# Hukum Siber
dan
# Keamanan Informasi

Dr. Agus Wibowo, M.Kom, M.Si, MM.

**Hukum Siber dan Keamanan Informasi**

**Penulis :**
Dr. Agus Wibowo, M.Kom, M.Si, MM.

**ISBN : 978-623-8642-49-6**

**Editor :**
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

**Penyunting :**
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

**Desain Sampul dan Tata Letak :**
Irdha Yunianto, S.Ds., M.Kom

**Penebit** :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

**Anggota IKAPI No:** 279 / ALB / JTE / 2023

**Redaksi :**
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

**Distributor Tunggal :**
**Universitas STEKOM**
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : info@stekom.ac.id

# KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa, karena atas rahmat-Nya kita dapat menyelesaikan buku yang berjudul "*Hukum Siber dan Keamanan Informasi"* ini dengan baik. Dalam era digital saat ini, isu mengenai hukum siber dan keamanan informasi semakin relevan dan menjadi perhatian utama di berbagai sektor, baik di pemerintahan, industri, maupun masyarakat.

Hukum siber merujuk pada peraturan dan norma yang mengatur perilaku di dunia maya. Hal ini mencakup berbagai aspek, seperti perlindungan data pribadi, hak kekayaan intelektual, serta pengaturan terhadap tindakan kejahatan siber. Sementara itu, keamanan informasi adalah upaya untuk melindungi informasi dari akses yang tidak sah, pengungkapan, perubahan, atau penghancuran. Keamanan informasi bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data.

Dalam konteks global yang semakin terhubung, pemahaman yang baik tentang hukum siber dan keamanan informasi menjadi sangat penting. Selain untuk melindungi individu dan organisasi dari potensi ancaman siber, pengetahuan ini juga diperlukan untuk mendorong inovasi dan perkembangan teknologi yang aman dan bertanggung jawab. Melalui tulisan ini, diharapkan pembaca dapat memahami lebih dalam tentang pentingnya hukum siber dan langkah-langkah yang dapat diambil untuk menjaga keamanan informasi di era digital ini.

Dalam Bab 1 Pendahuluan, dibahas berbagai aspek terkait ruang siber dan perkembangan hukum yang menyertainya. Pertama, dijelaskan mengenai ruang siber sebagai lingkungan digital yang terus berkembang, diikuti dengan tren hukum siber yang muncul seiring dengan meningkatnya penggunaan teknologi informasi. Selanjutnya, terdapat pembahasan tentang hak kekayaan intelektual yang relevan di dunia digital, serta strategi dan kebijakan keamanan siber yang diperlukan untuk mengurangi risiko yang mungkin timbul.

Bab ini juga mencakup isu-isu terkait keamanan jaringan, pentingnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam pengaturan ruang siber, serta aspek tanda tangan elektronik. Terakhir, dibahas mengenai pelanggaran yang dapat terjadi di ruang siber dan sanksi yang mungkin dikenakan sebagai konsekuensinya, sebelum diakhiri dengan ringkasan yang merangkum poin-poin penting yang telah dibahas.

Bab 2 mengklasifikasikan kejahatan dunia maya, mencakup kejahatan terhadap orang, harta milik, pemerintah, dan masyarakat secara umum, serta mengidentifikasi penyebab dan dampaknya, disertai beberapa contoh kejadian bersejarah. Bab 3 menjelaskan perlunya perlindungan hukum di dunia maya, dengan mengulas Undang-Undang Teknologi Informasi tahun 2000, tujuannya, cakupan, serta penerapan dan amandemennya. Bab 4 fokus pada tanggung jawab pidana dan perdata berdasarkan undang-undang tersebut, serta ketentuan hukum yang berlaku untuk kejahatan maya dan tanggung jawab perusahaan. Selanjutnya, Bab 5 menyajikan putusan bersejarah di India terkait kejahatan dunia maya, memberikan contoh konkret penerapan hukum. Bab 6 membahas tren terkini dalam hukum dunia maya, mencakup perkembangan teknologi dan regulasi yang berpengaruh. Akhirnya, Bab 7 menyimpulkan perlunya peninjauan kembali hukum dunia maya dan memberikan rekomendasi untuk meningkatkan perlindungan hukum serta respons terhadap kejahatan siber di masa depan.

Demikian kata pengantar ini kami sampaikan. Semoga tulisan ini bermanfaat dan memberikan wawasan yang berharga bagi kita semua. Terima Kasih.

Semarang, November 2024
Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM.

# DAFTAR ISI

# BAB 1
# PENDAHULUAN

## 1.1 RUANG SIBER

Ruang siber dapat didefinisikan sebagai lingkungan rumit yang melibatkan interaksi antara orang, perangkat lunak, dan layanan. Ruang siber dikelola oleh distribusi perangkat dan jaringan teknologi informasi dan komunikasi di seluruh dunia.Dengan manfaat yang dibawa oleh kemajuan teknologi, ruang siber saat ini telah menjadi tempat umum yang digunakan oleh warga negara, bisnis, infrastruktur informasi penting, militer, dan pemerintah dengan cara yang membuatnya sulit untuk menetapkan batasan yang jelas di antara kelompok-kelompok yang berbeda ini. Ruang siber diantisipasi akan menjadi lebih kompleks di tahun-tahun mendatang, dengan peningkatan jaringan dan perangkat yang terhubung dengannya.

Ruang lingkup tindak pidana siber mencakup berbagai definisi yang diajukan oleh para ahli dan peraturan perundang-undangan, yang dapat digunakan sebagai dasar untuk pengaturan hukum pidana siber. Sussan Brenner (2011) mengklasifikasikan cybercrimes ke dalam tiga kategori:

*"kejahatan di mana komputer menjadi target, kejahatan di mana komputer digunakan sebagai alat, dan kejahatan di mana penggunaan komputer adalah aspek sampingan."*

Sementara itu, Nicholson membedakan antara "computer crimes" sebagai objek dan subjek tindak pidana, serta instrumen kejahatan. Dalam hal ini, komputer bisa menjadi target kejahatan, lokasi kejahatan, atau alat untuk melakukan kejahatan tradisional secara lebih kompleks, seperti pencurian informasi kartu kredit.

Menurut instrumen PBB dalam Konferensi Kesepuluh tentang Pencegahan Kejahatan dan Perlakuan Terhadap Pelanggar di Wina pada April 2000, cybercrime dapat didefinisikan secara sempit sebagai "*computer crime*," yang meliputi perilaku ilegal yang menargetkan keamanan sistem komputer. Sebaliknya, secara luas, cybercrime mencakup semua perilaku ilegal yang terkait dengan sistem atau jaringan komputer, termasuk kepemilikan informasi ilegal.

Konvensi tentang Kejahatan Siber di Budapest pada tahun 2001 tidak memberikan definisi eksplisit tentang cybercrimes, tetapi mengkategorikannya menjadi beberapa bagian, termasuk pelanggaran terhadap kerahasiaan dan integritas data komputer, serta kejahatan terkait konten dan hak cipta. Black's Law Dictionary edisi kesembilan mendefinisikan kejahatan komputer sebagai kejahatan yang melibatkan penggunaan komputer, seperti sabotase atau pencurian data yang disimpan secara elektronik.

Ruang siber di Indonesia diatur oleh berbagai regulasi yang bertujuan memberikan kepastian hukum dan melindungi pengguna internet. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi fondasi hukum siber di negara ini, diundangkan pada tahun 2008 dan direvisi pada tahun 2016, yang mencakup perlindungan data pribadi, transaksi elektronik yang sah, dan penegakan hukum terhadap kejahatan siber. Selain itu, Indonesia juga

meratifikasi konvensi internasional terkait kejahatan siber, termasuk Convention on Cyber Crime, yang menjadi pedoman dalam menangani kejahatan dunia maya secara global.

Hukum siber meliputi berbagai aspek, mulai dari kejahatan dunia maya seperti akses ilegal dan penipuan online, hingga perlindungan konsumen dalam transaksi elektronik. Penegakan hukum terhadap kejahatan siber dilakukan oleh aparat penegak hukum yang terlatih, meskipun tantangan tetap ada karena sifat transnasional dari kejahatan ini, yang memerlukan kerjasama internasional. Secara keseluruhan, kerangka hukum yang terus berkembang di Indonesia berupaya menghadapi tantangan baru seiring kemajuan teknologi, dengan UU ITE sebagai pilar utama dalam mengatur aktivitas online dan memberikan perlindungan kepada pengguna.

**Keamanan siber**

Keamanan siber menunjukkan teknologi dan prosedur yang dimaksudkan untuk melindungi komputer, jaringan, dan data dari akses yang tidak sah, kelemahan, dan serangan yang diangkut melalui Internet oleh penjahat siber.ISO 27001 (ISO27001) adalah Standar Keamanan Siber internasional yang memberikan model untuk membuat, menerapkan, menjalankan, memantau, meninjau, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi. Kementerian Komunikasi dan Teknologi Informasi di bawah pemerintahan India menyediakan garis besar strategi yang disebut Kebijakan Keamanan Siber Nasional. Tujuan dari badan pemerintah ini adalah untuk melindungi infrastruktur publik dan swasta dari serangan siber.

**Pengaturan Tindak Pidana Siber di Indonesia**

Dalam konteks pengaturan tindak pidana siber, Indonesia mengikuti pedoman dari instrumen PBB yang memungkinkan pemahaman baik dalam arti luas maupun sempit. Secara luas, tindak pidana siber mencakup semua kejahatan yang memanfaatkan sistem elektronik. Ini berarti bahwa berbagai tindak pidana konvensional yang tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP), seperti pembunuhan dan perdagangan orang, bisa masuk dalam kategori tindak pidana siber jika dilakukan dengan bantuan teknologi. Selain itu, undang-undang seperti Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana dan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang juga termasuk dalam pengaturan ini.

Namun, dalam pengertian yang lebih sempit, pengaturan tindak pidana siber terfokus pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016. Meskipun UU ITE tidak secara eksplisit mendefinisikan kejahatan siber, undang-undang ini membagi tindak pidana menjadi beberapa kategori yang mengacu pada ketentuan dalam *Convention on Cybercrimes*. Beberapa kategori tersebut meliputi:

1. **Tindak Pidana Terkait Aktivitas Ilegal**:
   - ✓ Penyebaran konten yang melanggar kesusilaan, perjudian, penghinaan, pemerasan, berita bohong, serta ancaman kekerasan.
   - ✓ Akses ilegal dan penyadapan terhadap informasi elektronik.
2. **Tindak Pidana Gangguan**:
   - ✓ Gangguan terhadap data atau dokumen elektronik serta sistem elektronik.
   - ✓ Pemalsuan informasi dan dokumen elektronik.

**Pengaturan Tindak Pidana Siber Formil di Indonesia**

Di samping pengaturan materiil, UU ITE juga mencakup aspek formil, terutama dalam hal penyidikan. Pasal 42 UU ITE menyatakan bahwa penyidikan terhadap tindak pidana dalam UU ini dilakukan berdasarkan ketentuan dalam KUHAP. Artinya, prosedur penyidikan dalam KUHAP tetap berlaku kecuali ada ketentuan khusus dalam UU ITE.

Beberapa keunikan dalam penyidikan tindak pidana siber meliputi:

- Penyidik berasal dari Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil (PPNS) Kementerian Komunikasi dan Informatika.
- Penyidikan dilakukan dengan menjaga privasi dan kerahasiaan data.
- Proses penggeledahan dan penyitaan sistem elektronik harus sesuai dengan hukum acara pidana dan menjaga kepentingan pelayanan publik.

Prosedur untuk melaporkan tindak pidana siber dapat dilakukan oleh korban atau kuasa hukum yang mengajukan laporan ke unit Cybercrime Polri atau PPNS. Setelah penyelidikan dan penyidikan selesai, berkas perkara akan dilimpahkan ke penuntut umum untuk diproses di pengadilan.

Selain UU ITE, pengaturan terkait penanganan kasus cybercrime juga didasarkan pada peraturan pelaksana dan regulasi teknis di setiap instansi penyidik.

**Kebijakan Keamanan Siber**

Kebijakan keamanan siber adalah misi yang sedang berkembang yang melayani seluruh bidang pengguna dan penyedia Teknologi Informasi dan Komunikasi (TIK). Kebijakan ini meliputi:

(a) Pengguna rumahan
(b) Perusahaan kecil, menengah, dan besar
(c) Entitas pemerintah dan nonpemerintah

Kebijakan ini berfungsi sebagai kerangka otoritas yang mendefinisikan dan memandu aktivitas yang terkait dengan keamanan dunia maya. Kebijakan ini memungkinkan semua sektor dan organisasi dalam merancang kebijakan keamanan siber yang sesuai untuk memenuhi persyaratan mereka. Kebijakan ini menyediakan garis besar untuk melindungi informasi, sistem informasi, dan jaringan secara efektif.

Kebijakan ini memberikan pemahaman tentang pendekatan dan strategi Pemerintah untuk keamanan dunia maya di negara ini. Kebijakan ini juga menguraikan beberapa petunjuk untuk memungkinkan kerja sama lintas sektor publik dan swasta untuk melindungi informasi dan sistem informasi. Oleh karena itu, tujuan dari kebijakan ini adalah untuk menciptakan kerangka kerja keamanan siber, yang mengarah pada tindakan dan program terperinci untuk meningkatkan keamanan siber.

Kebijakan keamanan siber di Indonesia merupakan aspek penting dalam menghadapi ancaman digital yang terus berkembang. Dalam beberapa tahun terakhir, pemerintah telah mengembangkan berbagai regulasi dan strategi untuk memperkuat keamanan siber di seluruh sektor. Berikut adalah penjelasan rinci mengenai kebijakan keamanan siber di Indonesia:

**Regulasi Terkait Keamanan Siber**

Indonesia telah mengeluarkan beberapa undang-undang dan peraturan yang berkaitan dengan keamanan siber, antara lain:

1. **Undang-Undang Nomor 11 Tahun 2008:** tentang Informasi dan Transaksi Elektronik, yang telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016.
2. **Undang-Undang Nomor 27 Tahun 2022:** tentang Perlindungan Data Pribadi, yang mengatur pengelolaan data pribadi dan kewajiban penyelenggara sistem elektronik.
3. **Peraturan Pemerintah Nomor 71 Tahun 2019:** tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang menetapkan standar bagi penyelenggara sistem elektronik untuk menjaga keamanan dan keandalan sistem mereka.
4. **Peraturan Presiden Nomor 82 Tahun 2022:** tentang Perlindungan Infrastruktur Informasi Vital, yang berfokus pada perlindungan infrastruktur kritis.
5. **Peraturan Presiden Nomor 47 Tahun 2023:** tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, yang menjadi acuan bagi seluruh pemangku kepentingan dalam menyusun kebijakan keamanan siber.

**Strategi Keamanan Siber Nasional**

Pemerintah Indonesia juga telah merumuskan *Strategi Keamanan Siber Nasional* (SKSN), yang bertujuan untuk:

- ✓ Mewujudkan keamanan siber yang komprehensif.
- ✓ Melindungi ekosistem perekonomian digital nasional.
- ✓ Meningkatkan kapabilitas dan kesiapan menghadapi ancaman siber.

SKSN mencakup berbagai aspek seperti tata kelola, manajemen risiko, perlindungan infrastruktur vital, serta kerja sama internasional dalam bidang keamanan siber.

**Pendekatan Zero Trust**

Pendekatan Zero Trust mulai diperkenalkan sebagai strategi untuk meningkatkan keamanan siber. Konsep ini menekankan bahwa tidak ada entitas dalam jaringan yang dapat dipercaya secara otomatis, sehingga setiap interaksi harus divalidasi[1]. Pendekatan ini diharapkan dapat mengurangi risiko serangan siber dengan membangun pertahanan yang lebih kuat.

**Tantangan dan Kelemahan**

Meskipun telah ada kemajuan dalam kebijakan keamanan siber, Indonesia masih menghadapi beberapa tantangan:

- Kurangnya Regulasi Khusus: Hingga saat ini, Indonesia belum memiliki undang-undang khusus mengenai keamanan siber, berbeda dengan beberapa negara ASEAN lainnya.
- Keterbatasan Sumber Daya Manusia: Pengetahuan dan keterampilan terkait keamanan siber masih perlu ditingkatkan di kalangan tenaga kerja[3].
- Koordinasi Antarlembaga: Badan Siber dan Sandi Negara (BSSN) berfungsi sebagai koordinator namun tidak memiliki wewenang penuh atas semua lembaga pemerintah dalam hal keamanan siber.

Kebijakan keamanan siber di Indonesia terus berkembang dengan penguatan regulasi dan strategi untuk menghadapi ancaman digital. Pendekatan Zero Trust dan SKSN merupakan langkah penting menuju ekosistem digital yang lebih aman. Namun, tantangan seperti kurangnya regulasi khusus dan sumber daya manusia yang terbatas masih perlu diatasi untuk meningkatkan efektivitas kebijakan ini.

**Kejahatan Siber**

Kejahatan siber merupakan isu yang semakin penting di era digital saat ini. Di Indonesia, meskipun Undang-Undang Teknologi Informasi dan Transaksi Elektronik (UU ITE)

yang ditetapkan pada tahun 2008 memberikan kerangka hukum untuk aktivitas di dunia maya, istilah "kejahatan siber" tidak secara eksplisit didefinisikan. Hal ini menunjukkan bahwa banyak tantangan yang dihadapi dalam penegakan hukum terhadap kejahatan yang terjadi di dunia digital.

Secara global, kejahatan siber dapat dianggap sebagai sisi gelap dari kemajuan teknologi. Perbedaannya dengan kejahatan tradisional terletak pada metode dan ruang lingkupnya. Contohnya:

1. **Pencurian Tradisional**: Seorang pencuri membobol rumah Ram dan mencuri barang berharga yang ada di dalamnya.
2. **Peretasan**: Seorang hacker, dari lokasi yang tidak terduga, meretas komputer Ram dan mencuri data sensitif yang tersimpan di dalamnya, tanpa harus memasuki rumah Ram secara fisik.

**Definisi dalam UU ITE**

Undang-Undang ITE, meskipun tidak secara langsung menggunakan istilah "kejahatan siber", mencakup beberapa definisi penting yang berkaitan dengan keamanan informasi:

- **Akses dalam jaringan komputer** (Pasal 2(a)): Menyiratkan bahwa akses tanpa izin ke sistem komputer merupakan tindakan ilegal.
- **Komputer** (Pasal 2(i)): Didefinisikan sebagai perangkat elektronik yang dapat memproses data.
- **Jaringan komputer** (Pasal 2(j)): Merujuk pada sistem yang menghubungkan beberapa komputer untuk berkomunikasi.
- **Data** (Pasal 2(o)): Menyangkut informasi yang disimpan dalam bentuk digital.
- **Informasi** (Pasal 2(v)): Merujuk pada data yang telah diolah sehingga memiliki arti atau nilai.

