi dan diberi sanksi yang sesuai. Platform media sosial juga harus lebih bertanggung jawab dalam menangani kasus-kasus *cyber bullying* dengan cara yang lebih transparan dan efisien. Di sisi lain, masyarakat juga perlu lebih peduli terhadap isu ini dan memberikan dukungan kepada korban, baik secara emosional maupun dalam bentuk bantuan hukum jika diperlukan. Hanya dengan kolaborasi antara individu, keluarga, lembaga pendidikan, pemerintah, dan sektor swasta, kita dapat mengurangi

dampak negatif dari *cyber bullying* dan menciptakan dunia maya yang lebih aman dan ramah bagi semua orang.

2. Kejahatan terhadap Privasi dan Perlindungan Data Pribadi

Kejahatan terhadap privasi atau pelanggaran privasi digital menjadi salah satu bentuk kejahatan siber yang semakin meresahkan di era digital ini. Seiring dengan perkembangan teknologi dan peningkatan ketergantungan masyarakat terhadap dunia maya, setiap individu kini meninggalkan jejak digital yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Kejahatan ini terjadi ketika informasi pribadi seseorang, seperti identitas, data keuangan, atau bahkan preferensi pribadi, diakses atau digunakan tanpa izin dan sering kali untuk tujuan yang merugikan korban. Di dunia yang semakin terhubung, pelanggaran privasi ini tidak hanya merugikan individu, tetapi juga dapat mengancam stabilitas sosial dan keamanan nasional. Fenomena ini mencakup berbagai bentuk kejahatan, mulai dari pencurian identitas hingga pembobolan akun pribadi yang bisa berdampak luas, tidak hanya bagi individu tetapi juga perusahaan dan institusi yang menyimpan data pribadi.

Salah satu bentuk paling merusak dari kejahatan terhadap privasi adalah pencurian identitas. Dalam kasus ini, pelaku memperoleh informasi pribadi korban, seperti nomor identitas, data kartu kredit, atau informasi penting lainnya, untuk melakukan berbagai tindakan kriminal. Misalnya, pelaku dapat menggunakan data tersebut untuk mengajukan pinjaman atau melakukan pembelian secara ilegal dengan menggunakan kartu kredit korban. Pencurian identitas ini sering kali berlangsung tanpa sepengetahuan korban, yang membuatnya terkejut saat mengetahui adanya transaksi atau utang yang tidak dilakukan. Selain itu, tindakan ini juga dapat mencemari reputasi korban, karena terpaksa berurusan dengan masalah hukum atau keuangan yang timbul akibat pencurian tersebut. Kejahatan ini bukan hanya menuntut biaya finansial, tetapi juga waktu dan energi yang besar untuk memulihkan identitas dan reputasi korban.

Ancaman lain terhadap privasi adalah pembobolan akun atau *hacking*, yang merupakan salah satu metode yang paling sering digunakan oleh pelaku kejahatan siber. Dalam hal ini, pelaku akan mencoba mengakses akun pribadi korban, baik itu akun media sosial, akun perbankan, atau aplikasi lain yang menyimpan data pribadi.

Pembobolan akun dapat dilakukan dengan berbagai cara, mulai dari penggunaan teknik brute force untuk menebak kata sandi hingga serangan *phishing* yang lebih canggih. Setelah berhasil mengakses akun, pelaku dapat mengubah kata sandi, mencuri informasi sensitif, atau bahkan melakukan transaksi yang merugikan korban. Selain itu, pembobolan akun sering kali berdampak pada kerugian jangka panjang bagi korban, yang bisa termasuk pencurian uang, hilangnya data penting, hingga ancaman terhadap keselamatan pribadi jika informasi sensitif digunakan dengan niat jahat.

Kasus pembocoran data yang melibatkan Facebook dan Cambridge Analytica pada tahun 2018 menjadi salah satu contoh yang paling mencolok tentang bagaimana data pribadi bisa disalahgunakan. Dalam kasus ini, lebih dari 87 juta data pengguna Facebook digunakan secara tidak sah oleh perusahaan analitik Cambridge Analytica untuk tujuan politik. Pembocoran data ini memicu gelombang kekhawatiran global mengenai bagaimana data pribadi bisa dijual atau digunakan oleh perusahaan untuk kepentingan tertentu tanpa persetujuan dari pemilik data. Fenomena ini membahas pentingnya perlindungan data pribadi di dunia maya, serta ketidakberdayaan pengguna dalam melindungi datanya sendiri. Kasus ini juga memicu tuntutan agar platform teknologi besar lebih transparan dalam mengelola data pengguna dan bertanggung jawab atas penyalahgunaan data yang terjadi.

Penjualan data pribadi menjadi salah satu praktik yang semakin berkembang dalam kejahatan siber. Dalam beberapa tahun terakhir, telah muncul pasar gelap yang memungkinkan individu atau perusahaan untuk membeli dan menjual data pribadi tanpa kontrol yang jelas. Data yang dijual ini bisa mencakup berbagai jenis informasi, seperti nomor kartu kredit, alamat email, hingga riwayat belanja atau preferensi pribadi. Perusahaan-perusahaan ini, baik yang terlibat secara langsung dalam penjualan data maupun yang mengumpulkannya untuk tujuan pemasaran, sering kali melakukannya tanpa sepengetahuan atau persetujuan dari pemilik data. Dalam banyak kasus, data ini digunakan untuk menargetkan iklan yang sangat spesifik atau bahkan untuk melakukan serangan siber yang lebih besar. Praktik ini jelas melanggar hak privasi individu dan semakin memperburuk masalah yang dihadapi dalam melindungi data pribadi di dunia maya.

Untuk mengatasi ancaman ini, banyak negara yang telah mengeluarkan regulasi untuk melindungi data pribadi warganya. Salah

satu regulasi yang paling terkenal adalah *General Data Protection Regulation* (GDPR), yang diberlakukan oleh Uni Eropa pada tahun 2018. GDPR memberikan kontrol lebih besar kepada individu terkait penggunaan dan distribusi data pribadinya. Regulasi ini mewajibkan perusahaan untuk mendapatkan izin eksplisit dari pengguna sebelum mengumpulkan data pribadi dan memberi hak kepada individu untuk meminta penghapusan datanya jika tidak lagi ingin berbagi informasi tersebut. GDPR juga mengenakan denda yang signifikan bagi perusahaan yang melanggar aturan ini, sebagai upaya untuk mendorong perusahaan lebih bertanggung jawab dalam mengelola data pribadi.

Di Indonesia, upaya untuk melindungi privasi digital diwujudkan melalui Undang-Undang Perlindungan Data Pribadi yang disahkan pada tahun 2022. Undang-undang ini dirancang untuk mengatur cara-cara yang sah dan adil dalam pengumpulan, pemrosesan, dan distribusi data pribadi, serta memberikan hak kepada individu untuk mengontrol data pribadi. Undang-undang ini juga memberikan perlindungan hukum bagi individu jika datanya digunakan secara tidak sah atau disalahgunakan oleh pihak lain. Selain itu, UU ini juga memberikan kewajiban kepada perusahaan dan entitas lain untuk mengimplementasikan langkah-langkah yang efektif dalam melindungi data pribadi yang dikelola. Dengan adanya regulasi seperti ini, diharapkan dapat menciptakan iklim yang lebih aman dan terlindungi bagi para pengguna internet di Indonesia.

Meskipun regulasi dan kebijakan yang ada sangat penting, namun perlindungan privasi tidak hanya bergantung pada pihak pemerintah atau perusahaan teknologi. Pengguna internet juga memiliki peran penting dalam menjaga privasi digital. Salah satu langkah yang dapat diambil adalah dengan menerapkan keamanan siber yang baik, seperti penggunaan enkripsi untuk melindungi data yang dikirimkan melalui internet. Selain itu, autentikasi dua faktor (2FA) juga merupakan salah satu cara efektif untuk mengamankan akun pribadi dari akses yang tidak sah. 2FA menambahkan lapisan keamanan tambahan dengan meminta pengguna untuk memasukkan kode yang dikirimkan ke perangkat lain selain kata sandi. Langkah-langkah ini dapat membantu mencegah serangan siber yang lebih canggih dan memastikan bahwa data pribadi tetap aman dari pihak-pihak yang tidak bertanggung jawab.

Penting juga bagi pengguna untuk lebih waspada dalam membagikan informasi pribadi di dunia maya. Seringkali, para pelaku

kejahatan siber menggunakan teknik *phishing* untuk mencuri data pribadi, dengan cara menyamar sebagai entitas yang sah seperti bank atau perusahaan besar. Dalam kasus *phishing*, korban akan diminta untuk mengungkapkan informasi sensitif, seperti nomor kartu kredit atau kata sandi, dengan berpura-pura bahwa itu adalah langkah keamanan yang sah. Untuk menghindari jebakan ini, penting bagi pengguna untuk selalu memeriksa keaslian pesan yang diterima dan menghindari memberikan informasi pribadi melalui saluran yang tidak terpercaya.

Kejahatan terhadap privasi dan perlindungan data pribadi merupakan ancaman yang serius di dunia digital saat ini. Dampaknya dapat sangat merusak, baik bagi individu yang menjadi korban maupun bagi seluruh sistem sosial dan ekonomi yang bergantung pada kepercayaan dan keamanan data. Oleh karena itu, upaya untuk melindungi privasi digital harus dilakukan secara terpadu, melibatkan regulasi yang ketat, kesadaran masyarakat, dan tindakan preventif yang proaktif. Tanpa langkah-langkah ini, kejahatan terhadap privasi akan terus berkembang dan semakin sulit untuk dikendalikan. Keamanan data pribadi harus menjadi prioritas utama bagi semua pihak yang terlibat, baik individu, perusahaan, maupun pemerintah.

D. Penyebaran *Hoaks*, *Hate Speech*, dan Ujaran Kebencian

1. Pengertian dan Dampak Penyebaran *Hoaks*

Hoaks adalah informasi yang sengaja dibuat atau disebarkan dengan tujuan untuk menipu, menyesatkan, atau memanipulasi opini publik. Informasi ini seringkali tidak terverifikasi dan berisi klaim-klaim yang salah atau tidak berdasar, yang bisa sangat merugikan bagi masyarakat. Penyebaran *hoaks* dapat terjadi melalui berbagai saluran, terutama melalui media sosial, situs web, aplikasi pesan instan, dan platform digital lainnya. Dalam beberapa kasus, *hoaks* juga disebarkan oleh kelompok atau entitas tertentu yang memiliki tujuan untuk mempengaruhi opini publik, mengubah pandangan masyarakat, atau memperburuk situasi sosial yang ada. *Hoaks* dapat berupa berita palsu, teori konspirasi, atau bahkan informasi yang sengaja diciptakan untuk menimbulkan kebingungan atau ketakutan di kalangan masyarakat.

Penyebaran *hoaks* memiliki dampak yang sangat merugikan bagi masyarakat dan negara. Salah satu dampak paling signifikan adalah

munculnya ketidakpercayaan publik terhadap informasi yang sah dan sumber berita yang terpercaya. Ketika masyarakat terus-menerus terpapar dengan informasi palsu, cenderung menjadi lebih skeptis terhadap kebenaran dan kesulitan untuk membedakan antara informasi yang benar dan salah. Fenomena ini mengarah pada apa yang disebut sebagai "*post-truth era*," di mana opini dan persepsi pribadi sering kali lebih dihargai daripada fakta yang dapat dipertanggungjawabkan. Masyarakat yang terus disesatkan oleh *hoaks* menjadi lebih sulit untuk mempercayai informasi yang valid, sehingga berdampak pada kualitas debat publik dan pengambilan keputusan yang berbasis pada fakta.

Penyebaran *hoaks* dapat memperburuk ketegangan sosial yang sudah ada di masyarakat. *Hoaks* sering kali dibuat dan disebarkan untuk menciptakan polarisasi antar kelompok atau individu. *Hoaks* yang berkaitan dengan isu-isu sensitif, seperti agama, ras, atau politik, dapat memicu pertentangan antar kelompok yang berbeda. Dalam situasi seperti ini, *hoaks* dapat memperburuk ketegangan yang ada dan bahkan dapat mengarah pada konflik sosial. Salah satu contoh yang sangat relevan adalah *hoaks* yang berkaitan dengan ras atau agama, di mana informasi palsu yang disebarkan dapat menyebabkan kebencian atau ketegangan antara kelompok-kelompok tertentu dalam masyarakat, yang pada gilirannya dapat menimbulkan ketidakstabilan sosial.

Contoh konkret dari dampak *hoaks* dalam politik terjadi pada pemilu 2019 di Indonesia. Pada pemilu tersebut, banyak *hoaks* yang disebarkan melalui aplikasi WhatsApp dan media sosial yang berusaha mempengaruhi persepsi publik terhadap calon presiden dan isu-isu tertentu. Salah satu *hoaks* yang beredar adalah klaim palsu yang menyatakan bahwa salah satu pasangan calon presiden terlibat dalam kegiatan yang merugikan agama tertentu. *Hoaks* ini disebarkan dengan tujuan untuk menghasut kebencian dan memperburuk hubungan antar kelompok masyarakat yang memiliki afiliasi politik atau agama yang berbeda. Penyebaran informasi palsu semacam ini dapat mengganggu proses demokrasi, mempengaruhi hasil pemilu, dan merusak integritas sistem politik yang seharusnya berjalan dengan jujur dan adil.

Hoaks juga dapat merugikan individu atau kelompok tertentu, baik secara pribadi maupun profesional. Salah satu contoh yang paling merusak adalah *hoaks* yang mengandung fitnah atau pencemaran nama baik. *Hoaks* seperti ini dapat menyebabkan kerusakan yang serius terhadap reputasi seseorang atau organisasi, bahkan jika informasi

tersebut tidak benar. Individu atau kelompok yang menjadi korban *hoaks* tersebut mungkin harus menghadapi konsekuensi yang tidak adil, seperti kehilangan pekerjaan, kehilangan dukungan publik, atau bahkan menghadapi tuntutan hukum akibat pencemaran nama baik yang dilakukan oleh pihak yang tidak bertanggung jawab. Meskipun bukti yang mendukung kebenaran informasi tersebut tidak ada, dampak dari *hoaks* tetap dapat merusak kehidupan korban dalam waktu yang lama.

Salah satu tantangan besar dalam menghadapi penyebaran *hoaks* adalah sulitnya mendeteksi dan membuktikan kebenaran informasi di era digital ini. Dengan berkembangnya teknologi dan akses yang lebih luas ke platform online, penyebaran informasi palsu semakin cepat dan sulit untuk dikendalikan. *Hoaks* dapat menyebar dalam hitungan detik melalui media sosial, di mana banyak pengguna yang membagikan informasi tanpa memverifikasi kebenarannya terlebih dahulu. Selain itu, sifat dari *hoaks* yang sering kali sensasional atau mengandung unsur kejutan membuatnya lebih mudah untuk menarik perhatian dan lebih cepat tersebar. *Hoaks* yang menyebar dengan cepat ini sering kali lebih banyak dikonsumsi oleh masyarakat dibandingkan dengan informasi yang sah dan sudah terverifikasi.

Untuk mengatasi dampak buruk dari *hoaks*, banyak negara dan organisasi yang telah mengambil langkah-langkah untuk memperkenalkan sistem pemeriksaan fakta yang solid. Pemeriksaan fakta bertujuan untuk memastikan bahwa informasi yang disebarkan ke publik benar-benar terverifikasi dan dapat dipertanggungjawabkan. Berbagai platform media sosial seperti Facebook, Twitter, dan WhatsApp kini juga bekerja sama dengan organisasi pemeriksa fakta untuk menandai atau bahkan menghapus konten yang terbukti palsu. Namun, meskipun ada upaya-upaya ini, tantangan untuk menangani *hoaks* tetap besar. Kecepatan penyebaran informasi dan kurangnya kesadaran dari sebagian besar pengguna internet sering kali memperburuk situasi ini.

Penyebaran *hoaks* juga berpotensi merusak hubungan antar negara, terutama dalam konteks geopolitik dan diplomasi. *Hoaks* yang sengaja disebarkan untuk memanipulasi opini publik di negara tertentu dapat mempengaruhi hubungan internasional dan memperburuk ketegangan antar negara. Misalnya, *hoaks* yang berkaitan dengan kebijakan luar negeri atau isu keamanan internasional dapat digunakan untuk memperburuk citra suatu negara di mata dunia. Dalam era di mana

informasi dapat dengan mudah dipertukarkan di seluruh dunia, *hoaks* yang disebarkan melalui internet dapat dengan cepat menciptakan kesalahpahaman yang luas dan mengganggu hubungan antar negara.

Penyebaran *hoaks* tidak hanya terjadi dalam konteks politik atau sosial, tetapi juga dapat berdampak pada ekonomi. Dalam dunia bisnis, informasi palsu yang menyebar tentang perusahaan atau produk tertentu dapat merusak reputasi perusahaan tersebut dan menurunkan nilai sahamnya. *Hoaks* yang dibuat untuk merusak citra suatu perusahaan sering kali menciptakan ketidakpastian di pasar dan merugikan banyak pihak, mulai dari investor hingga konsumen. Bahkan, perusahaan yang memiliki reputasi baik sekalipun bisa terkena dampak serius jika *hoaks* yang merugikan menyebar tentangnya. Oleh karena itu, penting bagi perusahaan untuk menjaga komunikasi yang transparan dan bekerja sama dengan pihak berwenang untuk mengatasi masalah ini.

Dampak penyebaran *hoaks* sangat luas dan dapat merusak banyak aspek kehidupan sosial, politik, dan ekonomi. *Hoaks* bukan hanya sekadar informasi yang salah, tetapi juga merupakan ancaman serius terhadap stabilitas masyarakat dan negara. Oleh karena itu, penting bagi semua pihak, baik pemerintah, masyarakat, maupun perusahaan, untuk berperan aktif dalam menangani penyebaran *hoaks*. Upaya untuk meningkatkan literasi digital, memverifikasi informasi, dan memperkuat sistem hukum dalam menghadapi penyebaran informasi palsu sangatlah penting untuk mencegah kerusakan lebih lanjut yang disebabkan oleh *hoaks*.

2. *Hate Speech* dan Ujaran Kebencian di Dunia Digital

Hate speech atau ujaran kebencian adalah salah satu bentuk komunikasi yang berisi kebencian, diskriminasi, atau penghinaan terhadap individu atau kelompok berdasarkan identitas, seperti ras, agama, etnis, orientasi seksual, atau karakteristik lainnya. Dalam konteks dunia digital yang semakin berkembang pesat, ujaran kebencian ini semakin sering ditemukan dan disebarkan melalui berbagai platform media sosial, blog, dan forum daring. Di dunia maya, pengguna memiliki kebebasan untuk mengekspresikan pendapatnya tanpa pengawasan langsung, yang sering kali membuat batasan antara kebebasan berbicara dan ujaran kebencian menjadi kabur. Ujaran kebencian ini dapat berupa komentar yang menyinggung, ancaman fisik, atau penghinaan yang

ditujukan pada individu atau kelompok tertentu yang dianggap berbeda oleh pelaku.

Penyebaran *hate speech* dapat memiliki dampak yang sangat merugikan bagi stabilitas sosial dan keamanan masyarakat. Salah satu dampak utama dari ujaran kebencian adalah munculnya polarisasi dalam masyarakat. Ketika ujaran kebencian disebarkan dalam jumlah besar, hal ini dapat menciptakan kebencian yang mendalam antara kelompok yang berbeda. Polarisasi ini sering kali mengarah pada ketegangan rasial atau etnis yang semakin tajam, dan dalam beberapa kasus, dapat memperburuk diskriminasi yang sudah ada. Hal ini menciptakan lingkungan yang tidak aman bagi kelompok yang menjadi target ujaran kebencian tersebut, dan semakin memperburuk kesenjangan sosial yang ada dalam masyarakat.

Contoh nyata dari dampak *hate speech* dapat ditemukan dalam berbagai insiden kekerasan berbasis rasial atau agama. Di banyak negara, ujaran kebencian terhadap kelompok minoritas sering kali menjadi pemicu utama bagi terjadinya kekerasan antar kelompok. Sebagai contoh, di Indonesia, kelompok etnis atau agama tertentu terkadang menjadi sasaran ujaran kebencian yang disebarkan melalui platform digital, yang kemudian mengarah pada kerusuhan atau tindakan diskriminasi terhadapnya. Ujaran kebencian ini dapat mempengaruhi pola pikir individu dan kelompok yang lebih luas, menciptakan ketegangan yang lebih besar dan merusak ikatan sosial antar kelompok yang sebelumnya hidup berdampingan dengan damai.

Penyebaran *hate speech* juga dapat merusak hubungan antar individu dalam masyarakat yang plural. Ketika ujaran kebencian mengalir bebas di dunia maya, ini dapat menyebabkan rasa tidak aman di kalangan kelompok yang menjadi targetnya. Selain itu, dampak jangka panjang dari penyebaran ujaran kebencian ini adalah terciptanya masyarakat yang semakin terpolarisasi, di mana kepercayaan dan rasa saling menghormati antar kelompok semakin menipis. Ini memperburuk iklim sosial di tingkat lokal maupun nasional, dan dapat menyebabkan keretakan yang mendalam dalam hubungan antar sesama warga negara.

Penyebaran *hate speech* sering kali dipermudah oleh anonimitas yang diberikan oleh dunia maya. Dalam ruang digital, pelaku merasa lebih bebas untuk mengungkapkan kebencian tanpa takut akan konsekuensi langsung. Hal ini sangat berbeda dengan dunia nyata, di mana tindakan ujaran kebencian dapat langsung direspons oleh korban

atau oleh pihak berwenang. Anonimitas ini memberikan ruang bagi individu-individu untuk berbicara tanpa rasa takut akan dampaknya, sehingga membuatnya lebih sulit untuk mendeteksi dan mengatasi ujaran kebencian secara efektif. Dalam beberapa kasus, pelaku *hate speech* bahkan merasa bahwa dapat melakukannya tanpa adanya sanksi atau tindakan hukum yang nyata, yang menyebabkannya semakin berani dalam menyebarkan kebencian tersebut.

Untuk mengatasi masalah penyebaran *hate speech*, penting bagi platform digital untuk mengambil langkah-langkah preventif dalam mendeteksi dan menghapus konten yang melanggar norma-norma sosial dan hukum. Banyak platform media sosial, seperti Facebook, Twitter, dan YouTube, kini bekerja sama dengan berbagai organisasi untuk memerangi *hate speech* dengan menghapus konten-konten yang berisi ujaran kebencian dan mendeteksi aktivitas yang dapat merugikan masyarakat. Selain itu, platform-platform ini juga semakin dilibatkan dalam upaya untuk memitigasi dampak negatif dari penyebaran informasi berbahaya yang dapat merusak hubungan sosial dan menciptakan ketegangan di masyarakat. Penggunaan algoritma canggih untuk mendeteksi ujaran kebencian dan konten berbahaya di media sosial semakin berkembang untuk mempercepat respons terhadap *hoaks* dan ujaran kebencian.

Pemerintah Indonesia sendiri telah berupaya untuk mengatasi masalah *hate speech* melalui berbagai regulasi, salah satunya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini melarang penyebaran ujaran kebencian melalui media sosial dan platform digital lainnya. Namun, penerapan undang-undang ini tidak selalu mudah, karena sering kali ada ketegangan antara kebebasan berbicara dan batasan terhadap ujaran kebencian. Terkadang, penegakan hukum dalam kasus *hate speech* di dunia maya menjadi tantangan besar karena adanya perbedaan interpretasi tentang apa yang dianggap sebagai ujaran kebencian dan apa yang merupakan bentuk kebebasan berekspresi yang sah. Di sisi lain, meskipun sudah ada regulasi, masih banyak kasus yang tidak terdeteksi atau tidak diusut dengan serius, yang mengarah pada kesulitan dalam menanggulangi masalah ini secara tuntas.

Peran serta masyarakat juga sangat penting dalam menangani penyebaran *hate speech*. Masyarakat perlu dilibatkan dalam edukasi mengenai dampak dari ujaran kebencian dan pentingnya menjaga etika

dalam berkomunikasi di dunia maya. Literasi digital yang baik dapat membantu masyarakat untuk lebih berhati-hati dalam menyebarkan informasi dan mengidentifikasi konten yang berpotensi berbahaya. Upaya untuk menciptakan lingkungan digital yang sehat memerlukan kesadaran kolektif dari semua pihak, termasuk pengguna internet, penyedia layanan digital, dan pemerintah. Dengan meningkatnya kesadaran tentang bahayanya *hate speech*, diharapkan masyarakat dapat bersama-sama mengurangi dampak negatif yang ditimbulkan oleh ujaran kebencian di dunia maya.

Meskipun ada berbagai upaya yang dilakukan untuk mengatasi *hate speech*, masalah ini tetap menjadi tantangan besar. Terkadang, meskipun konten yang mengandung ujaran kebencian telah dihapus, dampaknya tetap terasa dalam bentuk ketegangan sosial dan kerusakan hubungan antar individu. Oleh karena itu, penting bagi masyarakat untuk tidak hanya mengandalkan teknologi atau regulasi hukum dalam mengatasi *hate speech*, tetapi juga untuk berfokus pada upaya-upaya preventif yang melibatkan nilai-nilai kemanusiaan dan saling menghormati. Hanya dengan demikian, kita dapat menciptakan ruang digital yang aman dan konstruktif bagi semua orang, di mana perbedaan dapat diterima dengan rasa hormat dan dialog yang membangun.

E. Peretasan dan Serangan Siber terhadap Infrastruktur Negara

1. Peretasan dan Ancaman terhadap Infrastruktur Kritis

Peretasan atau *hacking* merupakan ancaman serius terhadap keamanan siber yang dapat mengganggu stabilitas sebuah negara. Salah satu area yang sangat rentan terhadap peretasan adalah infrastruktur kritis. Infrastruktur kritis adalah elemen-elemen sistem penting yang menopang kelangsungan hidup masyarakat, seperti jaringan energi, transportasi, komunikasi, keuangan, dan sistem air. Jika infrastruktur ini terancam atau diserang, dampaknya bisa sangat luas, mulai dari kerusakan ekonomi hingga ancaman terhadap keamanan nasional. Karena peran vitalnya, infrastruktur kritis sangat dibutuhkan untuk menjalankan kegiatan negara dan kehidupan sehari-hari masyarakat.

Serangan terhadap infrastruktur kritis biasanya dilakukan oleh berbagai aktor yang memiliki motif politik, ekonomi, atau ideologis, bisa berupa kelompok teroris, individu yang bermotif pribadi, atau bahkan

negara yang menggunakan serangan siber sebagai bagian dari strategi geopolitik. Salah satu serangan yang sering digunakan dalam ancaman terhadap infrastruktur kritis adalah *Distributed Denial of Service* (DDoS). Serangan DDoS dilakukan dengan cara membanjiri sistem target dengan lalu lintas internet yang sangat tinggi sehingga membuat sistem tersebut tidak dapat diakses atau berfungsi dengan baik. Sebagai contoh, serangan DDoS terhadap Bank of Bangladesh pada tahun 2016 adalah salah satu insiden besar yang mengakibatkan pencurian lebih dari 81 juta dolar AS. Kejadian ini menunjukkan bagaimana peretasan terhadap sektor keuangan dapat menyebabkan kerugian besar, baik dari segi ekonomi maupun kepercayaan masyarakat terhadap sistem keuangan.

Peretasan menggunakan *malware* atau perangkat lunak berbahaya juga merupakan ancaman yang semakin nyata. *Malware* dapat merusak sistem, mencuri data penting, atau bahkan mengunci sistem dan menuntut tebusan untuk mengembalikannya. Salah satu serangan *malware* yang terkenal adalah serangan *ransomware* WannaCry yang terjadi pada tahun 2017. *Ransomware* ini berhasil menyerang ratusan ribu komputer di lebih dari 150 negara, termasuk rumah sakit-rumah sakit di Inggris yang sangat bergantung pada teknologi untuk menjalankan operasional. WannaCry mengenkripsi data di komputer yang terinfeksi dan meminta tebusan untuk membuka kembali akses ke data tersebut. Serangan ini mengakibatkan gangguan besar terhadap layanan publik dan organisasi yang menjalankan fungsi kritis, seperti rumah sakit yang harus menangguhkan beberapa layanan medis karena sistemnya tidak dapat diakses.

Peretasan terhadap infrastruktur kritis tidak hanya mengancam sektor publik, tetapi juga sektor swasta yang memiliki hubungan erat dengan sistem nasional. Misalnya, perusahaan-perusahaan energi, penyedia layanan komunikasi, dan lembaga-lembaga keuangan sering kali menjadi target utama peretas karena kerusakan yang ditimbulkan dari serangannya dapat langsung berdampak pada kehidupan sehari-hari masyarakat. Ketika sektor energi diserang, misalnya, dapat terjadi pemadaman listrik yang meluas yang mengganggu kehidupan sehari-hari masyarakat dan mempengaruhi operasi bisnis. Demikian pula, jika sektor komunikasi diserang, maka jaringan telekomunikasi dan internet yang sangat penting untuk konektivitas akan terganggu.

Ancaman terhadap infrastruktur kritis semakin terasa dengan meningkatnya ketergantungan negara pada sistem digital dan teknologi canggih. Dalam dunia yang semakin terhubung, infrastruktur kritis yang dulu mungkin terlindungi dari ancaman fisik kini juga menjadi sasaran utama serangan siber. Seiring dengan digitalisasi, potensi kerentanannya meningkat. Keamanan dunia maya menjadi aspek yang tidak bisa diabaikan dalam menjaga keberlanjutan fungsi negara dan masyarakat. Oleh karena itu, penting bagi pemerintah dan sektor terkait untuk mengambil langkah-langkah preventif guna meningkatkan ketahanan siber pada infrastruktur kritis. Salah satu langkah yang dapat dilakukan adalah dengan memperkuat sistem pertahanan siber, sehingga serangan dari aktor jahat bisa diminimalkan atau bahkan dicegah sejak dini.

Meningkatkan pelatihan dan kesadaran keamanan siber di kalangan individu yang terlibat dalam pengelolaan infrastruktur kritis juga menjadi hal yang sangat penting. Pelatihan ini tidak hanya ditujukan kepada tenaga ahli yang mengelola sistem siber, tetapi juga kepada karyawan dan pihak lain yang berinteraksi dengan teknologi, guna mengurangi kesalahan manusia yang sering kali menjadi celah bagi peretasan. Kesadaran akan pentingnya keamanan data dan informasi serta pengenalan terhadap potensi ancaman dapat membantu mengurangi resiko terjadinya peretasan atau serangan siber.

Penggunaan teknologi enkripsi yang lebih kuat untuk melindungi data sensitif menjadi salah satu langkah preventif yang sangat penting. Enkripsi memastikan bahwa data yang dikirim atau disimpan dalam sistem tidak dapat diakses oleh pihak yang tidak berwenang. Dengan mengimplementasikan enkripsi yang kuat, data yang tersimpan di server atau yang sedang dikirimkan antar perangkat akan lebih aman dari serangan. Teknologi enkripsi yang tepat dapat melindungi data kritis, termasuk informasi keuangan, data pribadi, dan data penting lainnya yang sangat dibutuhkan oleh negara maupun sektor swasta.

Keamanan siber untuk infrastruktur kritis juga membutuhkan kolaborasi yang erat antara sektor publik dan sektor swasta. Infrastruktur kritis sering kali melibatkan sektor swasta, seperti perusahaan energi dan penyedia layanan komunikasi, yang berperan kunci dalam menjaga keberlanjutan layanan yang sangat penting bagi masyarakat. Oleh karena itu, kolaborasi antara pemerintah dan sektor swasta sangat diperlukan dalam membangun sistem pertahanan siber yang lebih kuat dan efektif. Kerjasama ini juga meliputi pertukaran informasi mengenai ancaman

yang sedang berlangsung serta upaya mitigasi untuk mengurangi potensi kerusakan akibat serangan.

Penting bagi negara untuk memperbarui dan memperketat regulasi yang mengatur keamanan siber. Pembaruan regulasi yang sesuai dengan perkembangan teknologi dapat membantu mencegah terjadinya celah hukum yang memungkinkan serangan terhadap infrastruktur kritis. Penegakan hukum yang jelas dan tegas terhadap pelaku kejahatan siber dapat memberikan efek jera dan mencegah serangan lebih lanjut. Negara juga perlu memperkuat kerjasama internasional dalam menghadapi ancaman siber yang bersifat global. Mengingat serangan siber tidak mengenal batas negara, kerjasama internasional dalam berbagi informasi dan teknologi untuk melawan peretasan akan sangat bermanfaat.

Dengan meningkatnya ancaman terhadap infrastruktur kritis, perhatian terhadap keamanan siber harus menjadi prioritas utama. Melalui langkah-langkah preventif yang komprehensif, mulai dari penguatan sistem pertahanan hingga pelatihan keamanan siber, negara dan masyarakat dapat lebih siap menghadapi ancaman peretasan yang semakin kompleks. Mengingat dampak besar yang bisa ditimbulkan, menjaga infrastruktur kritis dari serangan siber menjadi kunci untuk memastikan keberlanjutan kehidupan sosial dan ekonomi di dunia yang semakin tergantung pada teknologi digital.

2. Respon Negara dan Kerjasama Internasional dalam Menghadapi Serangan Siber

Untuk menghadapi ancaman peretasan dan serangan siber yang semakin canggih, banyak negara telah membentuk kebijakan dan strategi keamanan siber yang terkoordinasi dan terpadu. Negara-negara besar seperti Amerika Serikat, China, dan Rusia, yang memiliki infrastruktur kritis yang sangat vital, telah mengembangkan unit-unit khusus yang bertanggung jawab untuk menangani dan mengatasi ancaman siber. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) dibentuk dengan tujuan untuk menjaga keamanan siber negara dan melindungi infrastruktur kritis dari serangan yang dapat merusak keamanan nasional. Pembentukan badan-badan semacam ini menunjukkan betapa seriusnya ancaman yang ditimbulkan oleh serangan siber terhadap negara, sehingga pengawasan dan perlindungan terhadap sistem digital negara menjadi semakin penting.

Sebagai contoh, di Amerika Serikat, pembentukan *Cybersecurity and Infrastructure Security Agency* (CISA) pada tahun 2018 menjadi langkah strategis untuk melindungi infrastruktur kritis negara dari ancaman siber. CISA tidak hanya bertugas untuk mengawasi dan melindungi sistem-sistem yang sangat penting, tetapi juga berperan dalam memberikan pelatihan kepada sektor publik dan swasta. Melalui program pelatihan ini, CISA bertujuan untuk meningkatkan pemahaman dan kesiapan masyarakat dalam menghadapi ancaman siber, serta memberinya alat dan pengetahuan untuk mengenali potensi risiko. Upaya CISA juga termasuk bekerja sama dengan berbagai lembaga internasional dalam rangka memperkuat pertahanan siber secara global. Kerjasama ini memungkinkan negara-negara untuk saling berbagi informasi dan strategi dalam melawan ancaman yang terus berkembang di dunia maya.

Di samping itu, kerjasama internasional berperan yang sangat penting dalam mengatasi serangan siber yang sering kali bersifat transnasional. Ancaman siber tidak mengenal batas negara, sehingga kerjasama antarnegara menjadi hal yang esensial dalam penanggulangan serangan yang dapat melibatkan lebih dari satu negara. Melalui forum seperti Forum Keamanan Siber Global dan lembaga-lembaga internasional seperti Interpol dan Europol, negara-negara dapat bekerja sama dalam mengidentifikasi, mencegah, dan merespons ancaman siber yang ada. Kerjasama ini juga mencakup berbagi informasi mengenai teknik-teknik mitigasi, deteksi, dan pemulihan sistem yang telah terinfeksi serangan siber. Hal ini sangat penting karena dengan berbagi pengetahuan dan pengalaman, negara-negara dapat memperkuat kemampuan dalam menangani ancaman yang lebih kompleks dan berkembang pesat.

Salah satu tantangan terbesar yang dihadapi dalam kerjasama internasional adalah masalah jurisdiksi. Ketika serangan siber melibatkan lebih dari satu negara, sulit untuk menentukan tanggung jawab hukum dan melacak pelaku yang beroperasi secara anonim. Kejahatan siber sering kali terjadi tanpa ada jejak fisik yang jelas, dan para pelaku sering menyembunyikan identitasnya dengan menggunakan teknologi yang mempersulit pelacakan. Akibatnya, banyak negara yang kesulitan dalam menuntut pelaku serangan siber secara efektif, terutama jika pelaku berada di negara yang memiliki kebijakan hukum yang berbeda atau bahkan tidak mendukung penegakan hukum internasional.

Oleh karena itu, banyak negara yang mendorong perlunya perjanjian internasional yang mengatur tentang kejahatan siber dan penegakan hukum dalam dunia maya, guna memberikan kejelasan hukum dan kerangka kerja yang jelas dalam menanggulangi serangan siber.

Peran aktor negara dalam serangan siber menjadi masalah yang semakin kompleks. Beberapa negara besar, dengan kemampuan teknologi yang canggih, sering kali terlibat dalam serangan siber yang dirancang untuk mencuri data, merusak infrastruktur, atau mengganggu stabilitas politik negara lain. Sebagai contoh, serangan siber yang diduga dilakukan oleh Rusia terhadap sistem pemilu di Amerika Serikat pada tahun 2016 menjadi sorotan internasional. Serangan ini berhasil mengakses data pemilih dan memengaruhi opini publik, yang pada gilirannya memicu ketegangan internasional dan merusak hubungan antara negara-negara besar. Hal ini menunjukkan bahwa serangan siber tidak hanya berdampak pada sektor ekonomi atau teknologi, tetapi juga dapat mengguncang stabilitas politik negara. Oleh karena itu, penting bagi komunitas internasional untuk terus memperkuat standar internasional terkait keamanan siber dan mengadopsi kebijakan yang dapat mengatasi ancaman dari negara-negara yang dapat menggunakan serangan siber sebagai bagian dari strategi geopolitiknya.

Sebagai bagian dari langkah preventif, beberapa negara juga telah meningkatkan investasi dalam teknologi deteksi dini dan sistem pemantauan untuk mencegah serangan yang lebih besar. Teknologi deteksi dini ini bertujuan untuk mendeteksi pola serangan sebelumnya dapat mencapai target dan menimbulkan kerusakan yang signifikan. Dengan menggunakan teknologi pemantauan yang lebih canggih, negara-negara dapat lebih cepat merespons ancaman yang datang, mengidentifikasi titik lemah dalam sistem, dan mengimplementasikan langkah-langkah mitigasi secara lebih efisien. Sistem pemantauan ini sangat penting, terutama bagi negara-negara yang memiliki infrastruktur kritis yang kompleks dan rentan terhadap ancaman siber.

Investasi dalam teknologi ini juga mencakup pengembangan algoritma kecerdasan buatan (AI) dan machine learning untuk menganalisis pola lalu lintas data yang mencurigakan. Dengan kemampuan untuk mengenali pola-pola anomali, teknologi ini dapat membantu mendeteksi serangan yang mungkin tidak terdeteksi oleh sistem keamanan tradisional. Teknologi AI dan machine learning dapat memproses data dalam jumlah besar dengan kecepatan yang lebih tinggi

dan tingkat akurasi yang lebih baik, sehingga mempercepat respons terhadap potensi serangan. Negara-negara yang lebih maju dalam hal teknologi sangat bergantung pada inovasi ini untuk melindungi infrastruktur kritis dari ancaman siber yang semakin kompleks.

Kerjasama internasional dalam bidang siber juga mencakup upaya untuk menetapkan standar global untuk keamanan siber. Dengan adanya standar internasional, negara-negara dapat lebih mudah berkoordinasi dalam melawan serangan siber yang melibatkan banyak negara. Standar ini juga membantu menciptakan kerangka kerja yang dapat diikuti oleh semua negara dalam memperkuat sistem pertahanan. Pembentukan standar ini melibatkan pihak-pihak yang berkompeten, seperti lembaga-lembaga internasional, perusahaan teknologi, dan pemerintah. Standar yang diterapkan di tingkat global ini diharapkan dapat menciptakan rasa saling percaya di antara negara-negara, yang pada gilirannya memperkuat kemampuan kolektif dalam menghadapi ancaman siber.

Penting bagi negara-negara untuk melibatkan sektor swasta dalam strategi keamanan siber. Sektor swasta sering kali memiliki akses ke teknologi terbaru dan berperan penting dalam menjaga keberlanjutan operasional infrastruktur kritis. Oleh karena itu, kerjasama yang erat antara sektor publik dan swasta sangat penting dalam membangun sistem pertahanan siber yang lebih kuat. Pemerintah perlu bekerja sama dengan perusahaan teknologi dan penyedia layanan siber untuk memastikan bahwa infrastruktur kritis aman dari potensi serangan. Sebagai tambahan, kolaborasi ini juga dapat mencakup berbagi informasi tentang ancaman terbaru dan upaya mitigasi yang dilakukan untuk menjaga keberlanjutan sistem dan data yang sensitif.

Dengan semakin meningkatnya ancaman serangan siber yang bersifat transnasional dan kompleks, kerjasama internasional dalam menghadapi peretasan dan ancaman terhadap infrastruktur kritis menjadi semakin penting. Negara-negara perlu bersatu dalam menghadapi ancaman ini dengan mengembangkan kebijakan yang lebih baik, memperkuat standar internasional, dan melibatkan sektor swasta dalam upaya penguatan pertahanan siber. Selain itu, investasi dalam teknologi deteksi dini dan sistem pemantauan menjadi kunci untuk mencegah dan mengurangi dampak dari serangan siber yang dapat merusak keamanan nasional dan internasional.

F. Perdagangan Ilegal di Dark Web

1. Pengertian dan Fenomena Perdagangan Ilegal di Dark Web

Dark web merupakan bagian dari internet yang tidak terindeks oleh mesin pencari tradisional, seperti Google atau Bing. Akses ke dark web biasanya memerlukan perangkat lunak khusus, seperti Tor (*The Onion Router*), yang memungkinkan penggunanya untuk mengunjugi situs-situs tersembunyi dengan tingkat anonimitas yang tinggi. Dalam dunia yang sulit dijangkau oleh kebanyakan orang ini, beragam aktivitas ilegal berlangsung dengan menggunakan sistem yang sangat sulit untuk dilacak. Salah satu aktivitas ilegal yang paling menonjol di dark web adalah perdagangan ilegal, yang mencakup berbagai macam barang dan layanan terlarang. Dalam konteks ini, dark web telah menjadi tempat yang menarik bagi individu atau kelompok yang ingin terlibat dalam kegiatan yang melanggar hukum tanpa terdeteksi oleh pihak berwenang.

Perdagangan ilegal di dark web mencakup berbagai kategori yang melanggar hukum dan memiliki dampak yang merugikan masyarakat. Salah satu kategori yang paling terkenal adalah perdagangan narkotika. Dark web menawarkan tempat yang sangat aman bagi para pengedar narkotika untuk menjual barang terlarang ini tanpa harus khawatir dengan pengawasan otoritas atau penegakan hukum. Transaksi yang terjadi dalam pasar gelap ini biasanya menggunakan cryptocurrency, seperti Bitcoin, yang menawarkan tingkat kerahasiaan dan anonimitas tinggi bagi para pelaku transaksi. Penggunaan cryptocurrency memungkinkan transaksi dilakukan dengan cara yang sulit untuk dilacak, sehingga memberi perlindungan bagi penjual dan pembeli dari deteksi pihak berwenang. Keberadaan pasar ini, yang biasanya beroperasi di bawah tanah dan sulit dilacak, memungkinkan penyebaran narkotika dalam skala yang jauh lebih besar dibandingkan dengan metode perdagangan narkoba konvensional.

Salah satu contoh fenomena yang paling terkenal dalam perdagangan narkotika di dark web adalah Silk Road. Silk Road merupakan sebuah pasar daring yang berfungsi sebagai platform untuk membeli dan menjual narkotika. Diluncurkan pada tahun 2011, Silk Road segera menjadi salah satu situs paling terkenal di dark web. Situs ini tidak hanya menawarkan berbagai jenis narkotika, tetapi juga menyediakan infrastruktur yang mendukung transaksi anonim, termasuk

penggunaan cryptocurrency untuk pembayaran. Dalam waktu singkat, Silk Road menarik banyak pengguna dari seluruh dunia, baik pengedar maupun pengguna narkotika, yang menjadikan pasar ini sebagai tempat utama untuk perdagangan barang-barang terlarang. Meskipun akhirnya Silk Road ditutup oleh pihak berwenang pada tahun 2013 setelah pelaksanaan operasi internasional yang besar, dampaknya sangat besar, karena pasar gelap ini telah memicu munculnya pasar-pasar serupa yang terus berkembang.

Meskipun Silk Road ditutup, perdagangan narkotika di dark web tidak berhenti begitu saja. Setelah penutupan Silk Road, banyak pasar gelap baru muncul dengan menggunakan nama berbeda dan sistem yang lebih canggih untuk menghindari deteksi dari pihak berwenang. Pasar-pasar baru ini mencoba untuk meminimalkan jejak digital agar lebih sulit untuk dilacak dan dibongkar. Misalnya, sering kali menggunakan sistem keamanan yang lebih baik, termasuk enkripsi yang lebih kuat dan struktur yang lebih tersembunyi, untuk melindungi identitas pengguna dan memastikan bahwa transaksi tetap anonim. Hal ini membuat pengawasan terhadap perdagangan narkotika di dark web semakin sulit, sehingga otoritas penegak hukum di berbagai negara harus bekerja keras untuk mencoba mengidentifikasi dan menutup pasar-pasar ilegal tersebut.

Senjata api juga menjadi salah satu barang yang sering diperdagangkan di dark web. Perdagangan senjata ini dilakukan oleh pihak-pihak yang ingin menghindari peraturan ketat yang ada di dunia nyata terkait penjualan dan kepemilikan senjata. Dark web memberikan peluang bagi para penjual dan pembeli senjata untuk melakukan transaksi dengan sangat rahasia dan tanpa pengawasan ketat. Dalam banyak kasus, perdagangan senjata ini dilakukan oleh individu atau kelompok yang memiliki motif untuk menghindari hukum atau bahkan untuk mempersenjatai diri secara ilegal. Cryptocurrency, yang sering digunakan untuk transaksi di dark web, menjadi alat yang sangat efektif dalam menyembunyikan identitas pembeli dan penjual senjata. Hal ini semakin memperburuk masalah perdagangan senjata ilegal, karena otoritas kesulitan dalam melacak pergerakan barang-barang tersebut.