Dengan memahami istilah-istilah ini, kita dapat melihat bahwa objek dari kejahatan siber adalah komputer atau data yang tersimpan di dalamnya. Ancaman kejahatan siber dapat berupa pencurian data, penipuan online, malware, dan berbagai bentuk serangan siber lainnya.

**Tantangan Penegakan Hukum**

Di Indonesia, penegakan hukum terhadap kejahatan siber masih menghadapi banyak tantangan. Banyak pelaku kejahatan siber beroperasi secara anonim dan lintas batas negara, sehingga sulit untuk menangkap dan menghukum mereka. Selain itu, pemahaman masyarakat mengenai keamanan siber juga masih rendah, yang dapat membuat mereka menjadi korban. Pemerintah dan lembaga terkait terus berupaya meningkatkan kesadaran akan pentingnya keamanan siber dan memperkuat regulasi untuk melindungi data serta informasi digital masyarakat. Upaya ini mencakup peningkatan pelatihan, kampanye edukasi, serta kolaborasi internasional dalam memberantas kejahatan siber.

**Kesimpulan**

Kejahatan siber di Indonesia adalah masalah yang kompleks dan terus berkembang. Meskipun UU ITE memberikan dasar hukum, masih diperlukan pembaruan dan penyesuaian untuk menghadapi tantangan baru yang muncul seiring dengan kemajuan teknologi. Kesadaran dan pemahaman masyarakat mengenai kejahatan siber juga perlu ditingkatkan untuk menciptakan lingkungan digital yang lebih aman.

**Sifat Ancaman**

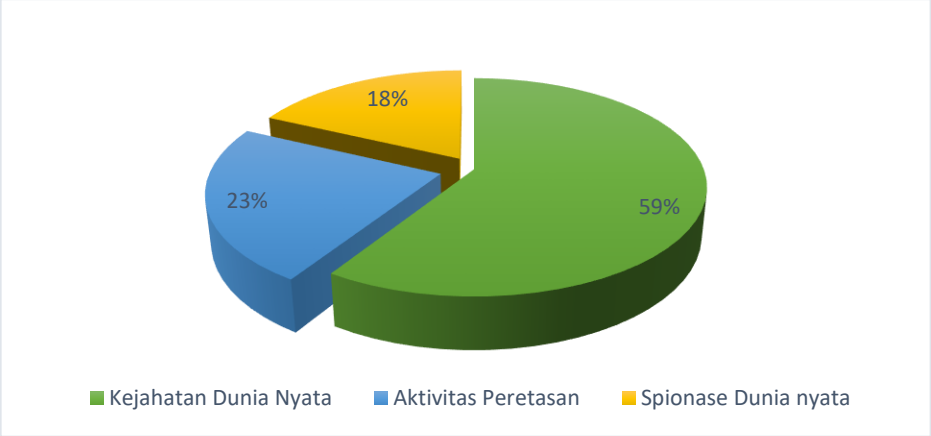
Di antara tantangan paling serius abad ke-21 adalah ancaman yang ada dan mungkin terjadi di bidang keamanan siber. Ancaman berasal dari berbagai sumber, dan ditandai dengan berbagai aktivitas yang mengganggu yang menargetkan individu, bisnis, infrastruktur nasional, dan pemerintah. Dampak dari ancaman ini menimbulkan risiko yang signifikan terhadap hal-hal berikut:

1. Keselamatan publik
2. Keamanan negara
3. Stabilitas komunitas internasional yang terhubung secara global.

Pemanfaatan teknologi informasi yang jahat dapat dengan mudah disembunyikan. Sulit untuk menentukan asal atau identitas pelaku kejahatan. Bahkan motivasi gangguan tersebut bukanlah tugas yang mudah untuk diketahui. Pelaku kejahatan dari aktivitas ini hanya dapat diketahui dari target, dampak, atau bukti tidak langsung lainnya. Pelaku ancaman dapat beroperasi dengan sangat bebas dari mana saja. Motif gangguan dapat berupa apa saja seperti:

1. Hanya menunjukkan kecakapan teknis
2. Pencurian uang atau informasi
3. Perluasan konflik negara, dll.

Penjahat, teroris, dan terkadang Negara sendiri bertindak sebagai sumber ancaman ini. Penjahat dan peretas menggunakan berbagai jenis alat dan pendekatan jahat. Dengan kegiatan kriminal yang mengambil bentuk baru setiap hari, kemungkinan terjadinya tindakan berbahaya pun semakin meluas.




**Gambar 1.1 Diagram Motif dibalik serangan**

**Memberdayakan Masyarakat**

Kurangnya kesadaran keamanan informasi di antara pengguna, yang bisa jadi adalah anak sekolah, administrator sistem, pengembang, atau bahkan CEO suatu perusahaan, menyebabkan berbagai kerentanan siber. Kebijakan kesadaran mengklasifikasikan tindakan dan inisiatif berikut untuk tujuan kesadaran, pendidikan, dan pelatihan pengguna:

(a) Program kesadaran lengkap yang akan dipromosikan di tingkat nasional.

(b) Program pelatihan komprehensif yang dapat memenuhi kebutuhan keamanan informasi nasional (Program keamanan TI di sekolah, perguruan tinggi, dan universitas).
(c) Meningkatkan efektivitas program pelatihan keamanan informasi yang berlaku. Merencanakan program pelatihan khusus domain (misalnya, Penegakan Hukum, Peradilan, E-Pemerintahan, dll.)
(d) Mendukung dukungan sektor swasta untuk sertifikasi keamanan informasi profesional.

**Pengaturan tindak pidana siber materil di indonesia**
**Misi dan Visi Program Keamanan Siber**

**A. Misi**

Misi berikut ini ditujukan untuk keamanan siber:

1. Menjaga keamanan informasi dan infrastruktur informasi di dunia maya.
2. Membangun kemampuan untuk mencegah dan menanggapi ancaman dunia maya.
3. Mengurangi kerentanan dan meminimalkan kerusakan akibat insiden dunia maya melalui kombinasi struktur kelembagaan, orang, proses, teknologi, dan kerja sama.

**B. Visi**

Membangun dunia maya yang aman dan tangguh bagi warga negara, bisnis, dan Pemerintah.

**C. Tujuan**

Pengungkapan Edward Snowden baru-baru ini tentang program pengawasan AS PRISM telah menunjukkan bagaimana jaringan badan hukum dan sistem komputer di luar yurisdiksi tertentu menjadi sasaran pengawasan tanpa sepengetahuan badan hukum tersebut. Kasus-kasus siber yang terkait dengan intersepsi dan pengintaian meningkat pada tingkat yang mengkhawatirkan. Untuk mengekang kejahatan semacam itu, hukum siber diamandemen secara teratur.

## 1.2 TREN HUKUM SIBER YANG BERKEMBANG

Laporan mengungkapkan bahwa tahun-tahun mendatang akan mengalami lebih banyak serangan siber. Jadi, organisasi disarankan untuk memperkuat rantai pasokan data mereka dengan metode pemeriksaan yang lebih baik.

Beberapa tren hukum siber yang berkembang tercantum di bawah ini:

1. Aturan regulasi yang ketat diberlakukan oleh banyak negara untuk mencegah akses tidak sah ke jaringan. Tindakan semacam itu dinyatakan sebagai pelanggaran pidana.
2. Pemangku kepentingan perusahaan seluler akan meminta pemerintah dunia untuk memperkuat sistem dan administrasi hukum siber untuk mengatur ancaman dan kejahatan seluler yang muncul.
3. Meningkatnya kesadaran akan privasi adalah tren mendatang lainnya. Pakar internet utama Google, Vint Cerf, telah menyatakan bahwa privasi mungkin sebenarnya merupakan anomali.
4. Cloud computing merupakan tren utama yang sedang berkembang. Dengan semakin banyaknya kemajuan dalam teknologi, sejumlah besar data akan mengalir ke cloud yang tidak sepenuhnya kebal terhadap kejahatan dunia maya.

5. Pertumbuhan Bitcoin dan mata uang virtual lainnya merupakan tren lain yang perlu diwaspadai. Kejahatan Bitcoin kemungkinan akan meningkat dalam waktu dekat.
6. Kedatangan dan penerimaan analisis data, yang merupakan tren utama lain yang harus diikuti, memerlukan perhatian yang tepat terhadap isu-isu yang berkaitan dengan Big Data.

**Ciptakan Kesadaran**

Meskipun pemerintah AS telah mendeklarasikan Oktober sebagai bulan Kesadaran Keamanan Siber Nasional, Indonesia mengikuti tren tersebut untuk menerapkan beberapa skema kesadaran yang ketat bagi masyarakat umum. Masyarakat umum sebagian menyadari kejahatan yang terkait dengan transfer virus. Namun, mereka tidak menyadari gambaran yang lebih besar dari ancaman yang dapat memengaruhi kehidupan dunia maya mereka. Sebagian besar pengguna internet sangat kurang pengetahuan tentang kejahatan dunia maya e-commerce dan perbankan daring. Tetap waspada dan ikuti kiat-kiat yang diberikan di bawah ini saat Anda berpartisipasi dalam aktivitas daring:

(a) Saring visibilitas informasi pribadi di situs sosial.
(b) Jangan biarkan tombol "ingat kata sandi" aktif untuk alamat email dan kata sandi apa pun
(c) Pastikan platform perbankan daring Anda aman.
(d) Awasi dengan cermat saat berbelanja daring.
(e) Jangan simpan kata sandi di perangkat seluler.
(f) Amankan detail login untuk perangkat seluler dan komputer, dll.

**Area Pengembangan**

**Tren Hukum Siber di Indonesia**

Tren hukum siber di Indonesia mengalami perkembangan signifikan seiring dengan meningkatnya ancaman kejahatan siber dan kebutuhan perlindungan data di era digital. Dengan jumlah pengguna internet yang terus meningkat, tantangan dalam hal keamanan siber dan perlindungan hak kekayaan intelektual semakin mendesak. Berikut adalah analisis mendalam mengenai tren hukum siber di Indonesia serta rekomendasi untuk penguatan kebijakan dan penegakan hukum.

**Peningkatan Kasus Kejahatan Siber**

Laporan dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa jumlah serangan siber di Indonesia meningkat tajam, dengan kenaikan 22% pada tahun 2022 dibandingkan tahun sebelumnya. Jenis serangan yang paling umum meliputi:

- **Phishing**: Penipuan melalui email atau pesan yang mengelabui korban untuk memberikan informasi pribadi.
- **Malware**: Penyebaran perangkat lunak berbahaya, seperti virus dan ransomware, yang dapat merusak sistem komputer.
- **Ransomware**: Serangan yang mengenkripsi data korban dan meminta tebusan untuk mengembalikannya.
- **Serangan DDoS**: Upaya untuk melumpuhkan sistem atau jaringan dengan membanjiri trafik.

**Kerangka Hukum yang Ada**

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

UU ITE, yang disahkan pada tahun 2008, merupakan regulasi utama yang mengatur aktivitas di dunia maya. Meskipun memberikan dasar hukum untuk penegakan hukum terhadap kejahatan siber, UU ini sering dikritik karena ketidakjelasan dalam beberapa pasalnya, yang dapat mengancam kebebasan berbicara. Revisi terbaru menambah ketentuan baru untuk menangani kejahatan siber yang lebih kompleks.

2. **Undang-Undang Perlindungan Data Pribadi (UU PDP)**

UU PDP yang disahkan memberikan perlindungan lebih terhadap data pribadi individu, menetapkan kewajiban bagi organisasi untuk menjaga keamanan data dan memberikan hak kepada individu untuk mengontrol informasi mereka.

**Tantangan dalam Penegakan Hukum**

1. Kesadaran Masyarakat yang Rendah

Tingkat kesadaran masyarakat mengenai ancaman kejahatan siber dan cara melindungi diri masih rendah. Banyak individu dan organisasi yang belum sepenuhnya memahami risiko dan pentingnya perlindungan data.

2. Keterbatasan Sumber Daya

Keterbatasan sumber daya dan keahlian teknis dalam menangani kejahatan siber menjadi hambatan besar bagi penegakan hukum. Penegak hukum sering kesulitan melacak dan menanggapi serangan siber yang semakin canggih.

3. Kerjasama Internasional

Serangan siber yang bersifat transnasional memerlukan kerjasama internasional dalam penegakan hukum. Indonesia perlu meratifikasi Konvensi Budapest tentang Kejahatan Siber untuk meningkatkan kolaborasi global dalam menangani isu ini.

**Langkah-Langkah Strategis ke Depan**

- **Peningkatan Regulasi**: Penyesuaian regulasi yang lebih spesifik dan tegas diperlukan untuk menangani modus operandi kejahatan siber yang terus berkembang. Penguatan pasal-pasal dalam UU ITE harus dilakukan agar lebih sesuai dengan tantangan saat ini.
- **Edukasi Masyarakat**: Program edukasi tentang keamanan siber kepada masyarakat, terutama pengguna internet dan pelaku usaha, sangat penting untuk menciptakan kesadaran akan ancaman siber. Ini dapat dilakukan melalui kampanye media, seminar, dan pelatihan.
- **Penguatan Kapasitas Penegakan Hukum**: Pemerintah harus meningkatkan kapasitas penegakan hukum dengan menyediakan pelatihan bagi aparat penegak hukum dan memperkuat lembaga terkait seperti BSSN. Pengembangan sumber daya manusia yang kompeten dalam bidang teknologi informasi dan keamanan siber menjadi krusial.

**Kesimpulan**

Tren hukum siber di Indonesia menunjukkan perlunya perhatian serius terhadap peningkatan regulasi, kesadaran masyarakat, dan kerjasama internasional dalam menghadapi ancaman kejahatan siber yang semakin kompleks. Dengan langkah-langkah strategis yang tepat, Indonesia dapat memperkuat kerangka hukum sibernya dan melindungi masyarakat serta data mereka dari berbagai ancaman digital. Upaya ini tidak hanya akan memberikan perlindungan hukum, tetapi juga meningkatkan kepercayaan masyarakat terhadap keamanan siber di tanah air.

Sebagai contoh lain pembaca akan melihat Tren Hukum Siber di India pada periode tahun 2013 dan Perkembangan Hukum Siber di India pada periode tahun 2014 adalah dua karya penelitian terkait hukum siber terkemuka dan tepercaya yang disediakan oleh *Perry4Law Organization* (P4LO) untuk tahun 2013 dan 2014. Ada beberapa masalah serius terkait hukum siber yang perlu segera dipertimbangkan oleh pemerintah India. Masalah tersebut diajukan oleh rangkuman hukum siber India tahun 2014 yang disediakan oleh P4LO dan Pusat Investigasi Kejahatan Siber India (CCICI). Berikut ini adalah beberapa isu utama:

(a) Hukum siber yang lebih baik dan strategi pencegahan kejahatan siber yang efektif
(b) Persyaratan pelatihan investigasi kejahatan siber
(c) Perumusan undang-undang enkripsi khusus
(d) Penerapan hukum komputasi awan secara hukum
(e) Perumusan dan penerapan kebijakan email
(f) Isu hukum pembayaran daring
(g) Legalitas perjudian daring dan apotek daring
(h) Legalitas Bitcoin
(i) Kerangka kerja pemblokiran situs web
(j) Regulasi aplikasi seluler

Dengan terbentuknya paksaan hukum siber, kewajiban bank untuk pencurian siber dan kejahatan siber akan meningkat pesat dalam waktu dekat. Bank-bank India perlu memiliki tim ahli hukum siber khusus atau mencari bantuan ahli eksternal dalam hal ini. Transaksi asuransi siber harus ditingkatkan oleh sektor asuransi India sebagai konsekuensi dari meningkatnya serangan siber dan kejahatan siber.

**Jaringan Internasional Keamanan Siber**

Untuk membuat jaringan internasional keamanan siber, sebuah konferensi diadakan pada bulan Maret 2014 di New Delhi, India. Tujuan yang ditetapkan dalam Konferensi Internasional tentang Hukum Siber & Kejahatan Siber adalah sebagai berikut:

1. Untuk mengenali tren yang berkembang dalam Hukum Siber dan undang-undang yang memengaruhi dunia maya dalam situasi saat ini.
2. Untuk meningkatkan kesadaran guna memerangi berbagai jenis kejahatan siber terkini yang memengaruhi semua investor dalam jaringan digital dan seluler.
3. Untuk mengenali area bagi para pemangku kepentingan jaringan digital dan seluler di mana Hukum Siber perlu dikembangkan lebih lanjut.
4. Untuk bekerja ke arah penciptaan jaringan internasional kejahatan siber. Otoritas hukum kemudian dapat menjadi suara yang signifikan dalam perluasan lebih lanjut undang-undang kejahatan siber dan hukum siber di seluruh dunia.

Membangun jaringan internasional keamanan siber di Indonesia sangat penting, terutama mengingat meningkatnya ancaman kejahatan siber yang dapat merugikan individu, perusahaan, dan negara. Konferensi Internasional tentang Hukum Siber & Kejahatan Siber yang diadakan di New Delhi pada Maret 2014 memberikan beberapa tujuan yang relevan untuk pengembangan hukum siber di Indonesia. Pertama, Indonesia perlu terus memantau dan mengenali tren yang berkembang dalam hukum siber serta regulasi yang mempengaruhi dunia maya. Dengan meningkatnya serangan siber, penting bagi pemerintah dan pemangku kepentingan untuk memperbarui dan menyesuaikan regulasi yang ada, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta

perubahannya melalui UU Nomor 19 Tahun 2016. Ini diperlukan untuk memastikan bahwa hukum siber dapat menangani isu-isu baru akibat perkembangan teknologi informasi.

Kedua, kesadaran akan kejahatan siber harus ditingkatkan di kalangan masyarakat dan pemangku kepentingan. Edukasi mengenai jenis-jenis kejahatan siber, seperti penipuan online, pencurian identitas, dan cyberbullying, sangat penting untuk melindungi pengguna internet dan investor dalam jaringan digital. Pemerintah dapat berkolaborasi dengan lembaga pendidikan dan organisasi non-pemerintah untuk menyelenggarakan kampanye kesadaran publik. Ketiga, ada kebutuhan mendesak untuk mengidentifikasi area di mana hukum siber perlu dikembangkan lebih lanjut, termasuk perlindungan data pribadi, regulasi cryptocurrency, dan penanganan kejahatan siber lintas negara. Dengan adanya kerjasama internasional, Indonesia dapat memperkuat hukum yang ada dan mengadopsi praktik terbaik dari negara lain.