Data pribadi yang dicuri juga menjadi salah satu barang yang sangat bernilai di pasar gelap ini. Data pribadi, seperti nomor kartu kredit, informasi identitas pribadi, dan data sensitif lainnya, sering kali dijual dengan harga yang cukup tinggi. Data ini diperoleh melalui

peretasan berbagai situs atau sistem yang tidak aman, dan kemudian dijual kepada pihak yang berniat menggunakan informasi tersebut untuk melakukan penipuan atau kejahatan lainnya. Perdagangan data pribadi di dark web merupakan ancaman besar bagi keamanan siber, karena data yang dicuri ini bisa digunakan untuk melakukan pencurian identitas, penipuan finansial, dan bahkan peretasan terhadap individu atau organisasi. Hal ini semakin meresahkan karena banyak pengguna internet yang tidak menyadari bahwa data pribadinya telah jatuh ke tangan yang salah.

Perdagangan data pribadi yang dicuri bukan hanya masalah bagi individu, tetapi juga bagi organisasi dan perusahaan. Data pelanggan yang dicuri dapat digunakan oleh para pelaku kejahatan untuk menyusup ke sistem perusahaan, melakukan penipuan, atau mencuri informasi berharga lainnya. Dalam beberapa kasus, data yang dicuri dapat digunakan untuk merusak reputasi perusahaan atau menyebabkan kerugian finansial yang signifikan. Selain itu, dengan semakin canggihnya teknologi dan metode yang digunakan oleh peretas, deteksi dan pemulihan data yang telah dicuri menjadi semakin sulit. Oleh karena itu, perlindungan data pribadi dan keamanan siber menjadi sangat penting dalam mencegah kerugian yang ditimbulkan oleh aktivitas perdagangan data di dark web.

Fenomena perdagangan ilegal di dark web ini tidak hanya mencakup barang-barang dan data yang dicuri, tetapi juga melibatkan berbagai layanan ilegal lainnya. Layanan-layanan ini dapat mencakup segala sesuatu dari jasa peretasan, pembunuhan bayaran, hingga jasa untuk mencuci uang hasil kejahatan. Dengan menggunakan platform yang tersembunyi di dark web, para pelaku kejahatan dapat dengan mudah mendapatkan layanan yang dibutuhkan untuk melaksanakan aktivitas ilegal dengan tingkat kerahasiaan yang tinggi. Ini menunjukkan bahwa dark web bukan hanya sekedar tempat untuk membeli dan menjual barang ilegal, tetapi juga menyediakan ruang untuk transaksi yang sangat berbahaya dan merugikan masyarakat luas.

Untuk mengatasi fenomena perdagangan ilegal di dark web, berbagai upaya telah dilakukan oleh pemerintah dan organisasi internasional. Penegakan hukum terhadap perdagangan ilegal di dark web sering kali menghadapi kendala besar, terutama karena sistem yang digunakan di dark web sangat sulit untuk dilacak dan diidentifikasi. Oleh karena itu, banyak negara yang meningkatkan kerjasama internasional

untuk membongkar jaringan perdagangan ilegal ini dan mengejar pelaku yang terlibat. Namun, meskipun upaya tersebut semakin gencar dilakukan, perdagangan ilegal di dark web tetap menjadi ancaman yang nyata, dan dibutuhkan lebih banyak inovasi dalam teknologi keamanan untuk mencegah penyebaran aktivitas ilegal ini.

Perdagangan ilegal di dark web terus berkembang, dengan munculnya pasar baru dan teknologi yang semakin canggih untuk melindungi transaksi dari pengawasan pihak berwenang. Oleh karena itu, penting bagi pemerintah, lembaga keamanan siber, dan organisasi internasional untuk terus meningkatkan kerjasama dan kapasitas dalam mengidentifikasi dan mengatasi masalah ini. Tanpa adanya langkah-langkah yang efektif untuk menanggulangi fenomena ini, perdagangan ilegal di dark web akan terus berkembang, memberikan dampak negatif bagi keamanan dan kesejahteraan masyarakat global.

2. Dampak Perdagangan Ilegal di Dark Web dan Upaya Penanggulangannya

Perdagangan ilegal di dark web memberikan dampak yang sangat besar dan luas, tidak hanya bagi individu yang terlibat, tetapi juga bagi masyarakat secara keseluruhan. Salah satu dampak sosial yang paling nyata adalah meningkatnya penyalahgunaan narkoba. Narkotika yang diperdagangkan secara bebas di dark web membuat akses kepada obat-obatan terlarang semakin mudah, bahkan bagi yang sebelumnya mungkin tidak memiliki koneksi dalam jaringan narkoba. Penyalahgunaan narkotika ini dapat memperburuk masalah kesehatan masyarakat, dengan meningkatkan jumlah pengguna, kecanduan, dan dampak negatif lainnya seperti kecelakaan, penyakit menular, atau bahkan kematian akibat overdosis. Selain itu, semakin banyaknya orang yang terlibat dalam perdagangan narkotika ini juga memperburuk tingkat kejahatan lainnya, seperti penipuan identitas dan pencurian data pribadi. Dengan sistem yang sangat terisolasi dan anonim, para pelaku kejahatan dapat dengan mudah menjual barang ilegal tanpa takut akan penangkapan.

Dampak sosial lainnya adalah peningkatan peredaran senjata ilegal. Dark web memberikan tempat yang aman bagi para penjual senjata untuk melakukan transaksi tanpa pengawasan ketat dari pemerintah atau otoritas. Senjata api yang diperjualbelikan di dark web sering kali digunakan dalam tindakan kriminal yang meresahkan, seperti

perampokan, pembunuhan, atau serangan teroris. Hal ini sangat membahayakan keamanan masyarakat, karena senjata yang seharusnya hanya boleh beredar di kalangan pihak yang sah, kini dapat dengan mudah dimiliki oleh individu yang tidak memiliki izin. Meningkatnya jumlah senjata ilegal juga memperburuk ketidakamanan dalam masyarakat, menyebabkan ketakutan dan kecemasan yang lebih besar di kalangan warga sipil.

Dampak sosial dari perdagangan ilegal di dark web juga mencakup penurunan kepercayaan terhadap sistem keamanan dan penegakan hukum. Ketika publik mengetahui bahwa barang-barang terlarang dapat dibeli dan dijual dengan bebas tanpa banyak hambatan, hal ini dapat mengurangi kepercayaan terhadap kemampuan pemerintah untuk melindungi warganya. Sebagai akibatnya, masyarakat mungkin merasa bahwa hukum tidak dapat menegakkan aturan secara efektif, yang dapat berujung pada hilangnya rasa aman dan kerugian dalam berbagai aspek kehidupan sosial. Penurunan kepercayaan ini juga memperburuk masalah lain yang terkait dengan kejahatan, seperti penurunan partisipasi dalam upaya pencegahan kejahatan, dan lemahnya dukungan terhadap kebijakan dan tindakan yang diambil oleh otoritas.

Perdagangan ilegal di dark web juga membawa dampak ekonomi yang sangat merugikan. Salah satu dampak ekonomi yang paling nyata adalah kerugian finansial yang ditimbulkan akibat pencurian identitas dan penipuan yang terjadi melalui platform gelap ini. Data pribadi yang dicuri melalui peretasan situs-situs terkenal sering dijual di dark web untuk digunakan dalam penipuan identitas atau pencurian dana. Transaksi-transaksi ini sering kali dilakukan dengan menggunakan cryptocurrency seperti Bitcoin, yang memberikan anonimitas dan menyulitkan pihak berwenang untuk melacak jalur aliran uang tersebut. Hal ini menyebabkan kerugian yang besar bagi individu dan organisasi yang menjadi korban, dan dapat berimbas pada perekonomian global secara keseluruhan, karena kebocoran data sensitif ini sering kali memengaruhi perusahaan besar, lembaga finansial, dan bahkan instansi pemerintah.

Transaksi di dark web yang dilakukan dengan menggunakan cryptocurrency semakin memperburuk masalah. Cryptocurrency memungkinkan pelaku untuk bertransaksi tanpa melibatkan pihak ketiga, yang pada gilirannya mengurangi kemungkinan terdeteksinya aktivitas ilegal tersebut. Dengan sistem pembayaran yang lebih sulit

untuk dilacak, penegakan hukum menjadi semakin sulit, bahkan bagi otoritas yang memiliki kemampuan teknologi tinggi. Cryptocurrency juga mengarah pada peningkatan ketergantungan pada uang digital yang sering kali digunakan dalam kegiatan ilegal, tanpa adanya pengawasan yang memadai. Hal ini menciptakan tantangan besar bagi penegak hukum dalam upayanya untuk memerangi perdagangan ilegal, karena harus dapat mengidentifikasi dan melacak jalur keuangan yang sangat sulit dibongkar.

Di tengah tantangan ini, pemerintah di seluruh dunia mulai mengambil langkah-langkah untuk menangani perdagangan ilegal di dark web. Salah satu cara yang digunakan adalah dengan memperkuat penegakan hukum melalui operasi-operasi gabungan yang melibatkan lembaga-lembaga internasional. Interpol dan Europol, misalnya, telah melakukan berbagai operasi untuk menutup pasar gelap yang beroperasi di dark web, salah satunya adalah penutupan pasar gelap terbesar yang dikenal dengan nama AlphaBay pada tahun 2018. AlphaBay adalah salah satu situs yang menjadi tempat utama bagi perdagangan narkotika, senjata, data pribadi yang dicuri, dan barang-barang ilegal lainnya. Penutupan pasar tersebut adalah langkah besar dalam mengurangi kegiatan ilegal di dark web, namun tetap saja, pasar-pasar baru terus bermunculan dengan menggunakan teknologi dan metode yang lebih canggih untuk menghindari deteksi.

Penyelidikan siber juga menjadi bagian integral dalam upaya menanggulangi perdagangan ilegal di dark web. Polisi dan lembaga keamanan siber kini menggunakan berbagai teknologi untuk melacak transaksi yang dilakukan menggunakan cryptocurrency dan mengidentifikasi individu yang terlibat dalam kegiatan ilegal. Meskipun hal ini meningkatkan efektivitas penegakan hukum, ada sejumlah tantangan besar yang harus dihadapi. Salah satu tantangan terbesar adalah kemampuan pelaku untuk beroperasi secara anonim melalui jaringan Tor dan penggunaan cryptocurrency, yang mempersulit upaya pelacakan dan pengungkapan identitasnya. Oleh karena itu, meskipun upaya penegakan hukum semakin kuat, masalah ini tetap sulit diatasi, karena teknologi yang digunakan oleh pelaku semakin canggih.

Kerjasama internasional dalam memerangi perdagangan ilegal di dark web sangat penting. Aktivitas yang terjadi di dark web tidak terbatas pada satu negara, dan sering melibatkan banyak negara yang beroperasi di tingkat global. Oleh karena itu, penting bagi negara-negara untuk

bekerja sama dalam meningkatkan kapasitas penegakan hukum dan memperkuat standar internasional terkait pertukaran data dan koordinasi operasi untuk menutup situs-situs gelap. Dalam banyak kasus, karena peraturan yang berbeda-beda di tiap negara, upaya internasional harus dilakukan agar tindakan terhadap perdagangan ilegal di dark web dapat berjalan secara efektif dan efisien. Tanpa kerjasama internasional yang solid, perdagangan ilegal di dark web akan terus berkembang, bahkan mungkin lebih canggih dan sulit dihentikan.

Meskipun langkah-langkah penegakan hukum semakin gencar dilakukan, banyak pihak yang menyadari bahwa penanggulangan perdagangan ilegal di dark web juga memerlukan pendekatan yang lebih holistik. Selain upaya penegakan hukum, penting untuk meningkatkan kesadaran dan pendidikan kepada masyarakat tentang potensi bahaya yang dapat ditimbulkan oleh kegiatan ilegal di dark web. Pendidikan ini dapat mencakup pemahaman tentang pentingnya keamanan data pribadi, cara melindungi informasi sensitif, dan mengenali tanda-tanda kegiatan ilegal di internet. Selain itu, upaya preventif lainnya adalah dengan memperkuat sistem keamanan di platform daring dan meningkatkan kesadaran tentang risiko yang terkait dengan penggunaan dark web.

Dampak yang ditimbulkan oleh perdagangan ilegal di dark web sangat besar dan luas, namun dengan kerjasama internasional yang lebih baik, peningkatan teknologi keamanan, dan penegakan hukum yang lebih efektif, tantangan ini bisa diatasi. Pemerintah, lembaga-lembaga internasional, dan masyarakat harus bekerja bersama untuk mencegah penyebaran aktivitas ilegal ini yang dapat merugikan banyak pihak. Jika langkah-langkah tersebut tidak diambil, maka dampak buruk dari perdagangan ilegal di dark web akan terus memburuk, dan dampaknya akan terasa semakin luas di tingkat global.

BAB IV
PENEGAKAN HUKUM DALAM KASUS TINDAK PIDANA SIBER

Penegakan hukum dalam kasus tindak pidana siber menjadi salah satu tantangan terbesar bagi sistem peradilan di seluruh dunia, terutama karena sifatnya yang terdesentralisasi dan sulit dilacak. Kejahatan siber melibatkan penggunaan teknologi canggih dan anonim, yang membuat pelaku dapat beroperasi dengan relatif aman dari pengawasan otoritas. Selain itu, peraturan hukum yang ada sering kali tidak dapat mengikuti perkembangan pesat teknologi informasi, sehingga menimbulkan kesenjangan dalam penegakan hukum. Tindak pidana siber mencakup berbagai jenis kejahatan, mulai dari peretasan, penipuan online, hingga penyebaran konten ilegal, yang semuanya dapat merugikan individu, perusahaan, dan bahkan negara. Dalam hal ini, penegakan hukum membutuhkan kerjasama antara lembaga penegak hukum nasional dan internasional, penggunaan teknologi forensik digital, serta pembaruan regulasi yang relevan untuk mengatasi kejahatan yang terus berkembang. Dengan meningkatnya kesadaran terhadap ancaman siber, berbagai negara berusaha untuk memperkuat kapasitas hukum untuk melindungi warganya dari potensi kerugian akibat tindakan kriminal yang terjadi di dunia maya. Keberhasilan penegakan hukum dalam kejahatan siber sangat bergantung pada integrasi antara hukum, teknologi, dan kebijakan internasional yang memungkinkan kerjasama global dalam mengatasi masalah ini secara efektif.

A. Peran Kepolisian dan Penyidik dalam Menangani Kejahatan Siber

1. Peran Kepolisian dalam Penanggulangan Kejahatan Siber

Keberhasilan penanggulangan kejahatan siber sangat bergantung pada peran aktif kepolisian, yang menjadi garda terdepan dalam melakukan pencegahan, penyelidikan, dan penindakan terhadap pelaku kejahatan yang beroperasi di dunia maya. Kejahatan siber merupakan jenis kejahatan yang sangat unik, karena tidak terbatas oleh batas-batas geografis dan hukum tradisional. Hal ini membuat kejahatan siber semakin sulit untuk diatasi tanpa keterlibatan langsung dari aparat penegak hukum, terutama kepolisian yang memiliki tanggung jawab utama dalam menjaga ketertiban dan keamanan nasional. Di Indonesia, Direktorat Tindak Pidana Siber (Dittipidsiber) di bawah Bareskrim Polri berperan yang sangat penting dalam melakukan penyelidikan terhadap berbagai kasus kejahatan siber, seperti peretasan, penipuan online, penyebaran *hoaks*, dan sejumlah bentuk kejahatan lainnya yang merugikan masyarakat. Keberadaan unit khusus seperti Dittipidsiber ini memberikan respon cepat dan efektif terhadap kasus-kasus yang berkaitan dengan dunia maya yang terus berkembang dengan pesat.

Peran kepolisian dalam penanggulangan kejahatan siber tidak hanya terbatas pada aspek penyelidikan dan penindakan semata. Salah satu aspek yang sangat krusial dalam mengatasi kejahatan siber adalah pengembangan kapasitas teknis dan pelatihan yang berkelanjutan bagi aparat penegak hukum. Seiring dengan semakin kompleksnya ancaman yang ada, polisi harus memiliki kemampuan untuk mengidentifikasi, menganalisis, dan mengatasi berbagai bentuk ancaman siber yang terus berkembang, seperti serangan *malware*, *ransomware*, dan peretasan yang melibatkan data sensitif. Penanggulangan kejahatan siber ini memerlukan keterampilan khusus dalam teknologi informasi, di mana polisi harus mampu memahami perangkat keras dan perangkat lunak yang digunakan oleh pelaku untuk melancarkan aksinya. Keterampilan teknis ini sangat penting untuk dapat mendeteksi, mengintersepsi, dan menangani ancaman yang timbul dalam ruang siber yang begitu luas.

Salah satu aspek lain yang tidak kalah penting adalah kemampuan dalam bidang forensik digital. Dalam kejahatan siber, bukti-bukti yang digunakan untuk mendukung penyelidikan dan penuntutan sering kali terletak dalam bentuk digital yang tidak dapat dilihat dengan

mata telanjang. Oleh karena itu, penyidik harus memiliki keterampilan khusus dalam mengumpulkan, menyimpan, dan menganalisis bukti digital dari perangkat elektronik dan jaringan komputer. Forensik digital adalah bidang yang sangat penting dalam proses investigasi, karena bukti-bukti yang ditemukan dalam jaringan atau perangkat elektronik ini sering kali dapat menjadi petunjuk penting yang mengarah pada identitas pelaku atau metode yang digunakan dalam kejahatan tersebut. Oleh karena itu, peningkatan kualitas dan jumlah tenaga ahli forensik digital dalam kepolisian sangat diperlukan untuk mendukung keberhasilan penanggulangan kejahatan siber.

Seiring dengan meningkatnya ancaman kejahatan siber, kepolisian di berbagai negara juga semakin berfokus pada kerjasama internasional dalam menangani masalah ini. Kejahatan siber, seperti peretasan data atau serangan DDoS, sering kali melibatkan pelaku dari berbagai negara, dan hal ini membutuhkan koordinasi yang erat antara lembaga penegak hukum internasional seperti Interpol, Europol, serta badan-badan hukum negara masing-masing. Kerjasama internasional ini sangat penting karena kejahatan siber sering kali memiliki dampak yang lebih besar daripada sekadar dampak lokal, dan penyelidikan yang melibatkan lebih dari satu negara akan mempermudah dalam melacak pelaku yang bersembunyi di luar negeri. Melalui kerjasama ini, kepolisian di berbagai negara dapat berbagi informasi, teknologi, dan sumber daya untuk mengidentifikasi dan menangani pelaku kejahatan siber yang beroperasi lintas negara.

Kerjasama dengan sektor swasta yang memiliki keahlian dalam bidang teknologi juga menjadi salah satu kunci keberhasilan dalam penanggulangan kejahatan siber. Perusahaan teknologi sering kali memiliki alat dan infrastruktur yang dapat membantu dalam mendeteksi dan mencegah kejahatan siber. Misalnya, perusahaan-perusahaan penyedia layanan internet, penyedia perangkat lunak, dan perusahaan keamanan siber memiliki kemampuan untuk mendeteksi pola-pola serangan yang dilakukan oleh hacker dan memberikan informasi yang sangat berharga kepada kepolisian. Selain itu, perusahaan teknologi juga sering memiliki akses ke data yang tidak bisa diperoleh oleh pihak kepolisian secara langsung, seperti data lalu lintas jaringan atau informasi terkait perangkat yang digunakan dalam serangan siber. Oleh karena itu, membangun hubungan yang erat antara kepolisian dan sektor

swasta menjadi sangat penting untuk meningkatkan efektivitas dalam penanggulangan kejahatan siber.

Salah satu contoh penting yang menunjukkan pentingnya kerjasama antara kepolisian dan sektor swasta adalah penanganan kasus peretasan besar-besaran yang melibatkan kebocoran data pada perusahaan-perusahaan besar atau lembaga pemerintah. Dalam kasus-kasus seperti ini, kepolisian perlu bekerja sama dengan perusahaan yang menjadi korban peretasan untuk melacak asal-usul serangan dan mencari pelaku yang bertanggung jawab. Proses ini melibatkan analisis forensik digital yang sangat mendalam, yang sering kali memerlukan keahlian khusus dari kedua belah pihak. Dalam beberapa kasus, perusahaan teknologi dapat memberikan bukti dan data yang diperlukan untuk menemukan jejak digital yang ditinggalkan oleh pelaku kejahatan. Kerjasama semacam ini menunjukkan pentingnya kolaborasi yang efektif antara sektor publik dan swasta dalam mengatasi ancaman siber yang terus berkembang.

Penyelidikan kejahatan siber juga memerlukan kemampuan untuk menangani bukti digital yang sangat rumit dan kompleks. Bukti digital yang ditemukan dalam kasus kejahatan siber sering kali tersembunyi dalam bentuk yang tidak terlihat oleh mata telanjang, seperti log file, jejak digital di internet, dan data yang sudah terhapus dari perangkat korban. Oleh karena itu, kepolisian harus memiliki alat yang canggih dan prosedur yang jelas dalam mengumpulkan dan menganalisis bukti-bukti ini. Tanpa kemampuan yang memadai dalam hal forensik digital, sulit bagi penyidik untuk menemukan bukti yang cukup untuk menuntut pelaku di pengadilan. Proses pengumpulan bukti ini harus dilakukan dengan sangat hati-hati dan terencana, karena kesalahan dalam penanganan bukti dapat merusak keseluruhan kasus.

Keberhasilan dalam menanggulangi kejahatan siber juga sangat bergantung pada kemampuan polisi dalam mengidentifikasi dan merespons ancaman yang terus berkembang di dunia maya. Seiring dengan semakin canggihnya teknologi, pelaku kejahatan siber terus berinovasi dengan menggunakan metode dan alat yang lebih canggih. Oleh karena itu, aparat kepolisian harus selalu mengikuti perkembangan teknologi dan tren serangan siber untuk tetap dapat menghadapi ancaman yang muncul. Selain itu, kepolisian juga harus meningkatkan pemahaman tentang hukum yang berlaku dalam dunia maya, termasuk hukum internasional, privasi data, dan kebijakan perlindungan

konsumen yang dapat membantunya dalam melaksanakan tugasnya dengan lebih efektif.

2. Peran Penyidik dalam Menangani Kejahatan Siber

Penyidik, terutama yang memiliki spesialisasi dalam kejahatan siber, berperan yang sangat penting dalam memastikan bahwa pelaku tindak pidana siber dapat diidentifikasi dan diproses secara hukum. Kejahatan siber adalah salah satu jenis kejahatan yang paling menantang di dunia saat ini, karena sifatnya yang tidak terbatas oleh ruang dan waktu. Kejahatan-kejahatan ini sering kali dilakukan di dunia maya, yang memungkinkan pelaku untuk menyembunyikan identitasnya dengan relatif mudah. Oleh karena itu, penyidik kejahatan siber perlu memiliki pengetahuan yang mendalam tentang teknologi informasi, perangkat lunak, dan berbagai alat yang digunakan oleh para pelaku kejahatan siber. Kemampuan untuk memahami dan menganalisis teknologi tersebut sangat penting, karena dapat membantu penyidik untuk mengidentifikasi jejak digital yang ditinggalkan oleh pelaku kejahatan.

Penyidik di bidang ini juga harus memiliki keterampilan dalam mengumpulkan dan menganalisis bukti digital yang dapat ditemukan di perangkat komputer atau jaringan internet yang terkait dengan kejahatan. Proses ini melibatkan berbagai metode dan teknik, yang salah satunya adalah forensik digital. Dalam banyak kasus, bukti yang ditemukan di dunia maya tidak tampak dengan mata telanjang, sehingga penyidik harus mampu menggunakan alat forensik yang canggih untuk mengakses, mengekstrak, dan menganalisis data yang terkandung dalam perangkat digital. Forensik digital merupakan salah satu bidang yang sangat penting dalam penyidikan kejahatan siber, karena banyak kasus kejahatan siber yang dapat diungkap hanya dengan cara menganalisis jejak digital yang ditinggalkan oleh pelaku. Misalnya, dalam kasus penipuan online atau *cyber fraud*, penyidik akan melakukan analisis terhadap transaksi yang dilakukan melalui internet, melacak jejak transaksi, dan menghubungkannya dengan identitas pelaku.

Penyidik kejahatan siber juga harus menguasai berbagai prosedur hukum yang berlaku dalam proses penyidikan. Kejahatan siber sering kali melibatkan pelanggaran terhadap hukum yang ada di berbagai negara, sehingga penyidik harus memahami hukum internasional serta hukum negara yang terkait dengan kasus yang sedang diselidiki. Selain

itu, penyidik harus dapat memastikan bahwa prosedur yang dilakukan selama proses penyidikan tidak melanggar hak asasi manusia atau privasi individu. Hal ini sangat penting karena kejahatan siber sering melibatkan akses ke data pribadi yang sangat sensitif, dan pelanggaran terhadap privasi dapat merusak integritas proses penyidikan. Oleh karena itu, penyidik harus sangat berhati-hati dalam mengumpulkan bukti dan memastikan bahwa bukti yang dikumpulkan sah menurut hukum, sehingga dapat diterima di pengadilan.

Salah satu peran penting yang dimainkan oleh penyidik dalam menangani kejahatan siber adalah untuk mengidentifikasi modus operandi yang digunakan oleh pelaku. Modus operandi ini adalah cara atau pola yang digunakan oleh pelaku kejahatan untuk melakukan tindak pidana. Dengan memahami modus operandi pelaku, penyidik dapat memberikan rekomendasi yang berguna dalam pencegahan kejahatan siber di masa depan. Misalnya, dalam kasus *cyber bullying* atau penyebaran konten ilegal di media sosial, penyidik perlu memahami bagaimana informasi yang melanggar hukum bisa tersebar begitu cepat dan siapa saja yang terlibat dalam penyebaran tersebut. Pemahaman tentang modus operandi pelaku ini sangat penting, karena hal ini dapat membantu dalam merancang strategi pencegahan yang lebih efektif dan mengurangi jumlah kasus kejahatan siber di masa mendatang.

Di Indonesia, Bareskrim Polri memiliki unit Cyber Crime yang berfokus pada penyidikan kasus-kasus siber. Unit ini bekerja untuk menangani berbagai jenis kejahatan siber yang terjadi, baik yang melibatkan individu maupun kelompok terorganisir. Keberadaan unit ini sangat penting, mengingat tingginya jumlah kasus kejahatan siber yang terjadi di Indonesia. Penyidik yang bekerja di unit ini juga memiliki tugas untuk memeriksa dan menganalisis berbagai bukti yang diperoleh dari perangkat elektronik, serta melacak jejak digital yang ditinggalkan oleh para pelaku. Selain itu, juga perlu bekerja sama dengan lembaga penegak hukum internasional, mengingat banyaknya kasus kejahatan siber yang melibatkan pelaku dari luar negeri. Kerjasama internasional ini sangat penting untuk memperluas jangkauan penyidikan dan memastikan bahwa pelaku dapat dihadapkan pada proses hukum, meskipun beroperasi di luar yurisdiksi negara tersebut.

Penyidik juga harus bekerja sama dengan berbagai pihak lain, seperti badan intelijen, penyedia layanan internet, dan perusahaan teknologi, untuk melacak jejak digital pelaku. Kejahatan siber sering kali

melibatkan transaksi yang dilakukan melalui platform digital atau mata uang kripto seperti Bitcoin, yang bisa sangat sulit untuk dilacak. Oleh karena itu, penyidik harus bekerja sama dengan perusahaan penyedia layanan digital untuk memperoleh data yang relevan dan membantunya dalam melacak jejak transaksi yang mencurigakan. Dalam beberapa kasus, penyidik perlu bekerja dengan lembaga internasional yang memiliki akses ke data yang berada di luar yurisdiksi. Kerjasama ini sangat penting, mengingat banyaknya platform digital yang beroperasi secara global, seperti dark web, yang sering kali digunakan untuk melakukan transaksi ilegal.

Penyidik juga harus mempertimbangkan aspek etika dalam proses penyidikan kejahatan siber. Salah satu tantangan besar yang dihadapi oleh penyidik adalah memastikan bahwa proses penyidikan dilakukan dengan cara yang sah dan sesuai dengan hukum yang berlaku, serta melindungi hak-hak individu yang terlibat. Misalnya, dalam mengakses data pribadi atau komunikasi elektronik yang melibatkan korban atau pelaku, penyidik harus memiliki izin hukum yang sah, seperti surat perintah pengadilan. Hal ini penting untuk memastikan bahwa bukti yang dikumpulkan selama penyidikan dapat diterima di pengadilan dan tidak melanggar hak privasi individu. Aspek etika ini sangat penting karena dapat memengaruhi kredibilitas dan legitimasi proses penyidikan, serta menjaga kepercayaan masyarakat terhadap sistem peradilan.

Penyidik juga harus memiliki keterampilan untuk menganalisis bukti digital dengan teliti, mengingat bukti yang ditemukan dalam kejahatan siber sering kali sangat kompleks dan tersembunyi. Bukti digital dapat mencakup log file, email, jejak transaksi, dan data yang mungkin sudah dihapus oleh pelaku. Oleh karena itu, penyidik harus dapat menggunakan alat dan teknik forensik digital yang canggih untuk memulihkan data yang telah dihapus dan menganalisis bukti yang tersembunyi. Proses ini sangat memerlukan ketelitian dan keahlian tinggi, karena setiap kesalahan dalam mengumpulkan atau menganalisis bukti dapat berakibat fatal bagi keberhasilan penyidikan dan proses hukum yang menyusul.

Keberhasilan penyidik dalam menangani kejahatan siber sangat bergantung pada kemampuan untuk terus belajar dan beradaptasi dengan perkembangan teknologi yang cepat. Kejahatan siber terus berkembang seiring dengan kemajuan teknologi, dan pelaku kejahatan semakin

canggih dalam menggunakan alat dan metode baru untuk melancarkan aksinya. Oleh karena itu, penyidik harus selalu mengikuti pelatihan dan pembaruan terkait teknik terbaru dalam bidang forensik digital dan kejahatan siber. Dengan demikian, penyidik dapat lebih siap dalam menghadapi berbagai tantangan yang muncul dan memastikan bahwa pelaku kejahatan siber dapat ditangkap dan dihadapkan pada proses hukum yang adil. Keberhasilan penyidikan ini tidak hanya bergantung pada keterampilan teknis, tetapi juga pada kolaborasi yang efektif antara penyidik, lembaga penegak hukum, sektor swasta, dan masyarakat internasional..

B. Bukti Elektronik dalam Proses Pembuktian Hukum

1. Definisi dan Peran Bukti Elektronik dalam Sistem Hukum

Bukti elektronik merujuk pada segala bentuk informasi atau data yang tersimpan dalam format digital, yang dapat digunakan sebagai alat pembuktian dalam proses hukum di pengadilan. Di era digital ini, hampir setiap aspek kehidupan manusia terhubung dengan teknologi, mulai dari komunikasi, transaksi, hingga penyimpanan data pribadi. Oleh karena itu, bukti elektronik menjadi elemen penting dalam penyelidikan dan pembuktian, terutama dalam kasus-kasus yang melibatkan kejahatan siber. Bukti elektronik bisa berupa data yang disimpan dalam perangkat elektronik seperti komputer, ponsel, server, dan perangkat penyimpanan lainnya, serta informasi yang disebarkan melalui jaringan internet, termasuk komunikasi elektronik, transaksi digital, dan data lainnya yang dapat diakses atau dianalisis. Bukti ini dapat digunakan untuk mengungkap fakta-fakta yang relevan dalam proses peradilan, terutama dalam konteks kejahatan yang terjadi di dunia maya.

Penerimaan bukti elektronik dalam sistem hukum menjadi semakin relevan seiring dengan pesatnya perkembangan teknologi. Beberapa jenis kejahatan kini tidak hanya terjadi di dunia fisik, tetapi juga di dunia maya, yang membuat pelakunya sering kali sulit untuk dilacak tanpa adanya bukti digital yang jelas. Misalnya, dalam kasus peretasan, penipuan online, atau perdagangan ilegal melalui platform digital, jejak yang ditinggalkan pelaku sering kali hanya dapat ditemukan dalam bentuk data yang tersimpan dalam sistem komputer atau server. Dalam konteks ini, bukti elektronik menjadi kunci utama untuk mendalami pola kejahatan dan mengidentifikasi pelaku. Hal ini juga

menjadi tantangan bagi sistem hukum untuk dapat menerima dan memproses bukti elektronik yang mungkin tidak sepenuhnya dipahami atau bahkan diakui oleh beberapa pihak sebagai bentuk bukti yang sah.

Pengadilan di banyak negara, termasuk Indonesia, telah mengakui bahwa bukti elektronik dapat diterima sebagai alat bukti yang sah dan relevan dalam proses hukum. Pengakuan ini sangat penting, terutama untuk menghadapi tantangan yang muncul akibat kejahatan yang dilakukan secara online. Kejahatan-kejahatan tersebut tidak terikat oleh batasan fisik atau geografis, sehingga membutuhkan pendekatan baru dalam hal pembuktian dan penyelidikan. Bukti elektronik, seperti log file, riwayat pencarian, email, pesan teks, dan data transaksi online, kini dapat diajukan di pengadilan sebagai bukti yang sah dalam berbagai jenis kasus. Ini menandakan bahwa hukum harus beradaptasi dengan perkembangan teknologi agar dapat tetap relevan dalam menanggapi kejahatan yang semakin kompleks.

Pada penerimaan bukti elektronik, terdapat beberapa keunggulan yang dimilikinya jika dibandingkan dengan bukti tradisional. Salah satu keunggulannya adalah sifat data digital yang lebih akurat dan tidak mudah dimanipulasi. Data digital cenderung memiliki jejak waktu dan urutan yang jelas, sehingga memberikan gambaran yang lebih rinci mengenai peristiwa yang terjadi. Misalnya, sebuah pesan yang dikirim melalui aplikasi pesan instan akan memiliki informasi tentang waktu pengiriman, penerima, dan pengirim yang tidak dapat diubah setelah pesan tersebut dikirim. Hal ini menjadikan bukti elektronik sebagai alat yang sangat andal dalam proses penyelidikan dan pembuktian di pengadilan.

Keunggulan lain dari bukti elektronik adalah kemampuannya untuk menghubungkan berbagai peristiwa dalam suatu kasus kejahatan. Dengan mengumpulkan dan menganalisis data yang tersebar di berbagai perangkat atau platform digital, penyidik dapat menemukan jejak digital yang memungkinkan melacak aktivitas pelaku. Sebagai contoh, dalam kasus penipuan online, bukti yang diperoleh dari transaksi yang dilakukan melalui sistem pembayaran digital atau email yang digunakan oleh pelaku dapat membantu penyidik untuk mengidentifikasi pelaku dan menggali lebih dalam tentang caranya melakukan kejahatan. Hal ini tidak hanya mempermudah penyidikan, tetapi juga mempercepat proses pembuktian dalam persidangan.

Salah satu tantangan besar dalam penerimaan bukti elektronik adalah bagaimana mengatasi masalah autentikasi dan integritas data. Data digital yang disimpan dalam perangkat elektronik atau disebarkan melalui internet rentan terhadap manipulasi atau perubahan, sehingga perlu adanya prosedur yang ketat untuk memastikan bahwa bukti tersebut tetap sah dan tidak terkontaminasi. Misalnya, dalam sebuah kasus peretasan, data yang diperoleh dari server atau komputer mungkin telah dimodifikasi oleh pihak yang tidak bertanggung jawab sebelum ditemukan oleh penyidik. Oleh karena itu, penting bagi aparat penegak hukum untuk mengikuti prosedur yang sah dalam pengumpulan bukti elektronik, seperti menggunakan metode forensik digital yang memastikan bahwa bukti yang diperoleh tetap utuh dan dapat dipertanggungjawabkan.

Bukti elektronik juga memiliki nilai yang sangat penting dalam kasus-kasus yang melibatkan kejahatan siber, seperti *cyber fraud*, *phishing*, *hacking*, dan *cyberbullying*. Dalam kejahatan-kejahatan ini, pelaku sering kali menggunakan teknologi untuk menutupi jejak, sehingga tanpa bukti elektronik yang jelas, akan sangat sulit untuk mengungkap siapa yang bertanggung jawab atas kejahatan tersebut. Bukti elektronik dalam kasus-kasus ini bisa berupa riwayat transaksi online, komunikasi melalui email atau media sosial, serta file-file yang disimpan di komputer atau perangkat lain yang digunakan oleh pelaku. Dengan mengumpulkan bukti-bukti ini, penyidik dapat menemukan pola-pola tertentu yang mengarah pada identifikasi pelaku dan mengungkap skema kejahatan yang dilakukan.

Penerimaan bukti elektronik di pengadilan juga memperkenalkan tantangan baru terkait dengan perlindungan privasi dan hak asasi manusia. Dalam mengakses dan menggunakan bukti elektronik, penyidik dan aparat penegak hukum harus mematuhi prosedur yang ditetapkan oleh hukum untuk memastikan bahwa hak individu tidak dilanggar. Misalnya, untuk mengakses data pribadi yang tersimpan di perangkat elektronik, penyidik harus memperoleh izin yang sah, seperti surat perintah dari pengadilan, untuk memastikan bahwa tindakan tersebut sesuai dengan hukum yang berlaku. Hal ini penting untuk menjaga agar bukti yang diambil tetap sah dan tidak melanggar hak privasi individu yang terlibat.

Seiring dengan meningkatnya kejahatan yang melibatkan teknologi digital, penting bagi sistem hukum untuk terus

mengembangkan pemahaman dan regulasi terkait dengan bukti elektronik. Banyak negara yang telah mengembangkan undang-undang khusus yang mengatur tentang pengumpulan, penyimpanan, dan penggunaan bukti elektronik dalam proses hukum. Misalnya, Undang-Undang ITE di Indonesia memberikan dasar hukum bagi pengumpulan bukti elektronik dalam kasus-kasus yang melibatkan tindak pidana siber. Namun, dengan cepatnya perkembangan teknologi, sistem hukum harus selalu memperbarui regulasi untuk mengakomodasi tantangan baru yang muncul, seperti penyalahgunaan teknologi atau perkembangan metode baru dalam kejahatan digital.

2. Tantangan dalam Menggunakan Bukti Elektronik dalam Proses Pembuktian

Meskipun bukti elektronik memiliki potensi besar dalam membantu proses pembuktian hukum, penggunaannya juga menghadapi berbagai tantangan yang perlu diatasi oleh aparat penegak hukum. Salah satu tantangan terbesar adalah validitas dan keaslian dari bukti elektronik. Data yang disimpan dalam format digital sangat rentan terhadap manipulasi, kerusakan, atau penghapusan yang disengaja oleh pelaku kejahatan. Oleh karena itu, untuk memastikan bahwa bukti elektronik dapat diterima di pengadilan, aparat penegak hukum harus memiliki prosedur yang jelas dalam mengumpulkan, mengamankan, dan menganalisis bukti digital.

Chain of custody atau rantai pengawasan terhadap bukti digital menjadi aspek yang sangat penting dalam memastikan keabsahan bukti elektronik. Setiap langkah dalam proses pengumpulan dan pemrosesan bukti elektronik harus tercatat dengan teliti untuk memastikan bahwa bukti tersebut tidak terkontaminasi atau diubah sebelum diajukan di pengadilan. Misalnya, dalam kasus peretasan atau penyebaran *malware*, bukti elektronik yang ditemukan dalam perangkat yang disita harus diperlakukan dengan hati-hati dan menggunakan prosedur yang telah distandarisasi, seperti forensik digital. Jika prosedur ini tidak dilakukan dengan benar, bukti tersebut dapat dianggap tidak sah di pengadilan, dan ini dapat menyebabkan kegagalan dalam proses pembuktian.

Interoperabilitas antara sistem perangkat lunak dan perangkat keras yang digunakan oleh penyidik juga menjadi tantangan dalam mengumpulkan bukti elektronik. Beberapa perangkat lunak atau sistem operasi mungkin menyimpan data dengan cara yang berbeda, dan ini

memerlukan keahlian khusus dalam menangani bukti yang berasal dari berbagai sumber. Keberagaman format data ini juga dapat mempersulit analisis bukti yang terkumpul, terutama jika data tersebut terdistribusi dalam platform yang berbeda atau terenkripsi.

Isu privasi juga menjadi perhatian utama ketika menggunakan bukti elektronik dalam proses pembuktian. Banyak bukti elektronik, seperti email, pesan teks, atau riwayat pencarian internet, dapat melibatkan informasi pribadi yang sangat sensitif. Dalam hal ini, aparat penegak hukum harus memastikan bahwa pengumpulan bukti tersebut dilakukan sesuai dengan prosedur hukum yang sah dan dengan menghormati hak-hak privasi individu yang terlibat. Oleh karena itu, penggunaan bukti elektronik dalam proses pembuktian harus dilakukan dengan hati-hati dan berdasarkan peraturan yang jelas, untuk menghindari penyalahgunaan atau pelanggaran terhadap hak-hak dasar individu.

Di Indonesia, meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah memberikan landasan hukum bagi penggunaan bukti elektronik dalam proses peradilan, tantangan-tantangan di atas tetap perlu diatasi dengan baik. Pengadilan Indonesia mulai mengakui dan menerima bukti elektronik dalam proses pembuktian, namun pelatihan bagi aparat penegak hukum, serta pengembangan prosedur dan teknologi yang lebih baik, tetap diperlukan untuk memastikan bahwa bukti elektronik dapat digunakan secara efektif dalam menegakkan hukum.

C. Peran Badan Siber dan Sandi Negara (BSSN) dalam Keamanan Digital

1. Tugas dan Fungsi BSSN dalam Meningkatkan Keamanan Siber Nasional

Badan Siber dan Sandi Negara (BSSN) merupakan lembaga yang memiliki peran sangat penting dalam menjaga dan meningkatkan keamanan siber nasional Indonesia. Berdiri sejak tahun 2017, BSSN dibentuk sebagai respons terhadap semakin kompleksnya ancaman yang muncul di dunia maya, serta untuk mengelola dan mengatur kebijakan keamanan siber di Indonesia. Keamanan siber kini menjadi isu yang sangat vital, karena perkembangan teknologi informasi dan komunikasi (TIK) yang semakin pesat tidak hanya membawa manfaat besar bagi

kemajuan negara, tetapi juga menimbulkan berbagai tantangan baru dalam bentuk ancaman siber. Ancaman tersebut mencakup serangan yang dapat mengganggu infrastruktur penting, merusak data sensitif, serta mengguncang stabilitas ekonomi dan keamanan nasional.

BSSN memiliki tugas utama dalam menyusun kebijakan dan regulasi terkait keamanan siber, yang bertujuan untuk memastikan bahwa sistem informasi yang digunakan oleh negara, baik itu oleh pemerintah, sektor vital, maupun masyarakat, terlindungi dengan baik. Kebijakan yang disusun oleh BSSN mencakup berbagai aspek, mulai dari perlindungan data pribadi, pencegahan serangan siber, hingga pemulihan dari serangan yang telah terjadi. BSSN tidak hanya bertanggung jawab untuk merancang kebijakan, tetapi juga untuk mengimplementasikan kebijakan tersebut dengan cara memberikan bimbingan teknis kepada instansi pemerintah dan sektor swasta yang menjadi bagian dari sistem informasi nasional.

BSSN juga memiliki peran penting dalam melakukan pemantauan terhadap segala bentuk potensi ancaman siber yang dapat mengguncang kestabilan negara. Salah satu kegiatan utama yang dilaksanakan oleh BSSN adalah monitoring lalu lintas data di berbagai sistem penting yang digunakan oleh instansi pemerintah dan sektor lainnya. Dalam melakukan pemantauan ini, BSSN menggunakan berbagai teknologi canggih untuk mendeteksi potensi serangan, seperti serangan *Distributed Denial of Service* (DDoS), *malware*, *phishing*, dan lainnya. Melalui sistem pemantauan ini, BSSN dapat mengidentifikasi potensi ancaman sejak dini dan memberikan respons yang cepat untuk mengatasi atau mengurangi dampak dari serangan tersebut.

BSSN juga berperan dalam mendeteksi dan mengatasi insiden siber yang terjadi di Indonesia. Insiden siber sering kali datang tanpa peringatan sebelumnya, dan dampaknya dapat sangat merugikan, baik bagi individu, perusahaan, maupun negara secara keseluruhan. Oleh karena itu, BSSN memiliki tim khusus yang siap bekerja untuk merespons insiden siber, baik itu yang melibatkan sektor publik maupun sektor swasta. Tugas tim ini tidak hanya sebatas mengatasi serangan yang sedang berlangsung, tetapi juga mencakup pemulihan sistem yang terdampak dan mencegah terjadinya kerusakan lebih lanjut.

Kerjasama antara BSSN dengan lembaga-lembaga lainnya juga menjadi aspek yang sangat penting dalam upaya menjaga keamanan siber nasional. Ancaman yang muncul di dunia maya tidak mengenal

batas negara, sehingga diperlukan kerjasama lintas negara dalam mengatasi kejahatan siber yang bersifat transnasional. BSSN bekerja sama dengan lembaga internasional seperti INTERPOL, serta berbagai badan keamanan siber dari negara-negara lain untuk melakukan pertukaran informasi dan strategi dalam menghadapi ancaman siber yang semakin kompleks. Selain itu, kerjasama ini juga mencakup upaya bersama dalam pencegahan kejahatan siber dan peningkatan kapasitas sumber daya manusia di bidang keamanan siber.

Salah satu langkah signifikan yang dilakukan oleh BSSN untuk memperkuat keamanan siber adalah pengembangan dan pengelolaan sistem perisai siber nasional. Sistem ini berfungsi untuk memantau dan menganalisis potensi ancaman yang ada, serta untuk memberikan perlindungan terhadap infrastruktur dan data penting yang dimiliki oleh negara. Pusat siber nasional yang dikelola oleh BSSN berfungsi sebagai garda terdepan dalam melakukan deteksi dini terhadap ancaman yang dapat membahayakan sistem informasi. Pusat siber ini bertugas untuk mengidentifikasi pola-pola serangan yang muncul, serta memberikan respons yang cepat dan tepat agar dampak dari serangan dapat diminimalisasi.

Keamanan data menjadi salah satu aspek yang paling krusial dalam menjalankan tugas BSSN. Data sensitif yang dimiliki oleh instansi pemerintah, lembaga vital negara, dan sektor swasta harus dijaga kerahasiaannya agar tidak jatuh ke tangan yang salah. Dalam hal ini, BSSN memiliki kewajiban untuk mengatur dan memastikan bahwa data yang berada dalam sistem informasi pemerintah terlindungi dengan baik, terutama data yang memiliki nilai strategis dan penting bagi negara, seperti data terkait pertahanan, keamanan, dan perekonomian. Selain itu, BSSN juga mengelola enkripsi data yang digunakan untuk melindungi informasi yang sensitif, agar data tersebut tetap aman meskipun berada di jaringan yang rentan terhadap serangan.