Selanjutnya, penciptaan jaringan internasional keamanan siber akan memungkinkan kolaborasi antara negara-negara dalam menangani kejahatan siber secara efektif. Indonesia harus berupaya untuk meratifikasi Konvensi Budapest tentang Kejahatan Siber, yang bertujuan untuk meningkatkan kerjasama internasional dalam penegakan hukum terkait kejahatan siber. Dengan menjadi bagian dari konvensi ini, Indonesia dapat berkontribusi dalam pengembangan hukum siber global dan mendapatkan akses terhadap sumber daya serta pengetahuan internasional.

Langkah-langkah strategis yang perlu diambil mencakup penyusunan kebijakan yang jelas terkait dengan keamanan siber, termasuk perlindungan data pribadi dan hak-hak pengguna internet. Pelatihan bagi aparat penegak hukum dan masyarakat mengenai hukum siber serta teknik pencegahan kejahatan siber juga sangat penting. Selain itu, membangun kerjasama dengan lembaga internasional untuk berbagi informasi dan teknologi dalam menangani kejahatan siber serta memperkuat penegakan hukum terhadap pelanggaran hukum siber dengan memberikan sanksi yang tegas bagi pelaku kejahatan adalah langkah-langkah yang krusial.

Dengan membangun jaringan internasional keamanan siber, Indonesia dapat lebih efektif dalam menghadapi tantangan kejahatan siber yang terus berkembang. Peningkatan kesadaran, pengembangan hukum yang relevan, serta kerjasama internasional adalah langkah-langkah penting untuk menciptakan ekosistem digital yang aman bagi seluruh masyarakat.

## 1.3. HAK KEKAYAAN INTELEKTUAL

Hak kekayaan intelektual merupakan hak hukum yang mencakup hak istimewa yang diberikan kepada individu yang merupakan pemilik dan penemu suatu karya, serta telah menciptakan sesuatu dengan kreativitas intelektualnya. Individu yang terkait dengan bidang seperti sastra, musik, penemuan, dan lain-lain, dapat diberikan hak tersebut, yang kemudian dapat digunakan dalam praktik bisnisnya. Pencipta/penemu memperoleh hak eksklusif terhadap segala penyalahgunaan atau penggunaan suatu karya tanpa sepengetahuannya terlebih dahulu. Namun, hak tersebut diberikan untuk jangka waktu terbatas guna menjaga keseimbangan. Daftar kegiatan berikut yang tercakup dalam hak kekayaan intelektual ditetapkan oleh Organisasi Hak Kekayaan Intelektual Dunia (WIPO):

(a) Desain industri

(b) Penemuan ilmiah
(c) Perlindungan terhadap persaingan tidak sehat
(d) Karya sastra, seni, dan ilmiah
(e) Penemuan di semua bidang usaha manusia
(f) Pertunjukan artis, rekaman suara, dan siaran
(g) Merek dagang, merek layanan, nama komersial, dan sebutan
(h) Semua hak lain yang timbul dari kegiatan intelektual di bidang industri, ilmiah, sastra, atau seni

**Jenis-jenis Hak Kekayaan Intelektual**

Hak Kekayaan Intelektual dapat diklasifikasikan lebih lanjut ke dalam kategori berikut:

(a) Hak cipta
(b) Paten
(c) Merek dagang
(d) Rahasia dagang, dll.


**Gambar 1.2 Jenis hak kekayaan intelektual**

**Keuntungan Hak Kekayaan Intelektual**

Hak kekayaan intelektual memiliki keuntungan sebagai berikut:

(a) Memberikan hak eksklusif kepada pencipta atau penemu.
(b) Mendorong individu untuk mendistribusikan dan berbagi informasi dan data alih-alih merahasiakannya.
(c) Memberikan pembelaan hukum dan menawarkan insentif bagi pencipta atas karya mereka.
(d) Membantu dalam pengembangan sosial dan finansial.

**Hak Kekayaan Intelektual di Indonesia**

Untuk memahami konteks *Hak Kekayaan Intelektual* (HKI) di Indonesia, kita perlu melihat kerangka hukum dan peraturan terbaru yang mengatur perlindungan HKI di negara

ini. Indonesia telah mengadopsi berbagai undang-undang untuk melindungi hak cipta, paten, merek dagang, dan desain industri, sejalan dengan komitmen internasional seperti TRIPS (*Trade-Related Aspects of Intellectual Property Rights*).

Kerangka Hukum HKI di Indonesia

1. Undang-Undang Paten:
   - Undang-Undang Nomor 13 Tahun 2016 tentang Paten menggantikan undang-undang sebelumnya dan mengatur sistem pendaftaran paten di Indonesia. Undang-undang ini memberikan perlindungan paten selama 20 tahun untuk penemuan baru yang memenuhi syarat kebaruan, langkah inventif, dan dapat diterapkan dalam industri.
2. Undang-Undang Merek:
   - Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis menggantikan Undang-Undang Merek yang lebih lama. Undang-undang ini memperkenalkan konsep merek non-tradisional dan memberikan perlindungan terhadap merek selama 10 tahun, yang dapat diperpanjang tanpa batas.
3. Undang-Undang Hak Cipta:
   - Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta memberikan perlindungan terhadap karya-karya kreatif seperti musik, seni, dan literatur. Perlindungan hak cipta berlaku otomatis saat karya diciptakan dan berlangsung selama masa hidup pencipta ditambah 70 tahun setelah kematiannya.
4. Desain Industri:
   - Undang-Undang Nomor 31 Tahun 2000 tentang Desain Industri mengatur perlindungan desain industri yang baru dan orisinal untuk jangka waktu 10 tahun, dengan kemungkinan perpanjangan.
5. Indikasi Geografis:
   - Perlindungan Indikasi Geografis diatur dalam Undang-Undang yang sama dengan merek, memberikan hak kepada produk yang berasal dari daerah tertentu dengan kualitas atau reputasi tertentu.

**Implementasi TRIPS di Indonesia**

Indonesia sebagai anggota WTO wajib mematuhi ketentuan TRIPS yang mengharuskan negara anggota untuk menyediakan perlindungan HKI yang memadai. Dalam hal ini, Indonesia telah melakukan harmonisasi peraturan nasional dengan ketentuan internasional, meskipun tantangan dalam implementasi masih ada, terutama terkait penegakan hukum dan kesadaran masyarakat mengenai pentingnya HKI.

**Tantangan dan Perkembangan Terkini**

Meskipun kerangka hukum telah ditetapkan, tantangan dalam penerapan HKI di Indonesia termasuk pelanggaran hak cipta dan merek, serta kurangnya pemahaman di kalangan masyarakat mengenai pentingnya perlindungan HKI. Pemerintah terus berupaya meningkatkan kesadaran melalui program edukasi dan kampanye tentang pentingnya menghormati HKI.Dengan demikian, meskipun Indonesia telah memiliki undang-undang yang komprehensif mengenai HKI, upaya untuk melindungi hak-hak tersebut secara efektif masih menjadi perhatian utama bagi pemerintah dan pemangku kepentingan lainnya.

Hak Kekayaan Intelektual (HKI) di Indonesia dan India memiliki beberapa kesamaan, terutama dalam hal kerangka hukum yang mengatur perlindungan terhadap hak cipta, paten,

merek dagang, dan desain industri. Kedua negara telah mengadopsi undang-undang yang sejalan dengan ketentuan internasional, seperti TRIPS (Trade-Related Aspects of Intellectual Property Rights), untuk meningkatkan perlindungan HKI.Namun, terdapat perbedaan signifikan dalam hal efektivitas penegakan hukum dan tingkat pelanggaran HKI. Indonesia sering kali menghadapi tantangan dalam melaksanakan perlindungan HKI secara efektif, seperti yang terlihat dari tingginya tingkat pembajakan dan pelanggaran hak cipta. Di sisi lain, India juga menghadapi masalah serupa, meskipun peringkatnya dalam perlindungan HKI lebih baik dibandingkan Indonesia

Kedua negara berusaha untuk meningkatkan kesadaran masyarakat tentang pentingnya HKI dan memperkuat sistem hukum mereka, tetapi masih banyak pekerjaan yang harus dilakukan untuk mencapai standar internasional yang diharapkan. Misalnya, Indonesia berada di peringkat rendah dalam Indeks Kekayaan Intelektual Internasional 2024, menunjukkan perlunya reformasi lebih lanjut untuk memperbaiki sistem HKI dan mendorong inovasi.

Setelah memahami konteks hak kekayaan intlektual di Indonesia, pembaca juga akan memahami pembahasan ringkas mengenai hak kekayaan intelektual di negara india.

**Hak Kekayaan Intelektual di India**

Untuk melindungi hak kekayaan intelektual di wilayah India, India telah menetapkan pembentukan kerangka konstitusional, administratif, dan yurisdiksi, baik yang menyiratkan hak cipta, paten, merek dagang, desain industri, atau bagian lain dari hak kekayaan intelektual. Pada tahun 1999, pemerintah mengeluarkan undang-undang penting berdasarkan praktik internasional untuk melindungi hak kekayaan intelektual. Mari kita lihat sekilas:

1. Undang-Undang Paten (Amandemen), 1999, memfasilitasi pembentukan sistem kotak surat untuk mengajukan paten. Undang-undang ini menawarkan hak pemasaran eksklusif untuk jangka waktu lima tahun.
2. Undang-Undang Merek Dagang, 1999, menggantikan Undang-Undang Merek Dagang dan Barang Dagangan, 1958.
3. Undang-Undang Hak Cipta (Amandemen), 1999, ditandatangani oleh Presiden India.
4. Undang-undang sui generis disetujui dan diberi nama Undang-Undang Indikasi Geografis Barang (Pendaftaran dan Perlindungan), 1999.
5. Undang-Undang Desain Industri, 1999, menggantikan Undang-Undang Desain, 1911.
6. Undang-Undang Paten (Amandemen Kedua), 1999, untuk selanjutnya mengubah Undang-Undang Paten tahun 1970 agar sesuai dengan TRIPS.

**Kekayaan Intelektual di Dunia Maya**

Setiap penemuan baru di bidang teknologi mengalami berbagai ancaman. Internet adalah salah satu ancaman tersebut, yang telah menguasai pasar fisik dan mengubahnya menjadi pasar virtual. Untuk melindungi kepentingan bisnis, sangat penting untuk menciptakan mekanisme manajemen dan perlindungan properti yang efektif dengan mempertimbangkan banyaknya bisnis dan perdagangan yang terjadi di Ruang Siber.

Saat ini, sangat penting bagi setiap bisnis untuk mengembangkan mekanisme manajemen IP dan strategi perlindungan yang efektif dan kolaboratif. Dengan demikian, ancaman yang terus muncul di dunia sibernetik dapat dipantau dan dibatasi.

Berbagai pendekatan dan undang-undang telah dirancang oleh para pembuat undang-undang untuk meningkatkan upaya dalam memberikan konfigurasi yang aman terhadap

ancaman siber tersebut. Namun, merupakan tugas pemilik hak kekayaan intelektual (HKI) untuk membatalkan dan mengurangi tindakan kriminal yang tidak jujur tersebut dengan mengambil tindakan proaktif.

## 1.4 STRATEGI KEAMANAN SIBER

Untuk merancang dan menerapkan dunia maya yang aman, beberapa strategi ketat telah diterapkan. Bab ini menjelaskan strategi utama yang digunakan untuk memastikan keamanan siber, yang meliputi hal-hal berikut:

1. Menciptakan Ekosistem Siber yang Aman
2. Menciptakan Kerangka Jaminan
3. Mendorong Standar Terbuka
4. Memperkuat Kerangka Regulasi
5. Menciptakan Mekanisme Keamanan TI
6. Mengamankan Layanan Tata Kelola Elektronik
7. Melindungi Infrastruktur Informasi Penting

**Strategi 1: Menciptakan Ekosistem Siber yang Aman**

Ekosistem siber melibatkan berbagai entitas yang bervariasi seperti perangkat (teknologi komunikasi dan komputer), individu, pemerintah, organisasi swasta, dll., yang berinteraksi satu sama lain karena berbagai alasan. Strategi ini mengeksplorasi gagasan untuk memiliki ekosistem siber yang kuat dan tangguh tempat perangkat siber dapat bekerja sama di masa mendatang untuk mencegah serangan siber, mengurangi efektivitasnya, atau menemukan solusi untuk memulihkan diri dari serangan siber. Ekosistem siber semacam itu akan memiliki kemampuan yang dibangun ke dalam perangkat sibernya untuk memungkinkan cara-cara tindakan yang aman untuk diatur di dalam dan di antara kelompok-kelompok perangkat. Ekosistem siber ini dapat diawasi oleh teknik-teknik pemantauan saat ini di mana produk-produk perangkat lunak digunakan untuk mendeteksi dan melaporkan kelemahan-kelemahan keamanan. Ekosistem siber yang kuat memiliki tiga struktur simbiosis - Otomatisasi, Interoperabilitas, dan Autentikasi.

1. Otomatisasi: Memudahkan penerapan langkah-langkah keamanan tingkat lanjut, meningkatkan kecepatan, dan mengoptimalkan proses-proses pengambilan keputusan.
2. Interoperabilitas: Memperkuat tindakan-tindakan kolaboratif, meningkatkan kesadaran, dan mempercepat prosedur pembelajaran. Ada tiga jenis interoperabilitas:
   (a) Semantik (yaitu, leksikon bersama berdasarkan pemahaman bersama)
   (b) Teknis
   (c) Kebijakan penting dalam mengasimilasi kontributor-kontributor yang berbeda ke dalam struktur pertahanan siber yang inklusif.
3. Autentikasi: Meningkatkan teknologi identifikasi dan verifikasi yang berfungsi untuk menyediakan:
   (a) Keamanan
   (b) Keterjangkauan
   (c) Kemudahan penggunaan dan administrasi
   (d) Skalabilitas
   (e) Interoperabilitas

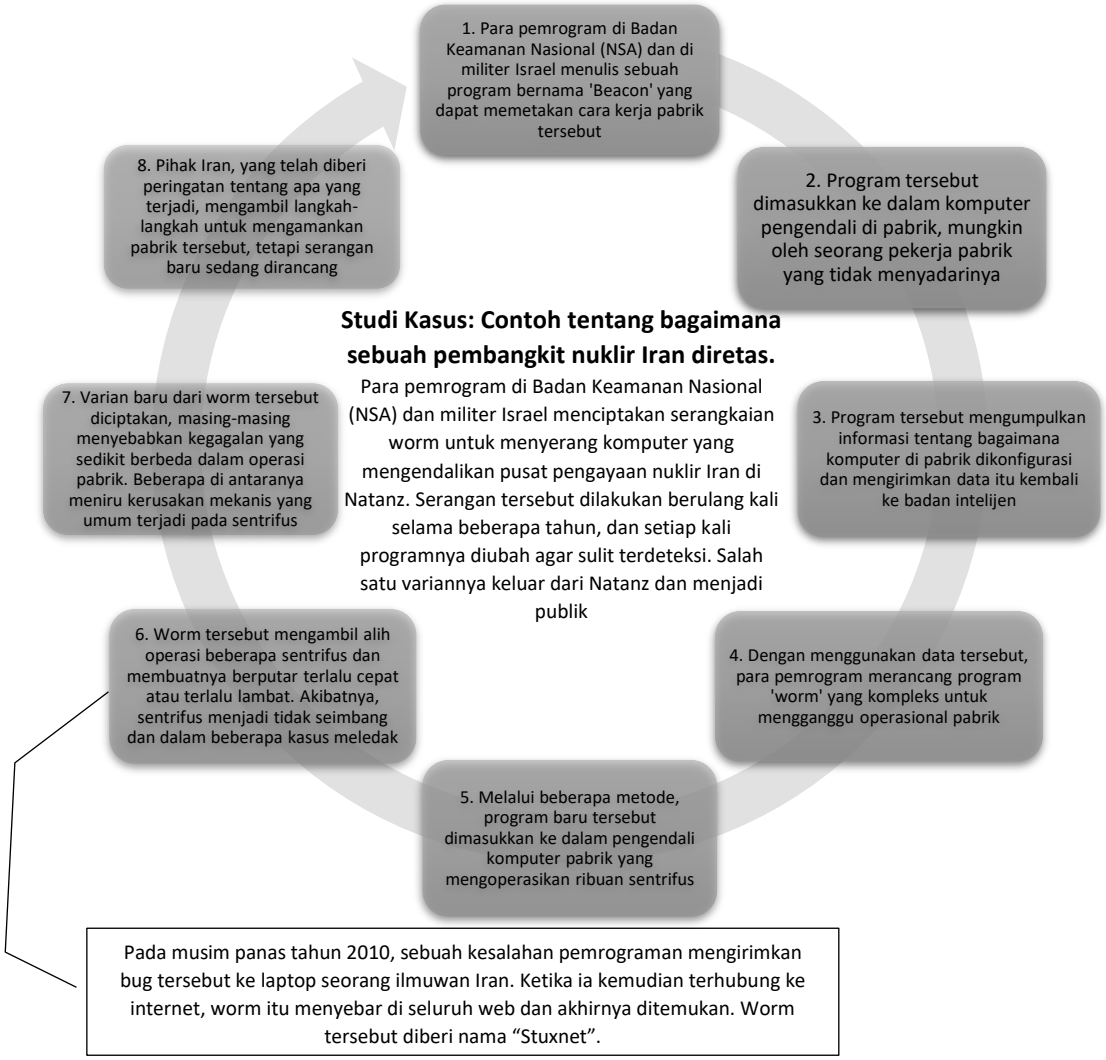
## Perbandingan Serangan

**Tabel 1.1Perbandingan Kategori Serangan terhadap Kemampuan Ekosistem Siber yang Diinginkan**

| | Kategori Serangan Siber | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Kemampuan Ekosistem Siber yang Diinginkan** | **Attrition** | **perangkat lunak perusak** | **Peretasan** | **Taktik Sosial** | **Penggunaan yang Tidak Tepat (Insider)** | **Tindakan Fisik; Kehilangan atau Pencurian** | **Komponen Ganda** | **Lainnya** |
| Otomatisasi | X | X | X | X | X | X | X | X |
| Otentikasi | X | X | X | X | | X | X | X |
| Interoperabilitas | X | X | X | X | | | X | |
| Identifikasi, Pemilihan, dan Penilaian Pertahanan Otomatis | X | X | X | X | X | X | X | X |
| Membangun Keamanan Di | X | X | X | X | | X | X | X |
| Aturan Bisnis-Pemantauan Perilaku Berbasis | X | X | X | X | X | X | X | X |
| Kesadaran Umum dan Pendidikan | X | X | X | X | X | X | X | X |
| Sasaran Bergerak | X | X | X | X | | | X | X |
| Pribadi | X | X | X | X | X | X | X | X |
| Manajemen Data Berbasis Risiko | X | X | X | X | X | X | X | X |
| Kesadaran Situasional | X | X | X | X | X | X | X | X |
| Ruang Kepercayaan yang Disesuaikan | X | X | X | X | | | X | X |

## Studi Kasus

Diagram berikut disiapkan oleh Guilbert Gates untuk The New York Times, yang menunjukkan bagaimana sebuah pabrik di Iran diretas melalui internet. Penjelasan: Sebuah program dirancang untuk menjalankan pabrik nuklir Iran secara otomatis. Sayangnya, seorang pekerja yang tidak menyadari ancaman tersebut memasukkan program tersebut ke dalam pengendali. Program tersebut mengumpulkan semua data yang terkait dengan pabrik dan mengirimkan informasi tersebut ke badan intelijen yang kemudian mengembangkan dan memasukkan worm ke dalam pabrik. Dengan menggunakan worm tersebut, pabrik tersebut dikendalikan oleh penjahat yang menyebabkan munculnya lebih banyak worm dan akibatnya, pabrik tersebut gagal total.