BSSN juga berfungsi untuk meningkatkan kapasitas dan kesadaran mengenai pentingnya keamanan siber di seluruh lapisan masyarakat. Salah satu cara untuk melakukan hal ini adalah dengan memberikan pelatihan dan pendidikan kepada masyarakat, baik di sektor pemerintah maupun sektor swasta, mengenai bagaimana cara mengidentifikasi dan mengatasi ancaman siber. Pelatihan ini meliputi penggunaan perangkat yang aman, teknik pengamanan data pribadi, serta cara melindungi sistem informasi dari serangan. Peningkatan

kapasitas ini bertujuan agar masyarakat dapat lebih siap menghadapi ancaman siber yang terus berkembang.

Peningkatan kesadaran akan pentingnya keamanan siber juga melibatkan sektor swasta, yang memiliki peran besar dalam menjaga keamanannya di dunia maya. Banyak perusahaan yang menyimpan data penting yang bisa menjadi sasaran empuk bagi pelaku kejahatan siber. Oleh karena itu, BSSN bekerja sama dengan sektor swasta untuk memastikan bahwa perusahaan-perusahaan tersebut memiliki sistem keamanan yang memadai untuk melindungi data dan informasi pelanggan. Kerjasama antara BSSN dan sektor swasta ini penting untuk menciptakan ekosistem yang aman di dunia maya, sehingga ancaman siber dapat diminimalisasi.

Pada akhirnya, tugas dan fungsi BSSN sangat krusial dalam menjaga keberlanjutan pembangunan negara di tengah perkembangan teknologi yang semakin pesat. Keamanan siber bukan hanya menjadi tanggung jawab satu lembaga atau instansi, tetapi merupakan tanggung jawab bersama antara pemerintah, sektor swasta, dan masyarakat. BSSN sebagai lembaga yang berwenang dalam mengelola dan menjaga keamanan siber nasional, terus bekerja keras untuk memperkuat sistem pertahanan siber Indonesia, agar negara dapat menghadapi berbagai ancaman siber yang mungkin terjadi di masa depan.

2. Kolaborasi BSSN dengan Instansi Terkait dan Sektor Swasta dalam Meningkatkan Ketahanan Siber

Badan Siber dan Sandi Negara (BSSN) memiliki tugas yang sangat penting dalam menjaga ketahanan siber nasional Indonesia. Namun, tugas ini tidak dapat dijalankan dengan efektif tanpa adanya kolaborasi dengan berbagai pihak terkait, baik itu di tingkat pemerintah, sektor swasta, maupun lembaga internasional. Keamanan siber di Indonesia memerlukan kerjasama lintas sektor karena ancaman siber yang semakin kompleks dan terus berkembang dapat menyerang berbagai aspek kehidupan digital, dari infrastruktur kritis hingga sektor yang lebih sensitif seperti data pribadi. Oleh karena itu, kolaborasi antar lembaga dan sektor menjadi aspek krusial dalam membangun ketahanan siber yang kokoh.

Untuk menjalankan perannya, BSSN bekerja sama erat dengan berbagai instansi pemerintah yang memiliki peran penting dalam menjaga keamanan negara. Salah satu mitra utama BSSN adalah

Kementerian Komunikasi dan Informatika (Kominfo), yang berfungsi untuk mengatur dan mengawasi sektor TIK di Indonesia. Kominfo, bersama BSSN, memastikan bahwa kebijakan dan regulasi terkait keamanan informasi serta infrastruktur digital diterapkan dengan baik di Indonesia. Selain itu, Kementerian Pertahanan juga berperan dalam menjaga aspek keamanan siber yang terkait dengan pertahanan negara, yang melibatkan ancaman terhadap data dan sistem yang sangat sensitif. Badan Intelijen Negara (BIN) turut berkontribusi dengan menyediakan informasi intelijen yang berguna untuk mendeteksi ancaman yang lebih besar dan lebih terorganisir.

Peran BSSN tidak terbatas pada kolaborasi dengan lembaga pemerintah saja. Sektor swasta, terutama perusahaan yang mengelola infrastruktur kritis, juga memiliki tanggung jawab besar dalam menjaga keamanan siber. Perusahaan telekomunikasi, penyedia layanan internet, dan lembaga keuangan merupakan beberapa contoh sektor yang harus menjaga sistem dan datanya agar tidak jatuh ke tangan yang salah. BSSN berperan sebagai penghubung yang menyatukan berbagai sektor ini, membantunya dalam merancang dan menerapkan kebijakan keamanan siber yang terintegrasi. Hal ini sangat penting, mengingat ancaman siber tidak mengenal batasan sektor atau instansi tertentu, dan satu serangan siber yang berhasil dapat mempengaruhi banyak pihak dalam waktu yang bersamaan.

Kolaborasi antara BSSN dan sektor swasta juga terwujud dalam program pelatihan dan simulasi yang dilakukan secara berkala. Salah satu contoh konkret dari kolaborasi ini adalah Simulasi Serangan Siber Nasional yang melibatkan berbagai sektor, baik pemerintah maupun swasta. Dalam simulasi ini, berbagai pihak diberi kesempatan untuk berlatih dalam menghadapi ancaman siber yang nyata, dan menguji sejauh mana kesiapannya dalam menanggulangi serangan. Simulasi ini bukan hanya bertujuan untuk meningkatkan kemampuan teknis, tetapi juga untuk memperkuat koordinasi antara sektor-sektor yang terlibat dalam menjaga keamanan siber.

BSSN juga melakukan peningkatan kapasitas melalui penyelenggaraan berbagai pelatihan, seminar, dan workshop yang berfokus pada keamanan informasi dan manajemen risiko siber. Pelatihan ini diberikan kepada berbagai pihak yang terlibat dalam sistem informasi negara, baik di sektor publik maupun swasta. Tujuan dari pelatihan ini adalah untuk memastikan bahwa semua pihak memahami

pentingnya pencegahan serangan siber dan memiliki keterampilan yang diperlukan untuk mengatasi insiden jika terjadi. Dengan memiliki pemahaman yang baik tentang keamanan informasi dan risiko yang ada, setiap sektor dapat lebih siap menghadapi ancaman siber yang semakin kompleks.

BSSN juga berperan dalam menetapkan standar keamanan informasi yang harus diterapkan oleh sektor swasta dan lembaga pemerintah di Indonesia. Standar ini bertujuan untuk memastikan bahwa setiap sistem yang digunakan oleh instansi terkait memiliki tingkat keamanan yang memadai. BSSN bekerja sama dengan Badan Standarisasi Nasional (BSN) dalam merancang dan mengatur standar yang harus diikuti oleh sektor-sektor yang terlibat. Melalui penerapan standar ini, BSSN berharap dapat meminimalkan potensi kerentanannya dan memastikan bahwa setiap sektor siap menghadapi serangan yang mungkin datang.

Ancaman siber sering kali tidak mengenal batas negara, sehingga kolaborasi internasional menjadi sangat penting dalam menghadapi ancaman yang lebih besar dan lebih terorganisir. Kejahatan siber lintas negara dapat melibatkan pelaku dari berbagai belahan dunia, yang memanfaatkan celah-celah dalam sistem yang ada untuk melakukan serangan. Untuk itu, BSSN menjalin hubungan erat dengan lembaga keamanan siber dari negara lain, seperti Interpol, Europol, dan lembaga-lembaga serupa yang berfungsi untuk menangani kejahatan siber. Kerja sama ini memungkinkan BSSN untuk mendapatkan informasi terbaru mengenai tren ancaman siber yang terjadi di dunia internasional, serta berbagi informasi yang relevan mengenai potensi ancaman yang dapat berimbas ke Indonesia.

Kolaborasi internasional tidak hanya terbatas pada pertukaran informasi terkait kejahatan siber, tetapi juga dalam bentuk bantuan teknis dan sumber daya untuk mengatasi ancaman yang lebih besar. Dalam beberapa kasus, serangan siber yang dilakukan oleh aktor-aktor yang beroperasi di luar negeri dapat membutuhkan kerjasama lintas negara untuk memitigasi dampaknya. Misalnya, serangan yang melibatkan *ransomware* atau serangan DDoS dapat mempengaruhi banyak negara, dan membutuhkan tindakan koordinasi untuk mengatasi penyebarannya. BSSN, melalui kerjasama internasional, dapat membantu Indonesia untuk mendapatkan akses ke sumber daya dan teknologi yang dibutuhkan untuk mengatasi serangan-serangan tersebut.

Salah satu tantangan besar dalam era transformasi digital saat ini adalah perlindungan data pribadi. Data pribadi, jika jatuh ke tangan yang salah, dapat digunakan untuk berbagai kejahatan seperti pencurian identitas, penipuan, atau bahkan pemerasan. Oleh karena itu, BSSN turut berperan aktif dalam pembangunan kebijakan perlindungan data pribadi, baik di sektor pemerintah maupun sektor swasta. BSSN bekerja sama dengan Kementerian Komunikasi dan Informatika dalam merumuskan regulasi yang melindungi data pribadi masyarakat Indonesia, dan memastikan bahwa regulasi tersebut diterapkan secara konsisten di seluruh sektor. Perlindungan data pribadi ini tidak hanya melindungi individu, tetapi juga memperkuat ketahanan siber nasional secara keseluruhan.

Pentingnya kolaborasi BSSN dengan berbagai pihak terkait semakin terlihat seiring dengan meningkatnya ancaman yang dihadapi Indonesia di dunia maya. Kejahatan siber dapat merusak tidak hanya reputasi suatu negara, tetapi juga dapat mengguncang stabilitas ekonomi, politik, dan sosial. Oleh karena itu, kolaborasi yang kuat antara pemerintah, sektor swasta, dan lembaga internasional sangat diperlukan untuk memastikan bahwa Indonesia memiliki ketahanan siber yang cukup untuk menghadapi ancaman tersebut. Melalui kerjasama ini, Indonesia dapat memperkuat kemampuan pertahanannya, meningkatkan ketahanan digitalnya, dan melindungi infrastruktur vital yang menjadi penopang kehidupan digital negara.

D. Tantangan dalam Investigasi dan Penuntutan Tindak Pidana Siber

1. Kompleksitas dan Kecepatan Perkembangan Teknologi

Perkembangan teknologi informasi dan komunikasi yang begitu pesat telah membawa dampak besar terhadap banyak aspek kehidupan, baik dalam hal kemudahan akses informasi, efisiensi komunikasi, hingga transformasi dalam berbagai sektor. Namun, di balik manfaat yang ditawarkan, perkembangan teknologi ini juga menimbulkan tantangan besar, terutama dalam konteks penanganan tindak pidana siber. Salah satu tantangan terbesar yang dihadapi oleh aparat penegak hukum dan lembaga terkait dalam menangani kejahatan siber adalah kompleksitas dan kecepatan perubahan teknologi. Dunia siber berkembang sangat cepat, sering kali lebih cepat daripada kemampuan aparat penegak

hukum untuk menanggapi dan menyesuaikan diri dengan perkembangan ini. Teknologi baru muncul setiap saat, dan sering kali digunakan oleh pelaku kejahatan untuk melakukan tindak pidana yang sulit terdeteksi dan ditangani.

Kecepatan perkembangan teknologi membuat pelaku kejahatan siber lebih mudah untuk mengelak dari identifikasi dan penuntutan, menggunakan berbagai alat dan metode yang terus berubah untuk menyembunyikan jejak digital, seperti teknologi enkripsi yang semakin canggih, serta alat-alat anonim yang dapat menyembunyikan identitas dan lokasinya. Misalnya, VPN (*Virtual Private Network*) dan Tor adalah dua contoh teknologi yang banyak digunakan oleh pelaku kejahatan siber untuk menyamarkan alamat IP dan membuatnya lebih sulit dilacak. Penggunaan alat-alat semacam ini memungkinkan pelaku untuk melancarkan serangan dari tempat yang jauh, bahkan di luar yurisdiksi negara tempat kejahatan itu dilakukan, yang menambah kerumitan dalam proses penyidikan dan penuntutan.

Salah satu contoh yang menggambarkan kompleksitas ini adalah serangan *ransomware*, yang sering kali melibatkan penyembunyian jejak pelaku melalui enkripsi. Dalam serangan *ransomware*, data yang berhasil dikunci oleh pelaku akan sulit dipulihkan tanpa adanya kunci enkripsi yang tepat. Para pelaku sering kali meminta tebusan dalam bentuk mata uang digital, seperti Bitcoin, yang menambah lapisan kerumitan dalam melacak aliran uang yang terkait dengan kejahatan tersebut. Selain itu, dalam serangan *phishing*, pelaku bisa saja menggunakan situs web palsu yang sangat mirip dengan situs resmi, yang membuat deteksi serangan menjadi semakin sulit bagi korban maupun pihak berwenang. Meskipun bukti-bukti sudah ada, identifikasi dan pelacakan sumber serangan menjadi lebih sulit karena teknologi yang digunakan oleh pelaku untuk menyembunyikan identitasnya sangat canggih.

Pelaku kejahatan siber sering kali bergerak dari satu negara ke negara lain, sehingga memperumit penuntutan secara hukum. Jurisdiksi internasional dalam kasus kejahatan siber adalah masalah besar yang seringkali membatasi efektivitas penegakan hukum. Server yang digunakan untuk melakukan kejahatan bisa berada di luar negeri, dan jika negara tersebut tidak memiliki kebijakan atau kerjasama yang memadai, proses penyidikan menjadi terhambat. Kejahatan siber yang melibatkan pelaku internasional memerlukan kerjasama lintas negara

dan perjanjian internasional yang jelas mengenai prosedur hukum yang dapat diterapkan. Hal ini sering kali menjadi kendala karena perbedaan regulasi antara negara-negara yang terlibat dalam proses penyidikan atau penuntutan.

Tantangan lainnya adalah terkait dengan pembuktian dan pengumpulan bukti dalam kejahatan siber. Seiring dengan semakin canggihnya teknologi, bukti yang relevan sering kali tidak dapat langsung ditemukan atau diakses dengan mudah. Bukti elektronik seperti jejak transaksi digital, email, atau log aktivitas mungkin tersembunyi di dalam server yang terenskripsi atau tersebar di berbagai platform yang berada di luar jangkauan penyidik. Bahkan ketika bukti telah dikumpulkan, pelaku kejahatan siber dapat dengan mudah menghapus atau memanipulasi bukti-bukti tersebut untuk menghilangkan jejaknya. Misalnya, perangkat lunak khusus bisa digunakan untuk menghancurkan file yang berisi bukti penting dalam waktu yang sangat singkat, atau untuk merusak data yang telah dikumpulkan.

Perkembangan teknologi yang begitu cepat mempengaruhi alat yang digunakan oleh aparat penegak hukum untuk mengumpulkan dan menganalisis bukti. Perangkat lunak penyelidikan dan alat analisis digital yang digunakan untuk menangani bukti siber harus selalu diperbarui untuk mengikuti perkembangan teknologi terbaru. Dalam konteks ini, lembaga penegak hukum harus memiliki kemampuan teknis yang sangat tinggi dan sumber daya yang cukup besar untuk dapat mengikuti perkembangan ini. Penyidik dan analis digital perlu dilatih secara teratur agar dapat mengoperasikan perangkat lunak dan alat-alat canggih yang digunakan dalam investigasi siber.

Keahlian yang dibutuhkan dalam menangani bukti digital juga sangat spesifik, karena bukti yang ditemukan di dunia maya memiliki sifat yang berbeda dengan bukti fisik. Data digital yang ditemukan di perangkat atau server bisa bersifat volatile, artinya data tersebut dapat hilang atau rusak dalam waktu singkat jika tidak segera diambil dan dianalisis dengan benar. Oleh karena itu, penyidik siber harus bekerja cepat dan akurat dalam mengumpulkan bukti. Penggunaan teknik yang tidak tepat atau keterlambatan dalam pengambilan data dapat mengakibatkan hilangnya bukti yang dapat digunakan dalam proses penyidikan dan penuntutan.

Kemampuan untuk menganalisis bukti digital juga semakin kompleks. Tidak hanya harus memeriksa file atau data yang dapat

terlihat secara langsung, tetapi juga harus mengidentifikasi pola, hubungan, atau jejak yang tidak langsung. Misalnya, log server atau metadata file yang tidak tampak jelas pada pandangan pertama dapat menyimpan informasi yang sangat penting untuk mengidentifikasi pelaku atau melacak jalannya kejahatan. Proses ini memerlukan pemahaman yang mendalam tentang teknologi serta keterampilan analisis yang sangat tinggi. Karena itu, lembaga yang menangani kejahatan siber seringkali membutuhkan tim yang terdiri dari berbagai ahli, termasuk ahli forensik digital, pengembang perangkat lunak, dan analis data.

Menghadapi tantangan ini, pihak berwenang juga perlu mengembangkan sistem yang lebih baik dalam kolaborasi internasional dan pertukaran informasi terkait kejahatan siber. Kerjasama antara negara-negara di dunia ini sangat penting untuk menghadapi kejahatan yang sering melibatkan pelaku lintas negara. Dengan adanya platform berbagi informasi dan data yang lebih baik, penyidik dapat memperoleh informasi yang diperlukan untuk menangani kejahatan siber secara lebih efektif. Selain itu, perjanjian internasional mengenai ekstradisi pelaku dan kerjasama dalam penyidikan juga menjadi langkah penting untuk mengatasi hambatan-hambatan yang terkait dengan yurisdiksi internasional.

Pada akhirnya, untuk dapat menanggulangi kejahatan siber yang semakin kompleks ini, dibutuhkan investasi yang besar dalam sumber daya manusia dan teknologi. Negara-negara harus terus mengembangkan kemampuan dalam menghadapi tantangan yang ditimbulkan oleh perkembangan teknologi yang cepat. Hal ini mencakup pengembangan kebijakan yang adaptif terhadap perkembangan teknologi, peningkatan kerjasama internasional, serta pembentukan lembaga dan unit yang khusus menangani kejahatan siber. Hanya dengan cara ini, penegakan hukum dapat berjalan dengan efektif, dan ancaman kejahatan siber yang terus berkembang dapat ditekan..

2. Isu Legal dan Hak Asasi Manusia

Investigasi tindak pidana siber tidak hanya menghadapi tantangan teknis yang berkaitan dengan teknologi yang berkembang pesat, tetapi juga berbagai isu legal dan hak asasi manusia yang harus dipertimbangkan secara hati-hati oleh aparat penegak hukum. Salah satu isu utama yang muncul dalam investigasi kejahatan siber adalah

perlindungan data pribadi dan hak privasi individu. Kejahatan siber sering kali melibatkan pengumpulan bukti yang bersifat sangat pribadi dan sensitif, seperti riwayat komunikasi elektronik, data transaksi digital, atau bahkan informasi terkait perilaku online seseorang. Dalam konteks ini, pengumpulan bukti yang relevan harus dilakukan dengan sangat hati-hati, dengan memperhatikan regulasi yang ada untuk memastikan bahwa hak-hak dasar individu, terutama hak privasi, tetap terjaga.

Di Indonesia, meskipun telah diterbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur mengenai penggunaan teknologi informasi, perlindungan data pribadi, dan transaksi elektronik, masalah perlindungan privasi data masih menjadi isu yang terus berkembang. Beberapa bagian dalam UU ITE belum cukup komprehensif untuk menangani isu perlindungan data pribadi secara maksimal. Selain itu, terdapat celah hukum yang belum sepenuhnya menyeimbangkan antara kebutuhan untuk mengungkap kejahatan siber dan perlindungan terhadap hak-hak individu. Ini mengarah pada kesulitan dalam menanggulangi kejahatan siber tanpa melanggar privasi atau hak asasi manusia yang dilindungi oleh konstitusi.

Pengumpulan bukti dalam kasus kejahatan siber harus dilakukan dengan mematuhi prosedur hukum yang sah, yang salah satunya adalah memperoleh izin dari otoritas yang berwenang sebelum melakukan penyitaan atau penggeledahan data. Tanpa prosedur yang tepat, bukti yang diperoleh dapat dianggap tidak sah atau tidak dapat diterima di pengadilan, yang dapat menghambat proses hukum. Oleh karena itu, aparat penegak hukum harus benar-benar memastikan bahwa menjalankan prosedur yang benar dalam pengumpulan bukti digital. Setiap kesalahan dalam proses ini, meskipun kecil, dapat berakibat fatal dan berpotensi menggugurkan kasus yang sedang ditangani.

Masalah lain yang dihadapi oleh aparat penegak hukum adalah perbedaan kebijakan antarnegara terkait dengan akses data, terutama data yang disimpan di server yang berada di luar negeri. Banyak server yang digunakan untuk menyimpan data penting terkait dengan kejahatan siber berada di luar jurisdiksi Indonesia. Hal ini menimbulkan kesulitan dalam mengakses bukti atau data yang relevan, karena untuk mengambil data tersebut, diperlukan kerjasama internasional yang melibatkan prosedur hukum yang panjang dan rumit. Proses ini bisa sangat memperlambat investigasi dan menghambat penuntutan, terutama jika

negara tempat data disimpan memiliki regulasi yang ketat atau tidak bekerja sama dalam hal pengungkapan bukti.

Regulasi internasional terkait dengan akses data dan penanganan bukti digital juga sering kali tidak seragam antarnegara. Masing-masing negara memiliki aturan yang berbeda tentang bagaimana data dapat diakses, baik oleh aparat penegak hukum dari negara asal ataupun negara lain. Beberapa negara mungkin tidak memiliki undang-undang yang memadai untuk menangani masalah privasi dan perlindungan data pribadi, sementara negara lainnya menerapkan regulasi yang sangat ketat. Hal ini menyebabkan terjadinya ketidaksesuaian antara regulasi satu negara dengan negara lainnya, yang tentunya memperburuk tantangan dalam penegakan hukum di ranah siber.

Pengumpulan dan penyajian bukti digital di pengadilan sering kali memunculkan tantangan tersendiri. Bukti elektronik yang diperoleh dari dunia maya sering kali dianggap lebih rentan terhadap perubahan atau manipulasi dibandingkan dengan bukti fisik. Oleh karena itu, pengadilan perlu memastikan bahwa bukti yang diajukan memiliki integritas yang tinggi dan dapat dipertanggungjawabkan. Salah satu cara untuk memastikan hal ini adalah dengan menerapkan prinsip *chain of custody*, yaitu jejak yang menunjukkan bahwa bukti tersebut tidak mengalami perubahan sejak diperoleh hingga disajikan di pengadilan. Jika prosedur ini tidak dipatuhi dengan ketat, bukti tersebut bisa saja dianggap tidak sah atau tidak dapat diterima, yang akan memengaruhi jalannya proses peradilan.

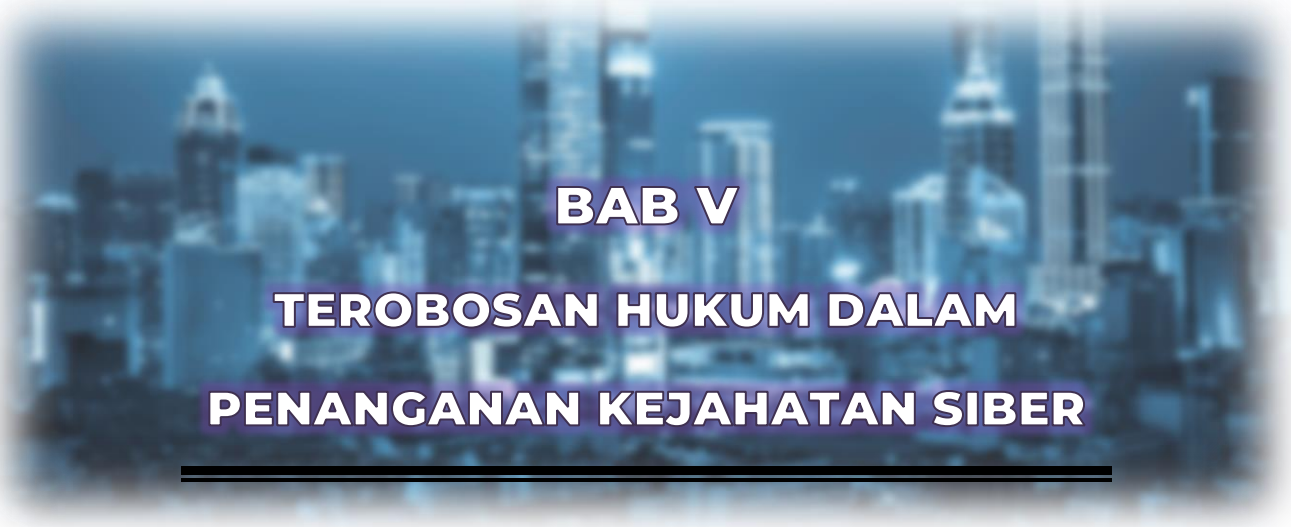
Salah satu tantangan besar dalam hal ini adalah memastikan bahwa bukti yang dikumpulkan tetap terjaga keasliannya. Bukti digital seperti file, log, atau rekaman komunikasi dapat dengan mudah dimanipulasi atau diubah. Oleh karena itu, aparat penegak hukum perlu menggunakan teknologi forensik yang tepat untuk memastikan bahwa bukti digital yang dikumpulkan adalah sah dan valid. Proses ini harus dilakukan dengan hati-hati agar tidak ada bukti yang hilang atau rusak selama penyelidikan. Selain itu, pemeriksaan bukti digital harus dilakukan oleh ahli yang memiliki pemahaman yang mendalam mengenai teknologi serta prosedur hukum yang berlaku.

Pada beberapa kasus, bukti yang diambil dari server atau perangkat lain bisa saja melibatkan informasi yang tidak relevan atau sensitif, yang jika dibuka atau diproses tanpa izin dapat melanggar privasi individu. Oleh karena itu, penting untuk membatasi pengambilan

data hanya pada informasi yang relevan dengan kasus yang sedang diselidiki. Hal ini bertujuan untuk mencegah terjadinya pelanggaran hak asasi manusia, terutama hak atas privasi, yang dapat merugikan pihak yang tidak bersalah.

Untuk menghadapi tantangan ini, penting untuk adanya kerangka hukum yang jelas mengenai pengumpulan bukti digital yang mempertimbangkan keseimbangan antara hak privasi individu dan kebutuhan untuk mengungkap tindak pidana siber. Negara perlu mengembangkan undang-undang yang lebih komprehensif mengenai perlindungan data pribadi dan prosedur hukum yang lebih efisien dalam mengakses bukti digital. Undang-undang tersebut harus memberikan pedoman yang jelas bagi aparat penegak hukum untuk dapat menjalankan tugasnya secara efektif, tanpa melanggar hak asasi manusia.

Meskipun tantangan-tantangan ini cukup besar, perkembangan teknologi dan pengetahuan hukum harus berjalan seiring untuk memastikan bahwa investigasi tindak pidana siber dapat dilakukan secara adil dan sah. Diperlukan adanya kerjasama antarnegara, penguatan regulasi di dalam negeri, serta peningkatan kesadaran akan pentingnya perlindungan hak asasi manusia dalam setiap langkah penegakan hukum di ranah siber. Dengan cara ini, diharapkan tindak pidana siber dapat diungkap dengan lebih efektif, tanpa mengorbankan hak-hak dasar individu yang harus dilindungi oleh negara.



BAB V
TEROBOSAN HUKUM DALAM PENANGANAN KEJAHATAN SIBER

Terobosan hukum dalam penanganan kejahatan siber menjadi hal yang sangat penting mengingat semakin kompleksnya ancaman digital yang dihadapi oleh negara dan masyarakat. Kejahatan siber, yang melibatkan berbagai tindakan kriminal yang dilakukan melalui teknologi informasi dan komunikasi, terus berkembang seiring dengan pesatnya kemajuan teknologi. Hal ini menuntut negara untuk terus berinovasi dalam mengadaptasi sistem hukum yang ada, agar dapat menangani kasus-kasus yang muncul dengan efektif. Di Indonesia, beberapa langkah hukum mulai diperkenalkan untuk merespon ancaman ini, termasuk peraturan yang lebih spesifik dan adaptif terhadap fenomena baru dalam dunia maya. Selain itu, berbagai terobosan dilakukan untuk memastikan bahwa proses penegakan hukum bisa mengikuti dinamika perkembangan teknologi yang begitu cepat. Penguatan regulasi mengenai perlindungan data pribadi, peningkatan kapasitas aparat penegak hukum dalam mengusut tindak pidana siber, serta kolaborasi internasional dalam penanganan kejahatan lintas negara menjadi bagian dari upaya untuk menciptakan kerangka hukum yang lebih responsif dan efisien. Dengan demikian, terobosan hukum ini diharapkan dapat meningkatkan efektivitas penanganan tindak pidana siber serta memberikan perlindungan yang lebih baik bagi masyarakat dan negara dari ancaman di dunia maya.

A. Penguatan Regulasi dan Harmonisasi UU ITE

1. Penguatan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang disahkan pada tahun 2008 telah menjadi landasan hukum utama

bagi pengaturan dan penanganan berbagai masalah yang terkait dengan teknologi informasi di Indonesia. Sebagai regulasi yang mengatur transaksi elektronik, penyalahgunaan informasi, serta kejahatan siber, UU ITE memiliki peran yang sangat penting dalam membentuk struktur hukum yang dapat menanggulangi berbagai tindakan kriminal yang terjadi di dunia maya. Kejahatan siber yang dimaksud mencakup berbagai tindakan yang merugikan individu, perusahaan, maupun negara, seperti penipuan online, pornografi, pencemaran nama baik, dan banyak lagi. Namun, dengan perkembangan teknologi yang semakin pesat serta semakin kompleksnya bentuk-bentuk kejahatan siber, kebutuhan untuk memperkuat dan memperbarui UU ITE menjadi semakin mendesak.

Salah satu tantangan terbesar dalam menghadapi perkembangan teknologi ini adalah kecepatan dan dinamika inovasi digital yang terjadi hampir setiap saat. Kejahatan siber yang muncul tidak hanya beroperasi di dalam negeri, tetapi sering kali melibatkan pelaku dari luar negeri. Hal ini membuat penegakan hukum menjadi lebih sulit karena adanya kendala terkait yurisdiksi dan perbedaan peraturan antarnegara. Misalnya, serangan siber yang melibatkan pelaku internasional sering kali menuntut kerja sama antarnegara dan prosedur hukum yang rumit untuk mengakses bukti yang disimpan di luar negeri. Dalam hal ini, penguatan UU ITE harus mencakup prosedur hukum yang memungkinkan aparat penegak hukum untuk menghadapi kejahatan siber lintas negara secara lebih efektif, serta meningkatkan kemampuan investigasi dalam mendeteksi dan menindak pelaku kejahatan siber di tingkat global.

Penguatan UU ITE juga sangat diperlukan dalam hal sanksi dan penegakan hukum. Saat ini, beberapa jenis kejahatan siber, seperti peretasan dan penipuan digital, sering kali tidak memiliki sanksi yang cukup jelas dan tegas dalam hukum Indonesia. Kejahatan-kejahatan ini semakin canggih dan sering kali melibatkan sejumlah pelaku yang tersebar di berbagai lokasi, membuatnya sulit untuk mengidentifikasi siapa yang bertanggung jawab. Oleh karena itu, perlu adanya penyempurnaan terhadap ketentuan sanksi yang dapat memberikan efek jera bagi pelaku, serta prosedur investigasi yang lebih komprehensif untuk menangani kejahatan siber dengan lebih efisien. Dengan demikian, penguatan UU ITE diharapkan dapat memberikan ruang yang

lebih luas bagi aparat penegak hukum untuk menindak pelaku kejahatan siber, dan pada saat yang sama memastikan bahwa keadilan tetap terjaga.

Penguatan UU ITE juga mencakup perlunya ketentuan yang lebih jelas terkait dengan perlindungan data pribadi. Dalam beberapa tahun terakhir, data pribadi menjadi semakin berharga, baik bagi individu maupun organisasi. Penyalahgunaan data pribadi dapat merugikan banyak pihak, dan kasus kebocoran data pribadi yang sering terjadi semakin menunjukkan pentingnya perlindungan yang lebih ketat terhadap informasi sensitif. UU ITE sebagai regulasi utama yang mengatur kejahatan siber harus memperbarui ketentuannya untuk mencakup perlindungan data pribadi yang lebih komprehensif. Hal ini akan mencakup kewajiban bagi penyedia platform digital untuk mengelola data pribadi dengan cara yang aman, serta memastikan bahwa pengguna dapat mengontrol penggunaan datanya secara lebih transparan dan terjamin.

Saat ini, regulasi terkait dengan perlindungan data pribadi di Indonesia masih terbilang lemah dibandingkan dengan negara-negara lain yang memiliki kebijakan lebih ketat, seperti Uni Eropa dengan *General Data Protection Regulation* (GDPR). Keberadaan peraturan yang lebih tegas tentang perlindungan data pribadi dalam UU ITE sangat diperlukan untuk mengatasi kekhawatiran masyarakat tentang penyalahgunaan data pribadi yang dapat terjadi di dunia maya. Hal ini termasuk di dalamnya pengaturan tentang bagaimana data pribadi dapat diproses, dibagikan, dan diakses oleh pihak ketiga, serta hak individu untuk menghapus atau memperbarui data pribadinya yang sudah disimpan oleh penyedia platform. Tanpa perlindungan yang memadai, data pribadi akan rentan terhadap pencurian atau penyalahgunaan yang dapat merugikan pemiliknya.

Salah satu aspek penting dalam penguatan UU ITE adalah peningkatan kesadaran publik dan pelatihan mengenai pentingnya perlindungan data pribadi. Masyarakat perlu diberikan pemahaman yang lebih baik tentang hak-haknya terkait data pribadi, serta bagaimana dapat menjaga informasi sensitif agar tidak jatuh ke tangan yang salah. Selain itu, penyedia platform digital juga harus bertanggung jawab untuk memberikan edukasi kepada pengguna mengenai pentingnya menjaga privasi dan keamanan data pribadinya. Dengan memperkuat aspek perlindungan data pribadi dalam UU ITE, diharapkan Indonesia dapat meningkatkan kepercayaan masyarakat terhadap penggunaan platform

digital, sekaligus memastikan bahwa hak privasi individu tetap terlindungi.

Penguatan UU ITE juga perlu menyentuh aspek perlindungan terhadap sektor-sektor penting yang menjadi sasaran utama serangan siber, seperti sektor perbankan, energi, dan infrastruktur kritis lainnya. Dalam era digital, kejahatan siber dapat menargetkan berbagai sektor yang mendukung kehidupan ekonomi dan sosial, sehingga dampaknya bisa sangat besar. Oleh karena itu, pengaturan mengenai perlindungan sektor-sektor vital ini harus diperkuat agar ancaman terhadap keutuhan negara dan perekonomian dapat diantisipasi dengan lebih baik. UU ITE harus memberikan dasar hukum yang jelas mengenai kewajiban sektor-sektor tersebut untuk menjaga sistem digital tetap aman dari potensi ancaman siber.

Salah satu upaya yang perlu dilakukan adalah dengan mengintegrasikan peraturan mengenai keamanan siber dalam regulasi sektoral yang lebih spesifik, seperti sektor perbankan, energi, dan transportasi. Dengan demikian, UU ITE dapat berfungsi sebagai landasan bagi kebijakan keamanan yang lebih detail dan aplikatif, sehingga sektor-sektor kritis ini memiliki sistem perlindungan yang lebih kuat terhadap ancaman yang datang dari dunia maya. Peningkatan kerjasama antara pemerintah, sektor swasta, dan masyarakat juga sangat penting untuk menciptakan ekosistem digital yang aman dan dapat diandalkan.

Penguatan UU ITE merupakan langkah penting dalam menghadapi tantangan baru yang muncul seiring dengan perkembangan teknologi informasi dan komunikasi. Dengan memperbarui dan memperkuat UU ITE, Indonesia dapat meningkatkan kemampuan dalam menangani kejahatan siber, melindungi data pribadi masyarakat, serta menjaga stabilitas sektor-sektor vital yang mendukung kehidupan negara. Dalam proses ini, perlu ada keseimbangan antara penegakan hukum yang tegas dan perlindungan terhadap hak asasi manusia, agar hukum siber Indonesia dapat berfungsi dengan optimal dan sesuai dengan perkembangan zaman. Penguatan ini tidak hanya akan memperkuat sistem hukum Indonesia, tetapi juga memberikan rasa aman bagi masyarakat dalam menggunakan teknologi digital.

2. Harmonisasi UU ITE dengan Peraturan Terkait Keamanan Siber dan Perlindungan Data Pribadi

Harmonisasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dengan peraturan lain yang berkaitan dengan keamanan siber dan perlindungan data pribadi sangat penting untuk menciptakan kerangka hukum yang lebih komprehensif dan efektif dalam menangani berbagai tantangan yang muncul di dunia maya. UU ITE yang disahkan pada tahun 2008 telah menjadi dasar utama bagi regulasi transaksi elektronik dan penyalahgunaan informasi di Indonesia. Namun, dengan perkembangan teknologi yang semakin pesat, regulasi ini perlu disesuaikan dengan kondisi terkini, terutama dengan munculnya peraturan baru yang lebih spesifik seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2020. Harmonisasi antara kedua undang-undang ini akan membantu menciptakan keselarasan antara aspek transaksi elektronik dan perlindungan data pribadi, yang merupakan dua hal yang saling terkait dalam dunia digital.

Salah satu tantangan utama dalam harmonisasi ini adalah perbedaan fokus dan cakupan antara UU ITE dan UU PDP. UU ITE lebih berfokus pada transaksi elektronik, penyalahgunaan informasi, dan tindak pidana siber secara umum. Sementara itu, UU PDP lebih terfokus pada perlindungan data pribadi, yang mencakup hak-hak individu atas data pribadinya serta kewajiban penyedia layanan digital untuk menjaga keamanan dan kerahasiaan data tersebut. Oleh karena itu, dalam rangka memastikan kedua peraturan ini berjalan seiring, perlu ada upaya untuk memperkuat hubungan antara keduanya sehingga masing-masing peraturan dapat saling mendukung dan tidak tumpang tindih. Misalnya, dalam UU ITE belum ada pengaturan yang cukup rinci mengenai mekanisme perizinan dan pengawasan terhadap pengumpulan, penyimpanan, dan pemrosesan data pribadi. Padahal, mekanisme ini merupakan bagian yang sangat penting dalam menjamin perlindungan terhadap data pribadi masyarakat.

Peraturan mengenai pengumpulan dan pengolahan data pribadi yang diatur dalam UU PDP perlu lebih ditekankan dalam UU ITE agar keduanya bisa berjalan secara sinergis. UU PDP mengatur hak-hak individu, seperti hak untuk mengetahui informasi tentang pengumpulan dan pemrosesan data, serta hak untuk mengakses, mengoreksi, dan menghapus data pribadi. Di sisi lain, UU ITE lebih mengatur tentang transaksi dan penyalahgunaan informasi yang terjadi dalam ruang

digital, tetapi kurang menekankan aspek perlindungan data pribadi secara mendetail. Oleh karena itu, perlu ada penyesuaian dalam UU ITE agar pengaturan tentang pengumpulan dan pemrosesan data pribadi lebih terintegrasi dengan ketentuan yang ada dalam UU PDP. Dengan demikian, kedua peraturan ini dapat berjalan harmonis, memberikan perlindungan yang lebih kuat kepada masyarakat dalam dunia digital.

Pada konteks ini, harmonisasi juga penting dilakukan dengan memperhatikan regulasi lain yang berhubungan dengan kejahatan siber, seperti peraturan terkait e-commerce, telekomunikasi, dan perlindungan konsumen. Seiring dengan berkembangnya dunia e-commerce, permasalahan yang sering terjadi adalah penyalahgunaan data konsumen, penipuan online, dan pencurian identitas. Banyak transaksi yang melibatkan data pribadi konsumen yang rentan disalahgunakan oleh pelaku kejahatan siber. Oleh karena itu, harmonisasi UU ITE dengan peraturan e-commerce dan perlindungan konsumen akan memastikan bahwa setiap transaksi yang terjadi di dunia maya tetap berada dalam kerangka hukum yang jelas dan terjamin keamanannya. Hal ini juga akan memberikan kepastian hukum bagi penyedia layanan e-commerce serta konsumen, sehingga dapat mengurangi potensi kerugian yang disebabkan oleh praktik-praktik kejahatan siber.

Peraturan-peraturan yang mengatur tentang telekomunikasi juga perlu diharmonisasikan dengan UU ITE. Infrastruktur telekomunikasi menjadi salah satu bagian penting dalam mendukung perkembangan teknologi informasi di Indonesia. Namun, infrastruktur ini juga menjadi sasaran utama serangan siber yang dapat merusak sistem komunikasi dan menyebabkan kerugian yang besar. Oleh karena itu, harmonisasi antara UU ITE dan regulasi yang berkaitan dengan sektor telekomunikasi akan memastikan bahwa operator telekomunikasi memiliki kewajiban yang lebih jelas dalam menjaga keamanan data dan informasi yang melewati jaringan. Regulasi yang lebih ketat dalam sektor ini akan memperkecil celah yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk menyusup ke dalam sistem yang ada.

Pengharmonisasian UU ITE dengan berbagai peraturan yang ada akan menciptakan satu sistem hukum yang lebih terpadu dan mampu mengakomodasi berbagai dinamika yang ada di dunia maya. Salah satu manfaat dari harmonisasi ini adalah pengurangan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber. Tanpa adanya kerangka hukum yang jelas dan komprehensif, banyak pelaku kejahatan yang

dapat menghindari sanksi hukum dengan memanfaatkan ketidakjelasan dalam regulasi yang ada. Dengan adanya harmonisasi yang baik antara UU ITE dan peraturan terkait, aparat penegak hukum akan lebih mudah dalam menegakkan hukum dan memastikan bahwa pelaku kejahatan siber mendapat sanksi yang setimpal.

Harmonisasi peraturan juga akan memperkuat perlindungan terhadap masyarakat. Kejahatan siber semakin berkembang, dan masyarakat sebagai pengguna teknologi digital sering kali menjadi korban dari tindak pidana yang terjadi di dunia maya. Oleh karena itu, penting untuk memastikan bahwa regulasi yang ada memberikan perlindungan yang optimal terhadap hak-hak individu, terutama terkait dengan data pribadi dan transaksi elektronik. Dengan adanya harmonisasi, masyarakat akan merasa lebih aman dalam menggunakan teknologi informasi dan komunikasi karena tahu bahwa hak-haknya terlindungi oleh hukum yang kuat dan jelas.

Meskipun harmonisasi antara UU ITE dan peraturan lainnya sangat penting, proses ini tentu tidak mudah. Peraturan yang sudah ada harus diperbarui dan disesuaikan dengan perkembangan teknologi yang pesat. Selain itu, implementasi dari peraturan yang sudah disesuaikan juga memerlukan dukungan dari berbagai pihak, baik pemerintah, sektor swasta, maupun masyarakat. Penyedia platform digital, misalnya, perlu dilibatkan dalam proses harmonisasi ini agar memahami kewajiban dan tanggung jawab dalam menjaga keamanan data pribadi dan transaksi elektronik. Selain itu, masyarakat juga perlu diberikan pemahaman yang lebih baik mengenai pentingnya perlindungan data pribadi dan bagaimana dapat menjaga keamanan datanya.

Indonesia perlu terus mengupayakan harmonisasi peraturan yang ada untuk menciptakan ekosistem digital yang aman, adil, dan terpercaya. Dengan adanya kerangka hukum yang kuat dan harmonis, Indonesia dapat lebih siap menghadapi tantangan kejahatan siber yang semakin kompleks. Harmonisasi ini tidak hanya akan menguntungkan masyarakat dan sektor swasta, tetapi juga meningkatkan citra Indonesia di mata dunia sebagai negara yang peduli terhadap perlindungan data pribadi dan keamanan digital. Dengan langkah-langkah yang tepat, Indonesia dapat menjadi contoh bagi negara lain dalam hal pengaturan dan penegakan hukum terkait dengan teknologi informasi dan komunikasi.

B. Pengembangan Teknologi Forensik Digital

1. Kemajuan dalam Teknologi Forensik Digital untuk Penanganan Kejahatan Siber

Seiring dengan pesatnya perkembangan ancaman di dunia maya, teknologi forensik digital telah berkembang pesat sebagai salah satu alat utama dalam penanganan tindak pidana siber. Forensik digital sendiri merujuk pada proses pengumpulan, analisis, dan presentasi bukti digital yang dapat digunakan dalam proses hukum, termasuk dalam investigasi kejahatan siber. Di Indonesia, meskipun masih dalam tahap pengembangan, teknologi forensik digital mulai berperan yang semakin penting dalam mendukung upaya penegakan hukum. Kemajuan teknologi ini memberikan harapan baru dalam mengungkap pelaku kejahatan siber yang sering kali sulit diidentifikasi dan ditangkap karena metode penyembunyian jejak digital yang digunakan oleh para pelaku.

Salah satu kemajuan terbesar dalam teknologi forensik digital adalah munculnya perangkat lunak yang semakin canggih yang dapat digunakan untuk memulihkan data yang terhapus atau dienkripsi. Salah satu contoh perangkat yang banyak digunakan adalah EnCase, yang memungkinkan penyidik untuk melakukan pemulihan data dari perangkat yang telah dihapus, bahkan jika data tersebut telah sengaja dihancurkan atau disembunyikan. FTK Imager juga merupakan alat yang sering digunakan dalam dunia forensik digital untuk membuat salinan bukti dari perangkat keras tanpa merusak data yang ada. Teknologi seperti ini sangat penting, mengingat pelaku kejahatan siber sering kali menggunakan berbagai cara untuk menghapus jejaknya, seperti dengan menghapus data, mengenkripsi informasi, atau menggunakan perangkat lunak yang dapat menghilangkan bukti dengan cepat. Dengan perangkat ini, penyidik bisa mendapatkan kembali bukti yang hilang dan mengungkapkan tindakan kejahatan yang sebelumnya tersembunyi.

Perkembangan teknologi *cloud forensics* semakin menjadi solusi yang efektif untuk mengatasi tantangan dalam mengumpulkan bukti yang disimpan di server cloud. Seiring dengan semakin banyaknya data yang dipindahkan dan disimpan di cloud, penyidik kini dihadapkan pada tantangan baru dalam hal aksesibilitas dan legalitas pengambilan data. Dengan adanya alat-alat canggih, penyidik dapat melakukan imaging terhadap data yang disimpan di platform cloud tanpa harus mengakses perangkat fisik secara langsung. Hal ini memungkinkan untuk

mengakses informasi yang relevan meskipun data tersebut disimpan di luar negara, yang sering kali menimbulkan permasalahan terkait dengan yurisdiksi hukum. Salah satu keuntungan utama dari teknologi cloud forensics adalah kemampuannya untuk mengakses dan menganalisis data tanpa melanggar peraturan internasional atau kebijakan perlindungan data yang berlaku di negara lain. Ini sangat penting mengingat banyak serangan siber, seperti serangan *ransomware* atau peretasan, yang melibatkan penyimpanan data di luar wilayah hukum suatu negara.