**Gambar 1.3 Studi kasus tentang keamanan siber**

## Jenis Serangan

**Tabel 1.2 menjelaskan kategori serangan**

| Kategori Serangan | Deskripsi Serangan |
|---|---|
| Pengurangan | Metode yang digunakan untuk merusak jaringan dan sistem. Metode ini meliputi:<br>• serangan penolakan layanan terdistribusi<br>• merusak atau menolak akses ke layanan atau aplikasi<br>• serangan penipisan sumber daya |
| Malware | Perangkat lunak berbahaya apa pun yang digunakan untuk mengganggu operasi komputer normal dan merusak aset informasi tanpa persetujuan pemiliknya. Setiap eksekusi dari perangkat yang dapat dilepas dapat meningkatkan ancaman malware. |
| Peretasan | Upaya untuk secara sengaja mengeksploitasi kelemahan guna mendapatkan akses yang tidak etis, biasanya dilakukan dari jarak jauh. Upaya ini dapat mencakup:<br>• serangan kebocoran data |

| | |
|---|---|
| | • serangan injeksi dan penyalahgunaan fungsi<br>• spoofing<br>• serangan status waktu<br>• serangan buffer dan struktur data<br>• manipulasi sumber daya<br>• penggunaan kredensial yang dicuri<br>• backdoor<br>• serangan kamus pada kata sandi<br>• eksploitasi autentikasi |
| Taktik Sosial | Menggunakan taktik sosial seperti penipuan dan manipulasi untuk memperoleh akses ke data, sistem, atau kontrol. Ini termasuk:<br>• pra-teks (survei palsu)<br>• menghasut phishing<br>• mengambil informasi melalui percakapan |
| Pemanfaatan yang Tidak Tepat (Ancaman Orang Dalam) | Penyalahgunaan hak atas data dan kontrol oleh individu dalam suatu organisasi yang dapat melanggar kebijakan organisasi. Ini termasuk:<br>• pemasangan perangkat lunak yang tidak sah<br>• penghapusan data sensitif |
| Tindakan Fisik/Kehilangan atau Pencurian Peralatan | Serangan yang Dilakukan Manusia seperti:<br>• pencurian token identitas dan kartu kredit<br>• mengutak-atik atau mengganti pembaca kartu dan terminal point of sale mengganggu sensor<br>• pencurian perangkat komputasi yang digunakan oleh organisasi, seperti laptop |
| Komponen Ganda | Teknik serangan tunggal yang berisi beberapa teknik dan komponen serangan tingkat lanjut. |
| Lainnya | Serangan seperti:<br>• serangan rantai pasokan<br>• investigasi jaringan |

**Strategi 2: Membuat Kerangka Jaminan**

Tujuan dari strategi ini adalah untuk merancang kerangka kerja yang sesuai dengan standar keamanan global melalui produk, proses, orang, dan teknologi tradisional.

Untuk memenuhi persyaratan keamanan nasional, kerangka kerja nasional yang dikenal sebagai Kerangka Jaminan Keamanan Siber dikembangkan. Kerangka kerja ini mengakomodasi organisasi infrastruktur penting dan pemerintah melalui tindakan "Pemberdayaan dan Dukungan".

Tindakan pemberdayaan dilakukan oleh badan pemerintah yang merupakan badan otonom yang bebas dari kepentingan komersial. Publikasi "Persyaratan Kepatuhan Kebijakan Keamanan Nasional" dan pedoman serta dokumen keamanan TI untuk memungkinkan penerapan dan kepatuhan keamanan TI dilakukan oleh otoritas ini.

Tindakan dukungan terlibat dalam layanan yang menguntungkan setelah memenuhi standar kualifikasi wajib dan tindakan tersebut meliputi hal-hal berikut:

1. Sertifikasi ISMS ISO 27001/BS 7799, audit sistem IS, dll., yang pada dasarnya merupakan sertifikasi kepatuhan.
2. Standar 'Kriteria Umum' ISO 15408 dan standar verifikasi modul Kripto, yang merupakan evaluasi dan sertifikasi produk Keamanan TI.
3. Layanan untuk membantu konsumen dalam penerapan keamanan TI seperti pelatihan tenaga kerja keamanan TI.

**Sertifikasi Perusahaan Tepercaya**

IT/ITES/BPO India perlu mematuhi standar internasional dan praktik terbaik tentang keamanan dan privasi seiring dengan perkembangan pasar alih daya. ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001, dll., adalah beberapa sertifikasi. Model yang ada seperti level CMM SEI secara eksklusif ditujukan untuk proses pengembangan perangkat lunak dan tidak membahas masalah keamanan. Oleh karena itu, beberapa upaya dilakukan untuk membuat model berdasarkan konsep sertifikasi mandiri dan sejalan dengan Software Capability Maturity Model (SW-CMM) dari CMU, AS. Struktur yang telah dihasilkan melalui asosiasi antara industri dan pemerintah tersebut, terdiri dari hal-hal berikut:

(a) standar
(b) pedoman
(c) praktik

Parameter ini membantu pemilik dan operator infrastruktur penting untuk mengelola risiko terkait keamanan siber.

**Strategi 3: Mendorong Standar Terbuka**

Standar memainkan peran penting dalam mendefinisikan cara kita menangani isu-isu terkait keamanan informasi di seluruh wilayah geografis dan masyarakat. Standar terbuka didorong untuk:

1. Meningkatkan efisiensi proses-proses utama,
2. Memungkinkan penggabungan sistem,
3. Menyediakan media bagi pengguna untuk mengukur produk atau layanan baru,
4. Mengatur pendekatan untuk menyusun teknologi atau model bisnis baru,
5. Menafsirkan lingkungan yang kompleks, dan
6. Mendukung pertumbuhan ekonomi.

Standar seperti ISO 27001 mendorong penerapan struktur organisasi standar, tempat pelanggan dapat memahami proses, dan mengurangi biaya audit.

**Strategi 4: Memperkuat Kerangka Regulasi**

Tujuan dari strategi ini adalah untuk menciptakan ekosistem dunia maya yang aman dan memperkuat kerangka regulasi. Mekanisme 24X7 telah dibayangkan untuk menangani ancaman dunia maya melalui Pusat Perlindungan Infrastruktur Informasi Kritis Nasional (NCIIPC). Tim Tanggap Darurat Komputer (CERT-In) telah ditunjuk untuk bertindak sebagai lembaga pusat untuk manajemen krisis. Beberapa hal penting dari strategi ini adalah sebagai berikut:

(a) Promosi penelitian dan pengembangan dalam keamanan siber.
(b) Mengembangkan sumber daya manusia melalui program pendidikan dan pelatihan.
(c) Mendorong semua organisasi, baik publik maupun swasta, untuk menunjuk seseorang untuk menjabat sebagai Kepala Petugas Keamanan Informasi (CISO) yang akan bertanggung jawab atas inisiatif keamanan siber.

(d) Angkatan Bersenjata India sedang dalam proses membangun komando siber sebagai bagian dari penguatan keamanan siber jaringan dan instalasi pertahanan.
(e) Implementasi kemitraan publik-swasta yang efektif sedang dalam proses yang akan sangat membantu dalam menciptakan solusi untuk lanskap ancaman yang terus berubah.

**Strategi 5: Menciptakan Mekanisme untuk Keamanan TI**

Beberapa mekanisme dasar yang ada untuk memastikan keamanan TI adalah: langkah-langkah keamanan berorientasi tautan, langkah-langkah keamanan ujung ke ujung, langkah-langkah berorientasi asosiasi, dan enkripsi data. Metode-metode ini berbeda dalam fitur aplikasi internalnya dan juga dalam atribut keamanan yang disediakannya. Mari kita bahas secara singkat.

**Pengukuran Berorientasi Tautan**

Mesin ini memberikan keamanan saat mentransfer data antara dua node, terlepas dari sumber dan tujuan akhir data.

**Pengukuran Ujung-ke-Ujung**

Mesin ini adalah media untuk mengangkut Unit Data Protokol (PDU) dengan cara yang terlindungi dari sumber ke tujuan sedemikian rupa sehingga gangguan pada tautan komunikasinya tidak melanggar keamanan.

**Pengukuran Berorientasi Asosiasi**

Pengukuran berorientasi asosiasi adalah serangkaian pengukuran ujung-ke-ujung yang dimodifikasi yang melindungi setiap asosiasi secara individual.

**Enkripsi Data**

Mesin ini mendefinisikan beberapa fitur umum sandi konvensional dan kelas sandi kunci publik yang baru-baru ini dikembangkan. Mesin ini mengodekan informasi dengan cara yang hanya dapat didekripsi oleh personel yang berwenang.

**Strategi 6: Mengamankan Layanan E-Governance**

Tata kelola elektronik (e-governance) merupakan instrumen yang paling berharga bagi pemerintah untuk menyediakan layanan publik secara akuntabel. Sayangnya, dalam skenario saat ini, tidak ada struktur hukum khusus untuk e-governance di India. Demikian pula, tidak ada undang-undang untuk penyediaan layanan publik secara elektronik wajib di India. Dan tidak ada yang lebih berbahaya dan merepotkan daripada melaksanakan proyek e-governance tanpa keamanan siber yang memadai. Oleh karena itu, mengamankan layanan e-governance telah menjadi tugas penting, terutama ketika negara melakukan transaksi harian melalui kartu. Untungnya, Bank Sentral India telah menerapkan langkah-langkah mitigasi risiko dan keamanan untuk transaksi kartu di India yang berlaku mulai 1 Oktober 2013. Bank tersebut telah menyerahkan tanggung jawab untuk memastikan transaksi kartu yang aman kepada bank, bukan kepada nasabah. "E-government" atau pemerintahan elektronik mengacu pada penggunaan Teknologi Informasi dan Komunikasi (TIK) oleh badan-badan pemerintah untuk hal-hal berikut:

(a) Penyediaan layanan publik yang efisien
(b) Memperbaiki efisiensi internal
(c) Mempermudah pertukaran informasi antara warga negara, organisasi, dan badan-badan pemerintah
(d) Menata ulang proses-proses administratif.

**Strategi 7: Melindungi Infrastruktur Informasi Penting**

Infrastruktur informasi penting merupakan tulang punggung keamanan nasional dan ekonomi suatu negara. Infrastruktur ini mencakup pembangkit listrik, jalan raya, jembatan, pabrik kimia, jaringan, serta gedung-gedung tempat jutaan orang bekerja setiap hari. Infrastruktur ini dapat diamankan dengan rencana kolaborasi yang ketat dan penerapan yang disiplin. Melindungi infrastruktur penting dari ancaman siber yang berkembang memerlukan pendekatan yang terstruktur. Pemerintah harus bekerja sama secara agresif dengan sektor publik dan swasta secara berkala untuk mencegah, menanggapi, dan mengoordinasikan upaya mitigasi terhadap upaya gangguan dan dampak buruk terhadap infrastruktur penting negara. Pemerintah dituntut untuk bekerja sama dengan pemilik dan operator bisnis untuk memperkuat layanan dan kelompok mereka dengan berbagi informasi tentang ancaman siber dan lainnya. Platform umum harus dibagikan dengan pengguna untuk mengirimkan komentar dan ide, yang dapat digunakan bersama untuk membangun fondasi yang lebih kuat guna mengamankan dan melindungi infrastruktur penting. Pemerintah Amerika Serikat telah mengeluarkan perintah eksekutif "Meningkatkan Keamanan Siber Infrastruktur Kritis" pada tahun 2013 yang memprioritaskan pengelolaan risiko keamanan siber yang terlibat dalam penyediaan layanan infrastruktur kritis. Kerangka kerja ini menyediakan klasifikasi dan mekanisme umum bagi organisasi untuk:

(a) Menetapkan arah keamanan siber yang ada,
(b) Menetapkan tujuan mereka untuk keamanan siber,
(c) Mengkategorikan dan memprioritaskan peluang untuk pengembangan dalam kerangka proses yang konstan, dan
(d) Berkomunikasi dengan semua investor tentang keamanan siber.

## 1.5. KEBIJAKAN UNTUK MENGURANGI RISIKO SIBER

Bab ini akan membahas berbagai kebijakan yang ditetapkan untuk meminimalkan risiko siber. Hanya dengan kebijakan yang ditetapkan dengan baik, ancaman yang dihasilkan di dunia maya dapat dikurangi.

**Peningkatan Penelitian dan Pengembangan dalam Keamanan Siber**

Karena ketergantungan yang terus meningkat pada Internet, tantangan terbesar yang kita hadapi saat ini adalah keamanan informasi dari para penjahat. Oleh karena itu, penting untuk meningkatkan penelitian dan pengembangan dalam keamanan siber sehingga kita dapat menemukan solusi yang kuat untuk mengurangi risiko siber.

**Penelitian Keamanan Siber**

Penelitian Keamanan Siber adalah bidang yang berkaitan dengan persiapan solusi untuk menangani penjahat siber. Dengan meningkatnya jumlah serangan internet, ancaman persisten tingkat lanjut, dan phishing, banyak penelitian dan pengembangan teknologi yang diperlukan di masa mendatang.

**Penelitian Keamanan Siber – Perspektif India**

Dalam beberapa tahun terakhir, India telah menyaksikan pertumbuhan yang sangat besar dalam teknologi siber. Oleh karena itu, India membutuhkan investasi dalam kegiatan penelitian dan pengembangan keamanan siber. India juga telah melihat banyak hasil penelitian yang berhasil yang diterjemahkan ke dalam bisnis, melalui munculnya perusahaan keamanan siber lokal.

**Intelijen Ancaman**

Penelitian untuk mengurangi ancaman siber sudah dimulai di India. Ada mekanisme respons proaktif untuk menangani ancaman siber. Aktivitas Penelitian dan Pengembangan sudah berlangsung di berbagai organisasi penelitian di India untuk melawan ancaman di dunia maya.

**Firewall Generasi Berikutnya**

Keahlian berbasis multi-identitas seperti Firewall Generasi Berikutnya yang menawarkan intelijen keamanan kepada perusahaan dan memungkinkan mereka menerapkan kontrol keamanan yang paling sesuai di perimeter jaringan juga sedang dikerjakan.

**Protokol dan Algoritma yang Aman**

Penelitian dalam protokol dan algoritma merupakan fase penting untuk konsolidasi keamanan siber di tingkat teknis. Penelitian ini mendefinisikan aturan untuk berbagi dan memproses informasi melalui dunia maya. Di India, penelitian tingkat protokol dan algoritma meliputi:

1. Protokol Perutean Aman
2. Protokol Autentikasi Efisien
3. Protokol Perutean yang Disempurnakan untuk Jaringan Nirkabel
4. Protokol Kontrol Transmisi Aman
5. Algoritma Simulasi Serangan, dll.

**Teknik Autentikasi**

Teknik autentikasi seperti Manajemen Kunci, Autentikasi Dua Faktor, dan Manajemen Kunci Otomatis memberikan kemampuan untuk mengenkripsi dan mendekripsi tanpa sistem manajemen kunci terpusat dan perlindungan berkas. Ada penelitian berkelanjutan yang dilakukan untuk memperkuat teknik autentikasi ini.

**BYOD, Keamanan Cloud dan Seluler**

Dengan adopsi berbagai jenis perangkat seluler, penelitian tentang tugas terkait keamanan dan privasi pada perangkat seluler telah meningkat. Pengujian keamanan seluler, Keamanan Cloud, dan mitigasi risiko BYOD (*Bring Your Own Device*) adalah beberapa area yang banyak diteliti.

**Forensik Siber**

Forensik Siber adalah penerapan teknik analisis untuk mengumpulkan dan memulihkan data dari sistem atau media penyimpanan digital. Beberapa bidang khusus yang tengah diteliti di India adalah:

1. Forensik Cakram
2. Forensik Jaringan
3. Forensik Perangkat Seluler
4. Forensik Memori
5. Forensik Multimedia
6. Forensik Internet

**Mengurangi Risiko Rantai Pasokan**

Secara formal, risiko rantai pasokan dapat didefinisikan sebagai:

Setiap risiko yang dapat dirusak oleh lawan, menuliskan beberapa fungsi jahat padanya, mendekonstruksi desain, instalasi, prosedur, atau pemeliharaan item pasokan atau sistem sehingga seluruh fungsi dapat menurun.

**Masalah Rantai Pasokan**

Rantai pasokan adalah masalah global dan ada persyaratan untuk mengetahui saling ketergantungan antara pelanggan dan pemasok. Dalam skenario saat ini, penting untuk mengetahui: Apa saja masalah SCRM? dan Bagaimana cara mengatasi masalah tersebut? Pendekatan SCRM (Manajemen Risiko Rantai Pasokan) yang efektif memerlukan kemitraan publik-swasta yang kuat. Pemerintah harus memiliki otoritas yang kuat untuk menangani masalah rantai pasokan. Bahkan sektor swasta dapat memainkan peran penting dalam sejumlah bidang. Kami tidak dapat memberikan solusi yang cocok untuk semua orang dalam mengelola risiko rantai pasokan. Bergantung pada produk dan sektornya, biaya untuk mengurangi risiko akan berbeda-beda. Kemitraan Publik-Swasta harus didorong untuk mengatasi risiko yang terkait dengan manajemen rantai pasokan.

**Mengurangi Risiko melalui Pengembangan Sumber Daya Manusia**

Kebijakan keamanan siber suatu organisasi dapat efektif, asalkan semua karyawannya memahami nilainya dan menunjukkan komitmen yang kuat untuk menerapkannya. Direktur sumber daya manusia dapat memainkan peran penting dalam menjaga keamanan organisasi di dunia maya dengan menerapkan beberapa poin berikut.

**Mengambil Kepemilikan atas Risiko Keamanan yang Ditimbulkan oleh Karyawan**

Karena sebagian besar karyawan tidak menganggap serius faktor risiko, peretas merasa mudah untuk menargetkan organisasi. Dalam hal ini, SDM memainkan peran penting dalam mendidik karyawan tentang dampak sikap dan perilaku mereka terhadap keamanan organisasi.

**Memastikan bahwa Langkah-Langkah Keamanan Praktis dan Etis**

Kebijakan perusahaan harus selaras dengan cara berpikir dan berperilaku karyawan. Misalnya, menyimpan kata sandi pada sistem merupakan ancaman, namun pemantauan berkelanjutan dapat mencegahnya. Tim SDM adalah pihak yang paling tepat untuk memberikan saran apakah kebijakan tersebut mungkin berhasil dan apakah kebijakan tersebut tepat.

**Mengidentifikasi Karyawan yang Mungkin Menyajikan Risiko Tertentu**

Penjahat dunia maya juga memanfaatkan bantuan orang dalam perusahaan untuk meretas jaringan mereka. Oleh karena itu, penting untuk mengidentifikasi karyawan yang mungkin menghadirkan risiko tertentu dan memiliki kebijakan SDM yang ketat untuk mereka.

**Menciptakan Kesadaran Keamanan Siber**

Keamanan siber di India masih dalam tahap evolusi. Ini adalah waktu terbaik untuk menciptakan kesadaran tentang berbagai masalah yang terkait dengan keamanan siber. Akan mudah untuk menciptakan kesadaran dari tingkat akar rumput seperti sekolah tempat pengguna dapat dibuat sadar tentang cara kerja Internet dan apa saja potensi ancamannya. Setiap warnet, komputer rumah/pribadi, dan komputer kantor harus dilindungi melalui firewall. Pengguna harus diinstruksikan melalui penyedia layanan atau gateway mereka untuk tidak melanggar jaringan yang tidak sah. Ancaman harus dijelaskan dengan huruf tebal dan dampaknya harus disorot. Mata pelajaran tentang kesadaran keamanan siber harus diperkenalkan di sekolah dan perguruan tinggi untuk menjadikannya proses yang

berkelanjutan. Pemerintah harus merumuskan undang-undang yang kuat untuk menegakkan keamanan siber dan menciptakan kesadaran yang memadai dengan menyiarkannya melalui iklan televisi/radio/internet.

**Berbagi informasi**

Amerika Serikat mengusulkan undang-undang yang disebut Undang-Undang Berbagi Informasi Keamanan Siber tahun 2014 (CISA) untuk meningkatkan keamanan siber di negara tersebut melalui peningkatan berbagi informasi tentang ancaman keamanan siber. Undang-undang semacam itu diwajibkan di setiap negara untuk berbagi informasi ancaman di antara warga negara.

**Pelanggaran Keamanan Siber Memerlukan Mekanisme Pelaporan Wajib**

Malware baru-baru ini bernama Uroburos/Snake adalah contoh dari meningkatnya spionase siber dan perang siber. Pencurian informasi sensitif adalah tren baru. Namun, sangat disayangkan bahwa perusahaan telekomunikasi/penyedia layanan internet (ISP) tidak berbagi informasi yang berkaitan dengan serangan siber terhadap jaringan mereka. Akibatnya, strategi keamanan siber yang kuat untuk melawan serangan siber tidak dapat dirumuskan.

Masalah ini dapat diatasi dengan merumuskan undang-undang keamanan siber yang baik yang dapat menetapkan rezim regulasi untuk pemberitahuan pelanggaran keamanan siber wajib dari pihak perusahaan telekomunikasi/ISP. Infrastruktur seperti jaringan listrik otomatis, pembangkit listrik termal, satelit, dll., rentan terhadap berbagai bentuk serangan siber dan karenanya program pemberitahuan pelanggaran akan memberi tahu lembaga untuk menanganinya.

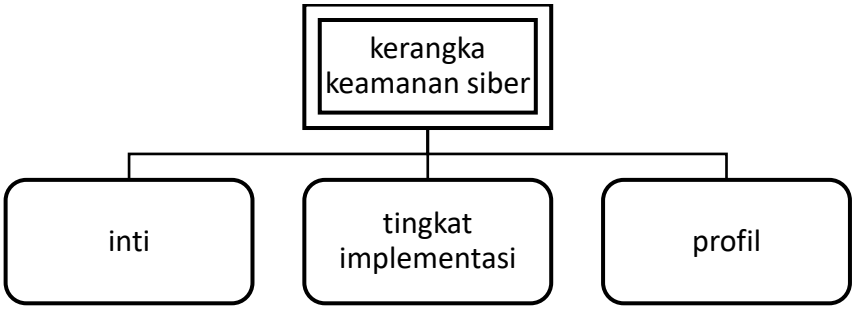
**Menerapkan Kerangka Kerja Keamanan Siber**

Meskipun perusahaan mengeluarkan biaya untuk inisiatif keamanan siber, pelanggaran data terus terjadi. Menurut The Wall Street Journal, "Pengeluaran keamanan siber global oleh industri infrastruktur penting diperkirakan mencapai $46 miliar pada tahun 2013, naik 10% dari tahun sebelumnya menurut Allied Business Intelligence Inc." Hal ini memerlukan penerapan kerangka kerja keamanan siber yang efektif.

**Komponen Kerangka Kerja Keamanan Siber**

Kerangka kerja terdiri dari tiga komponen utama:

(a) Inti,
(b) Tingkatan Implementasi, dan
(c) Profil Kerangka Kerja.




**Gambar 1.4 Keamanan Kerangka Keamanan Siber**

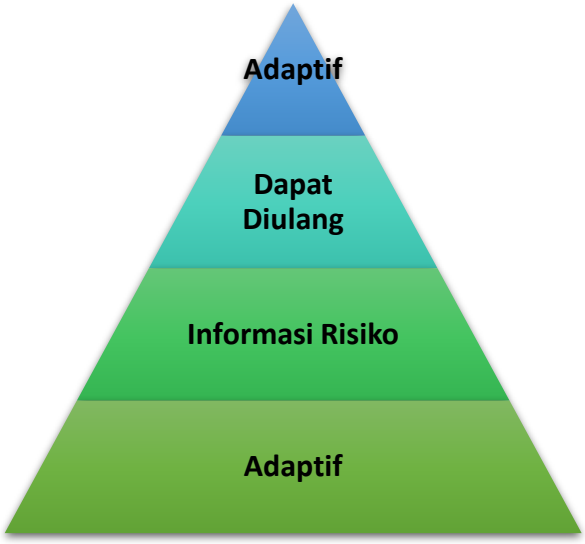
**Inti Kerangka Kerja**

Inti Kerangka Kerja adalah serangkaian aktivitas keamanan siber dan referensi yang berlaku yang memiliki lima fungsi yang simultan dan konstan—Identifikasi, Lindungi, Deteksi, Tanggapi, dan Pulihkan. Inti kerangka kerja memiliki metode untuk memastikan hal-hal berikut:

1. Mengembangkan dan menerapkan prosedur untuk melindungi kekayaan intelektual dan aset yang paling penting.
2. Memiliki sumber daya untuk mengidentifikasi setiap pelanggaran keamanan siber.
3. Memulihkan dari pelanggaran, jika dan ketika terjadi.

**Tingkatan Implementasi**

Tingkatan Implementasi Kerangka Kerja menentukan tingkat kecanggihan dan konsistensi yang digunakan organisasi dalam menerapkan praktik keamanan sibernya. Ada empat tingkatan berikut.




**Gambar 1.5**

- **Tingkat 1 (Sebagian):** Pada tingkat ini, profil manajemen risiko siber organisasi tidak ditetapkan. Ada kesadaran sebagian terhadap risiko keamanan siber organisasi di tingkat organisasi. Metodologi di seluruh organisasi untuk mengelola risiko keamanan siber belum dikenali.
- **Tingkat 2 (Berwawasan Risiko):** Pada tingkat ini, organisasi menetapkan kebijakan manajemen risiko siber yang disetujui langsung oleh manajemen senior. Manajemen senior berupaya menetapkan tujuan manajemen risiko yang terkait dengan keamanan siber dan menerapkannya.
- **Tingkat 3 (Dapat Diulang):** Pada tingkat ini, organisasi menjalankan langkah-langkah keamanan siber formal, yang diperbarui secara berkala berdasarkan kebutuhan. Organisasi mengenali ketergantungan dan mitranya. Organisasi juga menerima informasi dari mereka, yang membantu dalam mengambil keputusan manajemen berbasis risiko.
- **Tingkat 4 (Adaptif):** Pada tingkat ini, organisasi mengadaptasi praktik keamanan sibernya "secara real-time" yang berasal dari aktivitas keamanan siber sebelumnya

dan saat ini. Melalui proses pengembangan yang tiada henti dalam menggabungkan teknologi keamanan siber tingkat lanjut, kolaborasi waktu nyata dengan mitra, dan pemantauan berkelanjutan terhadap aktivitas pada sistem mereka, praktik keamanan siber organisasi dapat dengan cepat menanggapi ancaman canggih.

**Profil Kerangka Kerja**

Profil Kerangka Kerja adalah alat yang menyediakan platform bagi organisasi untuk menyimpan informasi mengenai program keamanan siber mereka. Profil memungkinkan organisasi untuk mengekspresikan tujuan program keamanan siber mereka dengan jelas.

**Di Mana Anda Memulai Penerapan Kerangka Kerja?**

Manajemen senior termasuk para direktur harus terlebih dahulu mengenal Kerangka Kerja. Setelah itu, para direktur harus berdiskusi secara terperinci dengan manajemen tentang Tingkatan Penerapan organisasi. Mendidik para manajer dan staf tentang Kerangka Kerja akan memastikan bahwa setiap orang memahami pentingnya hal tersebut. Ini merupakan langkah penting menuju keberhasilan penerapan program keamanan siber yang kuat. Informasi tentang Penerapan Kerangka Kerja yang ada dapat membantu organisasi dengan pendekatan mereka sendiri.

## 1.6 KEAMANAN JARINGAN

Keamanan jaringan adalah keamanan yang diberikan kepada jaringan dari akses dan risiko yang tidak sah. Administrator jaringan berkewajiban untuk mengambil tindakan pencegahan guna melindungi jaringan mereka dari potensi ancaman keamanan. Jaringan komputer yang terlibat dalam transaksi dan komunikasi rutin dalam pemerintahan, individu, atau bisnis memerlukan keamanan. Cara yang paling umum dan sederhana untuk melindungi sumber daya jaringan adalah dengan memberinya nama unik dan kata sandi yang sesuai.

**Jenis Perangkat Keamanan Jaringan**

- **Perangkat Aktif**: Perangkat keamanan ini memblokir lalu lintas yang berlebih. Firewall, perangkat pemindaian antivirus, dan perangkat penyaringan konten adalah contoh perangkat tersebut.
- **Perangkat Pasif**: Perangkat ini mengidentifikasi dan melaporkan lalu lintas yang tidak diinginkan, misalnya, perangkat deteksi intrusi.
- **Perangkat Pencegahan**: Perangkat ini memindai jaringan dan mengidentifikasi potensi masalah keamanan. Misalnya, perangkat pengujian penetrasi dan perangkat penilaian kerentanan.
- **Unified Threat Management (UTM)**: Perangkat ini berfungsi sebagai perangkat keamanan lengkap. Contohnya termasuk firewall, penyaringan konten, web caching, dll.
- **Firewall**: Firewall adalah sistem keamanan jaringan yang mengelola dan mengatur lalu lintas Jaringan berdasarkan beberapa protokol. Firewall membangun penghalang antara jaringan internal tepercaya dan internet. Firewall ada baik sebagai perangkat lunak yang berjalan pada perangkat keras maupun sebagai peralatan perangkat keras. Firewall yang berbasis perangkat keras juga menyediakan fungsi lain seperti bertindak sebagai server DHCP untuk jaringan tersebut. Sebagian besar komputer pribadi menggunakan firewall berbasis perangkat lunak untuk mengamankan data dari

ancaman dari internet. Banyak router yang melewatkan data antar jaringan berisi komponen firewall dan sebaliknya, banyak firewall dapat melakukan fungsi perutean dasar. Firewall umumnya digunakan dalam jaringan pribadi atau intranet untuk mencegah akses tidak sah dari internet. Setiap pesan yang masuk atau keluar dari intranet melewati firewall untuk diperiksa terkait langkah-langkah keamanan. Konfigurasi firewall yang ideal terdiri dari perangkat keras dan perangkat lunak. Firewall juga membantu menyediakan akses jarak jauh ke jaringan pribadi melalui sertifikat autentikasi dan login yang aman.

**Firewall Perangkat Keras dan Perangkat Lunak**

Firewall perangkat keras adalah produk yang berdiri sendiri. Produk ini juga ditemukan di router pita lebar. Sebagian besar firewall perangkat keras menyediakan minimal empat port jaringan untuk menghubungkan komputer lain. Untuk jaringan yang lebih besar misalnya, untuk tujuan bisnis tersedia solusi firewall jaringan bisnis. Firewall perangkat lunak dipasang di komputer Anda. Firewall perangkat lunak melindungi komputer Anda dari ancaman internet.

**Antivirus**

Antivirus adalah alat yang digunakan untuk mendeteksi dan menghapus perangkat lunak berbahaya. Awalnya, alat ini dirancang untuk mendeteksi dan menghapus virus dari komputer. Perangkat lunak antivirus modern tidak hanya memberikan perlindungan dari virus, tetapi juga dari worm, Trojan-horse, adware, spyware, keylogger, dll. Beberapa produk juga memberikan perlindungan dari URL berbahaya, spam, serangan phishing, botnet, serangan DDoS, dll.

**Penyaringan Konten**

Perangkat penyaringan konten menyaring email atau halaman web yang tidak menyenangkan dan menyinggung. Perangkat ini digunakan sebagai bagian dari firewall di perusahaan maupun di komputer pribadi. Perangkat ini menghasilkan pesan "Akses Ditolak" ketika seseorang mencoba mengakses halaman web atau email yang tidak sah. Konten biasanya disaring untuk konten pornografi dan juga untuk konten yang berorientasi pada kekerasan atau kebencian. Organisasi juga mengecualikan konten yang berhubungan dengan belanja dan pekerjaan. Pemfilteran konten dapat dibagi menjadi beberapa kategori berikut:

a. Pemfilteran web
b. Penyaringan situs web atau halaman
c. Pemfilteran email
d. Penyaringan email untuk spam
e. Konten lain yang tidak menyenangkan

**Sistem Deteksi Intrusi**

Sistem Deteksi Intrusi, juga dikenal sebagai Sistem Deteksi dan Pencegahan Intrusi, adalah peralatan yang memantau aktivitas berbahaya dalam jaringan, mencatat informasi tentang aktivitas tersebut, mengambil langkah-langkah untuk menghentikannya, dan akhirnya melaporkannya. Sistem deteksi intrusi membantu mengirimkan alarm terhadap aktivitas berbahaya apa pun dalam jaringan, membuang paket, dan mengatur ulang koneksi untuk menyelamatkan alamat IP dari penyumbatan apa pun. Sistem deteksi intrusi juga dapat melakukan tindakan berikut:

a. Memperbaiki kesalahan Cyclic Redundancy Check (CRC)

b. Mencegah masalah pengurutan TCP
c. Membersihkan opsi lapisan jaringan dan transportasi yang tidak diinginkan

## 1.7 UU ITE

Pemerintah Indonesia memberlakukan UU Teknologi Informasi (TI) dengan beberapa tujuan utama untuk menyediakan dan memfasilitasi transaksi elektronik, digital, dan daring yang sah, serta mengurangi kejahatan dunia maya.

**Fitur-fitur Menonjol UU TI**

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia telah mengalami beberapa perubahan signifikan, terutama dengan disahkannya UU No. 1 Tahun 2024 yang merupakan revisi kedua dari UU No. 11 Tahun 2008. Berikut adalah fitur-fitur menonjol dari UU TI yang relevan dalam konteks hukum di Indonesia:

1. Tanda Tangan Elektronik

UU ini mengganti istilah tanda tangan digital dengan tanda tangan elektronik. Perubahan ini bertujuan untuk menciptakan tindakan yang lebih netral terhadap teknologi, sehingga lebih inklusif bagi berbagai bentuk transaksi elektronik yang dilakukan di Indonesia.

2. Pengaturan Pelanggaran dan Hukuman

UU ITE menguraikan dengan jelas tentang pelanggaran, hukuman, dan jenis-jenis pelanggaran yang dapat terjadi dalam ruang siber. Hal ini memberikan kepastian hukum bagi pengguna internet dan penyelenggara sistem elektronik dalam menghadapi potensi kejahatan siber.

3. Sistem Dispensasi Peradilan untuk Kejahatan Siber

UU ini juga mencakup pengaturan mengenai Sistem Dispensasi Peradilan untuk kejahatan dunia maya, yang bertujuan untuk memberikan solusi hukum yang lebih cepat dan efisien dalam menangani kasus-kasus kejahatan siber.

4. Definisi Warnet

Dalam UU ini, terdapat definisi baru mengenai warnet (warung internet) sebagai fasilitas yang menawarkan akses internet kepada masyarakat umum dalam konteks bisnis. Hal ini penting untuk mengatur operasional warnet dan memastikan kepatuhan terhadap regulasi yang berlaku

5. Pembentukan Komite Penasihat Regulasi Siber

UU ITE mengatur pembentukan Komite Penasihat Regulasi Siber, yang berfungsi untuk memberikan masukan dan rekomendasi terkait kebijakan keamanan siber di Indonesia. Ini merupakan langkah penting dalam menciptakan kerangka kerja yang lebih baik untuk pengelolaan risiko siber.

6. Penambahan Ketentuan Baru

UU No. 1 Tahun 2024 juga menambahkan beberapa ketentuan baru, termasuk perlindungan anak dalam penggunaan sistem elektronik. Penyelenggara sistem elektronik diwajibkan untuk menyediakan mekanisme perlindungan bagi anak-anak yang menggunakan layanan mereka, termasuk informasi tentang batasan usia dan mekanisme pelaporan penyalahgunaan.