Penggunaan teknologi forensik digital juga sangat relevan dalam mengatasi masalah yang muncul dari perangkat mobile, seperti ponsel dan tablet, yang kini semakin sering menjadi sasaran utama dalam kejahatan siber. Keberadaan alat seperti Cellebrite memungkinkan penyidik untuk mengekstraksi dan menganalisis data dari perangkat mobile yang terkunci atau dienkripsi, yang biasanya menjadi tantangan besar dalam penyelidikan kejahatan siber. Banyak sekali jenis kejahatan siber yang melibatkan perangkat mobile, mulai dari penipuan online, perundungan siber (*cyberbullying*), hingga serangan *ransomware* yang dilakukan melalui aplikasi atau perangkat mobile. Dengan alat seperti Cellebrite, penyidik bisa membuka kunci perangkat dan mengakses bukti yang tersembunyi di dalamnya, termasuk pesan teks, log panggilan, riwayat lokasi, dan bahkan data aplikasi yang digunakan oleh pelaku untuk melakukan kejahatan.

Perkembangan teknologi forensik digital juga mencakup peningkatan dalam hal pemrosesan data dalam jumlah besar, atau yang biasa disebut dengan analisis big data. Dalam kejahatan siber, sering kali bukti yang ditemukan tersebar di berbagai tempat dan dalam format yang berbeda-beda, seperti file log, riwayat komunikasi, serta data transaksi. Untuk menangani hal ini, teknologi analisis big data memungkinkan penyidik untuk mengelola dan menganalisis jumlah data yang sangat besar dalam waktu singkat. Alat seperti X1 Social Discovery, yang dapat digunakan untuk menelusuri dan menganalisis data dari platform media sosial, membantu penyidik dalam menemukan pola dan hubungan antar data yang sebelumnya tidak terlihat. Teknologi ini mempermudah identifikasi pelaku kejahatan yang mungkin tidak diketahui sebelumnya atau untuk mengungkap jaringan pelaku kejahatan yang tersebar di berbagai wilayah.

Kemajuan lainnya dalam teknologi forensik digital adalah kemampuan untuk melakukan analisis forensik terhadap perangkat yang digunakan dalam serangan siber yang lebih kompleks, seperti botnet dan serangan DDoS (*Distributed Denial of Service*). Perangkat forensik digital kini semakin canggih dalam melacak pola serangan dan memetakan jaringan perangkat yang terlibat dalam serangan tersebut. Dengan menggunakan teknologi seperti analisis packet capture (PCAP), penyidik dapat menangkap dan menganalisis data yang lewat di jaringan selama serangan DDoS, yang memungkinkan untuk mengidentifikasi sumber serangan dan mengejar pelaku kejahatan siber. Teknologi ini sangat berguna dalam menangani serangan yang sifatnya terdistribusi dan sulit untuk dilacak secara tradisional.

Teknologi forensik digital juga telah mengembangkan kemampuannya dalam hal analisis metadata, yang sering kali menjadi petunjuk penting dalam penyelidikan kejahatan siber. Metadata dapat memberikan informasi tentang asal-usul file, waktu pembuatan, dan perubahan yang dilakukan pada file tersebut. Dalam beberapa kasus, pelaku kejahatan siber seringkali lupa atau tidak sengaja meninggalkan jejak yang bisa ditelusuri melalui metadata, yang akhirnya dapat digunakan untuk membongkar kasus. Dengan menggunakan perangkat forensik digital yang canggih, penyidik dapat menggali lebih dalam dan menemukan bukti yang mungkin terlewatkan pada analisis awal.

Kemajuan dalam teknologi forensik digital juga mempengaruhi cara penyidik melakukan analisis terhadap sistem yang lebih besar, seperti jaringan komputer dan server. Dalam hal ini, teknologi forensik kini semakin mampu menganalisis lalu lintas jaringan dan memetakan serangan yang dilakukan, bahkan dari pelaku yang tersembunyi di balik berbagai lapisan keamanan. Alat seperti Wireshark dan Network Miner memungkinkan penyidik untuk menganalisis paket data yang dikirimkan melalui jaringan dan mendapatkan informasi yang berguna dalam melacak serangan dan mengidentifikasi pelaku. Kemampuan ini memungkinkan penyidik untuk mengungkap serangan yang sebelumnya mungkin sulit untuk diidentifikasi, seperti serangan man-in-the-middle atau serangan berbasis *malware* yang menyebar melalui jaringan.

Dengan berkembangnya teknologi forensik digital, tantangan yang dihadapi oleh penyidik dalam mengungkap kejahatan siber semakin dapat diatasi. Namun, penggunaan teknologi ini juga memerlukan peningkatan dalam hal pelatihan dan sumber daya manusia

yang terampil di bidang forensik digital. Penyidik dan aparat penegak hukum perlu memiliki keterampilan yang cukup untuk menggunakan perangkat dan teknik terbaru dalam teknologi forensik agar dapat mengungkap bukti yang relevan dengan lebih efektif. Di Indonesia, meskipun ada kemajuan dalam hal teknologi, masih terdapat kebutuhan besar untuk meningkatkan kapasitas dan keahlian tenaga kerja di bidang ini agar dapat menangani kejahatan siber dengan lebih baik.

2. Tantangan dalam Pengembangan dan Implementasi Teknologi Forensik Digital di Indonesia

Pengembangan dan implementasi teknologi forensik digital di Indonesia menghadapi berbagai tantangan yang mempengaruhi efektivitas dan efisiensi dalam penanganan kejahatan siber. Salah satu tantangan terbesar adalah kurangnya sumber daya manusia yang terlatih dalam bidang forensik digital. Meskipun kemajuan dalam teknologi forensik digital telah pesat, peran sumber daya manusia yang kompeten tetap sangat penting untuk memastikan bahwa bukti digital yang ditemukan dapat dipertanggungjawabkan di pengadilan. Di Indonesia, penyidik siber yang memiliki keterampilan teknis yang cukup untuk menggunakan perangkat forensik yang canggih masih terbatas. Oleh karena itu, untuk memastikan keberhasilan dalam investigasi tindak pidana siber, perlu ada upaya yang lebih besar dalam meningkatkan kualitas pelatihan dan kompetensi bagi penyidik forensik digital, baik melalui pendidikan formal maupun program pelatihan yang terintegrasi dengan perkembangan teknologi terbaru. Tanpa peningkatan kapasitas penyidik, teknologi yang ada pun akan sulit untuk dimanfaatkan secara optimal dalam mendukung proses penegakan hukum.

Tantangan berikutnya yang cukup signifikan adalah keterbatasan dana dan kurangnya infrastruktur yang memadai untuk mendukung implementasi teknologi forensik digital. Alat dan perangkat forensik digital yang canggih, seperti perangkat lunak untuk pemulihan data atau analisis cloud, sering kali memerlukan investasi yang cukup besar. Banyak lembaga penegak hukum di Indonesia, terutama di daerah-daerah tertentu, mungkin tidak memiliki anggaran yang cukup untuk membeli perangkat-perangkat ini. Keterbatasan anggaran ini dapat menyebabkan ketertinggalan dalam pemanfaatan teknologi terbaru, yang pada akhirnya akan menghambat penyelidikan kejahatan siber yang semakin kompleks. Oleh karena itu, pemerintah dan lembaga terkait

perlu mengalokasikan lebih banyak dana untuk pengadaan peralatan forensik digital yang modern, serta mendukung pengembangan infrastruktur teknologi informasi yang dapat mendukung kelancaran investigasi siber di seluruh wilayah Indonesia. Tanpa infrastruktur yang memadai, upaya penanganan kejahatan siber akan terbatas dan kurang efektif.

Aspek hukum dan etika juga merupakan tantangan besar dalam pengembangan teknologi forensik digital di Indonesia. Pengumpulan bukti digital memerlukan perhatian khusus terhadap hak privasi individu. Dalam banyak kasus, penyidik harus mengambil data dari perangkat pribadi atau platform digital yang berisi informasi sensitif. Oleh karena itu, proses penyitaan dan pengambilan bukti harus dilakukan dengan sangat hati-hati untuk memastikan bahwa tidak ada pelanggaran terhadap hak privasi individu. Penyidik harus mengikuti prosedur hukum yang ketat, termasuk memperoleh izin dari otoritas yang berwenang, sebelum melakukan pengambilan atau penyitaan data dari perangkat atau server digital. Jika prosedur ini tidak dipatuhi, bukti yang ditemukan bisa dianggap tidak sah dan tidak dapat digunakan di pengadilan. Ini tentu dapat mempengaruhi hasil investigasi dan memperlambat proses hukum. Selain itu, bukti digital harus dijaga dengan sangat hati-hati agar tidak rusak atau terkontaminasi selama proses pengumpulan dan analisis. Hal ini memerlukan keahlian dan perhatian ekstra dari penyidik, serta prosedur yang baku untuk menjaga integritas bukti digital.

Perbedaan peraturan internasional terkait forensik digital menjadi tantangan tambahan dalam penyelidikan kejahatan siber di Indonesia. Banyak data yang relevan untuk penyidikan bisa saja disimpan di server luar negeri, yang berarti bahwa penyidik Indonesia harus berkoordinasi dengan otoritas negara lain untuk mengakses data tersebut. Namun, peraturan mengenai perlindungan data pribadi dan hak privasi antarnegara sering kali berbeda. Beberapa negara mungkin memiliki kebijakan yang lebih ketat terkait dengan pengambilan data pribadi, sementara negara lain lebih permisif. Ketidaksesuaian regulasi antarnegara ini dapat memperlambat proses permintaan data, yang pada akhirnya akan menghambat penyelidikan dan penuntutan kasus-kasus kejahatan siber yang melibatkan pelaku atau data di luar negeri. Hal ini mempertegas perlunya adanya kerjasama internasional yang lebih erat dalam penanganan kejahatan siber, serta harmonisasi peraturan

antarnegara untuk mempermudah proses pengambilan data secara sah dan efisien.

Meskipun teknologi forensik digital di Indonesia telah mengalami kemajuan, masih ada kebutuhan mendesak untuk meningkatkan infrastruktur dan sumber daya manusia dalam bidang ini. Upaya pemerintah untuk memperkuat kerjasama internasional dalam menangani kejahatan siber sangat diperlukan. Penyidik siber Indonesia perlu diberikan pelatihan yang lebih mendalam dan terstruktur mengenai teknologi forensik digital yang terus berkembang. Selain itu, kerjasama dengan lembaga internasional dapat membantu Indonesia mengatasi tantangan terkait pengambilan data internasional dan perbedaan regulasi yang ada. Sebagai contoh, Indonesia dapat mengadopsi perjanjian internasional terkait pertukaran data dan bukti digital yang memungkinkan akses data lintas batas tanpa melanggar hak privasi individu atau peraturan yang berlaku di masing-masing negara.

Untuk mengatasi masalah keterbatasan dana, pemerintah dan lembaga penegak hukum di Indonesia perlu mencari cara untuk mendapatkan sumber daya tambahan. Salah satu cara yang bisa dilakukan adalah melalui kemitraan dengan sektor swasta atau melalui kerjasama dengan lembaga internasional yang menyediakan bantuan teknis dan finansial. Selain itu, penting bagi Indonesia untuk memprioritaskan pengadaan teknologi forensik digital yang sesuai dengan kebutuhan dan tantangan yang dihadapi dalam penanganan kejahatan siber. Dengan perencanaan yang matang dan pengalokasian dana yang tepat, Indonesia dapat meningkatkan kapasitas teknologinya dalam menangani kejahatan siber yang semakin kompleks.

Pemerintah juga perlu memperhatikan kebutuhan akan pembaruan regulasi yang dapat mendukung pengembangan dan implementasi teknologi forensik digital. Pembaruan peraturan hukum yang mengatur penggunaan bukti digital di pengadilan juga penting untuk memastikan bahwa bukti yang ditemukan dapat diterima dan digunakan secara sah. Peraturan yang jelas tentang prosedur pengumpulan bukti digital, pengelolaan data pribadi, serta hak dan kewajiban para pihak yang terlibat dalam penyelidikan akan membantu meningkatkan kepercayaan masyarakat terhadap sistem peradilan digital. Penyusunan peraturan ini harus dilakukan dengan melibatkan berbagai pihak terkait, termasuk aparat penegak hukum, regulator, dan pakar teknologi informasi.

C. Peran *Artificial Intelligence* dalam Deteksi Kejahatan Siber

1. Penggunaan *Artificial Intelligence* dalam Mendeteksi dan Mencegah Kejahatan Siber

Artificial Intelligence (AI) telah muncul sebagai teknologi yang sangat berperan penting dalam deteksi dan pencegahan kejahatan siber. Dengan kemampuannya dalam memproses dan menganalisis data dalam jumlah besar, AI dapat mengidentifikasi pola-pola yang mencurigakan serta mendeteksi anomali yang mungkin menunjukkan adanya ancaman kejahatan siber. Kejahatan siber yang semakin kompleks dan berkembang pesat menuntut adanya sistem yang lebih canggih untuk mendeteksi ancaman sebelum benar-benar menimbulkan kerusakan. AI menawarkan solusi yang lebih efisien dan cepat dalam hal ini, dengan menggunakan berbagai teknik, seperti *machine learning* (ML), *deep learning*, dan *natural language processing* (NLP). Teknologi-teknologi ini memungkinkan sistem untuk belajar dan beradaptasi dengan cepat terhadap pola dan tren baru yang muncul di dunia maya, sehingga dapat memitigasi potensi ancaman yang lebih beragam.

Salah satu aplikasi paling penting dari AI dalam deteksi kejahatan siber adalah melalui penggunaan sistem deteksi intrusi berbasis AI. Sistem ini memanfaatkan algoritma machine learning untuk menganalisis lalu lintas data secara terus-menerus, serta mendeteksi aktivitas yang tidak biasa atau mencurigakan. Dalam hal ini, AI memiliki keunggulan dibandingkan dengan sistem tradisional yang hanya mengandalkan aturan statis. Dengan kemampuan untuk mempelajari pola-pola yang ada, AI dapat mengidentifikasi potensi serangan yang mungkin belum pernah tercatat sebelumnya. Misalnya, dalam serangan *phishing* yang semakin canggih, AI dapat menganalisis pola komunikasi dalam email atau pesan teks yang diterima oleh pengguna, memeriksa elemen-elemen seperti URL, metadata, dan tanda-tanda lain yang menunjukkan adanya upaya penipuan. Hal ini memungkinkan sistem untuk mendeteksi dan memperingatkan pengguna atau pihak yang berwenang sebelum serangan tersebut berhasil.

Teknologi *natural language processing* (NLP) yang merupakan bagian dari AI juga sangat berguna dalam mendeteksi jenis kejahatan siber berbasis teks. Salah satu contohnya adalah dalam memerangi penyebaran *hoaks* dan *hate speech* di media sosial. NLP memungkinkan komputer untuk memproses dan memahami bahasa manusia, sehingga

dapat digunakan untuk menganalisis konten teks yang beredar di platform digital. Algoritma NLP dapat mendeteksi teks yang mengandung kebencian, provokasi, atau informasi yang salah, yang sering kali digunakan untuk merusak reputasi individu, kelompok, atau bahkan negara. Dengan mendeteksi pesan-pesan semacam ini secara otomatis, AI dapat memberikan peringatan dini kepada otoritas terkait, memungkinkan untuk bertindak cepat sebelum dampaknya meluas. Penggunaan NLP dalam konteks ini sangat penting karena dapat mempercepat respons terhadap ancaman yang sangat cepat berkembang di dunia maya, yang kadang-kadang sulit untuk terdeteksi oleh manusia.

AI juga berperan dalam mempercepat respons terhadap ancaman yang ada. Sebagai contoh, dalam sistem keamanan berbasis AI, kemampuan untuk mendeteksi dan menanggulangi ancaman secara otomatis sangat membantu dalam mengurangi waktu respons yang biasanya sangat lambat jika hanya mengandalkan intervensi manusia. Serangan siber, seperti *ransomware* atau DDoS, sering kali memanfaatkan celah keamanan yang dapat dieksploitasi dalam waktu singkat. Dengan kemampuan untuk bekerja secara real-time, AI dapat segera mengidentifikasi ancaman dan bahkan mengambil langkah-langkah untuk menghentikan serangan sebelum dapat menyebabkan kerusakan lebih lanjut. Misalnya, AI dapat langsung memblokir IP yang terindikasi melakukan aktivitas mencurigakan atau mengalihkan lalu lintas data untuk menghindari serangan DDoS yang dapat membuat sistem menjadi tidak tersedia.

Kemampuan AI untuk memproses data dalam jumlah besar dan dalam waktu yang sangat singkat juga menjadi salah satu keunggulannya dalam mendeteksi serangan yang kompleks. Banyak serangan siber yang melibatkan sejumlah besar data dan trafik yang sulit dianalisis oleh manusia. Misalnya, serangan DDoS atau penipuan berbasis bot sering kali tersembunyi di balik lalu lintas data yang sangat besar. Dengan teknologi AI, sistem dapat menganalisis setiap paket data dan mendeteksi pola-pola yang mencurigakan yang dapat menunjukkan adanya serangan. Selain itu, AI juga dapat mengenali tanda-tanda serangan yang mungkin terlihat biasa pada pandangan pertama, namun sebenarnya menyembunyikan ancaman yang lebih besar. Kemampuan untuk mempelajari pola-pola baru dan beradaptasi dengan perubahan terus-menerus di dunia maya membuat AI menjadi alat yang sangat efektif untuk menjaga keamanan dunia maya.

Pada beberapa tahun terakhir, AI juga digunakan untuk mengidentifikasi dan mencegah serangan yang melibatkan perangkat *Internet of Things* (IoT). Banyak perangkat IoT yang terhubung ke internet memiliki celah keamanan yang dapat dimanfaatkan oleh para penjahat siber untuk melakukan serangan. AI dapat memonitor perangkat IoT dalam jaringan dan mendeteksi perilaku yang tidak biasa yang dapat mengindikasikan adanya serangan. Misalnya, jika sebuah perangkat IoT mulai mengirimkan data yang tidak sesuai dengan pola normalnya, sistem berbasis AI dapat segera memberi tahu administrator untuk melakukan tindakan yang diperlukan. Hal ini sangat penting, mengingat semakin banyaknya perangkat yang terhubung ke internet dan semakin kompleksnya ancaman yang dapat timbul dari perangkat-perangkat tersebut.

AI juga digunakan dalam pencegahan serangan siber dengan cara yang lebih proaktif. Salah satu contoh penerapannya adalah dalam sistem keamanan berbasis prediksi. Dengan menggunakan teknik machine learning, AI dapat menganalisis data historis tentang serangan siber dan memprediksi potensi ancaman di masa depan. Sebagai contoh, jika sistem mendeteksi bahwa serangan jenis tertentu sering kali terjadi pada waktu dan tempat tertentu, AI dapat memberikan peringatan kepada pihak yang berwenang atau bahkan mengambil langkah pencegahan untuk mengurangi risiko serangan. Dengan sistem prediksi berbasis AI, organisasi dapat lebih siap dalam menghadapi potensi ancaman sebelum serangan itu benar-benar terjadi.

Keunggulan lainnya dari AI dalam deteksi dan pencegahan kejahatan siber adalah kemampuannya untuk bekerja secara terus-menerus tanpa adanya kelelahan. Manusia memiliki keterbatasan dalam hal waktu dan konsentrasi, yang dapat mempengaruhi kemampuannya dalam mendeteksi ancaman yang terjadi sepanjang waktu. Sebaliknya, sistem berbasis AI dapat bekerja 24 jam sehari, 7 hari seminggu, tanpa terganggu oleh faktor-faktor eksternal. Hal ini sangat penting mengingat kejahatan siber sering kali terjadi pada waktu yang tidak terduga dan dapat sangat merusak jika tidak segera ditangani. Dengan sistem AI, perusahaan dan lembaga lainnya dapat memiliki lapisan perlindungan yang lebih konsisten dan terus-menerus terhadap ancaman dunia maya.

Penggunaan AI dalam deteksi dan pencegahan kejahatan siber juga tidak terbatas hanya pada identifikasi ancaman yang sudah ada. AI juga dapat digunakan untuk meningkatkan strategi pertahanan siber

secara keseluruhan dengan membantu merancang sistem keamanan yang lebih canggih. Dengan menganalisis data dan tren serangan yang ada, AI dapat memberikan wawasan yang lebih dalam tentang bagaimana serangan dilakukan dan memberikan rekomendasi tentang langkah-langkah yang dapat diambil untuk memperbaiki celah keamanan. Hal ini memungkinkan organisasi untuk lebih siap menghadapi serangan siber yang mungkin belum terdeteksi atau dipahami sebelumnya, serta membantu memperbaiki kebijakan keamanan yang ada untuk meningkatkan perlindungan.

Penerapan AI dalam deteksi dan pencegahan kejahatan siber menawarkan berbagai manfaat yang signifikan, mulai dari kemampuan untuk mendeteksi ancaman yang sangat kompleks hingga mempercepat respons terhadap serangan yang sedang berlangsung. Dengan kemampuannya untuk memproses data dalam jumlah besar dan dalam waktu yang sangat singkat, AI menjadi alat yang sangat berharga dalam dunia yang semakin terhubung secara digital ini. Seiring dengan semakin kompleksnya kejahatan siber, penggunaan AI akan menjadi semakin penting dalam menjaga dunia maya tetap aman dan terjaga.

2. Tantangan dalam Penggunaan AI dalam Deteksi Kejahatan Siber

Meskipun *Artificial Intelligence* (AI) memberikan banyak manfaat dalam mendeteksi kejahatan siber, penggunaannya dalam dunia keamanan siber juga dihadapkan pada sejumlah tantangan yang tidak dapat diabaikan. Salah satu tantangan utama yang dihadapi oleh sistem AI adalah akurasi dalam mendeteksi ancaman. AI sangat bergantung pada data yang digunakan untuk melatih modelnya, sehingga jika data yang dimasukkan ke dalam sistem tidak cukup representatif atau lengkap, maka hasil deteksi yang diberikan oleh sistem dapat menjadi kurang akurat atau bahkan salah. Sebagai contoh, jika dataset yang digunakan untuk melatih model AI tidak mencakup variasi yang cukup dalam jenis serangan siber atau tidak mencerminkan ancaman yang berkembang, AI mungkin akan gagal mengenali ancaman baru atau memberikan peringatan palsu. Dalam hal ini, kualitas data sangat penting, dan data yang bias atau tidak lengkap bisa mengarah pada deteksi yang tidak optimal, bahkan ketika sistem AI sendiri telah diterapkan dengan teknologi yang canggih.

Tantangan lain yang signifikan adalah kemampuan AI untuk beradaptasi dengan ancaman yang terus berkembang. Kejahatan siber adalah fenomena yang dinamis, di mana para pelaku terus berinovasi dan menciptakan metode serangan yang semakin canggih. Ini menuntut sistem AI yang digunakan untuk mendeteksi ancaman agar dapat terus diperbarui dan dilatih dengan dataset terbaru yang mencerminkan ancaman baru tersebut. Tanpa adanya pembaruan dan pelatihan model yang terus-menerus, sistem AI dapat menjadi usang dan tidak efektif dalam menghadapi ancaman siber yang terus berkembang. Hal ini membutuhkan investasi besar dalam sumber daya manusia dan waktu, karena melatih dan menguji model AI dengan dataset yang baru memerlukan keterlibatan banyak ahli dan waktu yang cukup lama. Ditambah lagi, serangan siber dapat terjadi dengan sangat cepat dan tanpa pemberitahuan, yang berarti bahwa sistem AI harus mampu memberikan respons real-time yang cepat terhadap ancaman yang muncul.

Keamanan dari sistem AI itu sendiri juga merupakan masalah yang tidak dapat dianggap remeh. Kejahatan siber tidak hanya menargetkan sistem yang digunakan untuk mendeteksi ancaman, tetapi juga dapat mengeksploitasi kelemahan dalam algoritma yang digunakan dalam sistem AI. Salah satu contoh dari hal ini adalah serangan adversarial machine learning, di mana penjahat siber dapat memanipulasi data input yang diberikan kepada model AI untuk membuat model tersebut gagal mendeteksi ancaman dengan benar. Dalam serangan semacam ini, pelaku sengaja menyuntikkan data yang dirancang untuk mengecoh sistem AI dan mengarahkan deteksinya ke arah yang salah. Akibatnya, AI yang sebelumnya efektif dalam mendeteksi ancaman bisa menjadi rentan terhadap serangan yang dimodifikasi sedemikian rupa agar bisa melewati deteksi. Oleh karena itu, menjaga integritas dan keamanan sistem AI itu sendiri menjadi tantangan yang besar, dan perlu dilakukan upaya untuk meningkatkan ketahanan sistem terhadap serangan semacam ini agar tetap efektif dalam menghadapi ancaman.

Salah satu tantangan signifikan lainnya dalam penggunaan AI dalam deteksi kejahatan siber adalah masalah etika dan privasi. Penggunaan teknologi AI yang dapat memantau dan menganalisis data pengguna secara menyeluruh menimbulkan kekhawatiran terkait hak privasi individu. Dalam beberapa kasus, AI digunakan untuk memantau

aktivitas online atau bahkan komunikasi pribadi pengguna, yang menimbulkan pertanyaan etis mengenai sejauh mana teknologi ini boleh digunakan tanpa melanggar hak-hak dasar individu. Misalnya, dalam upaya mendeteksi ancaman yang berasal dari komunikasi online, seperti *hoaks* atau penipuan, AI mungkin perlu menganalisis isi pesan yang bersifat pribadi. Penggunaan teknologi ini dengan cara yang terlalu invasif bisa melanggar privasi pengguna, sehingga penting untuk memastikan bahwa penggunaannya tetap mematuhi prinsip-prinsip etika yang berlaku, termasuk perlindungan privasi yang tegas dan penghormatan terhadap hak asasi manusia.

Penggunaan AI juga memunculkan masalah terkait dengan transparansi dan akuntabilitas. Meskipun AI dapat menawarkan solusi yang sangat efektif dalam mendeteksi kejahatan siber, keputusan yang diambil oleh algoritma AI tidak selalu mudah dipahami oleh manusia. Dalam banyak kasus, keputusan yang diambil oleh sistem AI dibuat berdasarkan pola yang diidentifikasi dalam data besar yang mungkin tidak dapat dijelaskan dengan cara yang mudah dimengerti oleh orang awam. Hal ini menimbulkan masalah terkait dengan transparansi, karena sulit bagi pihak yang terlibat, seperti lembaga penegak hukum atau pengguna, untuk mengetahui mengapa suatu keputusan atau deteksi tertentu dilakukan oleh sistem. Ketidakjelasan ini dapat mengurangi kepercayaan terhadap penggunaan AI dalam deteksi kejahatan siber, serta mempersulit proses audit dan verifikasi yang penting untuk memastikan bahwa keputusan yang diambil oleh AI benar-benar sah dan adil.

Masalah lain yang dihadapi oleh penggunaan AI dalam deteksi kejahatan siber adalah ketergantungan pada infrastruktur teknologi yang memadai. Agar sistem AI dapat bekerja secara optimal dalam mendeteksi ancaman, dibutuhkan infrastruktur yang kuat, termasuk perangkat keras yang cepat dan canggih, serta kapasitas penyimpanan data yang besar. Bagi banyak organisasi, terutama yang memiliki sumber daya terbatas, hal ini bisa menjadi kendala yang signifikan. Tanpa infrastruktur yang memadai, sistem AI tidak akan dapat memproses data dalam jumlah besar dengan cepat dan efisien. Oleh karena itu, pengembangan dan implementasi teknologi AI untuk deteksi kejahatan siber membutuhkan investasi yang tidak hanya melibatkan pengembangan perangkat lunak, tetapi juga pembaruan infrastruktur

teknologi yang mendukung sistem tersebut. Ini tentu menjadi tantangan bagi banyak lembaga yang bekerja dengan anggaran terbatas.

Masalah ketidakpastian hukum juga menjadi tantangan besar dalam penerapan AI dalam keamanan siber. Banyak negara, termasuk Indonesia, masih dalam tahap pengembangan regulasi yang berkaitan dengan penggunaan teknologi AI dalam bidang keamanan siber. Tanpa adanya regulasi yang jelas dan tegas mengenai penggunaan AI untuk deteksi kejahatan siber, akan sulit untuk menetapkan standar yang memadai tentang cara teknologi ini seharusnya diterapkan dalam konteks yang sah dan etis. Tanpa regulasi yang memadai, terdapat risiko bahwa penggunaan AI bisa disalahgunakan, baik untuk tujuan yang merugikan individu maupun untuk memperburuk masalah privasi atau hak asasi manusia. Oleh karena itu, penting bagi pemerintah dan pihak berwenang untuk mengembangkan kebijakan dan regulasi yang jelas terkait penggunaan AI dalam keamanan siber, yang tidak hanya melindungi keamanan tetapi juga menjunjung tinggi hak-hak dasar individu.

Kesenjangan dalam keterampilan dan pengetahuan di kalangan profesional keamanan siber juga menjadi masalah. Meskipun teknologi AI sangat bermanfaat, untuk dapat menggunakannya dengan efektif, diperlukan keahlian dan pelatihan khusus yang tidak semua profesional memiliki. Banyak perusahaan dan lembaga penegak hukum yang masih kekurangan tenaga ahli yang terlatih dalam bidang AI dan machine learning, yang membatasi kemampuan dalam memanfaatkan potensi teknologi ini secara maksimal. Tanpa adanya pelatihan yang memadai dan peningkatan keterampilan dalam penggunaan AI, sistem deteksi yang canggih ini bisa kehilangan efektivitasnya dalam menghadapi ancaman yang semakin kompleks.

D. Upaya Pencegahan Melalui Literasi Digital

1. Peran Literasi Digital dalam Meningkatkan Kesadaran Keamanan Siber

Literasi digital memiliki peran yang sangat penting dalam meningkatkan kesadaran dan pemahaman masyarakat tentang ancaman dan risiko yang ada di dunia maya. Pada dasarnya, literasi digital mencakup keterampilan dan pengetahuan yang diperlukan untuk mengakses, mengevaluasi, dan menggunakan informasi secara efektif di

dunia digital. Namun, lebih dari itu, literasi digital juga menyentuh aspek penting lainnya, yaitu pemahaman tentang bagaimana individu dan organisasi dapat melindungi dirinya dari ancaman kejahatan siber yang semakin canggih. Dengan meningkatnya penggunaan teknologi digital, terutama internet, ancaman yang datang dari dunia maya pun semakin beragam, dari pencurian identitas hingga serangan siber yang lebih kompleks. Oleh karena itu, literasi digital tidak hanya perlu diartikan sebagai kemampuan untuk menggunakan teknologi, tetapi juga sebagai kemampuan untuk mengenali dan merespons ancaman yang ada.

Pendidikan literasi digital bertujuan untuk memberikan pemahaman yang mendalam kepada masyarakat mengenai pentingnya menjaga keamanan pribadinya di dunia maya. Dalam hal ini, aspek pertama yang harus diperhatikan adalah pemberian pengetahuan tentang praktik dasar keamanan siber yang seharusnya dilakukan oleh setiap individu. Salah satu langkah pertama dalam menjaga keamanan pribadi adalah dengan menggunakan kata sandi yang kuat dan unik untuk setiap akun online. Penggunaan kata sandi yang mudah ditebak atau penggunaan kata sandi yang sama di berbagai akun online membuka celah bagi pelaku kejahatan siber untuk mengeksploitasi akun-akun tersebut. Selain itu, penting untuk mengajarkan kepada masyarakat cara mengenali serangan *phishing* yang sering kali menjadi taktik utama para penjahat siber. *Phishing* bisa datang dalam berbagai bentuk, mulai dari email palsu yang meminta informasi pribadi hingga situs web yang tampak seperti situs resmi namun sebenarnya dirancang untuk mencuri data pengguna. Masyarakat yang teredukasi dengan baik mengenai cara mengenali ancaman semacam ini akan lebih siap untuk menghindarinya.

Literasi digital juga mengajarkan kepada individu bagaimana cara menjaga dan melindungi data pribadinya agar tidak jatuh ke tangan yang salah. Banyak informasi pribadi yang kita berikan secara online, mulai dari data bank hingga informasi pribadi di media sosial. Jika data-data ini jatuh ke tangan yang tidak bertanggung jawab, bisa berakibat sangat merugikan, baik secara finansial maupun dalam hal reputasi. Oleh karena itu, penting untuk mengedukasi masyarakat tentang pentingnya menjaga data pribadi dengan tidak membagikan informasi sensitif kepada sembarang pihak dan menggunakan pengaturan privasi yang tepat di media sosial atau platform lainnya. Selain itu, pengguna juga perlu diberi pemahaman tentang pentingnya pembaruan perangkat lunak secara teratur dan penggunaan perangkat lunak antivirus untuk

melindungi perangkat dari ancaman *malware* atau virus yang dapat merusak sistem atau mencuri data pribadi.

Literasi digital juga memiliki dampak besar terhadap tingkat keamanan siber di dalam suatu organisasi. Bagi perusahaan atau lembaga yang memiliki data sensitif, penting untuk mengedukasi karyawan mengenai kebijakan keamanan siber yang harus diterapkan. Penggunaan teknologi yang canggih tanpa pemahaman yang tepat mengenai risiko yang dapat muncul dapat membuka peluang bagi kebocoran data atau serangan peretasan. Misalnya, jika seorang karyawan tidak mengetahui bahwa mengklik tautan yang mencurigakan dalam email dapat menginstal *malware* di perangkatnya, maka perangkat tersebut bisa saja digunakan untuk menyerang sistem perusahaan. Oleh karena itu, penting bagi perusahaan untuk mengadakan pelatihan rutin yang mengajarkan karyawan tentang ancaman yang ada, serta cara-cara yang dapat dilakukan untuk meminimalisir risiko tersebut, seperti tidak mengunduh file dari sumber yang tidak dikenal atau tidak membuka email yang mencurigakan.

Peningkatan literasi digital dalam sebuah organisasi dapat membantu menciptakan budaya keamanan yang lebih baik. Ketika semua karyawan memahami pentingnya menjaga keamanan siber, akan lebih berhati-hati dan lebih cenderung mengikuti prosedur keamanan yang sudah ditetapkan oleh perusahaan. Budaya ini sangat penting dalam mencegah terjadinya insiden yang berhubungan dengan keamanan data, yang dapat mengakibatkan kerugian finansial yang signifikan dan merusak reputasi perusahaan. Perusahaan yang memiliki tingkat literasi digital yang tinggi di kalangan karyawannya akan lebih siap untuk mengidentifikasi dan mencegah potensi ancaman yang mungkin muncul.

Kampanye kesadaran tentang pentingnya literasi digital harus dilakukan secara menyeluruh dan melibatkan semua lapisan masyarakat. Banyak orang yang mungkin tidak menyadari risiko yang dihadapi saat beraktivitas di dunia maya, terutama kelompok yang lebih tua atau yang belum terlalu akrab dengan teknologi digital. Kampanye yang dilakukan oleh pemerintah, lembaga pendidikan, atau organisasi non-profit bisa menjadi sarana yang efektif untuk menyebarkan pengetahuan tentang pentingnya literasi digital, serta bagaimana cara melindungi diri dari ancaman siber. Melalui berbagai media, baik itu iklan di televisi, internet, ataupun seminar-seminar pendidikan, masyarakat dapat

diberikan informasi yang mudah dipahami mengenai praktik-praktik dasar yang dapat meningkatkan keamanan di dunia maya.

Pentingnya literasi digital juga tidak bisa dilepaskan dari perkembangan teknologi yang semakin cepat. Setiap hari muncul teknologi baru yang mempengaruhi cara kita berinteraksi dengan dunia maya, mulai dari aplikasi baru hingga alat komunikasi yang lebih canggih. Untuk itu, masyarakat perlu diberikan pembekalan tentang cara-cara untuk beradaptasi dengan perkembangan teknologi ini tanpa mengabaikan aspek keamanannya. Dalam hal ini, literasi digital dapat memberikan pengetahuan yang penting tentang bagaimana teknologi baru dapat digunakan secara aman dan bagaimana cara untuk memitigasi risiko yang muncul. Dengan begitu, masyarakat bisa memanfaatkan teknologi terbaru untuk kepentingan pribadi dan profesional tanpa harus khawatir tentang ancaman yang mungkin datang.

Tantangan dalam mengedukasi masyarakat mengenai literasi digital adalah adanya kesenjangan akses terhadap teknologi itu sendiri. Meskipun semakin banyak orang yang memiliki akses internet, masih banyak pula yang tidak memiliki perangkat yang memadai atau akses ke pelatihan yang relevan. Kesenjangan ini sering kali ditemukan di daerah-daerah terpencil atau di kalangan kelompok yang kurang beruntung. Oleh karena itu, untuk memastikan bahwa literasi digital dapat merata, dibutuhkan upaya kolaboratif antara pemerintah, lembaga pendidikan, dan sektor swasta untuk menyediakan akses yang lebih baik terhadap teknologi dan pelatihan literasi digital. Ini adalah langkah penting untuk memastikan bahwa semua orang memiliki kesempatan yang sama untuk memanfaatkan dunia digital secara aman.

2. Tantangan dan Solusi dalam Meningkatkan Literasi Digital

Literasi digital telah menjadi salah satu aspek yang sangat penting dalam menghadapi ancaman kejahatan siber yang semakin berkembang. Dengan meningkatnya ketergantungan pada teknologi digital, masyarakat perlu memiliki pemahaman yang baik tentang cara melindungi dirinya dari potensi ancaman yang ada di dunia maya. Namun, meskipun pentingnya literasi digital semakin disadari, tantangan besar masih harus dihadapi dalam meningkatkan kesadaran dan pemahaman mengenai hal ini. Salah satu tantangan utama adalah adanya kesenjangan digital yang terjadi di berbagai wilayah, terutama di daerah pedesaan atau kawasan yang belum berkembang. Di daerah-daerah

tersebut, akses terhadap teknologi informasi yang memadai, seperti perangkat digital dan koneksi internet yang stabil, sangat terbatas. Hal ini menghalangi sebagian besar masyarakat untuk memperoleh pengetahuan dan keterampilan dasar yang diperlukan dalam menghadapi ancaman siber yang terus berkembang.

Kesenjangan ini menciptakan ketimpangan dalam kemampuan masyarakat untuk mengakses informasi yang diperlukan untuk melindungi dirinya secara digital, yang tidak memiliki akses yang memadai terhadap teknologi atau internet kemungkinan besar tidak akan memiliki pengetahuan tentang langkah-langkah dasar keamanan siber. Oleh karena itu, untuk meningkatkan literasi digital secara merata, perlu ada upaya khusus untuk mengatasi kesenjangan digital ini. Salah satu langkah yang dapat diambil adalah dengan memperluas jaringan internet dan meningkatkan akses perangkat teknologi di daerah-daerah yang kurang berkembang. Program-program pemerintah atau kerjasama dengan sektor swasta untuk menyediakan infrastruktur teknologi yang lebih baik sangat penting dalam hal ini.

Tantangan kedua yang tidak kalah penting adalah tingkat pemahaman yang rendah di kalangan sebagian besar masyarakat mengenai pentingnya literasi digital. Banyak orang masih belum sepenuhnya menyadari bahwa ancaman siber bukan hanya masalah yang dihadapi oleh individu yang bekerja di bidang teknologi informasi atau sektor yang terkait langsung dengan dunia digital. Ancaman siber dapat memengaruhi siapa saja yang menggunakan perangkat digital, baik itu untuk bekerja, belajar, atau berkomunikasi sehari-hari. Karena itu, peningkatan kesadaran tentang pentingnya literasi digital harus dilakukan secara lebih luas dan menyeluruh. Masyarakat umum, pelajar, serta pekerja profesional perlu diberikan pemahaman yang lebih baik tentang apa itu literasi digital dan bagaimana cara untuk melindungi dirinya dari berbagai bentuk ancaman yang dapat terjadi di dunia maya.

Untuk mengatasi masalah ini, perlu ada upaya sosialisasi yang lebih intensif mengenai literasi digital. Kampanye yang menyasar berbagai kalangan, mulai dari masyarakat umum hingga kalangan pelajar dan profesional, harus dilakukan dengan menggunakan berbagai media, seperti televisi, radio, media sosial, serta penyuluhan langsung melalui seminar dan pelatihan. Melalui kampanye ini, masyarakat dapat lebih memahami bahwa literasi digital tidak hanya berfokus pada kemampuan teknis, tetapi juga pada cara menjaga keamanan data pribadi dan

perangkatnya dari ancaman siber yang semakin canggih. Dengan meningkatnya pemahaman tentang ancaman tersebut, masyarakat akan lebih siap untuk melindungi dirinya dan meminimalisir potensi risiko yang ada.

Tantangan lainnya yang cukup besar dalam meningkatkan literasi digital adalah perubahan teknologi yang sangat cepat. Kejahatan siber terus berkembang seiring dengan pesatnya kemajuan teknologi, sehingga upaya untuk meningkatkan literasi digital harus selalu diperbarui agar tetap relevan dengan tren dan ancaman terkini. Hal ini tentu menjadi tantangan yang tidak mudah, mengingat teknologi digital yang berkembang dengan sangat cepat. Misalnya, bentuk-bentuk serangan siber yang dulu tidak dikenal kini menjadi hal yang sering ditemui, seperti serangan *ransomware* yang menargetkan sistem atau data pribadi, serta penggunaan teknik *phishing* yang semakin canggih untuk memanipulasi korban agar memberikan informasi pribadi. Oleh karena itu, untuk mengatasi tantangan ini, literasi digital harus disesuaikan dengan perkembangan teknologi terkini.

Salah satu solusi untuk mengatasi tantangan ini adalah dengan terus memperbarui kurikulum literasi digital yang ada. Kurikulum tersebut harus mengakomodasi teknologi terbaru dan mencakup pengetahuan yang relevan mengenai ancaman siber yang sedang berkembang. Oleh karena itu, pemerintah bersama dengan sektor pendidikan harus bekerja sama untuk memastikan bahwa program literasi digital yang diterapkan mulai dari tingkat pendidikan dasar hingga perguruan tinggi sesuai dengan kebutuhan saat ini. Sebagai contoh, kurikulum tersebut harus mencakup pemahaman dasar tentang bagaimana cara melindungi data pribadi di media sosial, penggunaan perangkat lunak antivirus yang baik, serta bagaimana mengidentifikasi serangan siber yang paling umum dilakukan oleh pelaku kejahatan digital.

Pemerintah juga perlu bekerja sama dengan sektor swasta untuk menyelenggarakan pelatihan dan kursus yang berkaitan dengan literasi digital secara lebih intensif. Program pelatihan ini bisa dilakukan baik untuk kalangan pelajar maupun pekerja profesional, dengan tujuan untuk meningkatkan keterampilan dalam menghadapi berbagai tantangan yang terkait dengan keamanan siber. Pelatihan yang diberikan sebaiknya meliputi berbagai aspek, mulai dari pengenalan ancaman siber yang umum hingga keterampilan lebih teknis terkait pencegahan dan deteksi

serangan siber. Melalui pelatihan ini, individu akan lebih siap untuk mengidentifikasi dan merespons ancaman yang dihadapi di dunia maya.

Tantangan lain yang harus dihadapi dalam meningkatkan literasi digital adalah kurangnya akses terhadap pelatihan yang relevan, terutama bagi kelompok-kelompok masyarakat yang lebih rentan terhadap ancaman siber. Sebagian besar program pelatihan literasi digital sering kali hanya dapat diakses oleh yang sudah memiliki akses terhadap teknologi dan internet. Oleh karena itu, untuk mengatasi masalah ini, pemerintah dan sektor terkait perlu menyediakan program pelatihan yang dapat diakses oleh semua kalangan, termasuk yang tinggal di daerah terpencil atau kurang berkembang. Salah satu solusi yang dapat diterapkan adalah dengan menggunakan teknologi berbasis mobile, seperti aplikasi atau video tutorial yang dapat diakses melalui ponsel pintar, yang lebih mudah dijangkau oleh masyarakat dengan akses internet terbatas.

Kerjasama antara pemerintah, sektor pendidikan, dan industri teknologi juga sangat penting dalam memperluas akses terhadap pelatihan literasi digital. Kolaborasi ini dapat mencakup pengembangan infrastruktur teknologi yang lebih baik di daerah-daerah yang tertinggal, serta pengadaan perangkat keras dan perangkat lunak yang dapat digunakan oleh masyarakat yang membutuhkan. Selain itu, sektor swasta juga bisa berkontribusi dengan menyelenggarakan program pelatihan atau workshop mengenai literasi digital secara gratis atau dengan biaya yang terjangkau, sehingga lebih banyak orang yang dapat ikut serta dalam pelatihan tersebut. Program-program semacam ini dapat membantu mengurangi kesenjangan digital dan memberikan kesempatan yang lebih besar bagi masyarakat untuk memperoleh pengetahuan yang diperlukan.

Untuk mengatasi tantangan-tantangan dalam meningkatkan literasi digital, dibutuhkan pendekatan yang komprehensif dan melibatkan berbagai pihak. Pemerintah, lembaga pendidikan, sektor swasta, serta masyarakat itu sendiri harus berperan aktif dalam memastikan bahwa literasi digital dapat diperoleh oleh semua kalangan tanpa terkecuali. Dengan demikian, masyarakat akan lebih siap untuk menghadapi ancaman siber yang semakin kompleks dan menjaga dirinya di dunia maya dengan lebih aman.

BAB VI
CYBERCRIME DALAM KONTEKS INTERNASIONAL

Cybercrime atau kejahatan siber telah berkembang menjadi ancaman global yang semakin kompleks, mengingat meningkatnya ketergantungan dunia terhadap teknologi digital dan internet. Kejahatan ini tidak hanya menargetkan individu, tetapi juga mengancam sistem keuangan, infrastruktur penting, serta keamanan negara di seluruh dunia. Dengan sifatnya yang lintas batas, *cybercrime* seringkali melibatkan aktor-aktor dari berbagai negara, menjadikannya tantangan besar bagi penegakan hukum internasional. Meskipun setiap negara memiliki pendekatan hukum yang berbeda-beda dalam menangani kejahatan siber, masalah ini memerlukan kerjasama internasional yang lebih erat. Organisasi internasional seperti Interpol, Europol, dan *United Nations* (UN) telah berupaya untuk membangun kerangka kerja global guna mengatasi ancaman ini, namun masih banyak tantangan yang harus dihadapi. Selain itu, dengan pesatnya perkembangan teknologi baru, seperti kecerdasan buatan dan blockchain, bentuk-bentuk *cybercrime* pun semakin canggih dan sulit terdeteksi, sehingga memerlukan pembaruan regulasi dan peningkatan kapasitas penegakan hukum di tingkat internasional. Dalam konteks ini, penting bagi negara-negara untuk bersinergi dalam berbagi informasi, teknologi, serta penguatan mekanisme hukum guna menghadapi ancaman yang semakin mendunia ini.