7. Perlindungan Data Pribadi

UU ini memberikan perhatian khusus terhadap perlindungan data pribadi pengguna, sejalan dengan tren global dalam menjaga privasi individu di era digital. Hal ini menjadi

semakin penting mengingat meningkatnya jumlah transaksi elektronik dan pertukaran data di ruang siber.

Dengan berbagai fitur menonjol tersebut, UU ITE di Indonesia berupaya untuk menciptakan lingkungan digital yang lebih aman, transparan, dan adil bagi semua pengguna. Revisi undang-undang ini mencerminkan respons pemerintah terhadap tantangan keamanan siber yang terus berkembang serta kebutuhan untuk melindungi hak-hak individu di dunia maya.

**Skema Undang-Undang HKI**

Poin-poin berikut mendefinisikan skema Undang-Undang HKI:

a. Undang-Undang HKI berisi 13 bab dan 90 bagian.
b. Empat bagian terakhir yaitu bagian 91 hingga 94 dalam Undang-Undang HKI Undang-Undang 2000 membahas amandemen terhadap Kitab Undang-Undang Hukum Pidana India 1860, Undang-Undang Bukti India 1872, Undang-Undang Bukti Buku Bankir 1891, dan Undang-Undang Bank Sentral India 1934 dihapus.
c. Dimulai dengan Aspek Pendahuluan di Bab 1, yang membahas tentang singkat, judul, cakupan, dimulainya, dan penerapan Undang-Undang di Bagian 1. Bagian 2 memberikan Definisi.
d. Bab 2 membahas tentang autentikasi catatan elektronik, tanda tangan digital, tanda tangan elektronik, dll.
e. Bab 11 membahas tentang pelanggaran dan hukuman. Serangkaian pelanggaran telah ditetapkan bersama dengan hukuman di bagian Undang-Undang ini.
f. Selanjutnya ketentuan tentang uji tuntas, peran perantara dan beberapa ketentuan lain-lain telah dinyatakan.
g. Undang-Undang ini disematkan dengan dua jadwal. Jadwal Pertama membahas Dokumen atau Transaksi yang tidak akan diterapkan Undang-Undang ini. Jadwal Kedua membahas tanda tangan elektronik atau teknik dan prosedur autentikasi elektronik. Jadwal Ketiga dan Keempat dihilangkan.

Perbandingan antara Undang-Undang Hak Kekayaan Intelektual (HKI) di Indonesia dan negara lain menunjukkan beberapa perbedaan utama yang mencakup aspek hukum, pendaftaran, dan penegakan hukum. Berikut adalah ringkasan perbedaan tersebut:

**1. Sistem Pendaftaran**

- Indonesia: Pendaftaran HKI bersifat sukarela untuk sebagian besar jenis HKI, kecuali untuk paten dan desain industri yang wajib didaftarkan. Perlindungan hanya diberikan kepada karya yang telah didaftarkan.
- Negara Lain (misalnya, Korea Selatan): Pendaftaran HKI bersifat wajib untuk semua jenis HKI. Perlindungan juga dapat diberikan kepada karya yang belum didaftarkan tetapi memenuhi syarat tertentu.

**2. Durasi Perlindungan**

- Indonesia: Hak cipta dilindungi selama hidup pencipta ditambah 70 tahun setelah kematiannya. Untuk paten, perlindungan berlangsung selama 20 tahun.
- Negara Lain (misalnya, Korea Selatan): Durasi perlindungan hak cipta adalah seumur hidup pencipta ditambah 50 tahun setelah kematiannya, yang lebih singkat dibandingkan dengan Indonesia.

**3. Pendekatan Perlindungan**

- Indonesia: Perlindungan HKI lebih berfokus pada pendaftaran formal dan tidak memberikan perlindungan otomatis bagi karya yang belum terdaftar.
- Negara Lain: Beberapa negara memberikan perlindungan otomatis kepada karya yang memenuhi kriteria tertentu tanpa perlu pendaftaran formal, sehingga lebih mendukung inovasi dan kreativitas.

**4. Kelembagaan dan Penegakan Hukum**

- Indonesia: Perlindungan HKI dikelola oleh Direktorat Jenderal Kekayaan Intelektual (Ditjen KI) di bawah Kementerian Hukum dan HAM, tetapi kapasitas penegakan hukum masih dianggap kurang efektif.
- Negara Lain (misalnya, Korea Selatan): Dikelola oleh Badan Hak Kekayaan Intelektual (KIPO) dengan sistem penegakan hukum yang lebih kuat dan efektif, serta dukungan kelembagaan yang lebih baik.

**5. Kesadaran Masyarakat dan Pemanfaatan**

- Indonesia: Kesadaran masyarakat mengenai pentingnya HKI masih rendah, yang mengakibatkan banyak pelanggaran dan kurangnya pemanfaatan HKI sebagai jaminan fidusia dalam pembiayaan.
- Negara Lain: Negara maju umumnya memiliki kesadaran masyarakat yang lebih tinggi tentang pentingnya HKI, serta sistem pembiayaan berbasis HKI yang lebih terstruktur dan efektif.

**6. Pengaturan Internasional**

- Indonesia: Telah meratifikasi berbagai perjanjian internasional seperti TRIPs Agreement, tetapi implementasinya masih menghadapi tantangan dalam hal harmonisasi hukum nasional dengan standar internasional[2][4].
- Negara Lain: Negara-negara maju sering kali memiliki sistem hukum yang lebih terintegrasi dengan standar internasional, memudahkan penegakan dan perlindungan HKI secara global.

Perbedaan-perbedaan ini menunjukkan bahwa meskipun Indonesia telah membuat kemajuan dalam pengaturan HKI, masih ada banyak ruang untuk perbaikan dalam hal pendaftaran, penegakan hukum, dan kesadaran masyarakat dibandingkan dengan negara lain.

**Penerapan Undang-Undang TI**

Penerapan Undang-Undang Teknologi Informasi (TI) di Indonesia melibatkan berbagai aspek, terutama terkait dengan regulasi penggunaan teknologi informasi, perlindungan data pribadi, dan penegakan hukum terhadap kejahatan siber. Berikut adalah beberapa poin penting mengenai penerapannya:

1. **Undang-Undang ITE**: Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan dasar hukum yang mengatur transaksi elektronik, informasi, dan komunikasi di Indonesia. UU ini mencakup ketentuan tentang kejahatan siber, penyebaran informasi, serta hak dan kewajiban pengguna dan penyelenggara sistem elektronik.
2. **Perlindungan Data Pribadi**: Dengan adanya UU Perlindungan Data Pribadi (UU PDP) yang mulai berlaku, terdapat ketentuan yang lebih jelas mengenai pengumpulan,

penggunaan, dan perlindungan data pribadi individu. Ini bertujuan untuk menjaga privasi dan memberikan hak kepada individu atas data mereka.

3. **Penegakan Hukum**: Kementerian Komunikasi dan Informatika (Kominfo) serta aparat penegak hukum seperti kepolisian aktif dalam menanggapi pelanggaran yang terjadi di dunia maya, termasuk penyebaran konten ilegal, penipuan online, dan pelanggaran privasi.
4. **Sosialisasi dan Edukasi**: Pemerintah juga melakukan sosialisasi kepada masyarakat tentang penggunaan internet yang aman, etika berkomunikasi di dunia maya, serta pentingnya menjaga keamanan data pribadi.
5. **Kerja Sama Internasional**: Mengingat sifat kejahatan siber yang lintas negara, Indonesia juga berpartisipasi dalam kerja sama internasional untuk menangani isu-isu terkait TI dan keamanan siber.

Penerapan undang-undang ini masih menghadapi berbagai tantangan, termasuk masalah kesadaran masyarakat, kecepatan teknologi yang berkembang, serta perlunya infrastruktur yang memadai untuk mendukung implementasi regulasi tersebut.

**Amandemen yang Dilakukan dalam Undang-Undang I.T**

Revisi Undang-Undang Informasi dan Transaksi Elektronik (ITE) di Indonesia, yang disahkan pada Desember 2023 dan resmi menjadi Undang-Undang No. 1 Tahun 2024, membawa sejumlah perubahan signifikan dalam kerangka hukum digital di negara ini. Berikut adalah beberapa poin utama mengenai amandemen tersebut:

**Poin Penting Amandemen UU ITE**

1. Perubahan Pasal dan Penambahan Pasal Baru: Sebanyak 14 pasal dari UU ITE yang ada telah diubah, dan tujuh pasal baru ditambahkan. Perubahan ini mencakup pengaturan mengenai, sertifikasi elektronik, transaksi elektronik, serta perlindungan anak sebagai pengguna sistem elektronik.
2. Fokus pada Keamanan dan Perlindungan Data: Amandemen ini bertujuan untuk meningkatkan kepastian hukum dan melindungi hak individu dalam ruang digital. Hal ini termasuk pengaturan terkait identitas digital, keamanan data, serta kewenangan pemerintah dalam mendorong ekosistem digital yang aman dan inovatif.
3. Peningkatan Kewenangan Penegakan Hukum: Amandemen memberikan penegasan mengenai kewenangan penyidik pegawai negeri sipil dalam menindak pelanggaran hukum di dunia maya, serta memperjelas ketentuan pidana untuk tindakan yang dilarang.

**Kontroversi dan Kritik**

Meskipun ada upaya untuk memperbaiki UU ITE, banyak kritik yang muncul terkait dengan keberadaan pasal-pasal karet yang berpotensi disalahgunakan untuk membungkam kebebasan berekspresi. Beberapa pasal yang dipertahankan dari versi sebelumnya, seperti pasal tentang pencemaran nama baik dan ujaran kebencian, dianggap masih bisa digunakan untuk mengkriminalisasi individu yang menyuarakan kritik.

Kekhawatiran Masyarakat Sipil. Koalisi Masyarakat Sipil untuk Advokasi UU ITE menyatakan bahwa revisi ini tidak cukup transparan dan mengabaikan partisipasi publik. Mereka menekankan pentingnya keterlibatan masyarakat dalam proses legislasi agar

peraturan yang dihasilkan benar-benar mencerminkan kebutuhan dan perlindungan hak asasi manusia.

Kesimpulan

Amandemen UU ITE mencerminkan upaya pemerintah Indonesia untuk menyesuaikan regulasi dengan perkembangan teknologi dan kebutuhan masyarakat digital. Namun, tantangan tetap ada dalam memastikan bahwa perubahan tersebut tidak mengorbankan kebebasan sipil dan hak asasi manusia. Dialog berkelanjutan antara pemerintah, masyarakat sipil, dan pemangku kepentingan lainnya akan sangat penting untuk mengawasi implementasi undang-undang baru ini.

**Tanggung Jawab Perantara**

Perantara, yang menangani catatan elektronik tertentu, adalah orang yang atas nama orang lain menerima, menyimpan, atau mengirimkan catatan tersebut atau menyediakan layanan apa pun sehubungan dengan catatan tersebut. Menurut definisi yang disebutkan di atas, hal ini mencakup hal-hal berikut:

a. Penyedia layanan telekomunikasi
b. Penyedia layanan jaringan
c. Penyedia layanan internet
d. Penyedia layanan hosting web
e. Mesin pencari
f. Situs pembayaran daring
g. Situs lelang daring
h. Pasar daring dan warnet

**Hal-hal Penting dari Undang-Undang yang Diubah**

Undang-undang yang baru diubah ini memiliki hal-hal penting berikut:

a. Menekankan masalah privasi dan menyoroti keamanan informasi.
b. Menjelaskan Tanda Tangan Digital.
c. Menjelaskan praktik keamanan rasional untuk perusahaan.
d. Berfokus pada peran Perantara.
e. Wajah-wajah baru Kejahatan Siber telah ditambahkan.

## 1.8 TANDA TANGAN

**Tanda Tangan Digital**

Tanda tangan digital adalah teknik untuk memvalidasi keabsahan pesan digital atau dokumen. Tanda tangan digital yang sah memberikan kepastian kepada penerima bahwa pesan tersebut dibuat oleh pengirim yang dikenal, sehingga pengirim tidak dapat menyangkal telah mengirim pesan tersebut. Tanda tangan digital sebagian besar digunakan untuk distribusi perangkat lunak, transaksi keuangan, dan dalam kasus lain yang berisiko dipalsukan.

**Tanda Tangan Elektronik**

Tanda tangan elektronik atau tanda tangan elektronik, menunjukkan bahwa orang yang menuntut untuk membuat pesan adalah orang yang membuatnya. Tanda tangan dapat didefinisikan sebagai skrip skematis yang terkait dengan seseorang. Tanda tangan pada dokumen merupakan tanda bahwa orang tersebut menerima tujuan yang tercatat dalam dokumen tersebut. Di banyak perusahaan teknik, segel digital juga diperlukan untuk lapisan

otentikasi dan keamanan lainnya. Segel dan tanda tangan digital sama dengan tanda tangan tulisan tangan dan segel bermaterai.

**Tanda Tangan Digital ke Tanda Tangan Elektronik**

Tanda Tangan Digital dan Tanda Tangan Elektronik adalah dua istilah yang sering digunakan dalam konteks hukum dan teknologi informasi, namun keduanya memiliki perbedaan yang signifikan. Berikut adalah penjelasan mengenai keduanya berdasarkan informasi yang tersedia.

Definisi dan Ruang Lingkup

1. Tanda Tangan Elektronik: Istilah ini mencakup semua bentuk tanda tangan yang digunakan dalam transaksi elektronik. Menurut Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, tanda tangan elektronik adalah tanda keaslian yang dilekatkan pada dokumen elektronik yang berfungsi sebagai alat verifikasi dan autentikasi. Tanda tangan elektronik dapat berupa simbol, gambar, atau bahkan teks yang menunjukkan persetujuan seseorang terhadap dokumen.
2. Tanda Tangan Digital: Ini adalah subkategori dari tanda tangan elektronik yang menggunakan teknik kriptografi untuk meningkatkan keamanan dan keaslian. Tanda tangan digital melibatkan penggunaan sertifikat digital yang diterbitkan oleh otoritas sertifikasi untuk memverifikasi identitas penandatangan. Ini memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan tanda tangan elektronik biasa.

**Tabel 1.3 Perbedaan Utama**

| Aspek | Tanda Tangan Elektronik | Tanda Tangan Digital |
|---|---|---|
| **Keamanan** | Keamanan bervariasi; tidak selalu terenkripsi. | Menggunakan kriptografi untuk keamanan tinggi. |
| **Autentikasi** | Metode autentikasi sederhana (misalnya, PIN). | Memerlukan sertifikat digital untuk autentikasi. |
| **Kekuatan Hukum** | Diakui secara hukum, tetapi tidak selalu kuat. | Memiliki kekuatan hukum yang lebih kuat. |
| **Verifikasi Integritas** | Tidak selalu menjamin integritas dokumen. | Menjamin integritas melalui hash unik dokumen. |
| **Penggunaan** | Umum untuk dokumen sehari-hari. | Digunakan untuk dokumen resmi dan sensitif. |

**Metode Autentikasi**

Menurut Komisi Perserikatan Bangsa-Bangsa tentang Hukum Perdagangan Internasional (UNCITRAL), metode autentikasi untuk tanda tangan elektronik dapat diklasifikasikan sebagai berikut:

1. Berdasarkan Pengetahuan Pengguna: Menggunakan kata sandi atau PIN.
2. Berdasarkan Ciri Fisik Pengguna: Menggunakan biometrik seperti sidik jari.
3. Berdasarkan Kepemilikan Objek: Menggunakan kode atau informasi pada kartu magnetik.
4. Metode Lain: Termasuk faksimili tanda tangan tulisan tangan atau nama yang diketik.

**Kesimpulan**

Meskipun Tanda Tangan Digital merupakan bagian dari Tanda Tangan Elektronik, keduanya memiliki fungsi dan aplikasi yang berbeda dalam konteks hukum dan transaksi elektronik. Tanda Tangan Digital menawarkan tingkat keamanan dan keandalan yang lebih tinggi, menjadikannya pilihan yang lebih baik untuk transaksi resmi dan sensitif, sementara Tanda Tangan Elektronik lebih fleksibel dan dapat digunakan dalam berbagai konteks sehari-hari tanpa memerlukan tingkat keamanan yang sama.

Berdasarkan UU MODEL UNCITRAL tentang Tanda Tangan Elektronik, teknologi berikut saat ini digunakan:

a. Tanda Tangan Digital dalam infrastruktur kunci publik (PKI)
b. Perangkat Biometrik
c. PIN
d. Kata Sandi
e. Tanda tangan tulisan tangan yang dipindai
f. Tanda Tangan dengan Pena Digital
g. Kotak klik “OK” atau “Saya Terima” atau “Saya Setuju” yang dapat diklik

## 1.9 PELANGGARAN DAN SANKSI

Konektivitas dunia yang semakin cepat telah memicu banyak kejahatan daring dan meningkatnya pelanggaran ini menyebabkan perlunya undang-undang untuk perlindungan. Agar dapat mengikuti perubahan generasi, Parlemen India mengesahkan Undang-Undang Teknologi Informasi 2000 yang telah dikonseptualisasikan pada Undang-Undang Model Komisi Perserikatan Bangsa-Bangsa tentang Hukum Perdagangan Internasional (UNCITRAL). Undang-undang tersebut mendefinisikan pelanggaran secara terperinci beserta sanksi untuk setiap kategori pelanggaran.