A. Perjanjian dan Kerjasama Internasional dalam Penanganan Kejahatan Siber

1. Perjanjian Internasional dalam Penanganan Kejahatan Siber

Penanganan kejahatan siber yang semakin kompleks memerlukan kerjasama internasional yang erat, mengingat sifat kejahatan ini yang lintas batas negara. Kejahatan siber tidak mengenal batas teritorial, dan sering kali melibatkan pelaku, korban, serta bukti yang tersebar di berbagai negara. Oleh karena itu, penanggulangan kejahatan siber memerlukan kerangka hukum yang dapat memfasilitasi kolaborasi lintas negara. Perjanjian internasional menjadi salah satu instrumen yang sangat penting dalam menciptakan kerjasama yang solid antara negara-negara untuk menghadapi ancaman ini. Perjanjian-perjanjian internasional ini tidak hanya berfungsi sebagai pedoman hukum, tetapi juga sebagai alat untuk memperkuat koordinasi antarnegara dalam menangani kejahatan siber.

Salah satu perjanjian internasional yang sangat signifikan dalam konteks penanganan kejahatan siber adalah Konvensi *Cybercrime* Budapest yang disahkan oleh Dewan Eropa pada tahun 2001. Konvensi ini menjadi dasar hukum internasional pertama yang mengatur tentang kejahatan siber dan telah diadopsi oleh banyak negara di seluruh dunia. Konvensi Budapest menetapkan kerangka hukum yang memfasilitasi pertukaran informasi antara negara-negara, mengatur prosedur investigasi, serta memberikan panduan mengenai penegakan hukum terhadap pelaku kejahatan siber. Selain itu, konvensi ini juga membahas tentang bagaimana menangani berbagai jenis kejahatan yang dilakukan melalui teknologi informasi, seperti peretasan, penyebaran *malware*, dan kejahatan terkait dengan perlindungan data pribadi.

Konvensi Budapest mencakup aspek yang lebih luas, seperti perdagangan ilegal dan pornografi anak yang dilakukan secara daring. Kejahatan-kejahatan ini telah menjadi perhatian global yang memerlukan penanganan bersama di tingkat internasional. Dengan adanya konvensi ini, negara-negara dapat bekerja sama dalam melakukan investigasi, mengumpulkan bukti, dan menuntut pelaku yang terlibat dalam kejahatan siber yang melintasi batas negara. Meskipun konvensi ini telah mengatur banyak hal terkait dengan kejahatan siber, tantangan yang ada adalah memastikan bahwa semua negara yang

terlibat dapat mematuhi dan mengimplementasikan ketentuan-ketentuan yang ada secara konsisten.

Terdapat pula perjanjian internasional lain yang berperan penting dalam upaya penanganan kejahatan siber, salah satunya adalah Perjanjian Kerjasama Keamanan Siber APEC. Perjanjian ini bertujuan untuk memfasilitasi kolaborasi antara negara-negara yang tergabung dalam *Asia-Pacific Economic Cooperation* (APEC) untuk menghadapi ancaman siber yang semakin berkembang. Dalam kerangka APEC, negara-negara sepakat untuk bekerja sama dalam berbagai aspek keamanan siber, termasuk pertukaran informasi terkait ancaman siber, peningkatan kapasitas pengawasan dan perlindungan data, serta penguatan kebijakan infrastruktur teknologi yang dapat mendukung ketahanan dunia maya di kawasan Asia-Pasifik.

Perjanjian APEC ini sangat relevan mengingat kawasan Asia-Pasifik merupakan salah satu wilayah yang paling terdampak oleh kejahatan siber, baik dalam hal serangan terhadap sektor bisnis, infrastruktur kritis, maupun ancaman terhadap data pribadi individu. Dalam perjanjian ini, negara-negara anggota berkomitmen untuk memperkuat kebijakan pengawasan dan kontrol data, serta meningkatkan kesiapan dalam menghadapi potensi serangan siber. Salah satu tujuan utama dari kerjasama ini adalah untuk memastikan bahwa negara-negara di kawasan Asia-Pasifik dapat saling membantu dalam mengidentifikasi, mencegah, dan merespons ancaman siber secara efektif.

Perjanjian internasional mengenai kejahatan siber tidak hanya berkaitan dengan aspek penegakan hukum, tetapi juga menyangkut perlindungan data dan hak asasi manusia. Banyak negara yang khawatir dengan risiko penyalahgunaan data pribadi dalam proses penanganan kejahatan siber. Oleh karena itu, dalam beberapa perjanjian internasional, terdapat ketentuan yang mengatur tentang perlindungan privasi data dan cara-cara yang sah dalam memperoleh serta mengakses informasi digital yang relevan. Ini penting agar penegakan hukum terhadap pelaku kejahatan siber tidak melanggar hak-hak individu, terutama terkait dengan privasi dan kebebasan berekspresi di dunia maya.

Meskipun ada berbagai perjanjian internasional yang mengatur kerjasama dalam penanganan kejahatan siber, implementasi dan penegakan hukum dari perjanjian-perjanjian ini tetap menghadapi

sejumlah tantangan. Salah satu tantangan terbesar adalah adanya perbedaan standar hukum dan kebijakan di masing-masing negara terkait dengan pengumpulan bukti, pengaturan privasi data, serta aturan mengenai internet. Negara-negara memiliki peraturan hukum yang berbeda-beda, dan ini sering kali menjadi penghalang dalam proses kerjasama internasional. Misalnya, negara dengan kebijakan perlindungan data yang lebih ketat mungkin merasa khawatir terhadap potensi penyalahgunaan informasi yang diperoleh selama proses penyelidikan, sementara negara lain mungkin lebih terbuka dalam hal berbagi data untuk tujuan penegakan hukum.

Keberagaman dalam sistem hukum ini juga menyebabkan kesulitan dalam penyusunan perjanjian internasional yang dapat diterima oleh semua negara. Setiap negara memiliki kebijakan dan prioritas yang berbeda, dan ini terkadang bertentangan dengan tujuan untuk menciptakan kerjasama yang lebih efektif dalam penanganan kejahatan siber. Sebagai contoh, negara-negara dengan sistem hukum yang lebih liberal dalam hal kebebasan informasi mungkin akan lebih cenderung untuk berbagi data secara terbuka, sementara negara yang lebih konservatif dalam hal privasi data mungkin akan menuntut ketentuan yang lebih ketat terkait dengan hak privasi individu.

Kejahatan siber yang terus berkembang pesat juga menuntut adanya pembaruan yang berkala terhadap perjanjian internasional yang ada. Kejahatan siber sering kali berkembang lebih cepat daripada kemampuan perjanjian internasional untuk meresponsnya, terutama dengan munculnya jenis ancaman baru yang lebih canggih. Misalnya, serangan siber yang melibatkan teknologi baru, seperti kecerdasan buatan (AI) atau *internet of things* (IoT), dapat menambah kompleksitas dalam investigasi dan penegakan hukum. Oleh karena itu, pembaruan terhadap ketentuan yang ada dalam perjanjian internasional sangat diperlukan untuk memastikan bahwa negara-negara dapat terus bekerja sama dalam menghadapi ancaman-ancaman baru ini.

Dengan berbagai tantangan yang ada, penting untuk terus mendorong perbaikan dalam kerjasama internasional dalam menghadapi kejahatan siber. Ini dapat dilakukan dengan meningkatkan komunikasi antarnegara, memperkuat kapasitas negara-negara berkembang dalam hal teknologi dan pelatihan, serta memastikan bahwa perjanjian internasional yang ada selalu disesuaikan dengan perkembangan teknologi terbaru. Sebagai tambahan, penting juga untuk memperhatikan

aspek hak asasi manusia dan perlindungan data pribadi dalam setiap upaya penegakan hukum terhadap kejahatan siber. Kerjasama yang lebih baik dan perjanjian internasional yang lebih komprehensif akan memungkinkan negara-negara untuk lebih efektif dalam menanggulangi ancaman kejahatan siber yang semakin mengglobal.

2. Kerjasama Internasional dalam Penanganan Kejahatan Siber

Kerjasama internasional dalam penanganan kejahatan siber merupakan aspek yang sangat penting untuk mengatasi ancaman yang semakin berkembang dalam dunia maya. Kejahatan siber tidak mengenal batas negara, sehingga kerjasama lintas negara menjadi kunci untuk memperkuat pertahanan dunia maya secara global. Dalam menghadapi tantangan ini, negara-negara tidak bisa bergerak secara terpisah-pisah. Oleh karena itu, berbagai organisasi internasional berperan penting dalam memfasilitasi kolaborasi dan memastikan bahwa upaya penanggulangan kejahatan siber berjalan efektif. Organisasi-organisasi seperti Interpol, Europol, serta badan-badan lainnya seperti ASEAN dan UN memberikan landasan penting bagi kerjasama antarnegara dalam menanggulangi kejahatan yang dilakukan melalui teknologi informasi ini.

Interpol adalah salah satu organisasi internasional yang memiliki peran sangat vital dalam kerjasama internasional di bidang penanggulangan kejahatan siber. Sebagai organisasi yang memiliki mandat untuk mendukung kepolisian di berbagai negara, Interpol menyediakan platform untuk pertukaran informasi dan koordinasi operasi internasional. Dengan keberadaan *Cybercrime* Directorate, Interpol memfasilitasi kolaborasi antara negara-negara yang terlibat dalam penyelidikan kejahatan siber, termasuk perdagangan ilegal, penipuan online, hingga serangan *ransomware*. Organisasi ini juga memiliki database internasional yang digunakan oleh negara-negara anggota untuk melacak pelaku kejahatan siber yang beroperasi lintas negara. Keberadaan Interpol ini memungkinkan berbagai negara untuk saling berbagi informasi penting yang dapat digunakan untuk memerangi kejahatan yang sulit dilacak dan sangat tersebar di berbagai wilayah.

Europol, yang memiliki fokus utama pada penegakan hukum di kawasan Uni Eropa, juga berperan krusial dalam memperkuat kerjasama internasional dalam penanganan kejahatan siber. Melalui *European Cybercrime Centre* (EC3), Europol mengkoordinasikan operasi siber di

antara negara-negara Uni Eropa. EC3 tidak hanya berfungsi sebagai pusat informasi, tetapi juga menyediakan pelatihan dan bantuan teknis kepada otoritas keamanan di negara-negara anggota. Dengan adanya EC3, Europol dapat membantu negara-negara Eropa dalam menghadapi ancaman siber yang berpotensi merusak sektor-sektor vital seperti infrastruktur kritis dan sektor keuangan. Europol juga berperan penting dalam berbagi informasi tentang tren ancaman terbaru dan memberi panduan bagi negara-negara anggota untuk meningkatkan kesiapan dalam menghadapi kejahatan siber yang semakin kompleks.

Organisasi internasional lainnya, seperti ASEAN (*Association of Southeast Asian Nations*), juga berperan penting dalam membangun kerjasama internasional dalam bidang keamanan siber. ASEAN telah mengembangkan inisiatif keamanan siber yang memungkinkan negara-negara anggotanya untuk bekerja sama dalam memerangi ancaman siber. Dalam kerangka kerja ini, negara-negara anggota ASEAN berbagi informasi tentang tren ancaman yang sedang berkembang dan memberikan dukungan satu sama lain dalam hal kebijakan serta pengaturan keamanan siber. Kerjasama antarnegara ASEAN ini sangat penting mengingat kawasan Asia Tenggara merupakan salah satu wilayah yang sangat rentan terhadap serangan siber, baik itu terhadap sektor publik, sektor bisnis, maupun sektor pribadi.

Forum global seperti GAC (*Global Forum on Cybersecurity*) juga berperan dalam memperkuat kerjasama internasional untuk menangani ancaman siber. Forum ini memberikan platform bagi negara-negara di seluruh dunia untuk berdiskusi tentang kebijakan, regulasi, dan teknologi yang berkaitan dengan keamanan siber. GAC memungkinkan negara-negara untuk berbagi pengetahuan, tantangan, serta pengalaman dalam menghadapi ancaman siber, sehingga dapat bekerja bersama-sama untuk menciptakan solusi yang lebih efektif dalam melindungi dunia maya dari berbagai ancaman yang muncul.

Meskipun ada banyak organisasi internasional yang memfasilitasi kerjasama lintas negara dalam penanganan kejahatan siber, tantangan tetap ada. Salah satu tantangan terbesar adalah perbedaan kebijakan dan prioritas antara negara-negara yang terlibat. Beberapa negara mungkin lebih fokus pada perlindungan data pribadi dan privasi, sementara negara lainnya lebih menekankan pada pencegahan kejahatan yang berkaitan dengan terorisme siber. Perbedaan ini sering kali menimbulkan kesulitan dalam menyusun kebijakan yang

komprehensif dan diterima oleh semua pihak, terutama ketika menyangkut pertukaran data dan informasi yang bersifat sensitif.

Masalah yurisdiksi juga menjadi hambatan utama dalam investigasi kejahatan siber lintas batas. Dalam banyak kasus, bukti atau data yang diperlukan untuk investigasi berada di negara yang berbeda dengan tempat kejadian atau lokasi pelaku kejahatan. Perbedaan dalam hukum dan regulasi terkait pengumpulan bukti, privasi data, dan pengaturan internet antarnegara sering kali membuat proses penyelidikan menjadi lebih kompleks dan memakan waktu. Hal ini menuntut adanya kesepakatan multilateral untuk mengatasi masalah ini dan memperkuat kerjasama antarnegara dalam hal pengaturan teknis dan pertukaran informasi yang lebih terintegrasi.

Dengan adanya tantangan-tantangan tersebut, penting bagi negara-negara untuk terus mendorong peningkatan kerjasama internasional dalam menangani kejahatan siber. Salah satu langkah yang bisa diambil adalah dengan memperbarui dan menyesuaikan kerangka hukum internasional yang ada agar lebih relevan dengan perkembangan teknologi yang pesat. Pembaruan ini diperlukan untuk memastikan bahwa negara-negara dapat tetap bersatu dalam menghadapi ancaman siber yang semakin kompleks dan beragam. Negara-negara juga harus lebih terbuka dalam berbagi data dan informasi yang relevan untuk meningkatkan efektivitas penanggulangan kejahatan siber.

Negara-negara juga perlu memperkuat kapasitas teknis dalam menghadapi ancaman siber. Ini bisa dilakukan dengan meningkatkan pelatihan bagi personel yang terlibat dalam penegakan hukum siber, serta menyediakan bantuan teknis bagi negara-negara yang memiliki keterbatasan dalam hal teknologi dan sumber daya. Kerjasama internasional dalam bentuk pelatihan dan bantuan teknis sangat penting untuk memperkuat kemampuan negara-negara, terutama yang sedang berkembang, dalam menghadapi ancaman siber yang semakin canggih.

Peningkatan kerjasama internasional dalam penanganan kejahatan siber juga harus melibatkan sektor swasta, terutama perusahaan-perusahaan teknologi yang berperan penting dalam menjaga infrastruktur dunia maya. Perusahaan-perusahaan ini memiliki pengetahuan dan sumber daya yang sangat dibutuhkan dalam menghadapi serangan siber. Oleh karena itu, penting bagi sektor swasta untuk bekerja sama dengan negara-negara dan organisasi internasional

dalam mengembangkan solusi yang dapat melindungi dunia maya dari ancaman yang terus berkembang.

Kerjasama internasional yang kuat dalam penanganan kejahatan siber akan memungkinkan negara-negara untuk saling mendukung dalam mengatasi ancaman yang tidak mengenal batas negara. Dengan berbagi informasi, sumber daya, dan keahlian, negara-negara dapat lebih siap dalam melawan kejahatan siber yang semakin kompleks. Keamanan dunia maya yang lebih baik akan memberikan perlindungan yang lebih besar bagi masyarakat, bisnis, serta pemerintah di seluruh dunia.

B. *Cybercrime* Convention (Budapest Convention) dan Implikasinya bagi Indonesia

1. *Cybercrime* Convention (Budapest Convention)

Konvensi *Cybercrime* atau yang lebih dikenal dengan Konvensi Budapest merupakan perjanjian internasional yang disahkan pada tahun 2001 oleh Dewan Eropa. Konvensi ini menjadi tonggak penting dalam upaya penanggulangan kejahatan siber secara global. Kejahatan siber yang terus berkembang dan semakin kompleks memerlukan pendekatan yang lebih terstruktur dan kolaboratif antarnegara. Konvensi ini dirancang untuk menyediakan dasar hukum yang jelas bagi negara-negara yang terlibat dalam penanggulangan kejahatan siber, dengan fokus pada kejahatan yang melibatkan teknologi informasi dan komunikasi. Salah satu tujuan utama dari Konvensi Budapest adalah untuk menciptakan kerangka hukum internasional yang konsisten, yang dapat diikuti oleh negara-negara anggota dalam mengatasi ancaman kejahatan siber yang sifatnya lintas batas.

Konvensi ini menetapkan pedoman yang harus diadopsi oleh negara-negara anggota dalam merumuskan peraturan perundang-undangan mengenai kejahatan siber. Beberapa jenis kejahatan yang diatur dalam Konvensi Budapest antara lain adalah kejahatan terhadap sistem komputer, akses ilegal terhadap data, penipuan siber, penyalahgunaan perangkat dan data, serta perdagangan ilegal yang dilakukan secara daring. Dengan adanya pedoman ini, negara-negara dapat menyelaraskan kebijakan dan peraturan mengenai kejahatan siber sehingga tidak ada tumpang tindih atau ketidaksesuaian dalam pengaturan hukum di masing-masing negara.

Salah satu aspek penting yang diatur dalam Konvensi Budapest adalah prosedur yang berkaitan dengan pengumpulan dan pengiriman bukti digital. Mengingat sifat kejahatan siber yang sering kali melibatkan bukti yang terdistribusi di berbagai negara, maka pengaturan mengenai pengumpulan bukti ini sangat penting untuk memperlancar investigasi lintas negara. Konvensi ini menyediakan prosedur hukum yang dapat digunakan oleh negara-negara untuk memudahkan pertukaran informasi dan bukti yang diperlukan dalam penyelidikan dan penuntutan kasus kejahatan siber yang melibatkan pelaku dan korban di berbagai negara.

Konvensi Budapest juga memberikan panduan terkait prosedur-prosedur yang diperlukan untuk mempercepat proses permintaan bantuan internasional. Kejahatan siber sering kali melibatkan pelaku yang beroperasi dari satu negara, sementara korban atau bukti ada di negara lain. Dengan adanya prosedur yang terstandarisasi ini, negara-negara yang terlibat dalam penyelidikan kejahatan siber dapat saling memberikan bantuan secara cepat dan efektif. Hal ini tentu saja sangat penting untuk memastikan bahwa proses penuntutan terhadap pelaku kejahatan siber tidak terhambat oleh masalah teknis atau administratif yang sering muncul dalam kasus lintas batas.

Konvensi Budapest juga mengatur tentang perlindungan data pribadi dalam konteks kejahatan siber. Mengingat banyaknya kasus kejahatan yang melibatkan pencurian identitas dan pembajakan data pribadi, konvensi ini mengharuskan negara-negara anggota untuk menetapkan peraturan yang melindungi data pribadi warganya. Ini termasuk langkah-langkah preventif yang dapat diambil untuk mencegah penyalahgunaan data pribadi serta prosedur hukum untuk menangani pelanggaran yang terjadi. Konvensi ini juga menekankan pentingnya melindungi hak asasi manusia dalam setiap aspek penegakan hukum terkait dengan kejahatan siber, termasuk dalam hal pengumpulan data dan pemrosesan informasi pribadi.

Salah satu tantangan utama dalam penanganan kejahatan siber adalah ketidakcocokan antara hukum dan kebijakan yang diterapkan oleh negara-negara yang berbeda. Konvensi Budapest, dengan memberikan pedoman yang terstandarisasi, membantu mengatasi masalah ini dengan memungkinkan negara-negara anggota untuk menyelaraskan peraturan. Konvensi ini tidak hanya berlaku untuk negara-negara Eropa, tetapi juga telah diadopsi oleh banyak negara di luar Eropa, termasuk negara-negara di Asia, Amerika Utara, dan

Amerika Latin. Hal ini mencerminkan pengakuan global terhadap pentingnya penanggulangan kejahatan siber secara kolaboratif dan lintas negara.

Keberadaan Konvensi Budapest juga memfasilitasi kerjasama internasional yang lebih erat dalam penyelidikan dan penuntutan kasus kejahatan siber. Negara-negara yang terikat oleh konvensi ini diharapkan untuk bekerja sama dalam berbagai bentuk, mulai dari pertukaran informasi, bantuan teknis, hingga penyediaan akses hukum yang lebih mudah terhadap bukti yang diperlukan dalam proses investigasi. Keberhasilan dalam penanganan kejahatan siber sangat bergantung pada kemampuan negara-negara untuk bekerja sama secara efektif, dan Konvensi Budapest memberikan kerangka hukum yang memungkinkan hal ini terjadi.

Meskipun Konvensi Budapest telah berhasil mengatur banyak aspek penting dalam penanggulangan kejahatan siber, ada beberapa tantangan yang perlu dihadapi dalam implementasinya. Salah satunya adalah perbedaan dalam kemampuan teknis dan sumber daya yang dimiliki oleh negara-negara anggota. Beberapa negara mungkin tidak memiliki infrastruktur atau teknologi yang memadai untuk mengimplementasikan ketentuan-ketentuan yang ada dalam konvensi ini. Oleh karena itu, kerjasama internasional tidak hanya terbatas pada aspek hukum, tetapi juga melibatkan bantuan teknis dan pelatihan untuk memastikan bahwa semua negara dapat melaksanakan ketentuan dalam Konvensi Budapest dengan baik.

2. Implikasi Konvensi Budapest bagi Indonesia

Indonesia, sebagai negara yang semakin bergantung pada teknologi digital, dihadapkan pada ancaman kejahatan siber yang terus berkembang. Kejahatan siber, yang tidak mengenal batas negara, sering kali melibatkan pelaku yang tidak dapat terdeteksi oleh sistem hukum nasional. Mengingat hal ini, Konvensi Budapest memberikan implikasi penting bagi Indonesia, terutama dalam aspek hukum, kebijakan, dan kapasitas penegakan hukum di tingkat nasional. Sebagai langkah awal, Indonesia meratifikasi Konvensi Budapest pada tahun 2018, yang menandakan komitmennya untuk lebih aktif dalam kerjasama internasional guna mengatasi kejahatan siber yang kini merupakan ancaman global. Ratifikasi ini menjadi bukti bahwa Indonesia menyadari

pentingnya pengaturan hukum internasional dalam menghadapi kejahatan siber yang lintas batas.

Salah satu implikasi utama yang timbul dari ratifikasi Konvensi Budapest adalah kewajiban Indonesia untuk mengadopsi kebijakan hukum yang selaras dengan standar internasional yang ditetapkan dalam konvensi tersebut. Konvensi Budapest mengatur berbagai aspek terkait kejahatan siber, termasuk akses ilegal ke sistem komputer, pencurian data pribadi, penyalahgunaan perangkat dan data, serta perdagangan ilegal secara daring. Untuk itu, Indonesia perlu melakukan harmonisasi terhadap peraturan perundang-undangannya, yang melibatkan pembaruan undang-undang yang ada, seperti Undang-Undang ITE, agar lebih sesuai dengan ketentuan dalam konvensi tersebut. Hal ini menjadi tantangan tersendiri bagi Indonesia karena harus mengintegrasikan pedoman internasional dalam konteks hukum domestik yang telah ada, sekaligus memastikan bahwa peraturan yang baru dapat diterima oleh masyarakat dan pemerintah.

Tantangan terbesar Indonesia dalam mengimplementasikan Konvensi Budapest adalah penyesuaian terhadap sistem hukum yang telah ada, terutama dalam hal penanganan bukti digital dan kerjasama internasional dalam investigasi. Konvensi ini mengharuskan negara-negara yang meratifikasi untuk memiliki mekanisme bantuan hukum yang cepat dan efisien, yang mencakup pertukaran bukti digital dan akses terhadap data yang diperlukan untuk investigasi dan penuntutan kasus kejahatan siber lintas batas. Dalam hal ini, Indonesia perlu meningkatkan kapasitas sumber daya manusia, baik dari sisi teknis maupun legal, agar dapat menjalankan kewajiban ini dengan baik. Pemerintah Indonesia harus mengembangkan infrastruktur yang memungkinkan pengumpulan dan pengiriman bukti digital antarnegara secara efisien, serta membangun mekanisme hukum yang memadai untuk memastikan kecepatan dan akurasi dalam proses tersebut.

Penerapan Konvensi Budapest juga mengharuskan Indonesia untuk meningkatkan kerjasama dengan lembaga-lembaga internasional yang berperan dalam penanggulangan kejahatan siber. Salah satunya adalah Interpol, yang menyediakan kanal komunikasi untuk pertukaran data dan intelijen terkait kejahatan siber. Indonesia juga perlu memperkuat kemitraannya dengan Europol, yang memiliki peran penting dalam koordinasi operasi siber di tingkat Uni Eropa, serta dengan lembaga-lembaga internasional lainnya. Penguatan kerjasama ini

penting agar Indonesia dapat memanfaatkan dukungan teknis dan sumber daya yang lebih luas dalam penyelidikan dan penuntutan kasus kejahatan siber yang melibatkan banyak negara.

Konvensi Budapest juga menekankan pentingnya keterlibatan penyedia layanan internet dalam mendeteksi dan mencegah kejahatan siber. Oleh karena itu, Indonesia perlu memperjelas peran penyedia layanan internet dalam konteks hukum dan pengaturan kejahatan siber. Hal ini meliputi kewajiban penyedia layanan untuk bekerja sama dengan pihak berwenang dalam mendeteksi kejahatan siber, baik melalui pengawasan lalu lintas data maupun dengan memberikan akses yang sah terhadap informasi yang relevan untuk investigasi. Kewajiban ini tentunya memerlukan penyusunan regulasi yang jelas dan terperinci, sehingga penyedia layanan dapat menjalankan tugasnya dengan benar tanpa melanggar privasi pengguna.

Ratifikasi Konvensi Budapest juga mendorong Indonesia untuk memperkuat infrastruktur hukum nasional dalam menghadapi tantangan kejahatan siber. Salah satu aspek yang perlu diperhatikan adalah pengembangan sistem hukum yang lebih responsif terhadap ancaman siber. Indonesia harus memastikan bahwa undang-undang yang ada dapat menanggapi perubahan cepat dalam teknologi dan tren ancaman siber. Ini termasuk memastikan bahwa hukum yang berlaku tidak ketinggalan zaman dan dapat memberikan sanksi yang efektif terhadap pelaku kejahatan siber, baik yang dilakukan secara domestik maupun lintas negara.

Ratifikasi Konvensi Budapest membawa pengaruh besar terhadap kerangka hukum nasional Indonesia. Dengan mengadopsi ketentuan internasional, Indonesia berkomitmen untuk semakin memperkuat upaya internasional dalam penanggulangan kejahatan siber. Selain itu, Indonesia juga diharapkan untuk memperbaharui kebijakan hukum yang relevan, baik dari sisi pengaturan perundang-undangan maupun implementasinya. Penguatan kerjasama internasional melalui mekanisme seperti Konvensi Budapest menjadi bagian integral dari strategi nasional Indonesia dalam menghadapi kejahatan siber yang semakin kompleks.

Ratifikasi ini juga membuka peluang bagi Indonesia untuk memperbaiki koordinasi antar lembaga di dalam negeri dalam menangani kejahatan siber. Badan Siber dan Sandi Negara (BSSN) diharapkan dapat berperan yang lebih signifikan dalam mendukung

penyelidikan dan penuntutan kasus kejahatan siber. Selain itu, Indonesia perlu meningkatkan kesadaran masyarakat mengenai pentingnya keamanan siber, dengan melibatkan sektor swasta dan lembaga pendidikan dalam kampanye perlindungan data pribadi dan pencegahan kejahatan siber. Kesadaran ini akan memperkuat fondasi bagi penegakan hukum yang lebih efektif di masa depan.

Pada jangka panjang, implementasi Konvensi Budapest di Indonesia akan berperan penting dalam menciptakan lingkungan digital yang lebih aman dan terpercaya. Sebagai negara dengan ekonomi digital yang berkembang pesat, Indonesia harus memastikan bahwa kerjasama internasional dan kebijakan domestik saling mendukung untuk memitigasi risiko kejahatan siber. Dengan demikian, Konvensi Budapest tidak hanya menjadi landasan hukum, tetapi juga memberikan peluang untuk memperkuat infrastruktur hukum dan kapasitas Indonesia dalam menghadapi kejahatan siber yang semakin kompleks dan berkembang.

C. Peran INTERPOL dan ASEAN dalam Penanggulangan Kejahatan Siber

1. Peran INTERPOL dalam Penanggulangan Kejahatan Siber

INTERPOL, atau *International Criminal Police Organization*, merupakan salah satu organisasi internasional yang berperan penting dalam penanggulangan kejahatan lintas negara, termasuk kejahatan siber yang semakin berkembang seiring kemajuan teknologi informasi. Didirikan pada tahun 1923, INTERPOL bertujuan untuk memfasilitasi kerja sama polisi antarnegara guna mengatasi berbagai bentuk kriminalitas yang tidak dapat diselesaikan secara unilateral oleh satu negara saja. Dalam konteks kejahatan siber, peran INTERPOL menjadi semakin sentral karena karakteristik kejahatan ini yang bersifat lintas batas, anonim, dan memerlukan penanganan yang terkoordinasi secara global. Kejahatan siber seperti peretasan, pencurian identitas, penipuan daring, dan serangan *malware* memerlukan respon yang tidak hanya cepat, tetapi juga terkoordinasi antar yurisdiksi negara.

Sebagai pusat koordinasi internasional dalam upaya penegakan hukum, INTERPOL mengelola jaringan informasi global yang memungkinkan pertukaran data intelijen secara real-time antar negara anggotanya. Jaringan ini menjadi fondasi penting bagi deteksi dini dan respons cepat terhadap berbagai serangan siber yang terjadi di berbagai

belahan dunia. INTERPOL memfasilitasi pertukaran informasi tentang pelaku, jaringan kejahatan, pola serangan, dan perangkat yang digunakan dalam operasi siber kriminal. Salah satu instrumen vital dalam koordinasi ini adalah I-24/7, sebuah jaringan komunikasi global yang menghubungkan seluruh negara anggota INTERPOL, yang memungkinkan penyebaran notifikasi tentang aktivitas kejahatan siber, serta permintaan bantuan investigasi lintas negara.

INTERPOL juga mendirikan satuan khusus yang menangani kejahatan siber secara lebih fokus dan mendalam, yaitu INTERPOL *Cybercrime Directorate*. Unit ini berkantor pusat di Singapura dan merupakan bagian dari *INTERPOL Global Complex for Innovation* (IGCI), yang menjadi pusat inovasi dan teknologi untuk memerangi kejahatan siber. Dalam praktiknya, unit ini menjalankan berbagai operasi gabungan dengan negara-negara anggota untuk mengidentifikasi, melacak, dan menangkap pelaku kejahatan siber yang beroperasi secara internasional. Tidak hanya berperan dalam penyelidikan langsung, unit ini juga membantu membangun sistem dan protokol keamanan siber di negara-negara yang memiliki kapasitas terbatas dalam menangani kejahatan digital.

Pada penguatan kapasitas penegak hukum, INTERPOL menyediakan berbagai pelatihan teknis dan workshop kepada aparat dari negara-negara anggota. Kegiatan ini mencakup pelatihan mengenai analisis forensik digital, pengamanan infrastruktur kritis, metode investigasi kejahatan siber, serta pelatihan dalam penggunaan perangkat lunak khusus untuk penelusuran pelaku siber. Program-program pelatihan ini didesain agar dapat menjembatani kesenjangan kapasitas antara negara maju dan negara berkembang, serta menciptakan standar keterampilan yang merata dalam menghadapi ancaman siber. Dengan begitu, semua negara anggota dapat secara efektif berpartisipasi dalam upaya global menanggulangi kejahatan siber.

INTERPOL juga berperan penting dalam memberikan bantuan hukum dan operasional dalam kasus kejahatan siber lintas negara. Organisasi ini dapat mengeluarkan red notice, yaitu permintaan kepada negara-negara anggota untuk membantu mencari dan menangkap tersangka kejahatan siber yang melarikan diri ke negara lain. Mekanisme ini sangat berguna ketika pelaku kejahatan melakukan aksinya dari luar yurisdiksi negara korban, atau ketika bukti digital tersebar di berbagai server di luar negeri. INTERPOL bertindak sebagai fasilitator untuk

mempermudah komunikasi antara lembaga penegak hukum dan sistem peradilan antar negara.

INTERPOL tidak bekerja sendiri dalam menghadapi kejahatan siber. Kolaborasi dengan organisasi internasional lainnya seperti Europol, UNODC (*United Nations Office on Drugs and Crime*), dan lembaga sektor swasta merupakan bagian integral dari strategi INTERPOL. Dalam kerja sama dengan Europol, misalnya, operasi gabungan dilakukan untuk membongkar jaringan kriminal siber internasional yang melakukan aktivitas seperti *phishing*, *skimming*, atau perdagangan data curian di dark web. Sementara itu, kemitraan dengan sektor swasta memungkinkan INTERPOL mengakses teknologi terbaru dan data penting yang relevan dalam penanganan kasus. Perusahaan-perusahaan keamanan digital seperti Trend Micro, Kaspersky, dan Microsoft turut menyediakan dukungan teknis dan informasi ancaman siber terkini.

INTERPOL juga mengembangkan berbagai platform analitik dan sistem pemantauan ancaman siber secara global. Salah satunya adalah Cyber Fusion Centre yang bertugas untuk mengumpulkan, menganalisis, dan menyebarkan informasi mengenai ancaman siber kepada negara-negara anggota secara tepat waktu. Melalui pusat ini, INTERPOL dapat memberikan peringatan dini kepada negara anggota yang sedang atau akan menjadi target serangan, serta memberikan dukungan teknis untuk memitigasi serangan tersebut. Pusat ini menjadi titik kunci dalam pengembangan strategi kolektif dalam menanggulangi kejahatan siber dan menjaga stabilitas digital di skala global.

Untuk menghadapi kejahatan siber, INTERPOL juga aktif mengembangkan kebijakan dan kerangka hukum internasional bersama negara-negara anggotanya. Hal ini bertujuan untuk menciptakan keselarasan hukum dalam penanganan kejahatan siber lintas negara, karena perbedaan sistem hukum sering kali menjadi hambatan utama dalam proses penyelidikan dan penuntutan. INTERPOL mendorong negara-negara anggota untuk meratifikasi instrumen hukum seperti Konvensi Budapest dan mengadopsi praktik terbaik yang telah terbukti efektif di berbagai negara. Melalui konferensi, publikasi, dan forum global, INTERPOL menjadi fasilitator diskusi internasional dalam membentuk tata kelola hukum global terhadap kejahatan siber.

2. Peran ASEAN dalam Penanggulangan Kejahatan Siber

ASEAN, sebagai organisasi kawasan Asia Tenggara yang beranggotakan sepuluh negara, memiliki peran strategis dalam menjaga keamanan regional, termasuk dalam menghadapi ancaman kejahatan siber yang semakin kompleks dan lintas batas. Seiring berkembangnya teknologi digital di kawasan ini, aktivitas sosial dan ekonomi semakin bergantung pada infrastruktur teknologi informasi, yang secara langsung meningkatkan potensi risiko serangan siber. Kejahatan siber, seperti penipuan daring, pencurian data pribadi, penyebaran *malware*, dan serangan terhadap infrastruktur kritikal, menjadi tantangan serius yang mengancam stabilitas ekonomi dan politik negara-negara anggota. Oleh karena itu, ASEAN tidak dapat mengabaikan kebutuhan akan kerja sama regional yang komprehensif untuk menangani kejahatan siber secara kolektif, terorganisir, dan sistematis.

Langkah awal ASEAN dalam merespons tantangan ini adalah dengan merancang kerangka kerja sama strategis yang tertuang dalam ASEAN *Cybersecurity Cooperation Strategy* yang diluncurkan pada tahun 2015. Strategi ini bertujuan untuk menyelaraskan visi dan upaya negara-negara anggota dalam memperkuat sistem keamanan siber nasional dan regional. Dalam strategi tersebut, ASEAN mendorong adanya peningkatan kapasitas nasional, koordinasi lintas sektor, dan pertukaran informasi yang terstruktur sebagai dasar dalam mengembangkan ketahanan siber kawasan. Selain itu, strategi ini juga menekankan pentingnya pembentukan standar kebijakan yang seragam dalam penanganan insiden siber serta perlindungan terhadap aset digital penting milik negara dan swasta.

ASEAN juga mendorong terbentuknya forum-forum kerja sama teknis dan kebijakan yang memungkinkan negara-negara anggota saling berbagi praktik terbaik dalam penanggulangan kejahatan siber. Salah satu inisiatif utama adalah pembentukan ASEAN *Cybercrime Operations Working Group*, yang mempertemukan aparat penegak hukum dari berbagai negara anggota untuk mendiskusikan upaya kolektif dalam investigasi dan penuntutan pelaku kejahatan siber lintas negara. Kelompok kerja ini secara rutin melakukan pertemuan, pertukaran data intelijen, serta pelatihan bersama yang bertujuan untuk meningkatkan keterampilan teknis aparat penegak hukum, khususnya dalam hal pengumpulan dan analisis bukti digital, penelusuran jejak siber, dan pengamanan sistem digital.

Pada pelaksanaannya, kerja sama regional ini juga membahas pentingnya harmonisasi kerangka hukum di kawasan Asia Tenggara. Perbedaan dalam pendekatan regulasi, tingkat kesiapan teknis, dan kapasitas penegakan hukum antar negara dapat menjadi kendala dalam penanganan kasus kejahatan siber lintas negara. Oleh karena itu, ASEAN mendorong negara-negara anggotanya untuk mengadopsi kerangka hukum yang sejalan dengan norma internasional seperti Konvensi Budapest, meskipun tidak semua negara anggota menjadi pihak dalam konvensi tersebut. Tujuannya adalah untuk mempermudah proses ekstradisi, pertukaran informasi, dan penyidikan bersama dalam kasus-kasus yang melibatkan lebih dari satu yurisdiksi hukum.

ASEAN juga menekankan pentingnya pelibatan pemangku kepentingan lainnya seperti sektor swasta dan masyarakat sipil dalam penguatan ketahanan siber. Melalui program-program seperti ASEAN ICT Masterplan dan *ASEAN Digital Ministers' Meetings*, negara-negara anggota bersama-sama menyusun kebijakan yang mendukung pertumbuhan ekonomi digital yang aman dan berkelanjutan. Kolaborasi dengan perusahaan penyedia jasa internet, perusahaan teknologi, dan operator infrastruktur kritis sangat diperlukan untuk mendeteksi, mencegah, dan menanggulangi potensi serangan siber sejak dini. Di sisi lain, keterlibatan masyarakat sipil dan media juga penting dalam meningkatkan kesadaran publik terhadap risiko keamanan digital.

Sebagai bagian dari komunitas global, ASEAN juga menjalin kemitraan strategis dengan organisasi internasional seperti INTERPOL, ITU (*International Telecommunication Union*), dan *Asia-Pacific Computer Emergency Response Team* (APCERT). Melalui kemitraan ini, ASEAN memperoleh akses ke data intelijen global, teknologi mutakhir, dan model kebijakan yang dapat diadopsi secara kontekstual di kawasan Asia Tenggara. Selain itu, ASEAN turut mendirikan *ASEAN-Singapore Cybersecurity Centre of Excellence*, sebuah pusat pelatihan dan penelitian yang bertujuan untuk membekali negara anggota dengan pengetahuan teknis dan strategis dalam menangani kejahatan siber, termasuk melalui simulasi insiden, pelatihan penanganan insiden, dan pengembangan kebijakan berbasis risiko.

Inisiatif lain yang tak kalah penting adalah pembentukan pusat respons insiden siber (*Computer Emergency Response Teams*/CERTs) di setiap negara anggota ASEAN, yang kemudian terintegrasi dalam jaringan regional. Tujuan dari integrasi ini adalah untuk menciptakan

sistem deteksi dan respons yang cepat dan terkoordinasi dalam menghadapi serangan siber yang bersifat lintas negara. Mekanisme ini memungkinkan negara anggota untuk segera mengidentifikasi sumber serangan, menginformasikan pihak-pihak terkait, serta mengambil langkah mitigasi yang sesuai. CERT regional juga berperan sebagai pusat koordinasi dalam penyebaran peringatan dini dan pengumpulan bukti digital untuk keperluan forensik siber.

Keberhasilan ASEAN dalam menanggulangi kejahatan siber sangat bergantung pada tingkat komitmen dan kesiapan teknis setiap negara anggotanya. Perbedaan kapasitas infrastruktur, keterbatasan sumber daya manusia, dan tantangan politik domestik menjadi faktor yang dapat menghambat efektivitas kerja sama regional. Oleh karena itu, ASEAN terus mendorong investasi dalam pendidikan dan pelatihan keamanan siber, pembentukan unit siber nasional yang kuat, serta peningkatan alokasi anggaran untuk sistem teknologi informasi pemerintah. Dengan begitu, kesenjangan antara negara anggota dapat diperkecil dan sinergi kawasan dalam menghadapi ancaman siber dapat lebih maksimal.

ASEAN juga mempromosikan pendekatan inklusif dalam memperkuat ekosistem digital yang aman dan tangguh. Hal ini dilakukan melalui penyuluhan dan kampanye publik tentang pentingnya literasi digital, keamanan data pribadi, serta perlindungan terhadap anak-anak dan kelompok rentan di ruang digital. Kegiatan seperti ASEAN Cyber Kids Camp, lokakarya keamanan siber untuk UMKM, dan kampanye anti-*hoaks* menjadi bagian dari upaya membangun budaya keamanan digital yang berkelanjutan di tingkat masyarakat. Dengan pendekatan ini, ASEAN tidak hanya berfokus pada dimensi teknis dan hukum, tetapi juga membangun fondasi sosial yang kuat untuk mengurangi kerentanan terhadap kejahatan siber di masa depan.

D. Studi Kasus Kejahatan Siber di Berbagai Negara

1. Kasus Kejahatan Siber di Amerika Serikat

Amerika Serikat merupakan salah satu negara yang sering menjadi target kejahatan siber, mengingat statusnya sebagai negara dengan perkembangan teknologi informasi yang pesat dan tingkat ketergantungan yang tinggi terhadap sistem digital. Salah satu kasus paling terkenal adalah serangan *ransomware* pada sistem kesehatan di

kota Atlanta, Georgia, yang terjadi pada tahun 2018. Serangan ini dilakukan oleh kelompok peretas yang menggunakan *ransomware* SamSam, yang berhasil menyusup ke dalam sistem jaringan kota dan mengunci data penting, termasuk data rumah sakit dan sistem pelayanan publik lainnya. Akibatnya, banyak layanan yang terganggu, dan kota Atlanta harus mengeluarkan dana lebih dari $17 juta untuk memulihkan sistem dan data yang terpengaruh.

Kejahatan siber lainnya di Amerika Serikat adalah serangan terhadap perusahaan Equifax, yang terjadi pada tahun 2017. Kelompok peretas berhasil mengakses data pribadi lebih dari 147 juta warga Amerika, termasuk informasi keuangan dan nomor jaminan sosial. Ini merupakan salah satu kasus pelanggaran data terbesar dalam sejarah yang mengguncang kepercayaan masyarakat terhadap sistem perlindungan data pribadi di dunia maya. Dalam kasus ini, Equifax dihukum dengan denda besar dan diharuskan untuk membayar kompensasi kepada korban. Peran negara dalam kasus-kasus tersebut sangat signifikan, mengingat undang-undang perlindungan data dan regulasi kejahatan siber di AS yang sangat ketat, seperti The Computer Fraud and Abuse Act (CFAA) dan The Data Breach Notification Laws. Kejadian ini juga mendorong adanya peningkatan upaya mitigasi ancaman siber dan pengembangan kebijakan baru yang lebih kuat dalam hal perlindungan data pribadi.

2. Kasus Kejahatan Siber di China

China juga menjadi negara dengan jumlah kejahatan siber yang signifikan, terutama dalam kasus peretasan data besar-besaran dan pencurian hak kekayaan intelektual. Salah satu contoh utama adalah kasus peretasan oleh kelompok peretas China yang dikenal sebagai APT10, yang dikenal karena melakukan serangan terhadap berbagai sektor di Amerika Utara, Eropa, dan Jepang, termasuk perusahaan teknologi besar dan lembaga pemerintahan. Kelompok ini diduga terkait dengan pemerintah China dan diduga terlibat dalam pencurian data yang melibatkan informasi sensitif dan hak kekayaan intelektual dari berbagai sektor industri.

Di China sendiri, kejahatan siber seperti perdagangan ilegal data pribadi dan serangan terhadap sistem keuangan juga cukup tinggi. Salah satu peristiwa besar yang menarik perhatian dunia adalah serangan terhadap perusahaan teknologi besar seperti Alibaba dan Tencent, yang

berhasil mengekspos informasi pribadi jutaan pengguna. Kejahatan siber di China sering kali melibatkan pihak yang berhubungan dengan aktivitas spionase industri dan cyber espionage yang dilakukan oleh aktor negara untuk mencuri informasi penting dari pesaing internasional.

Untuk menghadapi kejahatan siber, China telah mengembangkan regulasi yang ketat terkait dengan keamanan dunia maya, termasuk *Cybersecurity Law of the People's Republic of China* (2017) yang mengatur pengamanan data dan sistem informasi, serta menanggulangi serangan terhadap infrastruktur kritis negara. Selain itu, China juga memanfaatkan berbagai teknologi canggih untuk mendeteksi dan mencegah ancaman siber lebih dini, serta memperkuat kolaborasi dengan negara-negara lain dalam menangani serangan global.