**Pelanggaran**

Pelanggaran siber adalah tindakan tidak sah, yang dilakukan secara berkelas di mana komputer menjadi alat atau target atau keduanya. Kejahatan dunia maya biasanya mencakup hal-hal berikut:

a. Akses komputer yang tidak sah
b. Penipuan data
c. Serangan virus/worm
d. Pencurian sistem komputer
e. Peretasan
f. Penolakan serangan
g. Bom logika
h. Serangan Trojan
i. Pencurian waktu internet
j. Pembajakan web
k. Pengeboman email
l. Serangan Salami
m. Merusak sistem komputer secara fisik.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, yang diundangkan pada tahun 2008, mengatur berbagai pelanggaran yang berkaitan dengan penggunaan teknologi informasi dan internet. Berikut adalah beberapa jenis pelanggaran yang termasuk dalam UU TI tahun 2000:

**Jenis Pelanggaran dalam UU ITE**

1. **Pelanggaran Hak Cipta**
   Penggunaan karya cipta tanpa izin pemegang hak cipta, seperti pembajakan film, musik, dan perangkat lunak. Ini diatur dalam Pasal 30 dan Pasal 48 UU ITE, yang memberikan sanksi pidana bagi pelanggar.
2. **Hacking (Peretasan)**
   Tindakan memasuki sistem komputer atau jaringan tanpa izin dengan tujuan merusak atau mencuri data. Ini diatur dalam Pasal 30.
3. **Intersepsi Ilegal**
   Mengakses komunikasi elektronik tanpa izin, diatur dalam Pasal 31.
4. **Defacing**
   Mengubah tampilan situs web tanpa izin, biasanya dilakukan untuk merusak reputasi atau menyampaikan pesan tertentu. Ini diatur dalam Pasal 32.
5. **Pencurian Identitas**
   Menggunakan identitas orang lain untuk tujuan penipuan atau pencurian, diatur dalam Pasal 35.
6. **Penyebaran Konten Ilegal**
   Termasuk penyebaran pornografi, perjudian, dan fitnah melalui media elektronik, yang diatur dalam Pasal 27 dan Pasal 28.
7. **Cyber Espionage (Spionase Siber)**
   Kegiatan memata-matai dengan cara mengakses sistem jaringan komputer untuk mencuri data atau informasi penting.
8. **Penggunaan Informasi Palsu**
   Menyebarkan informasi yang tidak benar atau menyesatkan, termasuk berita palsu (hoaks), diatur dalam pasal-pasal terkait ujaran kebencian dan penipuan.
9. **Pengiriman Spam**
   Mengirimkan email tidak diinginkan secara massal yang dapat mengganggu pengguna lain.

**Sanksi atas Pelanggaran**

UU ITE menetapkan sanksi pidana bagi pelanggar yang bervariasi tergantung pada jenis pelanggaran, mulai dari denda hingga penjara. Misalnya, untuk pelanggaran hak cipta bisa dikenakan hukuman penjara hingga 7 tahun dan/atau denda hingga Rp 700 juta.

**Kesimpulan**

UU ITE bertujuan untuk melindungi hak-hak individu dan institusi dalam dunia digital serta memberikan kerangka hukum untuk menanggulangi kejahatan siber. Namun, beberapa pasal dalam undang-undang ini juga menuai kritik karena dianggap berpotensi disalahgunakan untuk membatasi kebebasan berekspresi dan akses informasi.

**Contoh**

Salah satu contoh kasus nyata pelanggaran siber di Indonesia adalah peretasan BPJS Kesehatan yang terjadi pada Mei 2021. Dalam insiden ini, situs resmi BPJS Kesehatan diretas, mengakibatkan kebocoran data pribadi sekitar 279 juta penduduk Indonesia. Data yang bocor termasuk Nomor Induk Kependudukan (NIK), nomor ponsel, email, alamat, dan informasi gaji.

Hacker yang dikenal dengan nama akun "Kotz" menjual dataset tersebut di forum online Raid Forums seharga 0,15 Bitcoin, yang setara dengan sekitar Rp 84,4 juta pada saat itu. Kejadian ini menimbulkan kekhawatiran besar mengenai keamanan data pribadi di Indonesia dan mendorong Kementerian Komunikasi dan Informatika (Kominfo) untuk meminta pemutusan akses tautan unduhan data serta memblokir forum tempat data tersebut dijual. Kasus ini mencerminkan tantangan serius yang dihadapi oleh lembaga publik dalam melindungi data sensitif dan pentingnya peningkatan sistem keamanan siber di seluruh sektor.

Kasus kebocoran data BPJS Kesehatan yang terjadi pada Mei 2021 mengungkapkan pentingnya perlindungan data pribadi serta konsekuensi hukum bagi pihak-pihak yang terlibat. BPJS Kesehatan dapat dikenakan sanksi administratif berdasarkan Undang-Undang Perlindungan Data Pribadi (UU PDP) dan UU ITE, yang meliputi peringatan tertulis, penghentian sementara pemrosesan data pribadi, penghapusan atau pemusnahan data yang bocor, serta denda administratif.

Jika terbukti ada kelalaian dalam menjaga keamanan data, lembaga tersebut juga dapat menghadapi tanggung jawab pidana sesuai dengan Pasal 32 UU ITE, yang mengatur pelanggaran kerahasiaan data dengan hukuman penjara hingga 8 tahun dan/atau denda maksimal Rp 2 miliar. Di sisi lain, individu pelaku peretasan yang berhasil mengakses dan menjual data pribadi dapat dikenakan hukuman penjara hingga 12 tahun serta denda yang signifikan, bergantung pada tingkat kerugian yang ditimbulkan. Secara keseluruhan, kasus ini menyoroti kebutuhan akan penegakan hukum yang tegas untuk mencegah kejadian serupa di masa depan dan melindungi hak privasi masyarakat.

## 1.10 RINGKASAN

Hukum Siber adalah satu-satunya penyelamat untuk memerangi kejahatan siber. Hanya melalui hukum yang ketat, keamanan yang tidak dapat ditembus dapat diberikan pada informasi negara. Undang-Undang TI India muncul sebagai undang-undang khusus untuk mengatasi masalah Kejahatan Siber. Undang-Undang tersebut dipertajam oleh Undang-Undang Amandemen tahun 2008. Kejahatan Siber terjadi sesekali, tetapi masih jarang dilaporkan. Oleh karena itu, kasus kejahatan siber yang sampai ke Pengadilan sangat sedikit.

Ada kesulitan praktis dalam mengumpulkan, menyimpan, dan menilai Bukti Digital. Oleh karena itu, Undang-Undang tersebut masih harus menempuh jalan panjang sebelum dapat benar-benar efektif. Dalam tutorial ini, kami telah mencoba membahas semua topik terkini dan utama yang terkait dengan Hukum Siber dan Keamanan TI. Kami ingin mengutip kata-kata dari seorang ahli hukum siber terkemuka dan advokat Mahkamah Agung, Tn. Pavan Duggal untuk menyimpulkan tutorial ini.

Sementara para pembuat undang-undang harus dipuji atas kerja mereka yang mengagumkan dalam menghapus berbagai kekurangan dalam Hukum Siber India dan membuatnya netral secara teknologi, namun tampaknya ada ketidaksesuaian besar antara harapan bangsa dan dampak yang dihasilkan dari undang-undang yang diamandemen. Aspek yang paling aneh dan mengejutkan dari amandemen baru adalah bahwa amandemen ini

berupaya menjadikan hukum siber India sebagai undang-undang yang ramah terhadap kejahatan siber.

Undang-undang yang sangat lunak terhadap penjahat siber, dengan hati yang lembut; undang-undang yang memilih untuk mendorong penjahat siber dengan mengurangi jumlah hukuman yang diberikan kepada mereka berdasarkan hukum yang ada, undang-undang yang menjadikan sebagian besar kejahatan siber yang ditetapkan berdasarkan UU TI sebagai pelanggaran yang dapat dibebaskan dengan jaminan; undang-undang yang kemungkinan akan membuka jalan bagi India untuk menjadi ibu kota kejahatan siber potensial di dunia.

**Tanya Jawab Umum**

**1. Apa itu Kejahatan Dunia Maya?**

Kejahatan dunia maya mengacu pada semua aktivitas yang dilakukan dengan maksud kriminal di dunia maya. Karena sifat internet yang anonim, para penjahat melakukan berbagai aktivitas kriminal. Bidang kejahatan dunia maya baru saja muncul dan bentuk-bentuk baru aktivitas kriminal di dunia maya semakin mengemuka setiap harinya.

**2. Apakah kita memiliki definisi lengkap tentang Kejahatan Dunia Maya?**

Tidak, sayangnya kita tidak memiliki definisi lengkap tentang kejahatan dunia maya. Namun, aktivitas daring apa pun yang pada dasarnya menyinggung perasaan manusia dapat dianggap sebagai kejahatan dunia maya.

**3. Apa saja berbagai kategori Kejahatan Dunia Maya?**

Kejahatan dunia maya pada dasarnya dapat dibagi menjadi tiga kategori utama:

a. Kejahatan dunia maya terhadap orang,
b. Kejahatan dunia maya terhadap properti, dan
c. Kejahatan dunia maya terhadap Pemerintah.

**4. Ceritakan lebih lanjut tentang Kejahatan dunia maya terhadap orang.**

Kejahatan dunia maya yang dilakukan terhadap orang-orang mencakup berbagai kejahatan seperti penyebaran pornografi anak, pelecehan menggunakan email, dan cyberstalking. Memposting dan mendistribusikan materi cabul merupakan salah satu kejahatan dunia maya terpenting yang diketahui saat ini.

**5. Apakah pelecehan dunia maya juga merupakan kejahatan dunia maya?**

Pelecehan dunia maya merupakan kejahatan dunia maya yang berbeda. Berbagai jenis pelecehan memang terjadi di dunia maya. Pelecehan dapat berupa pelecehan seksual, rasial, agama, atau lainnya. Pelecehan dunia maya sebagai kejahatan juga membawa kita ke area terkait lainnya, yaitu pelanggaran privasi warganet. Pelanggaran privasi warga daring merupakan kejahatan dunia maya yang serius.

**6. Apa itu kejahatan dunia maya terhadap properti?**

Kejahatan dunia maya terhadap semua bentuk properti mencakup pelanggaran komputer tanpa izin melalui dunia maya, vandalisme komputer, penyebaran program berbahaya, dan kepemilikan informasi terkomputerisasi tanpa izin.

**7. Apakah peretasan merupakan kejahatan dunia maya?**

Peretasan merupakan salah satu kejahatan dunia maya paling serius yang diketahui hingga saat ini. Sungguh mengerikan mengetahui bahwa orang asing telah membobol sistem komputer Anda tanpa sepengetahuan Anda dan telah merusak data rahasia yang berharga. Kebenaran pahitnya adalah bahwa tidak ada sistem komputer di dunia yang anti-retas. Telah disepakati secara bulat bahwa sistem apa pun, betapa pun amannya kelihatannya, dapat

diretas. Serangan penolakan layanan baru-baru ini yang terlihat di situs komersial populer seperti E-bay, Yahoo, dan Amazon adalah kategori baru Kejahatan Dunia Maya yang perlahan-lahan muncul sebagai kejahatan yang sangat berbahaya. Menggunakan kemampuan pemrograman sendiri untuk mendapatkan akses tidak sah ke komputer atau jaringan adalah kejahatan yang sangat serius. Demikian pula, pembuatan dan penyebaran program komputer berbahaya yang menyebabkan kerusakan yang tidak dapat diperbaiki pada sistem komputer adalah jenis Kejahatan Dunia Maya lainnya.

**8. Apa itu Kejahatan Dunia Maya terhadap Pemerintah?**

Terorisme Dunia Maya adalah salah satu contoh nyata kejahatan dunia maya terhadap pemerintah. Pertumbuhan Internet telah menunjukkan bahwa media dunia maya digunakan oleh individu dan kelompok untuk mengancam pemerintah serta meneror warga negara. Kejahatan ini terwujud dalam bentuk terorisme ketika seseorang meretas situs web yang dikelola pemerintah atau militer.

**9. Apakah ada undang-undang komprehensif tentang Kejahatan Dunia Maya saat ini?**

Saat ini, kita tidak memiliki undang-undang komprehensif tentang kejahatan dunia maya di mana pun di dunia. Inilah alasan mengapa badan investigasi seperti FBI menganggap Dunia Maya sebagai medan yang sangat sulit. Kejahatan dunia maya masuk ke dalam area abu-abu hukum Internet yang tidak sepenuhnya atau sebagian tercakup oleh undang-undang yang ada. Namun, negara-negara mengambil langkah-langkah penting untuk menetapkan undang-undang yang ketat tentang kejahatan dunia maya.

**10. Apakah ada kasus terbaru yang menunjukkan pentingnya memiliki undang-undang dunia maya tentang kejahatan dunia maya dalam yurisdiksi nasional suatu negara?**

Kasus terbaru virus "I love you" menunjukkan perlunya memiliki undang-undang dunia maya tentang kejahatan dunia maya di berbagai yurisdiksi nasional. Pada saat publikasi web fitur ini, Reuters telah melaporkan bahwa "Filipina belum menangkap tersangka pembuat virus komputer 'Love Bug' karena tidak memiliki undang-undang yang menangani kejahatan komputer, kata seorang perwira polisi senior". Faktanya adalah tidak ada undang-undang yang terkait dengan kejahatan dunia maya di Filipina.

**11. Apa itu Vishing?**

Vishing adalah praktik kriminal yang menggunakan pengaruh sosial atas sistem telepon, paling sering menggunakan fitur yang difasilitasi oleh Voice over IP (VoIP), untuk mendapatkan akses ke informasi sensitif seperti detail kartu kredit dari publik. Istilah ini merupakan gabungan dari "Voice" dan phishing.

**12. Apa itu Penipuan Surat?**

Penipuan surat merupakan pelanggaran menurut hukum federal Amerika Serikat, yang mencakup skema apa pun yang berupaya memperoleh uang atau barang berharga secara melawan hukum di mana sistem pos digunakan pada titik mana pun dalam melakukan tindak pidana.

**13. Apa itu ID Spoofing?**

Ini adalah praktik menggunakan jaringan telepon untuk menampilkan nomor pada tampilan Caller ID penerima yang bukan nomor stasiun asal yang sebenarnya.

**14. Apa itu Cyber espionage?**

Ini adalah tindakan atau praktik memperoleh rahasia dari individu, pesaing, rival, kelompok, pemerintah, dan musuh untuk keuntungan militer, politik, atau ekonomi menggunakan metode eksploitasi ilegal di internet.

**15. Apa arti Sabotase?**

Sabotase secara harfiah berarti kerusakan yang disengaja pada mesin atau material apa pun atau gangguan terhadap pekerjaan. Dalam konteks dunia maya, ini adalah ancaman terhadap keberadaan komputer dan satelit yang digunakan oleh aktivitas militer.

**16. Sebutkan negara demokrasi tempat Undang-Undang Pencemaran Nama Baik Dunia Maya pertama kali diperkenalkan.**

Korea Selatan adalah negara demokrasi pertama tempat undang-undang ini pertama kali diperkenalkan.

**17. Apa itu Bot?**

Bot adalah salah satu jenis perangkat lunak kejahatan paling canggih yang dihadapi internet saat ini. Bot mendapatkan nama uniknya dengan melakukan berbagai macam tugas otomatis atas nama penjahat dunia maya. Mereka berperan dalam serangan "denial of service" di internet.

**18. Apa itu Trojan dan Spyware?**

Trojan dan spyware adalah alat yang mungkin digunakan penjahat dunia maya untuk mendapatkan akses tidak sah dan mencuri informasi dari korban sebagai bagian dari serangan.

**19. Apa itu Phishing dan Pharming?**

Phishing dan Pharming adalah cara paling umum untuk melakukan pencurian identitas yang merupakan bentuk kejahatan dunia maya di mana penjahat menggunakan internet untuk mencuri informasi pribadi dari orang lain.

**20. Sebutkan beberapa kiat untuk mencegah kejahatan dunia maya.**

a. Baca cara terbaru peretas membuat penipuan phishing untuk mendapatkan akses ke informasi pribadi Anda.
b. Pasang firewall di komputer Anda untuk meminimalkan ancaman dan serangan yang tidak diinginkan.
c. Berhati-hatilah saat membuka email dan mengklik tautan. Anda harus berhati-hati saat mengunduh konten dari sumber yang tidak terverifikasi.
d. Buat kata sandi yang kuat untuk situs web mana pun tempat informasi pribadi disimpan.

# BAB 2
# KLASIFIKASI KEJAHATAN DUNIA MAYA

## 2.1 TAKSONOMI KEJAHATAN DUNIA MAYA

Dengan pertumbuhan yang sangat pesat di bidang teknologi komunikasi dan kemudahan transaksi di bawahnya, terjadi pertumbuhan dan perkembangan yang pesat di dunia. *World Wide Web* (www) terdengar seperti fenomena yang luas, tetapi yang mengejutkan adalah salah satu kualitasnya adalah ia telah mendekatkan dunia yang juga menjadikannya tempat yang sangat erat untuk ditinggali bagi para penggunanya.

Namun, hal itu juga mengakibatkan terciptanya tantangan besar dalam bentuk Kejahatan Dunia Maya. Kejahatan dunia maya adalah konsep yang rumit untuk didefinisikan dalam bahasa yang sederhana dan awam. Akan tetapi, dapat dikatakan bahwa ketika kejahatan apa pun dilakukan melalui Internet, hal itu dapat disebut sebagai Kejahatan Dunia Maya.

Ada berbagai kejahatan dunia maya yang terjadi di dunia saat ini yang didominasi oleh Teknologi Informasi dan Komunikasi. Bisa jadi peretas merusak situs web Anda, melihat informasi rahasia, mencuri rahasia dagang atau kekayaan intelektual dengan menggunakan internet. Hal itu juga dapat mencakup 'penolakan layanan' dan serangan virus yang mencegah lalu lintas reguler mencapai situs web Anda. Kejahatan dunia maya tidak terbatas pada pihak luar kecuali dalam kasus virus dan berkenaan dengan kejahatan dunia maya yang terkait dengan keamanan yang biasanya dilakukan oleh karyawan perusahaan/organisasi tertentu yang dapat dengan mudah mengakses kata sandi dan penyimpanan data perusahaan untuk tujuan ilegal mereka.

Kejahatan dunia maya juga mencakup kegiatan kriminal yang dilakukan dengan menggunakan komputer yang selanjutnya melanggengkan berbagai kejahatan, misalnya kejahatan keuangan, penjualan barang ilegal, pornografi, perjudian daring, kejahatan kekayaan intelektual, email, spoofing, pemalsuan, pencemaran nama baik dunia maya, cyber stalking, akses tidak sah ke sistem komputer, pencurian informasi yang terdapat dalam formulir elektronik, pemboman email, merusak sistem komputer secara fisik, dll. Meskipun lembaga penegak hukum bekerja untuk menangani masalah ini dan mencoba yang terbaik untuk menangani ancaman ini; Namun, kejahatan ini terus berkembang dengan pesat dan dengan demikian semakin banyak orang yang menjadi korban kejahatan dunia maya seperti peretasan, pencurian, pencurian identitas, dll.

Meskipun ada perlindungan yang diberikan oleh undang-undang terhadap kejahatan dunia maya tersebut, ada juga kebutuhan untuk melindungi informasi sensitif Anda dengan menggunakan keamanan yang tidak dapat ditembus yang menggunakan sistem perangkat lunak dan perangkat keras terpadu untuk mengautentikasi informasi yang dikirim atau diakses melalui Internet. Namun, sebelum seseorang dapat memahami rezim hukum seputar kejahatan dunia maya, seseorang perlu memahami berbagai kejahatan dunia maya yang terjadi di dunia kontemporer ini.