3. Kasus Kejahatan Siber di Estonia

Estonia menjadi salah satu negara yang paling sering disebut sebagai contoh sukses dalam hal keamanan siber nasional. Namun, negara ini juga pernah menjadi korban serangan siber besar-besaran pada tahun 2007, yang dikenal sebagai Estonian Cyberattacks. Pada serangan tersebut, berbagai situs pemerintah, bank, dan media di Estonia diserang dengan serangan DDoS (*Distributed Denial-of-Service*) yang menyebabkan gangguan signifikan terhadap layanan publik. Serangan ini dianggap sebagai salah satu serangan siber pertama yang berskala besar dan sangat terorganisir yang mengancam sebuah negara. Serangan ini diduga berasal dari kelompok yang pro-Rusia yang marah terhadap pemindahan monumen yang berhubungan dengan masa Soviet di Tallinn.

Serangan siber tersebut mengguncang banyak negara di dunia karena dampaknya yang luas terhadap sektor-sektor kritikal yang bergantung pada teknologi digital. Estonia, yang pada saat itu sudah memiliki *e-government system* yang sangat maju, melakukan langkah-langkah yang cepat untuk memperbaiki sistem dan memperkuat pertahanan siber nasionalnya. Sebagai tanggapan, Estonia memperkenalkan berbagai kebijakan baru terkait keamanan siber, termasuk penguatan sistem perlindungan data pribadi dan peningkatan kapasitas pertahanan siber di sektor publik dan swasta. Estonia juga menjadi anggota kunci dalam pengembangan *European Union Agency for Cybersecurity* (ENISA) dan berperan aktif dalam kerjasama internasional dalam penanggulangan kejahatan siber.

4. Kasus Kejahatan Siber di Rusia

Rusia merupakan salah satu negara yang sering dikaitkan dengan serangan siber yang didorong oleh motif politik dan spionase. Salah satu kasus yang paling terkenal adalah serangan terhadap pemilu Presiden Amerika Serikat pada tahun 2016 yang diduga melibatkan aktor negara Rusia. Serangan ini dilakukan dengan menggunakan *phishing*, pencurian data, dan pembocoran informasi yang ditujukan untuk mengganggu proses pemilihan dan mempengaruhi opini publik. Selain itu, Rusia juga sering dikaitkan dengan serangan *ransomware*, terutama yang dilakukan oleh kelompok peretas seperti Fancy Bear dan Cozy Bear, yang diduga memiliki hubungan dengan intelijen Rusia. Kelompok ini dikenal melakukan serangan terhadap organisasi internasional, lembaga pemerintah, dan perusahaan swasta dengan tujuan mencuri data sensitif dan mengakses informasi strategis.

Rusia memiliki undang-undang ketat mengenai kejahatan siber, seperti *The Federal Law on Information, Information Technology, and Information Protection* (2016), yang mengatur aspek perlindungan data, pengamanan infrastruktur digital, dan tanggung jawab pelaku serangan siber. Negara ini juga aktif terlibat dalam kerjasama internasional untuk mengatasi ancaman siber, meskipun terkadang menimbulkan ketegangan dengan negara-negara Barat. Melalui studi kasus kejahatan siber di berbagai negara ini, dapat terlihat bahwa kejahatan siber bukan hanya ancaman yang dihadapi oleh negara-negara maju, tetapi juga dapat menimpa negara-negara dengan sistem keamanan yang kuat sekalipun. Oleh karena itu, kerjasama internasional dan pengembangan kapasitas nasional menjadi kunci untuk menghadapi ancaman kejahatan siber yang terus berkembang.

BAB VII
KEJAHATAN SIBER DAN PERLINDUNGAN KORBAN

Kejahatan siber telah menjadi ancaman yang semakin besar di dunia digital saat ini, berdampak pada individu, perusahaan, hingga negara. Dengan pesatnya perkembangan teknologi dan adopsi internet dalam berbagai aspek kehidupan, kejahatan siber, seperti peretasan, penipuan online, dan pencurian data pribadi, semakin mudah dilakukan dan semakin sulit untuk diatasi. Korban dari kejahatan ini sering kali mengalami kerugian finansial yang besar, kerusakan reputasi, serta gangguan terhadap kehidupan pribadi dan profesional. Meskipun regulasi dan teknologi perlindungan telah berkembang, banyak korban yang masih merasa kesulitan dalam mencari perlindungan dan keadilan, terutama terkait dengan pembuktian dan pemulihan kerugian yang dialami. Hal ini menunjukkan perlunya upaya yang lebih besar untuk melindungi korban kejahatan siber, baik melalui penegakan hukum yang lebih tegas, penguatan regulasi, maupun peningkatan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi dan keamanan digital. Keberhasilan dalam menangani kejahatan siber tidak hanya bergantung pada teknologi dan kebijakan yang ada, tetapi juga pada bagaimana sistem hukum dan masyarakat dapat bekerja sama untuk memberikan perlindungan yang efektif bagi korban.

A. Hak-Hak Korban Kejahatan Siber

1. Hak atas Pemulihan dan Kompensasi

Pada konteks kejahatan siber yang kian meningkat, hak atas pemulihan dan kompensasi menjadi aspek penting dalam perlindungan terhadap korban. Kejahatan siber tidak hanya menimbulkan kerugian secara ekonomi, tetapi juga berimplikasi terhadap kondisi psikologis,

sosial, dan reputasi individu atau entitas yang terdampak. Korban sering kali kehilangan data, informasi pribadi, dan aset digital yang bernilai tinggi akibat aktivitas ilegal seperti peretasan, penipuan daring, dan pencurian identitas. Oleh karena itu, sistem hukum nasional dan internasional dituntut untuk menyediakan mekanisme yang memadai guna menjamin bahwa para korban mendapatkan hak-haknya secara utuh, termasuk dalam bentuk pengembalian kerugian dan pemulihan kondisi pasca-kejahatan.

Salah satu kerangka internasional yang secara eksplisit mengakui hak korban atas pemulihan dan kompensasi adalah Convention on *Cybercrime* dari Dewan Eropa tahun 2001. Meskipun konvensi ini lebih banyak mengatur tentang standar kriminalisasi dan kerja sama internasional dalam penanggulangan *cybercrime*, namun konvensi ini juga mendorong negara-negara pihak untuk membentuk mekanisme hukum domestik yang mampu menjamin perlindungan terhadap korban, termasuk restitusi dan kompensasi. Di samping itu, *United Nations Office on Drugs and Crime* (UNODC) dalam laporan tahun 2013 menekankan bahwa restitusi, kompensasi, dan rehabilitasi adalah bagian integral dari sistem peradilan yang adil dan inklusif. UNODC menyatakan bahwa pemulihan korban harus mencakup pemulihan finansial, pemulihan hak hukum, serta pemulihan sosial dan psikologis, terutama bagi korban yang mengalami trauma berat akibat eksploitasi digital.

Di Indonesia, regulasi yang menjamin hak korban atas pemulihan dari kejahatan siber dapat ditemukan dalam beberapa peraturan perundang-undangan. Salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016. Dalam pasal-pasalnya, UU ITE mengatur bahwa korban yang mengalami kerugian akibat penyalahgunaan data elektronik atau pelanggaran sistem informasi berhak untuk mengajukan permohonan pemulihan berupa pengembalian aset atau barang digital yang hilang. Selain itu, terdapat pula pengaturan tentang penyelesaian sengketa melalui mediasi, yang memberikan jalur alternatif untuk korban mendapatkan ganti rugi secara lebih cepat dan efisien di luar proses peradilan yang panjang dan rumit.

Mekanisme kompensasi korban juga mendapat penguatan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam pasal 97, undang-undang ini menyatakan bahwa

setiap orang yang mengalami kerugian akibat pelanggaran data pribadi berhak untuk memperoleh ganti rugi. Regulasi ini sangat penting dalam konteks kejahatan siber, mengingat banyaknya kasus kebocoran data yang menimbulkan kerugian besar, baik secara ekonomi maupun reputasi. Selain itu, undang-undang ini mewajibkan pengendali data untuk bertanggung jawab atas pengelolaan dan pengamanan data pribadi, sehingga jika terjadi pelanggaran, korban dapat menuntut ganti rugi sesuai dengan tingkat kerugian yang dialaminya. Langkah ini mencerminkan upaya negara untuk menyeimbangkan dinamika teknologi digital dengan perlindungan hak-hak individu di ruang siber.

Implementasi hak atas pemulihan dan kompensasi bagi korban kejahatan siber di Indonesia masih menghadapi berbagai tantangan serius. Pertama adalah rendahnya kesadaran korban terhadap hak-hak hukum yang dimiliki. Banyak korban yang tidak mengetahui bahwa dapat menuntut ganti rugi atau tidak memahami prosedur hukum yang harus ditempuh untuk mengajukan klaim kompensasi. Hal ini diperburuk dengan minimnya layanan bantuan hukum yang secara khusus menangani kasus-kasus kejahatan siber. Kedua, sistem peradilan di Indonesia masih cenderung lambat dalam memproses kasus kejahatan siber, terutama yang melibatkan bukti digital yang kompleks dan pelaku yang berada di luar yurisdiksi nasional. Akibatnya, proses pemulihan sering kali berjalan lambat dan tidak efektif bagi korban yang mengharapkan penyelesaian cepat.

Kendala lainnya adalah terbatasnya kapasitas lembaga penegak hukum dan lembaga keuangan dalam mengeksekusi putusan ganti rugi. Dalam banyak kasus, pelaku kejahatan siber menggunakan metode pencucian uang yang kompleks dan menyembunyikan aset hasil kejahatan di berbagai negara. Hal ini menyulitkan aparat penegak hukum untuk melacak dan menyita aset tersebut sebagai bagian dari restitusi kepada korban. Menurut Wall (2007), efektivitas pemulihan korban sangat bergantung pada keberadaan sistem yang terintegrasi antara lembaga peradilan, perbankan, dan otoritas keamanan siber. Tanpa koordinasi yang baik di antaranya, hak korban untuk mendapatkan kompensasi akan sulit direalisasikan meskipun putusan hukum telah dikeluarkan.

Untuk mengatasi hambatan tersebut, dibutuhkan langkah strategis dalam memperkuat regulasi dan prosedur pemulihan bagi korban kejahatan siber. Pemerintah perlu membentuk mekanisme yang

jelas dan mudah diakses untuk pengajuan klaim ganti rugi, termasuk penyediaan portal daring yang memungkinkan korban untuk melaporkan insiden dan menelusuri status kasus secara transparan. Layanan ini harus didukung oleh unit khusus di kepolisian, kejaksaan, dan peradilan yang dilengkapi dengan keahlian digital forensik dan hukum siber. Selain itu, perlu adanya insentif bagi sektor swasta seperti perbankan dan perusahaan teknologi untuk ikut serta dalam pemulihan korban melalui kemitraan publik-swasta dalam mendeteksi dan memulihkan aset korban.

Penting pula dilakukan upaya sosialisasi secara masif terkait hak-hak korban kejahatan siber melalui media digital, pendidikan, dan penyuluhan masyarakat. Pemerintah bersama dengan organisasi masyarakat sipil, akademisi, dan sektor swasta dapat menyusun modul edukasi tentang langkah-langkah yang harus diambil korban sejak insiden pertama terjadi hingga tahap pengajuan kompensasi. Edukasi ini tidak hanya bertujuan untuk meningkatkan kesadaran hukum masyarakat, tetapi juga membentuk budaya keamanan digital yang bertanggung jawab. Di samping itu, pendampingan psikologis juga harus disediakan, terutama bagi korban kejahatan siber yang mengalami tekanan mental berat akibat pencemaran nama baik, ancaman, atau eksploitasi seksual melalui teknologi.

Reformasi hukum yang komprehensif perlu dilengkapi dengan kerja sama internasional dalam penelusuran dan pemulihan aset lintas negara. Mengingat kejahatan siber sering kali dilakukan secara transnasional, dibutuhkan kesepakatan bilateral dan multilateral yang memungkinkan pertukaran informasi, ekstradisi pelaku, serta pengembalian aset kepada korban secara efisien. Indonesia dapat mengacu pada praktik-praktik internasional terbaik yang telah diterapkan oleh negara-negara anggota Uni Eropa atau negara-negara OECD yang memiliki pengalaman panjang dalam implementasi hak korban. Dengan memperkuat posisi korban dalam sistem hukum dan menjadikan pemulihan sebagai bagian sentral dalam penegakan keadilan, maka sistem peradilan pidana akan semakin inklusif dan berorientasi pada perlindungan korban.

Dengan demikian, hak atas pemulihan dan kompensasi bukan hanya menjadi kewajiban hukum negara, tetapi juga mencerminkan komitmen terhadap nilai-nilai keadilan dan kemanusiaan dalam era digital. Kejahatan siber sebagai tantangan baru dalam penegakan hukum

harus direspons dengan pendekatan holistik yang menempatkan korban sebagai subjek utama perlindungan hukum. Negara tidak cukup hanya memproses pelaku ke pengadilan, tetapi juga harus memastikan bahwa korban mendapatkan keadilan secara substantif melalui pemulihan atas kerugian yang dideritanya. Di masa depan, penguatan sistem kompensasi ini akan menjadi indikator penting dalam mengukur kualitas tata kelola keamanan digital dan sistem peradilan pidana yang adaptif terhadap dinamika kejahatan modern.

2. Hak atas Perlindungan Data Pribadi dan Privasi

Pada lanskap digital yang terus berkembang, kejahatan siber telah menjadi ancaman nyata terhadap hak-hak dasar manusia, khususnya hak atas perlindungan data pribadi dan privasi. Kejahatan siber seperti peretasan akun, pencurian identitas, serta kebocoran data pribadi bukan hanya menyebabkan kerugian finansial, tetapi juga berdampak pada martabat, keamanan, dan kenyamanan psikologis individu. Privasi yang dulunya dianggap sebagai hak yang bersifat pribadi kini menjadi bagian dari isu global yang memerlukan perhatian serius dari pemerintah, pelaku usaha, dan masyarakat luas. Dalam konteks ini, korban kejahatan siber harus diakui sebagai pihak yang memiliki hak hukum yang kuat untuk melindungi integritas data dan identitas pribadinya dari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Indonesia melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengambil langkah signifikan dalam memperkuat perlindungan terhadap hak individu atas data pribadi. UU ini memuat berbagai ketentuan yang memberikan hak langsung kepada subjek data, yaitu individu yang datanya dikumpulkan dan digunakan, untuk mengontrol bagaimana datanya dikelola. Dalam Pasal 15 hingga Pasal 18, subjek data memiliki hak untuk meminta penghapusan data (*right to erasure*), pembetulan data jika terdapat kekeliruan, serta pembatasan pemrosesan data jika dilakukan tanpa dasar hukum yang sah. Hak-hak ini bersifat restoratif, artinya bertujuan untuk mengembalikan kendali atas informasi pribadi kepada individu, terutama ketika menjadi korban kejahatan siber.

Kejahatan siber sering kali memanfaatkan data pribadi yang bocor untuk melakukan penipuan identitas, pemerasan, hingga kekerasan berbasis digital seperti *doxing* dan pelecehan daring. Dalam kasus-kasus

seperti ini, perlindungan data tidak cukup hanya pada aspek teknis atau administratif, tetapi harus pula menjangkau aspek hukum dan psikososial korban. Oleh karena itu, ketentuan dalam UU PDP menjadi penting sebagai payung hukum yang memberikan dasar legal bagi korban untuk menuntut hak-haknya, termasuk untuk menolak pemrosesan data lebih lanjut dan meminta transparansi mengenai siapa saja yang telah mengakses datanya. Hak ini diperkuat pula dengan kewajiban pengendali data untuk memperoleh persetujuan eksplisit sebelum memproses data pribadi, sebagaimana diatur dalam Pasal 20 dan Pasal 21 UU PDP.

Regulasi internasional juga memberikan pengakuan dan perlindungan yang luas terhadap hak atas data pribadi dan privasi. Salah satu instrumen penting adalah *General Data Protection Regulation* (GDPR) yang diberlakukan oleh Uni Eropa sejak 2018. GDPR menetapkan standar tinggi dalam perlindungan data pribadi, termasuk kewajiban pelaku pemrosesan data untuk melaporkan setiap insiden kebocoran data kepada otoritas pengawas dan individu yang terkena dampaknya dalam waktu maksimal 72 jam. Meskipun Indonesia belum menetapkan tenggat waktu serupa, Pasal 59 UU PDP tetap mewajibkan pengendali data untuk memberitahukan secara segera kepada subjek data jika terjadi kebocoran yang berpotensi menimbulkan kerugian. Kewajiban ini menunjukkan adanya keselarasan prinsip antara Indonesia dan kerangka hukum internasional mengenai pentingnya transparansi dan akuntabilitas dalam pengelolaan data pribadi.

Aspek penegakan hak privasi juga berkaitan erat dengan tanggung jawab penyedia layanan digital. Banyak kejahatan siber terjadi melalui platform daring yang gagal melindungi data pengguna secara memadai. Dalam Konvensi Budapest tentang Kejahatan Siber (Council of Europe, 2001), terdapat ketentuan yang mendorong negara dan penyedia jasa untuk menjaga kerahasiaan serta integritas data yang dikumpulkan dan disimpan dalam sistemnya. Konvensi ini menekankan perlunya penerapan langkah-langkah teknis dan administratif untuk mencegah akses tidak sah dan penyalahgunaan data. Dengan mengadopsi prinsip-prinsip ini, Indonesia diharapkan mampu memperkuat perlindungan terhadap korban kejahatan siber yang datanya telah terekspos akibat kelalaian atau kegagalan sistem penyedia layanan.

Aspek penting lainnya adalah hak korban untuk mendapatkan informasi yang jelas dan lengkap mengenai bagaimana datanya

digunakan dan siapa saja yang memiliki akses terhadapnya. Menurut UNODC (2013), korban kejahatan siber memiliki hak untuk menuntut transparansi dari pengendali data dan pihak ketiga yang memanfaatkan data tersebut. Informasi ini penting untuk menentukan sejauh mana pelanggaran telah terjadi serta untuk memperkuat posisi hukum korban dalam proses tuntutan ganti rugi. Dalam konteks Indonesia, hak atas informasi ini juga dapat digunakan untuk mendorong audit forensik terhadap sistem keamanan data yang bocor, sehingga korban memiliki bukti kuat untuk mendesak pertanggungjawaban dari pihak yang lalai menjaga datanya.

Pada tahap penyidikan dan persidangan, penting bagi sistem hukum untuk memastikan bahwa identitas dan data pribadi korban tetap terlindungi. Banyak korban enggan melapor karena takut identitas terbongkar dan menjadi sasaran intimidasi atau stigma sosial. Dalam penanganan kasus kejahatan siber, penyidik dan jaksa harus menerapkan prinsip perlindungan privasi korban, termasuk dengan menyunting (redaksi) data yang bersifat sensitif sebelum disampaikan kepada publik atau dalam berkas persidangan. Casey (2011) menekankan pentingnya menjaga privasi korban dalam proses digital forensics, karena pengungkapan informasi secara berlebihan dapat merugikan korban lebih lanjut dan melemahkan kepercayaan publik terhadap sistem peradilan.

Untuk itu, diperlukan sistem yang terintegrasi antara lembaga perlindungan data, penegak hukum, dan pengadilan agar perlindungan privasi korban dapat dilakukan secara konsisten. Peran lembaga seperti Otoritas Perlindungan Data (yang akan dibentuk sesuai amanat UU PDP) menjadi sangat krusial dalam mengawasi kepatuhan pengendali data terhadap kewajiban hukum dan menangani pengaduan dari korban kejahatan siber. Selain itu, diperlukan pelatihan khusus bagi aparat penegak hukum dalam menangani kasus pelanggaran privasi dan data pribadi, mengingat kompleksitas teknis dan hukum yang menyertai kasus-kasus ini. Dengan begitu, korban akan merasa lebih aman dan yakin bahwa hak-hak privasinya dihargai dan dilindungi oleh negara.

Di samping perlindungan hukum, pendekatan berbasis edukasi juga penting dalam meningkatkan kesadaran masyarakat tentang pentingnya privasi dan pengelolaan data pribadi. Banyak kasus kejahatan siber terjadi karena rendahnya literasi digital masyarakat, yang dengan mudah membagikan informasi sensitif tanpa memahami risikonya.

Pemerintah dan organisasi masyarakat sipil dapat bekerja sama dalam menyediakan materi edukasi dan kampanye kesadaran publik tentang hak atas data pribadi, cara menghindari penyalahgunaan data, serta langkah-langkah yang harus dilakukan ketika datanya bocor. Pendekatan preventif ini sangat penting untuk membentuk budaya digital yang menghormati hak-hak individu sekaligus memperkuat sistem keamanan nasional.

Hak atas perlindungan data pribadi dan privasi bagi korban kejahatan siber harus diakui sebagai bagian dari hak asasi manusia yang esensial dalam era digital. Tanpa perlindungan yang memadai, korban tidak hanya menanggung kerugian material, tetapi juga risiko trauma, isolasi sosial, dan gangguan psikologis yang mendalam. Oleh karena itu, peran negara menjadi sangat penting untuk memastikan bahwa hukum dan kebijakan yang ada benar-benar berpihak kepada korban. Dalam jangka panjang, penguatan perlindungan data pribadi akan menjadi fondasi penting bagi terciptanya ekosistem digital yang adil, aman, dan terpercaya. Dengan melindungi privasi korban, negara menunjukkan komitmennya dalam menjaga martabat manusia di tengah derasnya arus transformasi digital.

B. Perlindungan Data Pribadi dan Keamanan Digital

1. Pentingnya Perlindungan Data Pribadi dalam Era Digital

Di era digital yang terus berkembang dengan cepat, perlindungan data pribadi telah menjadi kebutuhan mendasar yang tak terelakkan. Masyarakat saat ini sangat bergantung pada teknologi untuk menjalankan berbagai aspek kehidupan, mulai dari komunikasi, transaksi keuangan, pendidikan, hingga layanan kesehatan. Ketergantungan ini telah menyebabkan data pribadi termasuk nama, alamat, nomor identitas, riwayat kesehatan, preferensi konsumen, dan informasi keuangan terkumpul dan tersimpan di berbagai platform digital. Data ini tidak hanya memiliki nilai ekonomi yang tinggi di pasar gelap siber, tetapi juga menjadi sasaran utama bagi pelaku kejahatan digital. Pencurian data pribadi tidak hanya merugikan individu dari sisi finansial, melainkan juga mengancam hak atas privasi dan keamanan secara menyeluruh, bahkan dapat mengarah pada pemerasan atau penyalahgunaan yang lebih kompleks.

Fenomena pencurian data pribadi telah menjadi salah satu bentuk kejahatan siber yang paling umum dan merusak. Pelaku kejahatan menggunakan berbagai metode seperti *phishing*, *malware*, hingga manipulasi sosial (*social engineering*) untuk mendapatkan akses tidak sah terhadap informasi sensitif. Dalam laporan European Commission (2020), disebutkan bahwa insiden kebocoran data dapat menimbulkan dampak yang luas, termasuk penipuan identitas yang membuat korban harus menghadapi konsekuensi hukum dan finansial yang tidak diperbuat. Data yang bocor juga dapat digunakan untuk membuat akun palsu, mengajukan kredit tanpa sepengetahuan korban, atau menyebarkan informasi palsu yang merusak reputasi korban. Oleh karena itu, perlindungan terhadap data pribadi tidak hanya bersifat administratif, tetapi juga menyangkut hak dasar manusia atas rasa aman dan kendali terhadap identitasnya.

Pentingnya perlindungan data pribadi dalam konteks ini telah mendorong lahirnya kebijakan hukum yang semakin ketat di berbagai negara. Uni Eropa, misalnya, telah memberlakukan *General Data Protection Regulation* (GDPR) sejak 2018 sebagai respons terhadap meningkatnya risiko terhadap data pribadi di era digital. GDPR memberikan individu berbagai hak, termasuk hak untuk mengetahui bagaimana datanya digunakan, hak untuk meminta penghapusan data, serta hak untuk mengajukan keberatan atas pemrosesan datanya. Selain itu, GDPR mewajibkan institusi yang mengelola data untuk menerapkan langkah-langkah keamanan yang ketat dan memberikan sanksi tegas bagi pelanggaran. Ketentuan ini menjadi standar global yang mendorong negara-negara lain, termasuk Indonesia, untuk menyusun peraturan serupa.

Indonesia melalui Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah menunjukkan komitmen yang sama dalam memperkuat hak-hak individu atas data pribadi. UU ini mengatur prinsip-prinsip dasar pengelolaan data, seperti keabsahan dasar hukum pengumpulan data, transparansi dalam pemrosesan, dan kewajiban pengendali data untuk menjaga kerahasiaan serta integritas data pribadi. Dalam Pasal 5 hingga Pasal 11, ditegaskan bahwa individu sebagai subjek data memiliki hak atas akses, pembetulan, penghapusan, serta penarikan persetujuan atas penggunaan datanya. Kehadiran UU ini memberikan pijakan hukum yang lebih kuat bagi masyarakat dalam

menuntut perlindungan dan keadilan ketika terjadi pelanggaran terhadap hak data pribadinya.

Di tengah berbagai regulasi yang telah diterapkan, tantangan terhadap perlindungan data pribadi tidak serta-merta hilang. Perkembangan teknologi yang sangat cepat sering kali melampaui kecepatan adaptasi hukum dan regulasi. Sistem kecerdasan buatan, *Internet of Things* (IoT), dan big data menjadi teknologi baru yang menyimpan potensi risiko baru terhadap pelanggaran data pribadi. Banyak perusahaan dan institusi masih belum memiliki sistem keamanan yang memadai, serta prosedur standar dalam menangani insiden kebocoran data. Tidak jarang pula perusahaan lalai memberi pemberitahuan kepada korban ketika terjadi kebocoran, sehingga individu tidak memiliki waktu yang cukup untuk mengambil tindakan mitigasi. Hal ini memperlihatkan bahwa perlindungan data pribadi tidak hanya tergantung pada keberadaan hukum, tetapi juga pada komitmen dan kapabilitas institusi dalam menegakkan hukum tersebut secara konsisten.

Aspek lain yang tidak kalah penting adalah perlunya kesadaran dan literasi digital di tingkat individu. Banyak kasus kebocoran data terjadi akibat kurangnya kewaspadaan masyarakat dalam menjaga informasi pribadinya di ruang digital. Penggunaan kata sandi yang lemah, kecenderungan membagikan informasi sensitif secara terbuka di media sosial, serta kebiasaan mengklik tautan yang tidak dikenal merupakan beberapa contoh kelalaian individu yang dapat dimanfaatkan oleh pelaku kejahatan siber. Oleh karena itu, pemerintah dan sektor swasta harus berperan aktif dalam memberikan edukasi publik tentang pentingnya perlindungan data pribadi. Kampanye kesadaran, pelatihan literasi digital, dan panduan praktis tentang keamanan siber menjadi langkah penting dalam membangun masyarakat yang tangguh secara digital.

Perlu adanya sinergi antara institusi pemerintah, pelaku industri, serta lembaga penegak hukum dalam menanggulangi pelanggaran terhadap data pribadi. Pengawasan terhadap praktik pengumpulan dan penggunaan data oleh perusahaan teknologi perlu diperketat, terutama dalam hal transparansi dan akuntabilitas. Di sisi lain, penegakan hukum terhadap pelaku kejahatan siber harus diperkuat dengan dukungan infrastruktur digital forensik dan peraturan peradilan yang relevan. Lembaga perlindungan data yang independen dan memiliki kewenangan

kuat menjadi pilar penting dalam mengawasi pelaksanaan UU PDP serta menangani pengaduan dari masyarakat. Tanpa sistem pengawasan yang efektif, perlindungan data pribadi hanya akan menjadi wacana tanpa implementasi nyata di lapangan.

Pada konteks global, kerja sama internasional juga menjadi faktor penting dalam menangani pelanggaran data pribadi lintas negara. Kejahatan siber sering kali dilakukan oleh pelaku dari yurisdiksi yang berbeda, sehingga memerlukan mekanisme kerja sama antarnegara untuk proses penyelidikan, penuntutan, dan pemulihan data. Konvensi seperti *Budapest Convention on Cybercrime* menjadi kerangka kerja internasional yang dapat dijadikan acuan bagi negara-negara, termasuk Indonesia, untuk memperkuat kolaborasi dalam pemberantasan kejahatan siber. Dengan adanya kolaborasi ini, negara dapat bertukar informasi, menyelaraskan standar hukum, serta meningkatkan kapasitas penegakan hukum untuk melindungi data pribadi warganya secara lebih efektif dan terpadu.

Di masa depan, perlindungan data pribadi akan menjadi salah satu indikator utama dalam menciptakan kepercayaan publik terhadap teknologi dan transformasi digital. Jika masyarakat merasa aman dan yakin bahwa datanya dikelola dengan baik, maka partisipasi dalam ekosistem digital akan meningkat. Sebaliknya, kegagalan dalam memberikan jaminan perlindungan dapat merusak kredibilitas sistem digital dan menurunkan kualitas demokrasi digital. Oleh karena itu, perlindungan data pribadi tidak boleh hanya dipandang sebagai kewajiban hukum, tetapi sebagai bagian dari komitmen etis dan sosial untuk menjaga martabat manusia dalam dunia yang semakin terdigitalisasi. Negara, sektor swasta, dan masyarakat sipil memiliki tanggung jawab bersama dalam memastikan bahwa transformasi digital yang berlangsung tidak mengorbankan hak fundamental atas privasi dan keamanan data pribadi.

2. Keamanan Digital dalam Menghadapi Kejahatan Siber

Untuk menghadapi era digital yang sarat dengan potensi ancaman siber, keamanan digital menjadi elemen yang semakin vital dalam menjaga keberlangsungan sistem informasi serta perlindungan data pribadi. Keamanan digital bukan hanya merupakan aspek teknis yang terbatas pada perangkat lunak atau perangkat keras, tetapi juga merupakan kerangka komprehensif yang mencakup kebijakan, prosedur,

serta perilaku yang bertujuan untuk mencegah, mendeteksi, dan merespons setiap bentuk pelanggaran keamanan informasi. Dalam konteks ini, penting untuk memahami bahwa kejahatan siber tidak mengenal batas geografis dan dapat menyerang siapa saja mulai dari individu, pelaku bisnis, hingga lembaga pemerintah. Oleh sebab itu, penguatan sistem keamanan digital bukan hanya menjadi tanggung jawab sektor teknologi informasi, melainkan juga harus melibatkan kesadaran dan partisipasi aktif dari seluruh lapisan masyarakat.

Salah satu fondasi dari keamanan digital modern adalah teknik enkripsi yang berfungsi mengamankan data dari akses tidak sah. Enkripsi bekerja dengan mengubah informasi dalam bentuk plaintext menjadi ciphertext, format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Penggunaan teknologi enkripsi telah menjadi standar dalam transaksi online, khususnya dalam sektor perbankan dan e-commerce, untuk melindungi informasi kartu kredit, identitas pengguna, dan riwayat transaksi dari peretas. Protokol keamanan seperti *Secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS) merupakan contoh penerapan enkripsi yang menjamin bahwa komunikasi antara pengguna dan server tetap aman dari intersepsi pihak ketiga. Seiring dengan berkembangnya teknologi, sistem enkripsi kini juga diterapkan pada penyimpanan cloud dan komunikasi pribadi, seperti dalam layanan pesan instan *end-to-end encryption*.

Penggunaan firewall juga menjadi komponen penting dalam arsitektur keamanan digital. Firewall berfungsi sebagai penghalang yang memantau dan mengendalikan lalu lintas jaringan berdasarkan aturan keamanan yang telah ditetapkan. Dengan menggunakan firewall, pengguna dapat mencegah akses ilegal atau mencurigakan yang mencoba masuk ke dalam sistem komputer atau jaringan internal. Firewall dapat berbentuk perangkat keras maupun perangkat lunak dan biasanya dikombinasikan dengan sistem deteksi intrusi (*Intrusion Detection Systems*/IDS) serta sistem pencegahan intrusi (*Intrusion Prevention Systems*/IPS). Ketiga elemen ini bekerja secara sinergis untuk menciptakan benteng pertahanan yang mampu melindungi data dan sistem dari berbagai macam serangan siber, mulai dari *malware* hingga serangan *Distributed Denial of Service* (DDoS).

Di Indonesia, upaya penguatan keamanan digital mendapat dukungan dari Badan Siber dan Sandi Negara (BSSN), sebuah institusi yang bertugas menyusun kebijakan dan strategi nasional dalam rangka

perlindungan terhadap aset digital negara. BSSN telah melakukan berbagai inisiatif, termasuk penyusunan pedoman keamanan informasi bagi instansi pemerintah dan swasta, kampanye literasi keamanan siber kepada masyarakat, serta pelatihan profesional di bidang keamanan informasi. BSSN juga bekerja sama dengan berbagai pihak, termasuk sektor swasta dan komunitas teknologi, untuk memperkuat deteksi dini dan respons cepat terhadap insiden siber yang berpotensi mengganggu stabilitas nasional. Peran strategis BSSN ini sangat krusial, terutama dalam menghadapi ancaman terhadap infrastruktur kritis seperti sektor energi, kesehatan, keuangan, dan transportasi.

Meski demikian, tantangan keamanan digital tidak berhenti pada tataran teknologi atau kelembagaan saja. Ancaman siber terus berevolusi, baik dari sisi metode maupun skala serangan. Serangan *ransomware* yang mengenkripsi seluruh data korban dan meminta tebusan dalam bentuk cryptocurrency, serta eksploitasi *zero-day vulnerabilities* yang memanfaatkan celah keamanan yang belum diketahui oleh vendor, merupakan bentuk serangan canggih yang membutuhkan pendekatan pengamanan yang adaptif dan berbasis pada kecerdasan buatan serta machine learning. Serangan-serangan ini tidak hanya menyebabkan kerugian finansial, tetapi juga dapat mengganggu operasional secara luas, bahkan menimbulkan dampak sosial dan politik jika menyerang sistem pemerintahan atau layanan publik vital.

Peran regulasi dalam penguatan keamanan digital menjadi sangat penting. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan dasar hukum bagi pengelolaan data dan perlindungan pengguna dari sisi privasi. Namun, penguatan hukum terhadap pelaku kejahatan siber juga harus dibarengi dengan pembentukan lembaga penegak hukum yang memiliki kemampuan teknis dan kapasitas digital forensik yang mumpuni. Penegakan hukum yang efektif akan menciptakan efek jera dan menjadi pencegah terhadap meningkatnya kasus-kasus kejahatan digital. Selain itu, pengadilan juga perlu diberikan kapasitas dan pemahaman terhadap karakteristik teknis kejahatan siber, sehingga proses hukum dapat berjalan dengan adil dan akurat.

Sektor swasta, sebagai pengelola sebagian besar data digital masyarakat, juga memiliki tanggung jawab besar dalam menjaga keamanan sistem dan informasi pengguna. Banyak kasus kebocoran data besar berasal dari kelalaian atau lemahnya sistem keamanan yang

dimiliki oleh perusahaan. Oleh karena itu, perusahaan wajib menerapkan prinsip-prinsip keamanan informasi berbasis ISO 27001 atau kerangka kerja keamanan lainnya yang relevan. Langkah-langkah seperti audit keamanan rutin, pemantauan sistem secara real-time, pelatihan keamanan bagi karyawan, dan manajemen risiko berbasis teknologi harus menjadi bagian integral dari kebijakan perusahaan. Kegagalan dalam melaksanakan tanggung jawab ini tidak hanya akan berdampak pada kerugian finansial, tetapi juga dapat merusak reputasi serta kepercayaan konsumen terhadap layanan yang diberikan.

Tidak ada sistem keamanan yang benar-benar kebal terhadap serangan. Oleh karena itu, pendekatan manajemen risiko menjadi sangat penting dalam perencanaan keamanan digital. Setiap institusi harus memiliki strategi mitigasi risiko, rencana tanggap darurat, serta kebijakan pemulihan bencana (*disaster recovery*) jika terjadi insiden siber. Perusahaan dan lembaga pemerintah harus melakukan simulasi keamanan secara berkala untuk menguji kesiapannya dalam merespons insiden nyata. Dalam banyak kasus, waktu respons yang cepat dan koordinasi yang efektif dapat meminimalisir dampak dari serangan siber dan mempercepat pemulihan sistem.

Kesadaran masyarakat juga merupakan faktor penentu keberhasilan dalam membangun lingkungan digital yang aman. Pendidikan dan literasi keamanan digital harus diperkuat sejak usia dini, termasuk dalam kurikulum pendidikan formal dan program pelatihan nonformal. Masyarakat perlu diberikan pemahaman mengenai pentingnya menjaga informasi pribadi, mengenali modus kejahatan siber, serta cara melaporkan insiden yang dialami. Pemerintah, bersama sektor swasta dan media, harus aktif dalam menyebarluaskan informasi mengenai ancaman siber dan langkah-langkah perlindungan yang dapat diambil secara mandiri. Kolaborasi multisektor ini merupakan pendekatan yang holistik dalam menciptakan ketahanan digital nasional yang tangguh.

Keamanan digital bukanlah tujuan akhir, melainkan proses berkelanjutan yang memerlukan pembaruan strategi, teknologi, dan kolaborasi yang dinamis. Ancaman siber akan terus berkembang seiring dengan inovasi teknologi, sehingga kemampuan adaptasi dan kesiapan sistem menjadi kunci utama dalam mempertahankan integritas digital. Indonesia sebagai negara dengan populasi digital yang besar harus menjadikan keamanan digital sebagai prioritas strategis nasional.

Dengan penguatan regulasi, teknologi, dan kesadaran kolektif, keamanan digital dapat diwujudkan sebagai fondasi utama untuk mendukung transformasi digital yang inklusif, adil, dan berkelanjutan di masa depan.

C. Mekanisme Pengaduan dan Bantuan Hukum bagi Korban

1. Mekanisme Pengaduan Tindak Pidana Siber di Indonesia

Di era digital yang semakin kompleks, kejahatan siber menjadi tantangan besar bagi sistem hukum dan penegakan keadilan di Indonesia. Berbagai bentuk tindak pidana yang terjadi di dunia maya, seperti pencemaran nama baik, penyebaran informasi palsu, pencurian identitas, dan peretasan data pribadi, telah meresahkan masyarakat dan menimbulkan kerugian yang signifikan. Oleh karena itu, mekanisme pengaduan yang efektif dan mudah diakses menjadi sangat penting bagi para korban kejahatan siber agar dapat memperoleh keadilan. Pemerintah Indonesia telah merespons kebutuhan ini dengan membentuk jalur hukum formal dan nonformal yang dapat dimanfaatkan oleh masyarakat. Keberadaan saluran pengaduan ini merupakan langkah maju dalam memberikan perlindungan hukum terhadap individu yang menjadi korban tindak pidana siber.

Secara umum, korban tindak pidana siber dapat melaporkan kejadian yang dialami ke Kepolisian Negara Republik Indonesia. Laporan ini biasanya diajukan ke unit khusus yang menangani kejahatan siber, yaitu Direktorat Tindak Pidana Siber (Dittipidsiber) yang berada di bawah Badan Reserse Kriminal (Bareskrim) Polri. Dalam proses pelaporan, korban diharuskan membawa bukti-bukti digital yang relevan untuk mendukung laporannya. Bukti tersebut bisa berupa tangkapan layar (*screenshot*), rekaman percakapan, dokumen transaksi digital, tautan internet, maupun log aktivitas yang menunjukkan terjadinya tindak pidana. Penyusunan bukti ini menjadi tantangan tersendiri karena tidak semua korban memahami format dan validitas data digital yang diperlukan dalam sistem hukum.

Di samping mekanisme konvensional melalui kantor polisi, pemerintah Indonesia juga menyediakan layanan daring yang memungkinkan masyarakat melaporkan tindak pidana siber secara digital. Salah satunya adalah platform lapor.go.id yang dikembangkan oleh Kementerian Pendayagunaan Aparatur Negara dan Reformasi

Birokrasi (KemenPAN-RB) bekerja sama dengan Ombudsman Republik Indonesia dan Unit Kerja Presiden bidang Pengawasan dan Pengendalian Pembangunan (UKP4). Melalui layanan ini, masyarakat dapat menyampaikan keluhan atau laporan secara online tanpa harus datang langsung ke kantor polisi. Platform ini tidak hanya menerima laporan kejahatan umum, tetapi juga mencakup pengaduan terkait kejahatan digital seperti pelecehan di media sosial, penyebaran data pribadi, dan penipuan daring.

Sejumlah Kepolisian Daerah (Polda) juga telah membuka saluran pelaporan melalui situs resmi atau akun media sosial, yang dirancang untuk menjangkau masyarakat luas, termasuk generasi muda yang lebih akrab dengan teknologi digital. Beberapa di antaranya bahkan menyediakan layanan chatbot untuk merespons laporan awal dan memberikan panduan kepada korban mengenai langkah-langkah yang harus dilakukan. Kehadiran media sosial sebagai sarana pelaporan juga memungkinkan penyebaran informasi secara cepat mengenai ancaman atau pola kejahatan yang sedang terjadi, sehingga masyarakat bisa lebih waspada. Namun, tetap diperlukan verifikasi lanjutan untuk memastikan validitas laporan sebelum ditindaklanjuti oleh pihak berwajib.

Korban juga memiliki opsi untuk mengakses layanan pendampingan hukum dari lembaga non-pemerintah. Lembaga Bantuan Hukum (LBH), Komnas Perempuan, Komnas HAM, dan Komisi Nasional Perlindungan Anak (Komnas PA) sering kali memberikan bantuan advokasi kepada individu atau kelompok yang menjadi korban kejahatan digital. Layanan ini mencakup konsultasi hukum, pendampingan dalam proses pelaporan ke polisi, serta bantuan dalam penyusunan dokumen dan bukti digital. Lembaga-lembaga ini juga berperan dalam mengedukasi masyarakat mengenai hak-hak digital serta bagaimana melindungi diri dari potensi ancaman di dunia maya. Dalam beberapa kasus, pendampingan dari lembaga semacam ini menjadi krusial, terutama ketika korban menghadapi pelaku yang memiliki kekuatan ekonomi atau politik yang besar.

Efektivitas mekanisme pengaduan ini masih menghadapi sejumlah kendala. Salah satu tantangan utama adalah rendahnya literasi digital di kalangan masyarakat umum, terutama di daerah terpencil atau kelompok usia lanjut. Banyak korban tidak memahami bahwa memiliki hak untuk melapor atau tidak mengetahui prosedur teknis yang diperlukan dalam mengajukan pengaduan. Selain itu, minimnya

pengetahuan mengenai cara mengamankan bukti digital atau menyimpannya secara benar juga mengakibatkan banyak laporan yang tidak dapat diproses secara hukum. Di sisi lain, masih ditemukan kelambanan dalam penanganan laporan, yang disebabkan oleh terbatasnya sumber daya manusia atau kapasitas teknis di lembaga penegak hukum.

Hambatan lainnya adalah ketersediaan akses terhadap saluran pengaduan itu sendiri. Di banyak wilayah Indonesia, khususnya di luar Jawa, akses terhadap layanan pelaporan digital masih terbatas akibat kendala jaringan internet atau kurangnya infrastruktur teknologi informasi. Hal ini menyebabkan ketimpangan antara masyarakat urban dan rural dalam hal kemampuan untuk melaporkan kejahatan siber. Pemerintah perlu memperluas jangkauan layanan pelaporan ini agar seluruh warga negara, tanpa memandang lokasi geografisnya, memiliki kesempatan yang sama dalam memperoleh keadilan. Perluasan akses ini juga harus dibarengi dengan pelatihan bagi aparat di tingkat daerah agar dapat menangani laporan secara profesional dan cepat.

Penting untuk memperbaiki mekanisme tindak lanjut terhadap laporan yang telah masuk. Tidak sedikit korban yang menyampaikan kekecewaan karena laporannya tidak mendapat respons memadai dari aparat penegak hukum, baik karena dianggap sebagai kasus ringan maupun karena ketidakmampuan dalam menelusuri pelaku kejahatan yang menyembunyikan identitasnya. Dalam konteks ini, penguatan kapasitas digital forensik serta kerja sama lintas negara menjadi krusial, mengingat banyak kasus kejahatan siber melibatkan jaringan internasional. Pemerintah Indonesia harus memperkuat kemitraan dengan organisasi global seperti INTERPOL dan ASEAN *Cybercrime* Operations Desk untuk menelusuri pelaku yang beroperasi lintas batas negara.

Upaya perbaikan mekanisme pengaduan juga harus melibatkan partisipasi publik secara aktif. Masyarakat perlu diberikan ruang untuk memberikan masukan terhadap proses pelaporan yang ada, termasuk menyampaikan kendala yang dihadapi. Keterlibatan publik dalam evaluasi kebijakan ini penting untuk memastikan bahwa sistem yang dibangun benar-benar responsif terhadap kebutuhan pengguna. Program edukasi publik mengenai kejahatan siber dan cara pelaporannya harus digencarkan, baik melalui media sosial, seminar, maupun kurikulum pendidikan formal. Pengetahuan ini dapat memberdayakan masyarakat

untuk tidak hanya menjadi pengguna teknologi yang pasif, tetapi juga warga digital yang sadar hukum dan mampu memperjuangkan hak-haknya.

Keberadaan mekanisme pengaduan tindak pidana siber di Indonesia merupakan elemen penting dalam sistem perlindungan hukum di era digital. Namun demikian, tantangan implementasi dan keterbatasan akses harus segera diatasi melalui pendekatan yang holistik dan kolaboratif. Dengan memperkuat kapasitas institusi penegak hukum, memperluas jangkauan teknologi pelaporan, meningkatkan literasi digital masyarakat, serta mendorong partisipasi masyarakat dalam pengawasan sistem, Indonesia dapat membangun sistem pengaduan yang tidak hanya tersedia secara formal, tetapi juga benar-benar berfungsi secara substansial bagi para korban. Melalui langkah-langkah ini, keadilan di ruang digital dapat diwujudkan secara nyata dan merata.

2. Bantuan Hukum dan Dukungan Psikologis untuk Korban Kejahatan Siber

Korban kejahatan siber di Indonesia tidak hanya berhadapan dengan masalah hukum yang kompleks, tetapi juga sering kali mengalami dampak emosional yang mendalam. Oleh karena itu, selain mekanisme pengaduan melalui aparat penegak hukum, penting untuk memastikan bahwa korban mendapatkan bantuan hukum dan dukungan psikologis yang memadai. Bantuan hukum yang efektif dapat membantu korban untuk memahami hak-haknya, mengakses jalur hukum yang sesuai, serta melindunginya dari potensi kesalahan dalam proses hukum yang dapat memperburuk situasinya. Di Indonesia, layanan bantuan hukum untuk korban kejahatan siber umumnya diberikan oleh lembaga-lembaga swasta, organisasi masyarakat, serta beberapa organisasi non-pemerintah (NGO) yang memiliki fokus pada isu-isu hukum digital dan perlindungan konsumen. Lembaga Bantuan Hukum (LBH) adalah salah satu institusi yang memiliki peran sentral dalam memberikan bantuan hukum bagi korban yang membutuhkan, terutama bagi yang tidak mampu membayar jasa pengacara.

Lembaga Bantuan Hukum seperti LBH Masyarakat, LBH Jakarta, atau LBH Surabaya, misalnya, menyediakan jasa bantuan hukum gratis atau dengan biaya yang terjangkau untuk masyarakat yang membutuhkan. Layanan yang diberikan tidak hanya terbatas pada konsultasi hukum tetapi juga mencakup pendampingan langsung dalam

proses pelaporan kasus kejahatan siber, pengumpulan bukti elektronik yang sah, dan memberikan bantuan hukum selama proses penyidikan hingga persidangan. Pendampingan hukum yang diberikan oleh lembaga-lembaga ini memiliki peran yang sangat penting karena sering kali korban tidak memiliki pengetahuan atau sumber daya untuk mengelola proses hukum yang kompleks, juga mungkin kesulitan dalam mengumpulkan bukti-bukti digital yang sah yang diperlukan untuk mendukung laporannya kepada aparat penegak hukum.

Misalnya, LBH Masyarakat telah secara aktif memberikan bantuan hukum dalam sejumlah kasus yang berkaitan dengan pelanggaran hak atas data pribadi dan pencurian identitas yang terjadi melalui internet. Dalam beberapa kasus, juga memberikan bantuan hukum dalam upaya mendapatkan kompensasi bagi korban yang mengalami kerugian finansial akibat tindak pidana siber. Proses hukum yang melibatkan bukti digital sering kali membutuhkan keahlian teknis untuk memastikan bahwa bukti tersebut diterima di pengadilan, yang membuat peran lembaga-lembaga ini menjadi sangat vital dalam menjamin bahwa korban mendapatkan perlindungan hukum yang adil. Selain itu, lembaga-lembaga ini juga bekerja untuk memastikan bahwa hak-hak korban diakui dan dilindungi dalam proses hukum yang lebih luas.

Korban kejahatan siber sering kali menghadapi dampak psikologis yang signifikan sebagai akibat dari perundungan daring (*cyberbullying*), pencurian identitas, atau penyalahgunaan data pribadi. Kejahatan siber seperti perundungan daring dapat menyebabkan gangguan mental yang serius pada korban, termasuk depresi, kecemasan, dan gangguan stres pascatrauma (PTSD). Untuk itu, penting bagi korban untuk mendapatkan dukungan psikologis yang memadai untuk membantunya mengatasi dampak emosional dari kejahatan yang dialami. Beberapa lembaga, seperti Yayasan Suara Hati dan Komnas Perempuan, menyediakan layanan konseling dan psikologis bagi korban yang mengalami gangguan mental akibat perundungan atau pelecehan seksual melalui media digital.

Dukungan psikologis ini dapat berupa konseling individu atau kelompok yang difokuskan untuk membantu korban mengelola trauma yang dialami. Pemberian terapi atau dukungan psikologis yang berkelanjutan juga diperlukan untuk membantu korban pulih dari dampak emosional yang mendalam. Hal ini sangat penting karena

dampak psikologis dari kejahatan siber, khususnya yang melibatkan perundungan daring, sering kali tidak terlihat oleh masyarakat umum, tetapi sangat nyata dan dapat berkelanjutan dalam waktu yang lama. Beberapa korban mungkin merasa terisolasi, kehilangan rasa percaya diri, atau merasa terancam dalam kehidupannya setelah menjadi sasaran kejahatan siber. Oleh karena itu, membutuhkan pendekatan holistik yang tidak hanya mencakup aspek hukum, tetapi juga pemulihan mental.

Lembaga-lembaga non-pemerintah yang menyediakan layanan psikologis juga berperan dalam memberikan edukasi kepada masyarakat mengenai pentingnya menjaga kesehatan mental di dunia digital, berusaha mengurangi stigma sosial yang sering kali dialami oleh korban kejahatan siber, yang dapat merasa malu atau tidak diakui dalam proses hukum. Dalam hal ini, kolaborasi antara pemerintah, lembaga bantuan hukum, dan organisasi masyarakat sangat penting untuk memberikan dukungan yang komprehensif bagi korban kejahatan siber.

Tantangan terbesar dalam memberikan bantuan hukum dan dukungan psikologis kepada korban kejahatan siber adalah kurangnya kesadaran masyarakat tentang hak-haknya dan tentang layanan yang tersedia. Banyak korban yang tidak tahu bahwa ia berhak mendapatkan bantuan hukum atau tidak tahu ke mana harus melapor. Hal ini sering kali disebabkan oleh ketidakpahaman tentang prosedur hukum yang berlaku, serta kurangnya akses informasi mengenai layanan dukungan yang tersedia. Oleh karena itu, sosialisasi dan kampanye edukasi yang lebih luas sangat diperlukan untuk memastikan bahwa setiap orang tahu hak-haknya dan cara untuk mendapatkan bantuan.

Pemerintah dan lembaga terkait juga perlu meningkatkan aksesibilitas layanan bantuan hukum dan psikologis bagi korban di daerah-daerah yang sulit dijangkau. Penyediaan layanan secara daring atau melalui telemedicine dapat menjadi solusi untuk menjangkau korban yang berada di daerah terpencil atau yang tidak memiliki akses ke layanan secara langsung. Ini akan memastikan bahwa bantuan hukum dan psikologis dapat diakses oleh seluruh lapisan masyarakat, tanpa terkecuali. Pendekatan ini dapat mempercepat pemulihan bagi korban kejahatan siber, baik dari segi hukum maupun mental.

Kerjasama antara pemerintah, lembaga-lembaga hukum, serta organisasi non-pemerintah juga harus ditingkatkan untuk menciptakan sistem yang lebih terintegrasi dalam penanganan kejahatan siber. Layanan yang diberikan kepada korban harus dapat saling melengkapi,

mulai dari pengaduan ke aparat hukum hingga pemulihan mental bagi korban. Dalam hal ini, penting untuk menciptakan satu sistem rujukan yang memungkinkan korban untuk mendapatkan layanan yang sesuai dengan kebutuhannya, baik dalam aspek hukum maupun dukungan psikologis.

Dukungan psikologis bagi korban kejahatan siber juga harus diperkuat dengan program-program pemulihan yang dapat memperbaiki kualitas hidupnya setelah kejadian. Program-program ini harus tidak hanya memberikan bantuan pada saat kejadian, tetapi juga mendukung korban dalam jangka panjang untuk memulihkan kepercayaan dirinya dan meningkatkan kesejahteraan psikologis. Oleh karena itu, penting untuk membangun jaringan dukungan sosial yang luas yang melibatkan keluarga, teman, serta masyarakat sekitar korban untuk menciptakan lingkungan yang mendukung proses pemulihan. Dengan pendekatan yang lebih holistik dan berbasis komunitas ini, korban kejahatan siber dapat memperoleh keadilan yang lebih baik, baik secara hukum maupun dalam aspek emosional.

D. Peran Masyarakat dalam Pencegahan Kejahatan Siber

1. Kesadaran dan Edukasi Digital untuk Masyarakat

Meningkatkan kesadaran dan edukasi digital di masyarakat merupakan langkah awal yang krusial dalam pencegahan kejahatan siber. Kejahatan siber, yang semakin berkembang dengan pesatnya teknologi digital, memerlukan peran aktif masyarakat untuk dapat mencegah dan mengurangi potensi ancamannya. Dalam dunia yang serba terhubung ini, ancaman terhadap data pribadi dan sistem informasi bukan hanya datang dari pihak luar, tetapi juga dapat dipengaruhi oleh perilaku pengguna internet itu sendiri. Seringkali, ketidaktahuan atau kelalaian pengguna mengenai bahaya yang ada di dunia maya menjadi celah bagi pelaku kejahatan siber untuk melakukan aksinya. Oleh karena itu, meningkatkan literasi digital di kalangan masyarakat menjadi hal yang mendasar agar dapat memahami risiko yang ada di dunia maya serta bagaimana cara melindungi diri dari ancaman tersebut.

Sebagai langkah awal untuk meningkatkan kesadaran ini, penting untuk memberikan pelatihan atau seminar yang berfokus pada etika digital dan cara-cara untuk melindungi diri saat beraktivitas di dunia maya. Misalnya, mengajarkan masyarakat untuk mengenali tanda-tanda

penipuan online, seperti *phishing*, yang sering kali digunakan oleh pelaku kejahatan untuk mencuri data pribadi korban. Mengetahui cara-cara untuk mengenali *phishing* akan memungkinkan pengguna untuk lebih berhati-hati dalam membuka email atau tautan yang mencurigakan. Selain itu, penting juga untuk memberikan pemahaman mengenai pentingnya penggunaan kata sandi yang kuat, yang merupakan langkah pertama dalam melindungi akun-akun digital pribadi dari akses yang tidak sah. Hal ini, meskipun sederhana, dapat mencegah banyak upaya peretasan yang dapat merugikan pengguna.

Salah satu upaya besar yang dilakukan pemerintah Indonesia dalam hal edukasi digital adalah melalui program "Siberkreasi" yang diluncurkan oleh Kementerian Komunikasi dan Informatika (Kominfo) pada tahun 2021. Program ini bertujuan untuk meningkatkan literasi digital di Indonesia dengan memberikan edukasi mengenai cara-cara aman beraktivitas di dunia maya. Program ini mencakup pelatihan untuk mengenali potensi bahaya di dunia digital, baik itu dalam bentuk penipuan, peretasan, ataupun penyebaran informasi palsu atau *hoaks* yang dapat merugikan individu maupun kelompok. Dalam program ini, masyarakat tidak hanya diajarkan tentang bagaimana melindungi dirinya, tetapi juga diberikan pemahaman mengenai etika digital dan cara menggunakan teknologi secara bijak. Diharapkan dengan program seperti ini, masyarakat Indonesia akan semakin paham mengenai pentingnya menjaga privasi dan keamanan data pribadinya.

Edukasi digital juga harus menyasar pengguna individu, perusahaan, dan lembaga yang memiliki akses terhadap data pribadi. Perusahaan yang beroperasi di dunia digital, khususnya platform digital dan institusi keuangan, memegang tanggung jawab besar dalam menjaga data pribadi pelanggannya. Perusahaan harus memiliki kebijakan privasi yang ketat dan secara aktif memberikan edukasi kepada pelanggannya tentang bagaimana menjaga keamanan akun pribadi. Lembaga-lembaga ini, yang sering kali menjadi sasaran utama serangan siber, perlu melakukan langkah-langkah pencegahan yang tidak hanya melibatkan keamanan teknis, tetapi juga penyuluhan kepada pengguna mengenai risiko dan cara-cara untuk menghindarinya. Pengguna yang sadar akan risiko yang ada akan lebih berhati-hati dan tidak mudah menjadi korban kejahatan siber.

Penting juga untuk menciptakan kampanye sosialisasi yang tidak hanya dilakukan secara terbatas, tetapi mencakup seluruh lapisan

masyarakat. Di beberapa daerah, terutama di wilayah yang kurang berkembang, kesadaran akan bahaya siber dan pentingnya menjaga data pribadi masih sangat rendah. Oleh karena itu, edukasi digital harus diperluas ke daerah-daerah tersebut, menggunakan berbagai metode yang lebih mudah dijangkau oleh masyarakat, seperti melalui media sosial, radio, atau televisi lokal. Program-program ini bisa membantu memperkenalkan konsep literasi digital kepada masyarakat yang belum terbiasa dengan teknologi informasi.

Penyuluhan mengenai keamanan digital juga perlu disesuaikan dengan perkembangan teknologi yang terus berubah. Kejahatan siber berkembang sangat pesat, dan dengan setiap kemajuan teknologi baru, muncul pula potensi ancaman baru. Misalnya, dengan maraknya penggunaan aplikasi berbasis cloud dan *internet of things* (IoT), muncul pula tantangan baru dalam hal keamanan data. Oleh karena itu, edukasi digital harus terus berkembang untuk mengimbangi perkembangan teknologi tersebut. Pengguna harus diberikan pemahaman mengenai cara-cara baru untuk melindungi perangkatnya dan data pribadinya di dunia digital yang semakin kompleks.

Penting juga untuk mengajarkan masyarakat tentang etika digital, yaitu bagaimana berperilaku dengan bijak di dunia maya. Ini mencakup pemahaman mengenai penyebaran informasi yang benar, serta dampak dari penyebaran informasi palsu atau *hoaks*. *Hoaks* yang disebarkan melalui media sosial, misalnya, tidak hanya dapat merugikan individu, tetapi juga dapat mengancam kestabilan sosial. Oleh karena itu, penting untuk mengajarkan masyarakat tentang pentingnya memverifikasi informasi sebelum membagikannya. Ini juga berhubungan dengan pengembangan budaya digital yang bertanggung jawab dan saling menghormati di dunia maya.

Pendidikan mengenai keamanan digital juga harus menjadi bagian dari kurikulum pendidikan di sekolah-sekolah. Mengingat anak-anak dan remaja saat ini sangat terpapar teknologi digital, penting untuk membekalinya dengan pengetahuan tentang cara melindungi dirinya di dunia maya. Kurikulum ini bisa mencakup dasar-dasar keamanan siber, cara menjaga privasi, serta pemahaman tentang etika dan tanggung jawab digital. Dengan mengenalkan hal ini sejak dini, diharapkan generasi muda akan lebih siap dalam menghadapi berbagai ancaman digital yang mungkin ditemui di kemudian hari.

Keberhasilan upaya edukasi ini sangat bergantung pada kerjasama antara pemerintah, sektor swasta, lembaga pendidikan, serta organisasi masyarakat. Kerja sama ini sangat penting untuk menciptakan program edukasi yang komprehensif dan menyeluruh yang tidak hanya mengedukasi masyarakat tentang bagaimana melindungi dirinya, tetapi juga tentang pentingnya berperan aktif dalam menciptakan ekosistem digital yang aman dan bertanggung jawab. Keamanan digital tidak hanya menjadi tanggung jawab individu atau pemerintah saja, tetapi merupakan tanggung jawab bersama yang melibatkan seluruh komponen masyarakat. Oleh karena itu, langkah-langkah preventif yang didukung dengan edukasi yang tepat akan sangat membantu dalam mengurangi ancaman kejahatan siber di Indonesia.

Dengan meningkatnya kesadaran masyarakat tentang pentingnya menjaga data pribadi dan memahami bahaya yang ada di dunia maya, diharapkan dapat tercipta masyarakat yang lebih aman dan terlindungi dari ancaman siber. Edukasi digital bukan hanya soal perlindungan data pribadi, tetapi juga tentang membangun budaya digital yang positif dan bertanggung jawab di tengah kemajuan teknologi yang terus berkembang.

2. Partisipasi Aktif dalam Pelaporan dan Pemantauan Kejahatan Siber

Partisipasi aktif masyarakat dalam pelaporan dan pemantauan kejahatan siber merupakan bagian yang tidak terpisahkan dari upaya pencegahan dan penanggulangan ancaman yang semakin berkembang. Dalam dunia digital yang semakin kompleks, masyarakat memiliki peran penting dalam mendeteksi dan menanggulangi berbagai bentuk kejahatan siber, mulai dari pencurian identitas hingga penyebaran informasi palsu (*hoaks*). Tindak lanjut dari laporan dan pemantauan yang dilakukan oleh masyarakat dapat membantu pihak berwajib untuk merespons dengan cepat dan mencegah kerugian yang lebih besar, baik bagi individu maupun masyarakat secara keseluruhan. Melalui pelaporan yang cepat dan akurat, ancaman siber dapat dikenali lebih dini, dan langkah-langkah preventif dapat segera diambil.

Di Indonesia, pemerintah telah menyediakan berbagai saluran bagi masyarakat untuk melaporkan kasus-kasus kejahatan siber, salah satunya adalah melalui platform lapor.go.id. Platform ini memungkinkan masyarakat untuk melaporkan kejadian-kejadian mencurigakan yang

ditemui di dunia maya, seperti percakapan yang berpotensi menipu atau serangan siber yang lebih terorganisir. Melalui platform ini, proses pelaporan menjadi lebih mudah, transparan, dan terorganisir. Selain itu, pihak berwajib, seperti Polri dan Direktorat Tindak Pidana Siber, dapat langsung merespons laporan yang diterima dengan cara yang lebih efisien dan terkoordinasi. Hal ini menjadi sangat penting karena kejahatan siber tidak mengenal batasan wilayah, dan sering kali mempengaruhi banyak orang dalam waktu yang sangat singkat.

Pelaporan yang dilakukan oleh masyarakat juga sangat penting dalam hal memantau dan menanggulangi penyebaran *hoaks* yang merupakan bagian dari kejahatan siber yang sangat merugikan. *Hoaks* yang disebarkan melalui media sosial dan platform digital lainnya sering kali memicu kebingungan, ketakutan, bahkan kerusakan reputasi bagi individu atau kelompok tertentu. Bahkan, dalam beberapa kasus, penyebaran *hoaks* dapat menyebabkan konflik sosial atau kerusakan ekonomi, seperti dalam kasus penipuan yang menargetkan kelompok tertentu. Oleh karena itu, peran aktif masyarakat dalam memverifikasi informasi yang beredar dan melaporkan informasi yang mencurigakan menjadi sangat krusial. Masyarakat yang sadar akan dampak dari penyebaran informasi palsu dapat mencegah kerugian lebih lanjut dengan tidak turut menyebarkan informasi yang belum jelas kebenarannya.

Masyarakat juga dapat membantu dengan mengingatkan dan mengedukasi sesama pengguna internet mengenai cara-cara untuk melindungi dirinya dari kejahatan siber. Misalnya, memberikan pemahaman tentang pentingnya memperbarui kata sandi secara berkala, atau menggunakan autentikasi dua faktor untuk akun-akun digital yang penting. Kebiasaan ini dapat secara signifikan mengurangi potensi peretasan yang sering kali disebabkan oleh penggunaan kata sandi yang lemah atau mudah ditebak. Dengan saling mengingatkan satu sama lain, masyarakat dapat menciptakan budaya digital yang lebih aman dan bertanggung jawab. Hal ini juga dapat membentuk sikap kolektif untuk menjaga keamanan bersama di dunia maya.

Pentingnya partisipasi aktif masyarakat dalam pencegahan kejahatan siber tidak hanya terbatas pada individu. Perusahaan dan sektor swasta juga memiliki peran yang sangat besar dalam menciptakan ekosistem digital yang aman. Sebagai contoh, perusahaan yang bergerak di bidang teknologi informasi atau e-commerce harus memiliki sistem

yang memadai untuk mengidentifikasi dan menangani potensi kejahatan siber yang dapat merugikan konsumen. Selain itu, juga memiliki tanggung jawab untuk mengedukasi penggunanya tentang praktik-praktik terbaik dalam menjaga keamanan data pribadi dan menghindari ancaman siber. Dengan adanya kerjasama antara perusahaan, masyarakat, dan pemerintah, upaya pencegahan dan pelaporan kejahatan siber akan semakin efektif.

Masyarakat yang lebih aktif dalam pelaporan juga akan membantu lembaga pemerintah untuk memperbarui dan meningkatkan kebijakan serta regulasi terkait dengan keamanan digital. Pemerintah, melalui badan-badan yang berwenang, seperti Badan Siber dan Sandi Negara (BSSN) dan Kepolisian Negara Republik Indonesia, dapat mengambil langkah-langkah yang lebih cepat dan tepat sasaran dalam menangani kasus kejahatan siber dengan dukungan data dan laporan yang diberikan oleh masyarakat. Di samping itu, peran serta masyarakat dalam memberikan umpan balik dan melaporkan kejadian-kejadian tertentu yang mungkin terlewatkan oleh otoritas juga sangat penting untuk memperbaiki sistem yang ada dan menciptakan kebijakan yang lebih adaptif terhadap perkembangan teknologi.

Salah satu tantangan terbesar dalam mengedukasi masyarakat untuk aktif melaporkan kejahatan siber adalah kurangnya pemahaman tentang apa yang dimaksud dengan kejahatan siber dan bagaimana cara mengidentifikasi ancaman tersebut. Untuk itu, pemerintah dan lembaga terkait perlu melakukan sosialisasi yang lebih luas tentang jenis-jenis kejahatan siber yang sering terjadi, serta bagaimana cara melaporkan dan menghadapinya. Hal ini akan membantu masyarakat agar lebih paham dan siap untuk melapor jika menjadi korban atau menyaksikan kegiatan mencurigakan yang berkaitan dengan dunia maya. Penyuluhan yang dilakukan harus mencakup berbagai saluran komunikasi, baik online maupun offline, agar seluruh lapisan masyarakat dapat terjangkau.

Dengan meningkatnya peran aktif masyarakat dalam pelaporan dan pemantauan kejahatan siber, diharapkan akan terbentuk budaya digital yang lebih sehat dan aman. Budaya ini bukan hanya berkaitan dengan penggunaan teknologi secara bijak, tetapi juga dengan saling menghormati dan menjaga keamanan serta privasi orang lain. Masyarakat yang sadar akan pentingnya menjaga ruang digital yang aman akan lebih berhati-hati dalam berbagi informasi pribadi dan lebih waspada terhadap potensi ancaman yang ada. Budaya ini juga harus

dimulai sejak dini, dengan mengintegrasikan pendidikan tentang keamanan digital ke dalam kurikulum sekolah, sehingga generasi muda lebih siap menghadapi tantangan dunia maya yang semakin kompleks.

Kolaborasi antara masyarakat, sektor swasta, dan pemerintah dalam menciptakan kesadaran dan partisipasi aktif ini adalah kunci keberhasilan dalam mengurangi kejahatan siber. Tanpa adanya kerja sama yang erat, upaya pencegahan kejahatan siber akan terhambat, dan dampaknya akan lebih besar dirasakan oleh masyarakat. Oleh karena itu, penting untuk terus memperbarui strategi dan kebijakan dalam melibatkan masyarakat secara aktif dalam mencegah dan melaporkan kejahatan siber. Dengan melakukan langkah-langkah yang tepat dan melibatkan seluruh elemen masyarakat, ancaman siber dapat diminimalkan dan tercipta ruang digital yang lebih aman dan terjamin.

BAB VIII
MASA DEPAN PENANGGULANGAN TINDAK PIDANA SIBER

Masa depan penanggulangan tindak pidana siber dihadapkan pada tantangan yang semakin kompleks seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Dengan kemajuan teknologi yang terus berkembang, kejahatan siber pun semakin beragam dan canggih, menciptakan ancaman yang lebih besar bagi individu, perusahaan, dan negara. Di masa depan, penanggulangan kejahatan siber tidak hanya akan bergantung pada upaya hukum dan penegakan hukum yang ada, tetapi juga pada inovasi teknologi yang dapat mendeteksi, mencegah, dan mengurangi dampak dari ancaman tersebut. Kemajuan dalam bidang kecerdasan buatan (AI), big data, serta teknologi blockchain dapat menjadi solusi efektif untuk memperkuat sistem keamanan dan mempercepat penanganan kasus-kasus siber. Selain itu, kerjasama internasional yang lebih erat juga akan menjadi kunci, mengingat sifat kejahatan siber yang melintasi batas negara. Peningkatan literasi digital di masyarakat juga akan berperan penting dalam upaya pencegahan, di mana kesadaran pengguna internet mengenai risiko dan cara melindungi diri dari serangan siber menjadi langkah awal yang strategis. Dengan berbagai terobosan ini, diharapkan penanggulangan kejahatan siber dapat semakin efektif dan responsif terhadap dinamika dunia maya yang terus berubah.

A. Tantangan Hukum di Era *Artificial Intelligence* dan Big Data

1. Isu Privasi dan Perlindungan Data Pribadi

Salah satu tantangan terbesar dalam menghadapi perkembangan teknologi *Artificial Intelligence* (AI) dan Big Data adalah perlindungan data pribadi dan privasi individu. Di era digital ini, data pribadi merupakan salah satu komoditas paling berharga, namun juga paling

rentan terhadap penyalahgunaan. Big Data mengumpulkan, menganalisis, dan menyebarkan informasi dalam jumlah besar, sementara AI menggunakan data tersebut untuk membuat keputusan otomatis. Hal ini menciptakan berbagai masalah terkait pengumpulan, penyimpanan, dan penggunaan data pribadi.

Menurut Zuboff (2019), fenomena ini dikenal sebagai "*Surveillance Capitalism*," di mana data pribadi dikumpulkan tanpa persetujuan eksplisit dari individu dan digunakan untuk tujuan yang dapat merugikan privasinya. Salah satu contoh nyata adalah penggunaan data pribadi oleh perusahaan besar untuk menentukan iklan yang relevan, yang sering kali dilakukan tanpa pemberitahuan yang cukup kepada pengguna atau tanpa memperoleh izin yang memadai. Di Eropa, masalah ini diatasi dengan pengenalan *General Data Protection Regulation* (GDPR), yang mulai berlaku pada 2018, sebagai upaya untuk memberikan perlindungan yang lebih ketat terhadap data pribadi individu. GDPR menekankan pentingnya persetujuan yang jelas dan eksplisit, serta hak untuk mengakses dan menghapus data pribadi yang telah dikumpulkan (Voigt & Von dem Bussche, 2017).

Meskipun negara-negara seperti Uni Eropa telah memiliki regulasi yang ketat, negara-negara lain, termasuk Indonesia, masih mengalami kesulitan dalam merumuskan hukum yang mampu mengimbangi perkembangan teknologi ini. Sebagai contoh, Undang-Undang Perlindungan Data Pribadi di Indonesia, yang baru saja disahkan pada tahun 2022, berusaha untuk memberikan kerangka hukum yang lebih jelas dalam melindungi data pribadi, namun tantangan tetap ada dalam hal implementasi dan pengawasan yang efektif.

Penerapan AI dalam pengolahan data seringkali membawa risiko diskriminasi dan bias. Algoritma yang digunakan oleh AI, yang berbasis pada data yang ada, sering kali memperkuat ketidaksetaraan sosial yang sudah ada. Misalnya, dalam bidang perekrutan pekerjaan, AI yang dilatih dengan data historis dapat secara tidak sadar mendiskriminasi kandidat berdasarkan jenis kelamin, ras, atau usia, yang melanggar prinsip-prinsip dasar hak asasi manusia. Oleh karena itu, tantangan hukum di era ini juga mencakup upaya untuk memastikan bahwa algoritma yang digunakan dalam pengambilan keputusan berbasis data harus dapat diakses dan dipertanggungjawabkan, serta memastikan bahwa hak individu untuk tidak didiskriminasi tetap terjaga (O'Neil, 2016).

2. Akuntabilitas dan Tanggung Jawab dalam Penggunaan AI

Tantangan hukum lainnya yang muncul di era AI dan Big Data adalah terkait dengan akuntabilitas dan tanggung jawab atas keputusan yang diambil oleh sistem AI. Ketika algoritma AI membuat keputusan otomatis, baik dalam konteks bisnis, kesehatan, atau bahkan hukum, muncul pertanyaan mendasar mengenai siapa yang harus bertanggung jawab jika keputusan tersebut menyebabkan kerugian. Apakah tanggung jawab tersebut terletak pada pengembang algoritma, pengguna teknologi, atau penyedia platform yang memanfaatkan teknologi tersebut?

Contoh paling nyata dari masalah ini adalah dalam bidang otomotif, di mana kendaraan otonom yang menggunakan AI dapat terlibat dalam kecelakaan. Misalnya, dalam kasus kecelakaan yang melibatkan mobil otonom, pertanyaan yang muncul adalah siapa yang harus bertanggung jawab? Apakah tanggung jawab tersebut jatuh kepada perusahaan pembuat mobil, pembuat perangkat lunak AI, atau individu yang mengemudikan kendaraan? Menurut Binns (2018), hal ini menciptakan kebingungan dalam penentuan akuntabilitas hukum, terutama karena algoritma yang digunakan oleh kendaraan otonom sulit untuk dipahami sepenuhnya oleh pihak yang terlibat dalam proses hukum.

Tantangan lainnya terkait dengan penggunaan AI dalam sistem peradilan dan penegakan hukum. Beberapa negara telah mulai mengimplementasikan AI dalam sistem pengadilan untuk menganalisis bukti, memprediksi hukuman, atau bahkan untuk mengambil keputusan hukum secara otomatis. Hal ini memunculkan masalah terkait dengan hak asasi manusia, khususnya dalam hal transparansi dan keadilan. Misalnya, jika sebuah algoritma digunakan untuk memutuskan hukuman seseorang, apakah individu tersebut akan mendapatkan pengadilan yang adil jika algoritma tersebut tidak dapat dijelaskan atau dipertanggungjawabkan?

Pada konteks ini, penting bagi negara untuk memiliki regulasi yang memadai terkait penggunaan AI dalam proses pengambilan keputusan, agar teknologi ini tidak disalahgunakan dan tetap menghormati prinsip-prinsip hukum yang berlaku, termasuk keadilan dan hak atas proses yang transparan. Salah satu solusi yang telah diusulkan oleh sejumlah pakar hukum adalah pengembangan "*AI audit trails*", yang dapat memberikan penjelasan yang jelas tentang bagaimana

algoritma mencapai kesimpulannya dan memastikan bahwa keputusan yang diambil oleh sistem AI dapat diuji dan dipertanggungjawabkan (Chesney & Citron, 2019).

B. Keamanan Siber dalam Transformasi Digital Indonesia

1. Tantangan Keamanan Siber dalam Era Transformasi Digital

Transformasi digital di Indonesia membawa dampak besar bagi berbagai sektor kehidupan, mulai dari pemerintahan hingga dunia bisnis dan pendidikan. Peningkatan penggunaan teknologi digital di berbagai aspek kehidupan ini memberikan potensi yang besar untuk meningkatkan produktivitas dan efisiensi ekonomi. Sektor e-commerce dan layanan berbasis cloud, misalnya, berkembang pesat dan menjadi bagian integral dari kehidupan sehari-hari. Namun, meskipun transformasi digital ini menawarkan berbagai kemudahan, tantangan besar dalam hal keamanan siber juga muncul seiring dengan peningkatan penggunaan teknologi tersebut. Dalam konteks ini, penting untuk memahami bahwa meskipun teknologi berkembang, ancaman terhadap sistem digital yang ada juga semakin kompleks.

Salah satu tantangan utama yang dihadapi Indonesia dalam mengamankan dunia digital adalah tingginya angka serangan siber yang terjadi setiap tahunnya. Data yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2020 menunjukkan bahwa serangan siber di Indonesia meningkat tajam, dengan jenis serangan yang paling sering terjadi seperti *phishing*, *malware*, dan *ransomware*. Serangan-serangan ini tidak hanya merugikan individu, tetapi juga sektor-sektor bisnis besar yang bergantung pada sistem digital untuk operasional. Pencurian data pengguna yang terjadi pada beberapa platform e-commerce besar pada tahun 2020, yang melibatkan informasi pribadi dan keuangan, adalah contoh nyata betapa rentannya ekosistem digital yang ada di Indonesia. Kejahatan siber semacam ini menimbulkan kerugian materiil yang besar dan merusak reputasi perusahaan yang menjadi target.

Salah satu penyebab utama mengapa serangan siber masih sering terjadi adalah kurangnya kesadaran akan pentingnya keamanan siber di kalangan masyarakat dan perusahaan. Banyak individu yang belum memahami betapa pentingnya melindungi data pribadinya dari ancaman di dunia maya. Hal yang sama juga berlaku bagi perusahaan-perusahaan,

baik skala kecil maupun besar, yang belum memiliki sistem keamanan yang memadai untuk melindungi data sensitif. Sebagai contoh, beberapa usaha kecil dan menengah yang bergantung pada e-commerce sering kali tidak memiliki kebijakan atau langkah-langkah proteksi data yang cukup, sehingga menjadi sasaran empuk bagi peretas yang mencari celah dalam sistemnya.

Tantangan lainnya adalah keterbatasan kapasitas infrastruktur digital yang aman. Infrastruktur yang belum memadai dapat menyebabkan celah yang dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melancarkan serangan. Dube et al. (2020) mengungkapkan bahwa Indonesia menghadapi tantangan besar dalam hal pengembangan infrastruktur keamanan siber yang mampu mendukung berbagai sistem digital yang terus berkembang. Tanpa dukungan infrastruktur yang kuat, sektor-sektor penting yang bergantung pada teknologi digital, seperti sektor keuangan, kesehatan, dan pemerintahan, rentan terhadap berbagai bentuk serangan siber yang dapat merusak stabilitas dan keamanan negara.

Pemerintah Indonesia, melalui Badan Siber dan Sandi Negara (BSSN), telah berupaya untuk mengatasi tantangan ini dengan mengeluarkan berbagai kebijakan yang mendukung pembangunan infrastruktur keamanan siber. Salah satu kebijakan utama adalah Rencana Aksi Keamanan Siber Nasional (RAKSN), yang bertujuan untuk menciptakan sistem yang lebih aman dan dapat diandalkan dalam menghadapi berbagai ancaman di dunia maya. Program ini mencakup berbagai langkah strategis, mulai dari pembangunan kapasitas teknis hingga sosialisasi kepada masyarakat mengenai pentingnya proteksi data dan langkah-langkah yang dapat diambil untuk menjaga keamanan pribadi dan organisasi.

Meskipun telah ada berbagai inisiatif yang dikeluarkan oleh pemerintah, masih banyak tantangan yang harus dihadapi dalam menciptakan sistem keamanan yang terintegrasi dan menyeluruh. Salah satunya adalah perlunya peningkatan kapasitas dan kemampuan teknis di seluruh sektor, baik itu sektor publik maupun swasta, untuk menghadapi ancaman siber yang semakin beragam. Peningkatan literasi digital juga harus menjadi bagian dari solusi, karena kesadaran masyarakat tentang pentingnya langkah-langkah proteksi yang tepat adalah kunci untuk mencegah kejahatan siber sejak dini.

Pembangunan infrastruktur yang lebih baik di sektor digital juga sangat diperlukan agar Indonesia dapat menjadi negara yang lebih siap menghadapi potensi ancaman siber yang datang dari luar maupun dalam negeri. Infrastruktur yang dimaksud tidak hanya mencakup perangkat keras atau perangkat lunak yang digunakan dalam sistem digital, tetapi juga sumber daya manusia yang memiliki kemampuan untuk mengelola dan melindungi sistem-sistem tersebut. Oleh karena itu, pelatihan dan pendidikan dalam bidang keamanan siber harus diberikan kepada tenaga kerja yang terlibat dalam pengelolaan sistem digital, baik di sektor pemerintah maupun swasta.

Tantangan lainnya adalah peran sektor swasta yang masih perlu diperkuat dalam hal perlindungan data dan sistemnya. Banyak perusahaan, terutama di sektor e-commerce dan fintech, yang belum menerapkan kebijakan proteksi data yang cukup ketat. Sektor-sektor ini, yang menjadi bagian penting dari perekonomian digital Indonesia, sangat rentan terhadap ancaman siber karena volume transaksi yang besar dan data sensitif yang dikelola. Oleh karena itu, perusahaan harus diingatkan bahwa tidak hanya bertanggung jawab terhadap keuntungan yang dihasilkan, tetapi juga terhadap data dan privasi pengguna yang menjadi bagian dari sistem digital.

Penting untuk terus memperbarui kebijakan dan strategi dalam menghadapi perkembangan teknologi yang cepat. Dunia maya terus berkembang dengan pesat, dan dengan itu juga ancaman terhadap sistem digital semakin beragam dan canggih. Oleh karena itu, pemerintah, sektor swasta, dan masyarakat harus bekerja sama untuk menciptakan ekosistem digital yang aman, dengan saling mendukung satu sama lain dalam upaya pencegahan dan penanggulangan kejahatan siber. Keterlibatan semua pihak dalam menghadapi tantangan ini akan sangat menentukan sejauh mana Indonesia dapat memanfaatkan potensi transformasi digital tanpa mengorbankan keamanan siber.

2. Strategi Keamanan Siber untuk Mendukung Transformasi Digital

Transformasi digital yang sedang berlangsung di Indonesia membawa dampak besar terhadap berbagai sektor kehidupan, termasuk pemerintahan, bisnis, pendidikan, dan pelayanan publik. Namun, pesatnya perkembangan ini juga memunculkan tantangan dalam hal keamanan siber. Oleh karena itu, untuk mendukung transformasi digital

yang aman dan berkelanjutan, Indonesia perlu mengembangkan strategi keamanan siber yang komprehensif. Strategi ini tidak hanya melibatkan kebijakan yang jelas dan terarah, tetapi juga penguatan kapasitas sumber daya manusia (SDM) serta pengembangan teknologi yang mumpuni untuk menghadapi ancaman siber yang semakin kompleks.

Menurut Kuncoro (2020), strategi keamanan siber yang efektif harus mencakup tiga elemen utama: penguatan regulasi dan kebijakan, peningkatan kapasitas SDM di bidang keamanan siber, dan pengembangan teknologi untuk mencegah serta menangani ancaman siber. Tiga elemen ini saling terkait dan saling mendukung untuk menciptakan ekosistem digital yang aman dan dapat diandalkan. Tanpa adanya penguatan regulasi yang jelas, sulit bagi negara dan sektor swasta untuk memastikan bahwa standar keamanan yang tinggi diterapkan dalam setiap aspek aktivitas digital. Oleh karena itu, penguatan regulasi dan kebijakan menjadi langkah pertama yang sangat penting dalam membangun sistem keamanan yang kuat.

Salah satu regulasi yang sangat signifikan dalam meningkatkan keamanan data pribadi adalah pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. UU ini memberikan landasan hukum yang kuat untuk melindungi data pribadi individu dalam ruang digital, dan perusahaan yang mengelola data pribadi di Indonesia diwajibkan untuk mematuhi standar keamanan yang ketat. Dengan adanya undang-undang ini, individu dapat merasa lebih aman dalam beraktivitas di dunia maya, karena ada jaminan bahwa data pribadinya akan terlindungi dan tidak akan disalahgunakan. Selain itu, perusahaan yang terbukti tidak memenuhi standar keamanan data akan dikenakan sanksi, yang memberikan insentif untuk memperkuat sistem keamanan.

Penguatan regulasi saja tidak cukup untuk menghadapi ancaman siber yang semakin beragam. Indonesia juga harus meningkatkan kapasitas sumber daya manusia (SDM) di bidang keamanan siber. Salah satu tantangan besar yang dihadapi adalah kurangnya tenaga ahli yang kompeten dalam bidang ini. Di sektor publik, misalnya, banyak instansi pemerintah yang masih kekurangan tenaga ahli yang dapat mengelola dan menjaga keamanan sistem digital. Di sektor swasta, meskipun beberapa perusahaan besar telah mulai menyadari pentingnya keamanan siber, banyak perusahaan kecil dan menengah yang belum memprioritaskan perlindungan data dan sistem.

Untuk mengatasi masalah ini, pendidikan dan pelatihan terkait dengan keamanan siber harus diperkuat. Pemerintah Indonesia, bekerja sama dengan universitas dan lembaga pendidikan, perlu menciptakan program studi yang fokus pada keamanan siber. Program ini dapat melahirkan tenaga ahli yang tidak hanya menguasai teori, tetapi juga memiliki keterampilan praktis yang dibutuhkan untuk menghadapi ancaman siber. Selain itu, pelatihan terus-menerus untuk profesional di sektor publik dan swasta sangat diperlukan agar selalu siap menghadapi ancaman yang berkembang.

Pengembangan teknologi yang canggih juga berperan penting dalam strategi keamanan siber Indonesia. Ancaman siber saat ini semakin canggih dan berkembang dengan pesat, sehingga teknologi yang digunakan untuk melawan ancaman tersebut juga harus lebih maju. Salah satu teknologi yang dapat digunakan untuk memperkuat pertahanan siber adalah kecerdasan buatan (AI). Teknologi AI dapat digunakan untuk mendeteksi serangan siber secara real-time dan memberikan respons yang cepat dan tepat. Dengan menggunakan algoritma yang canggih, sistem AI dapat menganalisis pola lalu lintas data dan mendeteksi anomali yang mungkin menunjukkan adanya serangan.

Teknologi enkripsi juga sangat penting dalam menjaga kerahasiaan dan integritas data. Enkripsi adalah metode untuk mengamankan data dengan cara mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi. Teknologi enkripsi ini digunakan dalam berbagai sektor, terutama di sektor keuangan dan perbankan, untuk melindungi transaksi digital yang dilakukan oleh individu maupun perusahaan. Dengan menggunakan enkripsi yang kuat, data sensitif seperti informasi kartu kredit dan rekening bank dapat dilindungi dari ancaman peretas yang ingin mengaksesnya.

Teknologi blockchain juga memiliki potensi besar dalam meningkatkan keamanan siber, terutama di sektor perbankan dan e-commerce. Blockchain adalah teknologi yang memungkinkan transaksi digital dilakukan secara transparan dan aman, dengan menggunakan buku besar terdistribusi yang tidak dapat diubah tanpa konsensus dari semua pihak yang terlibat. Dengan menggunakan teknologi blockchain, transaksi digital dapat dilakukan dengan tingkat keamanan yang sangat tinggi, karena setiap perubahan dalam sistem harus dicatat dalam blockchain dan tidak dapat dimanipulasi. Teknologi ini dapat diterapkan

dalam berbagai sektor, seperti pembayaran digital, identitas digital, dan sistem pemantauan logistik.

Integrasi kebijakan yang jelas, penguatan kapasitas SDM, dan pengembangan teknologi canggih merupakan langkah-langkah yang saling mendukung untuk menciptakan sistem keamanan siber yang efektif. Indonesia harus terus berinovasi dalam mengembangkan dan menerapkan teknologi terbaru untuk mengatasi ancaman siber yang semakin beragam dan canggih. Oleh karena itu, kolaborasi antara pemerintah, sektor swasta, dan lembaga pendidikan sangat diperlukan untuk menciptakan ekosistem digital yang aman, transparan, dan dapat diandalkan.

Meskipun tantangan yang dihadapi dalam menghadapi ancaman siber cukup besar, dengan adanya strategi yang tepat, Indonesia dapat membangun sistem keamanan siber yang mampu mendukung transformasi digital secara berkelanjutan. Keberhasilan strategi ini akan bergantung pada kemampuan negara untuk mengimplementasikan kebijakan yang tepat, memperkuat kapasitas SDM, dan memanfaatkan teknologi terbaru untuk mengatasi ancaman siber. Dengan demikian, Indonesia dapat menciptakan ruang digital yang aman dan dapat mendukung pertumbuhan ekonomi serta kemajuan teknologi di masa depan.

C. Kebijakan Pencegahan Kejahatan Siber di Sektor Publik dan Swasta

1. Kebijakan Pencegahan Kejahatan Siber di Sektor Publik

Pencegahan kejahatan siber di sektor publik sangat penting mengingat sektor ini mengelola berbagai data sensitif yang bersifat strategis dan vital bagi negara. Di antaranya adalah data kependudukan, data pajak, serta informasi terkait kebijakan, peraturan, dan program-program pemerintah yang berdampak langsung pada masyarakat. Keamanan data dan sistem informasi negara menjadi hal yang sangat krusial untuk menjaga stabilitas negara serta mencegah potensi kejahatan siber yang dapat merusak reputasi pemerintah, menurunkan kepercayaan publik, dan menimbulkan kerugian material maupun immaterial yang besar. Oleh karena itu, kebijakan yang mendukung perlindungan data dan sistem informasi negara harus diprioritaskan.

Pemerintah Indonesia telah menyadari pentingnya keamanan siber dan mengambil langkah-langkah strategis untuk mencegah ancaman di sektor publik. Salah satu kebijakan utama yang telah diterapkan adalah pembentukan Badan Siber dan Sandi Negara (BSSN) berdasarkan Peraturan Presiden No. 53 Tahun 2017. BSSN memiliki peran yang sangat vital dalam mengkoordinasikan kebijakan keamanan siber nasional serta menyusun standar keamanan yang berlaku di seluruh sektor, baik publik maupun swasta. BSSN juga bertanggung jawab untuk memantau potensi ancaman siber yang dapat mengancam keamanan data dan infrastruktur strategis negara.

Salah satu langkah nyata yang telah diambil oleh BSSN adalah penyusunan Rencana Aksi Keamanan Siber Nasional (RAKSN). RAKSN ini bertujuan untuk memastikan bahwa setiap sektor penting di Indonesia, baik yang berhubungan langsung dengan pemerintah maupun sektor lainnya, memiliki sistem keamanan siber yang memadai. Langkah ini tidak hanya bertujuan untuk melindungi data dan sistem yang ada di pemerintahan, tetapi juga untuk menciptakan infrastruktur siber yang dapat mencegah terjadinya serangan siber yang dapat merugikan negara. Melalui RAKSN, pemerintah Indonesia berkomitmen untuk menciptakan ekosistem digital yang aman dan terlindungi dari berbagai ancaman yang datang, baik dari dalam negeri maupun luar negeri (Kurniawan, 2020).

Salah satu aspek penting dalam pencegahan kejahatan siber di sektor publik adalah perlindungan terhadap data pribadi masyarakat. Data pribadi yang dikelola oleh instansi pemerintah sering kali sangat sensitif dan menjadi sasaran utama bagi pelaku kejahatan siber. Untuk itu, perlindungan terhadap data pribadi menjadi fokus utama dalam kebijakan keamanan siber Indonesia. Salah satu kebijakan besar yang telah diimplementasikan adalah pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. UU ini mengatur dengan sangat ketat bagaimana data pribadi harus dikelola dan dilindungi oleh lembaga pemerintah maupun sektor swasta yang terlibat dalam pengolahan data.

Pada praktiknya, UU PDP mewajibkan setiap lembaga pemerintah yang mengelola data pribadi untuk memenuhi standar perlindungan data yang sangat ketat. Misalnya, lembaga pemerintah harus menggunakan teknologi enkripsi yang kuat untuk melindungi data yang disimpan dan ditransmisikan. Selain itu, lembaga-lembaga ini juga

diwajibkan untuk melakukan audit keamanan secara berkala untuk memastikan bahwa data yang dikelola tidak dapat diakses oleh pihak yang tidak berwenang. Implementasi UU PDP ini diharapkan dapat meningkatkan kepercayaan publik terhadap pengelolaan data pribadi, serta memberikan perlindungan yang maksimal terhadap data sensitif yang dimiliki oleh pemerintah (Sutopo & Kurniawan, 2021).

Indonesia juga aktif bekerja sama dengan negara-negara lain dalam menghadapi ancaman kejahatan siber lintas batas. Kejahatan siber tidak mengenal batas geografis, dan serangan dunia maya sering kali datang dari negara lain yang sulit untuk ditanggulangi tanpa adanya kerjasama internasional. Oleh karena itu, Indonesia menandatangani berbagai perjanjian internasional yang memungkinkan pertukaran informasi mengenai ancaman siber serta praktik terbaik dalam menangani serangan siber. Kerjasama ini sangat penting untuk memperkuat ketahanan siber nasional dan mengurangi risiko serangan yang dapat merusak sistem dan data vital negara.

Perjanjian internasional ini tidak hanya mencakup kerjasama dalam hal pertukaran informasi mengenai ancaman siber, tetapi juga dalam hal penyelidikan dan penegakan hukum terhadap pelaku kejahatan siber yang beroperasi di lintas negara. Kerjasama internasional ini juga memungkinkan Indonesia untuk mendapatkan bantuan teknis dan informasi terkait alat dan teknologi terbaru yang dapat digunakan untuk mendeteksi dan mencegah ancaman siber. Dengan adanya kerja sama internasional ini, Indonesia dapat lebih siap menghadapi serangan siber yang berasal dari luar negeri serta memperkuat sistem keamanan siber di dalam negeri (Purwanto, 2021).

Meskipun berbagai kebijakan dan inisiatif telah diimplementasikan, tantangan terbesar dalam pencegahan kejahatan siber di sektor publik adalah kesenjangan implementasi kebijakan antara pemerintah pusat dan pemerintah daerah. Tidak semua pemerintah daerah memiliki anggaran dan kapasitas yang memadai untuk melaksanakan kebijakan keamanan siber dengan efektif. Banyak pemerintah daerah yang masih kekurangan sumber daya manusia yang terampil di bidang keamanan siber, serta infrastruktur teknologi yang memadai untuk melaksanakan kebijakan yang telah ditetapkan.

Penting untuk memberikan dukungan lebih lanjut kepada pemerintah daerah, baik dalam bentuk pendanaan, pelatihan sumber daya manusia, maupun infrastruktur teknologi yang diperlukan untuk

meningkatkan kemampuan dalam menangani ancaman siber. Pemerintah pusat perlu memastikan bahwa setiap daerah, baik yang berada di pusat kota maupun di daerah terpencil, memiliki kapasitas yang cukup untuk melindungi data dan informasi publik. Dengan demikian, kebijakan keamanan siber di sektor publik dapat diterapkan secara merata di seluruh Indonesia, tanpa terkecuali.

Penting untuk meningkatkan kesadaran di kalangan pejabat pemerintah daerah mengenai pentingnya keamanan siber dan perlindungan data pribadi. Sering kali, minimnya pemahaman tentang ancaman siber dan potensi risikonya menjadi penghambat dalam upaya implementasi kebijakan keamanan siber. Oleh karena itu, program pelatihan dan edukasi yang terstruktur harus diberikan kepada para pejabat pemerintah daerah agar dapat lebih memahami pentingnya perlindungan data dan sistem informasi serta dapat bertindak lebih proaktif dalam mencegah terjadinya serangan siber.

2. Kebijakan Pencegahan Kejahatan Siber di Sektor Swasta

Di sektor swasta, kebijakan pencegahan kejahatan siber sangat penting karena banyak perusahaan yang mengelola data pribadi konsumen atau informasi sensitif yang dapat menjadi sasaran serangan siber. Dalam beberapa tahun terakhir, kesadaran akan pentingnya perlindungan data semakin meningkat di kalangan pelaku usaha. Hal ini seiring dengan meningkatnya ancaman siber yang semakin kompleks dan beragam. Banyak perusahaan yang mulai memperkuat kebijakan keamanan siber dengan mematuhi standar internasional, seperti ISO 27001, yang membantu dalam membangun sistem manajemen keamanan informasi yang terstruktur dan efektif.

Sebagai respons terhadap ancaman yang terus berkembang, banyak perusahaan di Indonesia mulai berinvestasi dalam perangkat lunak keamanan yang canggih untuk melindungi datanya dari potensi ancaman. Salah satu kebijakan yang banyak diterapkan adalah penggunaan sistem keamanan berbasis risiko. Dalam hal ini, perusahaan melakukan analisis mendalam untuk mengetahui potensi ancaman dan risiko terhadap data serta infrastruktur. Dengan demikian, perusahaan dapat merancang kebijakan dan memilih teknologi yang tepat untuk mengatasi masalah tersebut.

Perusahaan-perusahaan juga semakin mengintegrasikan teknologi enkripsi yang lebih kuat, sehingga data yang disimpan dan

dikirimkan tetap terlindungi dengan baik dari serangan. Selain itu, sistem otentikasi dua faktor (2FA) juga diterapkan untuk meningkatkan lapisan keamanan. Teknologi ini menambahkan langkah verifikasi tambahan saat seseorang mencoba mengakses akun atau data penting, yang dapat meminimalisir kemungkinan kebocoran data (Sutopo, 2020). Perusahaan besar yang beroperasi di sektor e-commerce, perbankan, dan sektor lainnya yang mengelola data pribadi juga diwajibkan untuk mengikuti regulasi perlindungan data pribadi, seperti yang tercantum dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Undang-undang ini mewajibkan perusahaan untuk mematuhi prosedur perlindungan data yang ketat dan menerapkan langkah-langkah untuk mencegah penyalahgunaan data pribadi. Perusahaan yang tidak mematuhi regulasi ini akan dikenakan sanksi administratif, yang bertujuan untuk mendorong perusahaan untuk lebih serius dalam menjaga keamanan datanya (Purwanto & Hendriyana, 2021).

Beberapa perusahaan juga membentuk unit khusus yang bertugas untuk menangani insiden siber. Unit ini bertanggung jawab untuk segera mendeteksi, menanggulangi, dan melaporkan insiden yang terjadi, serta mengurangi dampak dari serangan siber yang mungkin terjadi. Keberadaan unit khusus ini sangat penting untuk memastikan bahwa setiap insiden yang terjadi dapat ditangani dengan cepat dan tepat sehingga tidak berdampak buruk bagi perusahaan dan pelanggannya. Namun, meskipun kebijakan keamanan siber di sektor swasta mulai berkembang, masih ada sejumlah tantangan yang harus dihadapi oleh perusahaan, terutama oleh Usaha Mikro, Kecil, dan Menengah (UMKM). Salah satu masalah terbesar adalah kesenjangan teknologi antara perusahaan besar dan UMKM. Perusahaan besar umumnya memiliki anggaran yang lebih besar dan sumber daya yang memadai untuk mengimplementasikan kebijakan keamanan yang canggih. Sebaliknya, banyak UMKM yang belum memiliki kapasitas yang cukup untuk mengadopsi teknologi keamanan yang memadai, meskipun juga mengelola data konsumen yang sangat sensitif.

Untuk mengatasi masalah ini, diperlukan inisiatif dari pemerintah dan sektor swasta untuk menyediakan pelatihan, serta dukungan teknis bagi UMKM. Pelatihan ini dapat meliputi berbagai topik terkait dengan cara melindungi data pelanggan, cara menghadapi ancaman siber, serta teknologi yang dapat digunakan untuk memperkuat sistem keamanannya. Selain itu, pemerintah dapat menyediakan insentif

atau bantuan teknis untuk membantu UMKM dalam mengadopsi sistem keamanan yang lebih baik. Di sisi lain, penting juga untuk mendorong perusahaan-perusahaan besar untuk berbagi pengetahuan dan sumber daya dengan UMKM dalam hal keamanan siber. Kolaborasi antara perusahaan besar dan UMKM ini dapat membantu memperkecil kesenjangan dalam hal kapasitas keamanan siber dan memastikan bahwa seluruh sektor swasta, baik perusahaan besar maupun kecil, dapat beroperasi dalam ekosistem digital yang aman dan terlindungi. Dengan dukungan yang tepat, UMKM juga dapat memitigasi risiko dan melindungi datanya dengan lebih baik.

D. Menuju Sistem Keamanan Digital yang Lebih Kuat dan Berkeadilan

1. Meningkatkan Infrastruktur Keamanan Digital di Indonesia

Keamanan digital di Indonesia semakin menjadi perhatian utama seiring dengan pesatnya transformasi digital yang terjadi dalam berbagai sektor. Dalam era yang didominasi oleh teknologi informasi, semakin banyak data yang dikelola secara digital, mulai dari data pribadi hingga data perusahaan, yang semuanya rentan terhadap ancaman siber. Infrastruktur yang aman dan kuat sangat diperlukan untuk mendukung sistem keamanan yang efektif, yang dapat menghindarkan masyarakat dan sektor bisnis dari ancaman yang datang dari dunia maya. Salah satu langkah penting yang dilakukan oleh pemerintah Indonesia untuk memperkuat infrastruktur keamanan digital adalah dengan membentuk Badan Siber dan Sandi Negara (BSSN). BSSN memiliki peran utama dalam merancang dan mengimplementasikan kebijakan keamanan siber nasional serta memberikan pelatihan kepada sektor publik dan swasta dalam hal pengamanan data dan sistem informasi.

Meskipun upaya dari pemerintah sudah berjalan, tantangan besar masih dihadapi, terutama dalam hal penyediaan infrastruktur yang memadai di berbagai sektor, khususnya di daerah-daerah yang kurang berkembang. Ketimpangan ini berpotensi menjadi celah yang dimanfaatkan oleh pelaku kejahatan siber. Infrastruktur keamanan siber yang tidak merata di seluruh Indonesia bisa membuka peluang bagi serangan yang merusak. Untuk itu, dibutuhkan kerjasama yang lebih erat antara pemerintah, sektor swasta, dan organisasi internasional untuk memastikan bahwa semua lapisan masyarakat, baik yang berada di pusat

maupun daerah, memiliki akses yang sama terhadap infrastruktur yang aman dan canggih. Salah satu cara yang dapat dilakukan adalah dengan mengembangkan pelatihan untuk meningkatkan keterampilan dalam bidang keamanan siber, yang akan membantu membangun kapasitas manusia dalam menghadapi ancaman digital.

Penting bagi Indonesia untuk fokus pada sektor-sektor kritikal yang menjadi sasaran potensial bagi serangan siber. Sektor-sektor seperti energi, perbankan, dan transportasi memiliki peranan vital dalam perekonomian Indonesia, sehingga perlindungannya harus menjadi prioritas utama. Infrastruktur yang mendukung sektor-sektor ini harus diperkuat dengan penggunaan teknologi mutakhir, seperti firewall yang canggih, sistem deteksi intrusi, serta perangkat otentikasi yang dapat mengidentifikasi dan mencegah serangan siber lebih dini. Keamanan pada sektor-sektor tersebut harus dijaga agar sistem yang ada tetap berjalan dengan baik, mengingat bahwa gangguan pada sektor-sektor vital ini bisa menimbulkan dampak yang sangat luas bagi masyarakat dan perekonomian negara.

Peningkatan infrastruktur keamanan digital juga harus melibatkan sektor swasta, terutama perusahaan-perusahaan besar yang mengelola data dalam jumlah besar. Perusahaan-perusahaan seperti yang bergerak di bidang e-commerce dan perbankan digital harus mengambil langkah lebih tegas dalam memperkuat sistem keamanan. Salah satu upaya yang bisa dilakukan adalah dengan mengimplementasikan teknologi enkripsi yang kuat untuk melindungi data pribadi pelanggan, serta menggunakan sistem otentikasi dua faktor (2FA) sebagai langkah perlindungan tambahan. Penggunaan teknologi-teknologi ini akan sangat membantu dalam mengurangi risiko kebocoran data yang bisa merugikan perusahaan dan mengancam privasi pelanggan.

Pengembangan pusat data yang aman juga menjadi salah satu langkah krusial dalam memperkuat infrastruktur keamanan digital. Pusat data yang dikelola dengan baik dapat memastikan bahwa informasi penting tersimpan dengan aman dan terlindungi dari ancaman luar. Untuk itu, pemerintah bersama sektor swasta perlu memastikan bahwa pusat-pusat data yang dibangun di Indonesia mematuhi standar internasional dalam hal perlindungan data dan keamanan sistem. Pusat data yang memenuhi standar ini tidak hanya akan meningkatkan kepercayaan pengguna, tetapi juga memperkuat ketahanan sistem informasi di Indonesia terhadap ancaman siber.

Seiring dengan semakin kompleksnya ancaman siber, Indonesia perlu terus berinovasi dalam mengembangkan teknologi keamanan digital yang lebih maju. Salah satu pendekatan yang bisa digunakan adalah dengan memanfaatkan kecerdasan buatan (AI) untuk mendeteksi dan merespons ancaman secara real-time. AI dapat digunakan untuk mengidentifikasi pola serangan yang mencurigakan dan memberikan peringatan lebih cepat kepada pihak yang berwenang. Teknologi ini juga memungkinkan sistem untuk belajar dan beradaptasi dengan ancaman baru yang muncul, sehingga tingkat keberhasilan dalam menangani serangan siber dapat ditingkatkan. Pengembangan teknologi seperti ini akan sangat membantu dalam menciptakan sistem keamanan yang lebih efektif dan responsif terhadap ancaman yang ada.

Sektor pendidikan juga memiliki peran penting dalam membangun infrastruktur keamanan digital yang lebih baik di Indonesia. Pendidikan yang berfokus pada keamanan siber harus ditanamkan sejak dini untuk menciptakan generasi yang memiliki pemahaman yang lebih baik tentang pentingnya menjaga keamanan digital. Program-program pelatihan dan pendidikan yang mengajarkan keterampilan teknis dalam keamanan siber harus terus diperluas, baik untuk sektor publik maupun swasta. Hal ini akan memastikan bahwa negara memiliki tenaga ahli yang siap menghadapi tantangan keamanan digital yang terus berkembang.

Kolaborasi antara sektor publik dan swasta juga harus diperkuat untuk menciptakan sistem keamanan digital yang lebih menyeluruh. Pemerintah dapat bekerja sama dengan perusahaan-perusahaan teknologi besar untuk mengembangkan sistem keamanan yang lebih canggih, serta berbagi informasi terkait potensi ancaman yang sedang berkembang. Selain itu, kerjasama internasional juga sangat penting, mengingat ancaman siber sering kali bersifat global dan lintas negara. Indonesia perlu terlibat dalam jaringan kerja sama internasional yang memungkinkan pertukaran informasi dan praktik terbaik dalam hal keamanan siber, sehingga negara dapat memperkuat ketahanannya terhadap serangan yang bersifat lintas batas.

Upaya untuk meningkatkan kesadaran masyarakat akan pentingnya keamanan digital harus menjadi prioritas. Pendidikan dan penyuluhan mengenai cara-cara melindungi data pribadi dan mengenali potensi ancaman harus dilakukan secara menyeluruh kepada seluruh lapisan masyarakat. Tanpa kesadaran yang tinggi di kalangan

masyarakat, semua langkah penguatan infrastruktur keamanan digital akan kurang efektif. Oleh karena itu, kampanye kesadaran siber harus dijalankan secara terus-menerus, baik oleh pemerintah, lembaga pendidikan, maupun sektor swasta, untuk menciptakan budaya keamanan digital yang kuat di Indonesia.

2. Menjamin Keadilan dalam Akses dan Perlindungan Keamanan Digital

Untuk menciptakan sistem keamanan digital yang adil, sangat penting untuk memastikan bahwa setiap individu, tanpa memandang latar belakang atau lokasi geografis, memiliki akses yang setara terhadap perlindungan digital yang memadai. Dalam dunia yang semakin terhubung, ketidaksetaraan dalam akses terhadap teknologi dan pengetahuan tentang keamanan digital dapat menjadi celah yang memperburuk kerentanannya terhadap serangan siber. Di Indonesia, ketidakmerataan ini sering kali terjadi antara daerah perkotaan dan pedesaan, serta di antara individu yang memiliki latar belakang pendidikan atau ekonomi yang lebih rendah. Oleh karena itu, kebijakan yang menekankan keadilan sosial harus menjadi prioritas dalam pengembangan dan implementasi sistem keamanan digital yang berkelanjutan.

Salah satu cara untuk mencapai hal tersebut adalah dengan meningkatkan literasi digital di seluruh lapisan masyarakat. Literasi digital tidak hanya berkaitan dengan kemampuan dasar untuk menggunakan teknologi, tetapi juga mencakup pemahaman yang lebih dalam mengenai risiko yang ada di dunia maya dan bagaimana cara melindungi diri darinya. Masyarakat yang teredukasi dengan baik tentang ancaman siber akan lebih mampu mengenali potensi bahaya dan mengambil langkah-langkah pencegahan yang diperlukan untuk melindungi data pribadinya. Oleh karena itu, pemerintah, sektor swasta, dan lembaga pendidikan perlu bekerja sama untuk mengembangkan berbagai program pelatihan, seminar, dan kampanye yang dapat menjangkau seluruh elemen masyarakat. Program-program ini harus bersifat inklusif, mencakup segala lapisan masyarakat, termasuk yang berada di daerah terpencil atau kurang memiliki akses terhadap teknologi.

Sebagai contoh, pemerintah dapat meluncurkan program edukasi tentang keamanan digital yang difokuskan pada kelompok-kelompok masyarakat yang lebih rentan, seperti anak-anak, lansia, dan individu

yang baru mengenal dunia digital. Dalam program-program ini, materi tentang cara menghindari penipuan online, pentingnya penggunaan kata sandi yang kuat, serta bagaimana melindungi data pribadi, dapat disosialisasikan dengan cara yang mudah dipahami oleh berbagai kelompok masyarakat. Selain itu, sektor swasta juga harus terlibat dalam meningkatkan kesadaran mengenai keamanan digital. Perusahaan-perusahaan yang bergerak di bidang teknologi dapat berperan aktif dalam menyediakan informasi dan alat yang diperlukan untuk melindungi data pengguna, sekaligus menyelenggarakan pelatihan-pelatihan terkait.

Salah satu aspek penting lainnya dalam menjamin keadilan dalam perlindungan data dan keamanan digital adalah penyusunan kebijakan dan regulasi yang mengutamakan kesetaraan. Dalam hal ini, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022 memberikan kerangka hukum yang lebih kuat untuk melindungi data pribadi masyarakat Indonesia. Namun, meskipun UU ini memberikan pengaturan yang lebih ketat mengenai perlindungan data pribadi, implementasinya harus memperhatikan aspek keadilan, terutama terkait dengan akses teknologi yang berbeda-beda di berbagai daerah. Untuk itu, penting bagi pemerintah untuk memastikan bahwa kebijakan ini tidak hanya berlaku untuk entitas yang memiliki sumber daya yang cukup, tetapi juga dapat diterapkan secara adil oleh instansi pemerintah dan sektor swasta yang berada di daerah-daerah dengan keterbatasan teknologi.

Untuk memastikan kebijakan ini berjalan dengan baik, pemerintah harus menyediakan dukungan yang cukup bagi daerah-daerah yang memiliki keterbatasan sumber daya. Misalnya, dengan memberikan bantuan berupa perangkat keras dan perangkat lunak yang sesuai, serta pelatihan kepada pemerintah daerah dan sektor swasta untuk memastikan bahwa dapat mengimplementasikan kebijakan tersebut secara efektif. Implementasi yang tidak memadai di daerah-daerah tertentu dapat menciptakan ketidakadilan, di mana sebagian masyarakat terlindungi dengan baik, sementara yang lainnya tetap rentan terhadap ancaman siber.

Pengembangan dan implementasi sistem keamanan digital yang kuat juga memerlukan pengawasan dan penegakan hukum yang tegas. Tanpa adanya mekanisme pengawasan yang efektif, kebijakan yang telah diterapkan dapat disalahgunakan atau diabaikan. Oleh karena itu,

pemerintah harus memperkuat lembaga penegak hukum yang bertugas menangani kejahatan siber, serta memberikan pelatihan khusus yang relevan dengan perkembangan teknologi yang semakin pesat, seperti teknologi berbasis cloud dan blockchain. Dengan adanya pengawasan yang transparan dan responsif, pelanggaran terhadap kebijakan keamanan siber dan perlindungan data pribadi dapat ditindak dengan adil, sesuai dengan ketentuan yang berlaku.

Penting juga bagi lembaga penegak hukum untuk memiliki kemampuan dalam mendeteksi dan menyelidiki serangan siber yang lebih kompleks. Serangan siber saat ini semakin canggih dan sering kali melibatkan teknologi baru, seperti serangan terhadap sistem berbasis cloud atau eksploitasi kelemahan dalam teknologi blockchain. Oleh karena itu, lembaga penegak hukum perlu terus memperbarui kemampuan teknis agar dapat menangani kasus-kasus yang terkait dengan ancaman siber terbaru. Hal ini juga penting untuk memastikan bahwa dapat bertindak cepat dan efisien dalam menanggulangi serangan, serta memberikan perlindungan yang setara bagi semua warga negara, tanpa memandang status sosial atau lokasi geografis.

Pemerintah juga perlu memastikan bahwa terdapat kesetaraan dalam hal akses terhadap saluran pengaduan dan bantuan hukum terkait kejahatan siber. Masyarakat, terutama yang berada di daerah-daerah yang lebih terisolasi, harus dapat mengakses layanan ini dengan mudah. Ini bisa dilakukan dengan mengembangkan pusat-pusat pengaduan yang dapat diakses secara online maupun offline, sehingga masyarakat dapat segera melaporkan insiden yang dialami dan mendapatkan bantuan hukum yang diperlukan. Selain itu, penting juga untuk menjamin bahwa semua individu memiliki hak yang setara untuk mendapatkan informasi mengenai bagaimana melindungi dirinya dari ancaman siber, termasuk akses ke alat dan perangkat yang dapat membantunya menjaga keamanan data pribadi.

Pada konteks ini, transparansi juga berperan kunci. Pemerintah harus menyediakan informasi yang jelas dan terbuka mengenai kebijakan perlindungan data dan keamanan siber, serta bagaimana masyarakat dapat berpartisipasi dalam upaya melindungi data pribadinya. Informasi yang disampaikan harus mudah dipahami oleh seluruh lapisan masyarakat, termasuk yang tidak memiliki latar belakang teknis. Dengan cara ini, seluruh masyarakat dapat merasa terlibat dalam menciptakan ekosistem digital yang aman, adil, dan setara.

DAFTAR PUSTAKA

Al-Fadly, M. (2020). *Cybercrime* and Its Impact on E-Commerce in Indonesia. Journal of Information Technology, 13(4), 112-126.

Amnesty International. (2019). Freedom of Expression and Hate Speech: Legal Boundaries and Social Implications.

Andi Hamzah. (2001). Delik-Delik Khusus. Jakarta: Sinar Grafika.

APJII. (2021). Penetrasi dan Perilaku Pengguna Internet di Indonesia 2021.

APNIC. (2022). Cybersecurity Threats in the Asia Pacific Region.

Arief, Barda Nawawi. (2012). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan. Jakarta: Kencana.

Australian National University. (2018). Cybersecurity and National Security: The New Frontier of Threats.

Bada, A., Sasse, M. A., & Nurse, J. R. (2019). *Cybercrime*: Understanding the Global Threat. Oxford University Press.

Badan Siber dan Sandi Negara (BSSN). (2020). Laporan Tahunan Keamanan Siber Indonesia 2020. Jakarta: Badan Siber dan Sandi Negara Republik Indonesia.

Barda Nawawi Arief. (2022). Pembaharuan Hukum Pidana dalam Konteks KUHP Nasional. Semarang: Badan Penerbit Universitas Diponegoro.

Bareskrim Polri. (2023). Laporan Tahunan Kejahatan Siber. Jakarta.

Bertino, E., Sandhu, R., & Niazi, M. (2019). Digital Forensics: Challenges and Advances. Springer.

Binns, R. (2018). The Ethics of Autonomous Systems: A Critical Review. Technology and Ethics, 45(2), 213-229.

Blair, J., & Schauf, T. (2017). Digital Evidence and the Law: A Guide for Legal Professionals. Elsevier.

Boulton, M. (2019). The Impact of Hate Speech on Social Harmony. Oxford University Press.

Brenner, Susan W. (2010). *Cybercrime*: Criminal Threats from Cyberspace. Santa Barbara: Praeger.

BSSN. (2023). Laporan Statistik Serangan Siber di Indonesia Tahun 2022. Jakarta: Badan Siber dan Sandi Negara.

Budapest Convention. (2001). Convention on *Cybercrime*. Council of Europe.

Casey, E. (2011). Handbook of Digital Forensics and Investigation. Academic Press.

Casey, Eoghan. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.

Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(3), 1753-1802.

Cybersecurity and Infrastructure Security Agency (CISA). (2020). National Infrastructure Protection Plan (NIPP): Cybersecurity and Critical Infrastructure.

Cybersecurity Ventures. (2023). *Cybercrime* Report 2023.

Department of Homeland Security. (2018). Cybersecurity and Infrastructure Security: The Growing Threat of Cyberattacks.

Dewi, S. (2019). Hukum dan Kebijakan Perlindungan Privasi di Era Digital. Jakarta: Rajawali Pers.

Dube, L., Kauffman, R., & Hevner, A. R. (2020). Cybersecurity in the Digital Economy: A Case Study on Indonesia's Challenges. Journal of Cybersecurity and Digital Trust, 5(2), 34-50.

Dutton, W. H. (2018). The Internet and the Future of Cybersecurity: Challenges for Governments. Oxford University Press.

European Commission (2017). Estonia's National Cybersecurity Strategy: A Case Study. European Commission.

European Union Agency for Cybersecurity (ENISA). (2019). Cybersecurity for Critical Infrastructure Protection.

Facebook. (2018). Facebook Data Breach and Privacy Concerns.

Facebook-Cambridge Analytica Data Scandal. (2018). The Guardian.

Federal Trade Commission (FTC) (2017). Equifax Data Breach: What You Need to Know. Federal Trade Commission.

Federal Trade Commission (FTC). (2020). Consumer Sentinel Network Data Book.

Fogg, B. J. (2003). Persuasive Technology: Using Computers to Change What We Think and Do. Elsevier.

Garrett, B. (2013). Digital Forensics and Cyber Crime: 5th International Conference, ICDF2C 2013. Springer.

Goh, P., & Tan, K. (2021). Adversarial Machine Learning and AI Security in Cyber Threat Detection. International Journal of Cyber Security, 22(2), 200-215.

Government of Russia (2016). The Federal Law on Information, Information Technology, and Information Protection. Government of Russia.

Hidayat, R. (2020). Cyber Terrorism in Southeast Asia: Threats and Security Measures. Jakarta: Cybersecurity and Policy Journal.

Hidayat, S. (2021). Perbandingan Perlindungan Data Pribadi di Negara Asia Tenggara. Jakarta: Indonesian Digital Law Journal.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime* and Digital Forensics: An Introduction. Routledge.

IBM. (2023). Cost of a Data Breach Report 2023.

Indonesian Ministry of Communications and Information Technology. (2022). Regulation on Online Hate Speech and Misinformation.

Interpol. (2022). *Cybercrime*. https://www.interpol.int/en/Crimes/*Cybercrime*

Interpol. (2023). *Cybercrime* Threat Response Report.

Jansen, W., & Ayers, R. (2013). Guidelines on Digital Evidence. National Institute of Standards and Technology (NIST).

Kaspersky. (2021). The State of Cybersecurity 2021: Trends in *Cybercrime*.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). Harmonisasi Regulasi Keamanan Siber di Indonesia. Jakarta: Kominfo.

Khan, M., & Al-Hadhrami, T. (2021). AI for Cybersecurity: A Comprehensive Review. Journal of Computer Security, 29(4), 324-337.

Komnas HAM. (2022). Laporan Tahunan Hak Asasi Manusia Indonesia.

KUHP (Wetboek van Strafrecht voor Nederlandsch-Indië).

Kuncoro, M. (2020). Strategi Keamanan Siber Indonesia dalam Menyongsong Era Digital. Jurnal Teknologi Informasi, 15(1), 24-38.

Kurniawan, Y. (2020). Keamanan Siber di Indonesia: Tantangan dan Kebijakan Pemerintah. Jurnal Keamanan Nasional, 8(3), 45-56.

Livingstone, S., & Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies. Journal of Child Psychology and Psychiatry.

Luh, D. & Prayoga, P. (2021). Harmonisasi Undang-Undang ITE dan Perlindungan Data Pribadi: Tantangan dan Solusi. Jurnal Hukum Digital, 8(3), 215-233.

MAFINDO. (2022). Laporan Tahunan Penyebaran *Hoaks* di Indonesia.

Mahendra, D. & Nugroho, Y. (2019). Analisis Penguatan Undang-Undang ITE dalam Menanggulangi Kejahatan Siber di Indonesia. Jurnal Hukum & Teknologi, 12(2), 118-136.

Martin, M. (2007). The 2007 Cyberattacks Against Estonia: A Comparative Analysis. International Journal of Cybersecurity.

McAfee. (2020). The Cost of *Cybercrime*: Impact on National Security and Economy.

McKemmish, R. (2016). Forensic Investigation of *Cybercrime*: Emerging Trends and Technologies. Springer.

Microsoft. (2020). Digital Crime and Cyber Fraud: The Growing Threat.

National Cyber Security Centre (2018). Cybersecurity Laws in China: A Review. National Cyber Security Centre.

National Cyber Security Centre (NCSC). (2020). The Rise of Privacy Breaches and Identity Theft.

National Institute of Standards and Technology (NIST). (2019). Framework for Improving Critical Infrastructure Cybersecurity.

NATO Cooperative Cyber Defence Centre of Excellence (2019). The Legal Framework of Cybersecurity and Digital Evidence. NATO CCDCOE Publications.

NIST (National Institute of Standards and Technology). (2021). Cybersecurity Framework: Managing Cyber Risks to Critical Infrastructure.

Nugroho, A., & Utami, P. (2020). Hukum Siber Indonesia. Yogyakarta: Pustaka Pelajar.

Nugroho, R. (2023). Global Standards in Data Protection and Cybersecurity: A Comparative Analysis. Yogyakarta: Gadjah Mada University Press.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group.

Oxford Internet Institute. (2022). Global Inventory of Organized Social Media Manipulation.

Patel, J. (2019). Ethics and Privacy Concerns in Artificial Intelligence for Cybersecurity. Journal of Ethical AI and Technology, 7(1), 58-72.

Pew Research Center. (2020). The Spread of Fake News on Social Media: A Global Perspective.

Pew Research Center. (2020). The State of Cyberbullying: A Global Concern.

Pomerantsev, P. (2018). Nothing is True and Everything is Possible: The Surreal Heart of the New Russia. Faber & Faber.

Proofpoint. (2022). State of the Phish Report.

Purwanto, A. (2021). Keamanan Siber di Indonesia: Kolaborasi Antar Sektor Publik dan Swasta. Jurnal Manajemen Keamanan, 13(4), 112-125.

Purwanto, A. (2021). Transformasi dan Penguatan Regulasi Keamanan Siber di Indonesia. Bandung: Universitas Padjadjaran Press.

Putri, D. A., & Nugraha, M. A. (2021). "Evaluasi Hukum terhadap Implementasi UU ITE dalam Kasus Pencemaran Nama Baik di Media Sosial." Jurnal Hukum & Teknologi, 3(2).

Rafique, M., & Niazi, M. (2020). Advancements in Cyber Forensics: A Guide to Investigating the Digital Criminal Landscape. Elsevier.

Raghavan, M., & Vo, J. (2020). Digital Evidence in Law and Practice: A Guide for Lawyers and Forensic Experts. Wiley.

Regulasi Perlindungan Data Pribadi (UU No. 27/2022), Pemerintah Republik Indonesia.

SAFEnet. (2021). Catatan Situasi Hak Digital Indonesia.

Satya, D. (2020). Perlindungan Data Pribadi dalam UU ITE dan Implikasinya terhadap Keamanan Siber. Jakarta: Kominfo.

Shinder, D. L., & Cross, M. (2021). Scene of the *Cybercrime*: Computer Forensics Handbook. Elsevier.

Shrestha, S., & Raghav, S. (2020). Challenges and Future Directions of AI in Cybersecurity. Springer.

Smith, R. (2020). Artificial Intelligence in Cybersecurity: Detection, Prevention, and Automation. Wiley.

Soedarto. (2015). Hukum Pidana dan Perkembangannya. Semarang: Fakultas Hukum UNDIP.

Stuxnet: An Overview of Cyber Warfare. (2011). International Journal of Cyber Security, 5(4), 102-114.

Suryanto, D. (2021). “Tantangan Penegakan Hukum Siber di Indonesia.” Jurnal Kriminologi Indonesia, 17(1).
Susanto, P. (2020). Harmonisasi Hukum di Era Digital: Mengatasi Tantangan Kejahatan Siber di Indonesia. Yogyakarta: Andi Publisher.
Sutopo, A. (2020). Kebijakan Keamanan Siber di Sektor Swasta. Jurnal Teknologi dan Keamanan Digital, 12(2), 89-102.
Symantec. (2019). Internet Security Threat Report.
The Data Protection Commission, Singapore. (2022). Annual Report 2022.
Tim Penyusun Hukumonline. (2023). Poin-Poin Penting KUHP Baru: Penjelasan dan Implikasi. Jakarta: Hukumonline.
Tiwari, S., & Khandelwal, H. (2019). Digital Forensics: An Introduction to Digital Investigation. Springer.
UN Women. (2020). Online and ICT-facilitated Violence Against Women and Girls.
Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
United Nations Office on Drugs and Crime (UNODC). (2019). Cyber Terrorism: A Global Threat to National Security.
United Nations Office on Drugs and Crime (UNODC). (2019). *Cybercrime*: A Growing Threat to Privacy and Security.
United Nations. (2020). Combating Hate Speech in the Digital Age: Guidelines for Government and Civil Society.
UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional).
UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, jo. UU No. 19 Tahun 2016.
UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008.
Verizon. (2023). Data Breach Investigations Report (DBIR).
Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer Vieweg.
Wall, David S. (2007). *Cybercrime*: The Transformation of Crime in the Information Age. Polity Press.
Widodo Ekatjahjana. (2023). “Problematika Hukum Pidana Siber dalam Perspektif KUHP Baru.” Jurnal Hukum dan Teknologi, 8(1).

World Economic Forum. (2023). Global Cybersecurity Outlook 2023.
World Health Organization (WHO). (2018). The Role of Media and Social Networks in Spreading Hoaxes and Misinformation.
Yusof, R. & Abdullah, M. (2017). Impact of Cyber Terrorism on National Security and Infrastructure. International Journal of Computer Science, 13(2), 120-135.
Zetter, K. (2016). China's APT10 Cyber Espionage Group Hacks US and Japanese Firms. Wired.
Zhang, X., & Liu, Y. (2019). Artificial Intelligence for Network Security and *Cybercrime* Detection. Springer.
Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
Zuckerman, E. (2017). How Social Media Fuels the Spread of Misinformation. Harvard University Press.

GLOSARIUM

Cybercrime	Kejahatan yang dilakukan melalui perangkat teknologi informasi atau sistem digital, baik secara langsung terhadap perangkat tersebut maupun melalui pemanfaatan jaringan komputer untuk melakukan tindak pidana seperti penipuan, pencurian data, atau peretasan.
Data	Informasi dalam bentuk digital yang dikumpulkan, disimpan, dan diolah oleh sistem komputer untuk berbagai tujuan, mulai dari komunikasi hingga analisis informasi.
Digital	Segala sesuatu yang berkaitan dengan data atau sistem yang berbasis bilangan biner (0 dan 1), yang menjadi dasar pengoperasian teknologi informasi dan komunikasi modern.
Enkripsi	Proses konversi data menjadi bentuk kode tertentu yang hanya dapat dibaca oleh pihak yang memiliki kunci atau otorisasi, digunakan untuk menjaga kerahasiaan dan keamanan informasi digital.
Forensik	Cabang ilmu yang digunakan untuk menginvestigasi kejahatan dengan mengumpulkan, menganalisis, dan memverifikasi bukti, termasuk bukti digital dalam kasus kejahatan siber.
Hoaks	Informasi palsu atau bohong yang sengaja dibuat dan disebarkan untuk menipu, memprovokasi, atau memanipulasi opini publik di ruang digital.
Hukum	Sistem aturan dan norma yang disusun oleh otoritas yang sah untuk mengatur kehidupan masyarakat, dengan sanksi yang mengikat bagi pelanggar, serta berfungsi sebagai pedoman dan pelindung dalam interaksi sosial, termasuk dalam ranah digital.

Jaringan	Sekumpulan perangkat komputer dan sistem komunikasi yang terhubung satu sama lain untuk memungkinkan pertukaran data dan informasi secara elektronik, baik dalam skala lokal maupun global.
Malware	Singkatan dari malicious software, yaitu perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses ilegal ke sistem komputer atau data pengguna.
Penegakan	Proses implementasi dan pelaksanaan hukum oleh aparat yang berwenang seperti polisi, jaksa, dan hakim, guna memastikan bahwa setiap pelanggaran hukum, termasuk kejahatan siber, ditindak sesuai aturan yang berlaku.
Peretasan	Aksi tidak sah yang dilakukan untuk mendapatkan akses ke sistem komputer, jaringan, atau data, biasanya dengan tujuan mencuri, merusak, atau memanipulasi informasi digital.
Phishing	Teknik penipuan daring di mana pelaku menyamar sebagai entitas terpercaya untuk memperoleh informasi sensitif dari korban, seperti kata sandi, nomor rekening, atau data pribadi lainnya.
Privasi	Hak individu untuk mengontrol data pribadi, termasuk hak untuk mengetahui, mengakses, dan membatasi siapa yang dapat melihat atau menggunakan informasi tersebut.
Regulasi	Peraturan tertulis yang ditetapkan oleh pemerintah atau lembaga berwenang untuk mengatur dan mengendalikan suatu bidang tertentu, seperti penggunaan teknologi dan pencegahan kejahatan siber, agar tercipta ketertiban dan perlindungan hukum.
Siber	Merujuk pada segala hal yang berkaitan dengan ruang digital atau jaringan komputer, termasuk aktivitas komunikasi, transaksi, dan pertukaran informasi yang terjadi melalui sistem teknologi informasi dan internet.

Spam	Pesan elektronik yang dikirim secara massal dan tidak diinginkan oleh penerima, biasanya berisi iklan atau konten menyesatkan yang dapat mengganggu atau membahayakan pengguna internet.
Undang-undang	Produk hukum yang disahkan oleh lembaga legislatif dan menjadi dasar legal formal dalam penanganan berbagai persoalan, termasuk untuk mengatur kejahatan yang terjadi di ruang digital.
Yuridiksi	Kewenangan hukum yang dimiliki oleh suatu negara atau lembaga untuk mengadili dan menetapkan hukum atas suatu tindakan atau peristiwa, termasuk dalam konteks lintas negara dalam kasus kejahatan siber.

INDEKS

A

akademik · 40
aksesibilitas · 96, 156
audit · 24, 107, 143, 150, 167, 175

B

big data · 97, 146, 165
blockchain · 115, 165, 172, 183

C

cloud · 96, 99, 148, 159, 168, 183

D

digitalisasi · 22, 53
distribusi · 18, 19, 37, 44
domestik · 13, 125, 126, 127, 132, 138

E

e-commerce · 4, 9, 17, 22, 30, 31, 32, 33, 94, 148, 161, 168, 169, 170, 172, 177, 179
ekonomi · 1, 3, 7, 9, 10, 12, 16, 17, 29, 31, 34, 35, 37, 45, 48, 51, 54, 56, 62, 77, 82, 92, 127, 130, 131, 137, 139, 144, 152, 161, 168, 173, 181
entitas · 44, 45, 138, 182, 194
etnis · 48, 49

F

finansial · 3, 6, 9, 12, 29, 31, 33, 34, 35, 37, 42, 60, 62, 101, 109, 110, 137, 138, 141, 144, 145, 149, 150, 155
fintech · 170
firewall · 148, 179
fundamental · 147

G

genetika · 23

geografis · 1, 4, 66, 73, 148, 175, 181, 183

H

hoaks · 1, 11, 21, 38, 45, 46, 47, 48, 50, 66, 102, 107, 132, 158, 159, 160, 161

I

implikasi · 31, 124, 125
infrastruktur · 2, 7, 13, 15, 24, 26, 27, 29, 34, 35, 36, 37, 38, 51, 52, 53, 54, 55, 56, 57, 58, 67, 77, 78, 79, 80, 82, 92, 94, 99, 101, 107, 112, 114, 115, 117, 120, 121, 124, 125, 126, 127, 128, 130, 131, 132, 134, 135, 146, 149, 153, 169, 170, 174, 175, 176, 178, 179, 180
inklusif · 12, 132, 138, 140, 151, 181
integrasi · 11, 17, 21, 65, 131
integritas · 2, 4, 13, 18, 31, 46, 70, 74, 87, 100, 106, 141, 142, 145, 150, 172
internet of things · 118
investasi · 9, 12, 31, 56, 57, 85, 99, 106, 107, 132
investor · 38, 48

K

kolaborasi · 36, 41, 53, 57, 68, 72, 79, 80, 81, 82, 85, 89, 116, 117, 119, 134, 147, 150, 156, 173, 180
komoditas · 7, 22, 165
komprehensif · 8, 18, 20, 21, 25, 54, 86, 88, 90, 91, 93, 94, 114, 119, 121, 130, 140, 147, 156, 160, 171, 203
komputasi · 8
konkret · 46, 80
konsistensi · 24
kredit · 4, 9, 30, 42, 43, 45, 59, 145, 148, 172
kripto · 71

M

manifestasi · 3
manipulasi · 8, 10, 13, 30, 74, 75, 87, 145

O

otoritas · 26, 58, 59, 61, 62, 63, 65, 86, 100, 103, 120, 139, 142, 162, 193

P

politik · 1, 6, 9, 13, 16, 23, 34, 36, 43, 46, 48, 51, 56, 82, 130, 132, 135, 149, 152

R

real-time · 103, 106, 127, 150, 172, 180
regulasi · 1, 2, 3, 6, 15, 16, 18, 21, 22, 24, 25, 26, 27, 29, 32, 38, 43, 44, 45, 50, 51, 54, 65, 75, 77, 80, 82, 84, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 100, 101, 108, 115, 120, 121, 126, 131, 133, 134, 137, 138, 139, 146, 149, 151, 162, 166, 167, 171, 177, 182, 203
relevansi · 20, 21

S

siber · i, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 42, 43, 44, 45, 51, 52, 53, 54, 55, 56, 57, 60, 61, 63, 65, 66, 67, 68, 69, 70, 71, 72, 74, 75, 76, 77, 78, 79, 80, 81,82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 137,138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 165, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 193, 194, 195, 203
stabilitas · 1, 29, 37, 38, 42, 48, 49, 51, 56, 77, 82, 92, 129, 130, 149, 169, 173
stigma · 143, 156

T

transformasi · 6, 82, 144, 147, 151, 168, 170, 173, 178
transparansi · 107, 142, 143, 145, 146, 167, 183

W

workshop · 80, 114, 128

BIOGRAFI PENULIS

Dr. Kiki Kristanto, S.H., M.H.

Kiki Kristanto adalah nama penulis yang dilahirkan di Kota Palangka Raya Kalimantan Tengah pada tanggal 08 Maret 1983. Penulis menyelesaikan pendidikan sekolah dasar pada tahun 1995, melanjutkan pendidikan tingkat SMP lulus tahun 1998, melanjutkan pendidikan tingkat SLTA lulus tahun 2001. Setelah lulus SLTA, penulis melanjutkan pendidikan ke jenjang pendidikan tinggi (strata 1) pada Fakultas Hukum Universitas Palangka Raya lulus tahun 2005. Pada tahun 2008, penulis melanjutkan pendidikan strata 2 MIH pada Fakultas Hukum Universitas Airlangga Surabaya yang lulus pada tahun 2009. Tahun 2017 penulis melanjutkan pendidikan Strata 3 Ilmu Hukum pada Program Doktor Ilmu Hukum Fakultas Hukum Universitas Brawijaya dan lulus tahun 2020. Penulis saat ini aktif sebagai tenaga pengajar pada Fakultas Hukum Universitas Palangka Raya dengan status Pegawai Negeri Sipil golongan IVa dengan jabatan fungsional Lektor Kepala. Selain sebagai tenaga pengajar, penulis juga aktif sebagai Ketua Satgas PPKPT UPR dan Kaprodi Magister Ilmu Hukum FH UPR.

Dr. Rakhmat Baihaki, S.H., M.H.

Rakhmat Baihaki adalah nama Penulis di lahirkan di Kota Banjarmasin Kalimantan Selatan pada tanggal 20 Agustus 1979. Penulis menyelesaikan pendidikan sekolah dasar pada tahun 1992, melanjutkan pendidikan tingkat SMP lulus 1995, kemudian melanjutkan pendidikan tingkat SLTA lulus tahun 1998, setelah lulus SLTA, penulis melanjutkan pendidikan ke jenjang pendidikan tinggi (Strata 1) pada Sekolah Tinggi Ilmu Hukum Sultan Adam Banjarmasin lulus tahun 2003, pada tahun 2015 penulis melanjutkan pendidikan strata 2 Magister Ilmu Hukum pada Fakultas Hukum Universitas Lambung Mangkurat Banjarmasin dan lulus tahun 2017, Tahun 2020 penulis melanjutkan pendidikan strata 3 Ilmu Hukum pada Program Doktor Ilmu Hukum Fakultas Hukum Universitas Islam Sultan Agung Semarang dan lulus tahun 2022. Penulis saat ini aktif sebagai Jaksa pangkat Jaksa Madya Golongan IVa dengan jabatan Kepala Seksi Tindak Pidana Khusus Kejaksaan Negeri Palangka Raya. Selain melaksanakan tugas dan fungsi Jaksa, Penulis juga aktif sebagai tenaga pengajar pada program strata 2 Fakultas Hukum Universitas Palangka Raya.

TINDAK PIDANA SIBER DI INDONESIA

REGULASI, TANTANGAN, DAN PENEGAKAN HUKUM

Buku referensi "Tindak Pidana Siber di Indonesia: Regulasi, Tantangan, dan Penegakan Hukum" membahas secara komprehensif dinamika kejahatan siber yang kian kompleks di era digital, mulai dari bentuk-bentuk tindak pidana siber hingga kerangka hukum yang mengaturnya di Indonesia. Disusun berdasarkan analisis terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi terkait lainnya, buku referensi ini juga membahas berbagai tantangan yang dihadapi aparat penegak hukum dalam menghadapi pelaku kejahatan siber, baik dari segi kapasitas teknis, koordinasi antarlembaga, hingga persoalan yuridiksi lintas negara. Dengan pendekatan kritis dan berbasis studi kasus, buku referensi ini memberikan pandangan solutif terhadap pembaruan kebijakan dan peningkatan efektivitas penegakan hukum siber.

PT MEDIA PENERBIT INDONESIA

mediapenerbitindonesia.com
+6281362150605
Penerbit Idn
@pt.mediapenerbitidn

ISBN 978-634-7184-75-7
9 786347 184757