## 2.2 KLASIFIKASI KEJAHATAN DUNIA MAYA

Jumlah Kejahatan Dunia Maya yang dilakukan terus bertambah setiap harinya, dan sangat sulit untuk mengetahui apa yang sebenarnya merupakan kejahatan dunia maya dan apa yang merupakan kejahatan konvensional. Namun, untuk menghadapi tantangan ini, kejahatan dunia maya yang paling umum dapat dikategorikan dan dibahas di bawah judul-judul berikut:

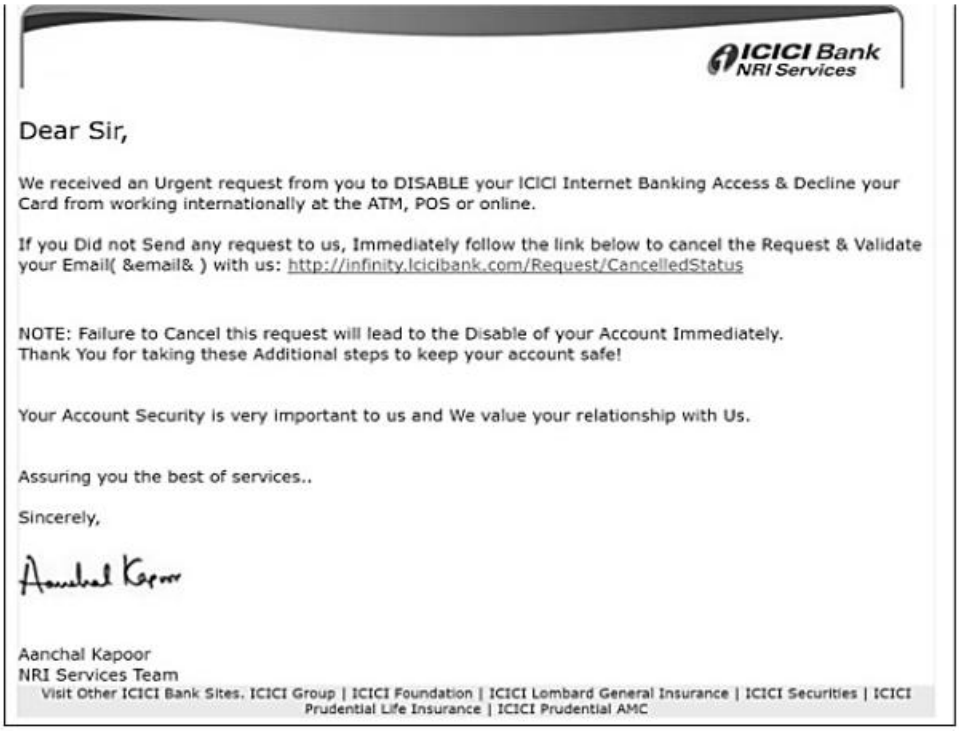
1. Kejahatan Dunia Maya terhadap Orang;
2. Kejahatan Dunia Maya terhadap Properti;
3. Kejahatan Dunia Maya terhadap Pemerintah;
4. Kejahatan Dunia Maya terhadap Masyarakat.

**Kejahatan Dunia Maya terhadap Orang**

Ada beberapa pelanggaran yang memengaruhi kepribadian seseorang dan dapat didefinisikan sebagai:

1) Pelecehan melalui Email: Ini adalah jenis pelecehan yang sangat umum dilakukan melalui surat, lampiran file & folder, yaitu melalui email. Saat ini, pelecehan umum terjadi seiring dengan meningkatnya penggunaan situs jejaring sosial, seperti Facebook.com, Twitter.com, dll.
2) Cyber-Stalking: Artinya, ancaman fisik yang diungkapkan atau tersirat yang menciptakan rasa takut melalui penggunaan teknologi komputer seperti internet, email, telepon, pesan teks, webcam, situs web, atau video.
3) Penyebaran Materi Cabul: Termasuk pemaparan Tidak Senonoh/Pornografi (pada dasarnya pornografi anak), hosting situs web yang berisi materi terlarang ini. Hal-hal cabul ini dapat membahayakan pikiran remaja dan cenderung merusak atau merusak pikiran mereka.
4) Malware: Malware adalah perangkat lunak yang mengendalikan komputer individu mana pun untuk menyebarkan bug ke perangkat orang lain atau profil jejaring sosial. Perangkat lunak tersebut juga dapat digunakan untuk membuat 'botnet'—jaringan komputer yang dikendalikan dari jarak jauh oleh peretas, yang dikenal sebagai 'herders,' untuk menyebarkan spam atau virus.
5) Pencemaran nama baik: Tindakan menuduh seseorang dengan maksud untuk merendahkan martabat orang tersebut dengan cara meretas akun emailnya dan mengirim beberapa email dengan bahasa vulgar ke akun email orang yang tidak dikenal.
6) Peretasan: Ini berarti kontrol/akses yang tidak sah atas sistem komputer dan tindakan peretasan menghancurkan seluruh data serta program komputer. Peretas biasanya meretas jaringan telekomunikasi dan seluler.
7) Peretasan: Ini adalah salah satu kejahatan dunia maya paling serius yang diketahui hingga saat ini. Merupakan perasaan yang mengerikan untuk mengetahui bahwa orang asing telah membobol sistem komputer Anda tanpa sepengetahuan dan persetujuan Anda dan telah merusak data dan informasi rahasia yang berharga.

8) Spoofing Email: Email palsu dapat dikatakan sebagai email yang salah menggambarkan asalnya. Ini menunjukkan asalnya berbeda dari yang sebenarnya.
9) Spoofing SMS: Spoofing adalah pemblokiran melalui spam yang berarti pesan tak diundang yang tidak diinginkan. Di sini pelaku mencuri identitas orang lain dalam bentuk nomor telepon seluler dan mengirim SMS melalui internet dan penerima menerima SMS dari nomor telepon seluler korban. Ini adalah kejahatan dunia maya yang sangat serius terhadap setiap individu.
10) Carding: Ini berarti kartu ATM palsu, yaitu kartu Debit dan Kredit yang digunakan oleh penjahat untuk keuntungan moneter mereka melalui penarikan uang dari rekening bank korban secara tidak jujur. Selalu ada penggunaan kartu ATM yang tidak sah dalam jenis kejahatan dunia maya ini.
11) Kecurangan & Penipuan: Ini berarti orang yang melakukan tindakan kejahatan dunia maya yaitu mencuri kata sandi dan penyimpanan data telah melakukannya dengan niat yang salah yang mengarah pada penipuan dan kecurangan.
12) Pornografi Anak: Ini melibatkan penggunaan jaringan komputer untuk membuat, mendistribusikan, atau mengakses materi yang mengeksploitasi anak di bawah umur secara seksual.
13) Phishing: Phishing hanyalah salah satu dari banyak penipuan di Internet, Phishing mencoba menipu orang agar menyerahkan uang mereka. Phishing mengacu pada penerimaan email yang tidak diminta oleh nasabah lembaga keuangan, yang meminta mereka memasukkan nama pengguna, kata sandi, atau informasi pribadi lainnya untuk mengakses akun mereka karena suatu alasan. Nasabah diarahkan ke replika palsu dari situs web lembaga asli saat mereka mengeklik tautan pada email untuk memasukkan informasi mereka, sehingga mereka tidak menyadari bahwa penipuan telah terjadi. Penipu kemudian memiliki akses ke rekening bank online nasabah dan dana yang ada di rekening tersebut. Pesan penipuan di atas adalah contoh klasik penipuan phishing. Beginilah cara penipu beroperasi. Alamat situs lengkapnya sama kecuali "s" hilang dalam "https" dan huruf kecil "L" digunakan sebagai ganti "i" seperti pada ICICI. Alamat tersebut tampak mirip dengan alamat Web bank ICICI. Anda mungkin menerima pesan serupa dari penipu. Mohon JANGAN klik tautan tersebut.



ICICI Bank
NRI Services

Dear Sir,

We received an Urgent request from you to DISABLE your ICICI Internet Banking Access & Decline your Card from working internationally at the ATM, POS or online.

If you Did not Send any request to us, Immediately follow the link below to cancel the Request & Validate your Email( &email& ) with us: http://infinity.icicibank.com/Request/CancelledStatus

NOTE: Failure to Cancel this request will lead to the Disable of your Account Immediately.
Thank You for taking these Additional steps to keep your account safe!

Your Account Security is very important to us and We value your relationship with Us.

Assuring you the best of services..

Sincerely,

Aanchal Kapoor
NRI Services Team

Visit Other ICICI Bank Sites. ICICI Group | ICICI Foundation | ICICI Lombard General Insurance | ICICI Securities | ICICI Prudential Life Insurance | ICICI Prudential AMC

14) Vishing: Vishing adalah praktik kriminal menggunakan rekayasa sosial dan Voice over IP (VoIP) untuk mendapatkan akses ke Informasi pribadi dan keuangan pribadi dari publik untuk tujuan imbalan finansial. Istilah tersebut merupakan gabungan dari "suara" dan phishing.
15) Jaringan bot: Kejahatan dunia maya yang disebut 'Jaringan Bot', di mana pengirim spam dan pelaku kejahatan dunia maya lainnya mengambil alih kendali komputer dari jarak jauh tanpa disadari pengguna, meningkat pada tingkat yang mengkhawatirkan. Komputer terhubung ke Jaringan Bot ketika pengguna tanpa sadar mengunduh kode berbahaya seperti Trojan horse yang dikirim sebagai lampiran email. Komputer yang terpengaruh tersebut, yang dikenal sebagai zombi, dapat bekerja sama setiap kali kode jahat di dalamnya diaktifkan, dan mereka yang berada di balik serangan Bot Networks mendapatkan kekuatan komputasi dari ribuan sistem yang mereka miliki. Penyerang sering kali mengoordinasikan kelompok besar sistem yang dikendalikan Bot, atau jaringan Boot, untuk memindai sistem yang rentan dan menggunakannya untuk meningkatkan kecepatan dan jangkauan serangan mereka. Jaringan Boot menciptakan masalah unik bagi organisasi karena dapat ditingkatkan dari jarak jauh dengan eksploitasi baru dengan sangat cepat dan ini dapat membantu penyerang mendahului upaya keamanan.
16) Serangan oleh Ancaman: Ini mengacu pada ancaman terhadap seseorang dengan rasa takut akan nyawa mereka atau nyawa keluarga mereka melalui penggunaan jaringan komputer, yaitu, E-mail, video atau telepon.
17) Buffer overflow: Ini adalah cara yang paling umum untuk membobol komputer. Buffer dibuat untuk menampung sejumlah data yang terbatas. Ketika meluap, data tersebut masuk ke buffer yang berdekatan yang dapat menyebabkan data ditimpa. Dalam

serangan buffer overflow, data tambahan dapat berisi instruksi yang memicu tindakan tertentu. Tindakan ini dapat menyebabkan kerusakan pada file dan/atau mengubah data.

**Kejahatan terhadap Hak Milik Orang**

Karena perdagangan internasional berkembang pesat, di mana para pelaku bisnis dan konsumen semakin banyak menggunakan komputer untuk membuat, mengirimkan, dan menyimpan informasi dalam bentuk elektronik, bukan dokumen kertas tradisional. Ada beberapa pelanggaran yang memengaruhi hak milik orang, yaitu sebagai berikut:

a) Kejahatan Hak Kekayaan Intelektual: Hak kekayaan intelektual terdiri dari sekumpulan hak. Setiap tindakan melawan hukum yang menyebabkan pemiliknya kehilangan sebagian atau seluruh haknya merupakan pelanggaran. Bentuk umum pelanggaran HAKI dapat dikatakan sebagai pembajakan perangkat lunak, pelanggaran hak cipta, merek dagang, paten, desain, dan pelanggaran merek layanan, pencurian kode sumber komputer, dll.
b) Pembajakan perangkat lunak: Banyak orang tidak menganggap pembajakan perangkat lunak sebagai pencurian. Mereka tidak akan pernah mencuri satu rupee pun dari seseorang, tetapi tidak akan berpikir dua kali sebelum menggunakan perangkat lunak bajakan. Ada persepsi umum di antara pengguna komputer biasa untuk tidak menganggap perangkat lunak sebagai "properti". Hal ini telah menyebabkan pembajakan perangkat lunak menjadi bisnis yang berkembang pesat. Pembajak perangkat lunak menjual perangkat lunak bajakan dalam media fisik (biasanya CD ROM) melalui jaringan dealer yang dekat. Tersangka menggunakan peralatan duplikasi CD berkecepatan tinggi untuk membuat banyak salinan perangkat lunak bajakan. Perangkat lunak ini dijual melalui jaringan vendor perangkat keras dan perangkat lunak komputer
c) Cyber Squatting: Artinya, dua orang mengklaim Nama Domain yang sama baik dengan mengklaim bahwa mereka telah mendaftarkan nama tersebut terlebih dahulu dengan hak untuk menggunakannya sebelum yang lain atau menggunakan sesuatu yang mirip dengan itu sebelumnya. Misalnya dua nama yang mirip, yaitu www.yahoo.com dan www.yaahoo.com.
d) Cyber Vandalism: Vandalisme berarti dengan sengaja menghancurkan atau merusak properti orang lain. Jadi vandalisme siber berarti menghancurkan atau merusak data ketika layanan jaringan dihentikan atau terganggu. Hal ini dapat mencakup segala jenis kerusakan fisik yang dilakukan pada komputer seseorang. Tindakan ini dapat berupa pencurian komputer, beberapa bagian dari komputer, atau periferal yang terpasang pada komputer.
e) Peretasan Sistem Komputer: Hacktivisme menyerang mereka yang termasuk Twitter Terkenal, platform blog dengan akses/kontrol tidak sah atas komputer. Karena aktivitas peretasan akan ada kehilangan data serta komputer. Juga penelitian khususnya menunjukkan bahwa serangan tersebut tidak terutama ditujukan untuk

keuntungan finansial juga untuk menurunkan reputasi orang atau perusahaan tertentu. Peretas adalah pengguna yang tidak sah yang mencoba atau memperoleh akses ke suatu sistem informasi. Peretasan adalah kejahatan meskipun tidak ada kerusakan yang terlihat pada sistem, karena merupakan pelanggaran privasi data. Ada beberapa kelas Peretas.

- Peretas Topi Putih - Mereka percaya bahwa berbagi informasi adalah hal yang baik, dan bahwa merupakan tugas mereka untuk berbagi keahlian mereka dengan memfasilitasi akses ke informasi. Namun, ada beberapa peretas topi putih yang hanya "bersenang-senang" di sistem komputer.
- Peretas Topi Hitam - Mereka menyebabkan kerusakan setelah intrusi. Mereka dapat mencuri atau mengubah data atau memasukkan virus atau worm yang merusak sistem. Mereka juga disebut 'cracker'.
- Peretas Topi Abu-abu - Biasanya etis tetapi terkadang melanggar etika peretas Peretas akan meretas jaringan, komputer mandiri, dan perangkat lunak. Peretas jaringan mencoba mendapatkan akses tidak sah ke jaringan komputer pribadi hanya untuk tantangan, rasa ingin tahu, dan distribusi informasi. Cracker melakukan intrusi tidak sah dengan kerusakan seperti mencuri atau mengubah informasi atau memasukkan malware (virus atau worm) atau komputer korban.

f) Menularkan Virus: Virus adalah program yang menempel pada komputer atau file dan kemudian mengedarkan diri ke file lain dan ke komputer lain di jaringan. Mereka biasanya memengaruhi data di komputer, baik dengan mengubah atau menghapusnya. Serangan worm memainkan peran utama dalam memengaruhi sistem komputerisasi individu.

g) Packet Sniffing: Ini digunakan oleh peretas dan ahli forensik. Data bergerak dalam bentuk paket dan ukurannya bervariasi tergantung pada lebar pita jaringan dan jumlah data. Peretas menyadap transmisi antara komputer A dan B. Yang dibutuhkan peretas hanyalah alamat IP dari salah satu komputer dan data apa pun dapat dicuri. Data tidak dicuri karena sniffer tidak melakukan itu. Sebaliknya, mereka menyalin hex dan menerjemahkannya menjadi data asli. Inilah sebabnya mengapa firewall sulit mendeteksinya karena mereka hanya menyediakan keamanan tingkat aplikasi.

h) Cyber Trespass: Artinya, mengakses komputer seseorang tanpa izin yang sah dari pemiliknya dan tidak mengganggu, mengubah, menyalahgunakan, atau merusak data atau sistem dengan menggunakan koneksi internet nirkabel.

i) Salami Attack: Serangan tersebut digunakan untuk melakukan kejahatan keuangan. Kuncinya di sini adalah membuat perubahan tersebut tidak signifikan sehingga dalam satu kasus tidak akan terlihat sama sekali. Misalnya, seorang karyawan bank memasukkan program ke server bank, yang memotong sejumlah kecil uang dari rekening setiap nasabah.

j) Internet Time Thefts: Pada dasarnya, pencurian waktu internet termasuk dalam peretasan. Ini adalah penggunaan oleh orang yang tidak berwenang atas jam-jam Internet yang dibayar oleh orang lain. Orang yang memperoleh akses ke ID pengguna

dan kata sandi ISP orang lain, baik dengan meretas atau dengan memperoleh akses ke sana dengan cara ilegal, menggunakannya untuk mengakses Internet tanpa sepengetahuan orang lain. Anda dapat mengidentifikasi pencurian waktu jika waktu Internet Anda harus sering diisi ulang, meskipun jarang digunakan.

k) Trojan dan Rats: Trojan horse adalah program yang tampaknya melakukan apa yang diinginkan pengguna sementara mereka sebenarnya melakukan sesuatu yang lain seperti menghapus file atau memformat disk. Yang dilihat pengguna hanyalah antarmuka program yang ingin dijalankannya. RAT adalah Trojan akses jarak jauh yang menyediakan pintu belakang ke dalam sistem tempat peretas dapat mengintip ke dalam sistem Anda dan menjalankan kode berbahaya.

l) Penipuan Data: Penipuan data melibatkan perubahan data sebelum atau selama input ke komputer. Dengan kata lain, informasi diubah dari cara yang seharusnya dimasukkan oleh seseorang yang mengetik data, virus yang mengubah data, programmer basis data atau aplikasi, atau siapa pun yang terlibat dalam proses penyimpanan informasi dalam berkas komputer. Pelakunya bisa siapa saja yang terlibat dalam proses pembuatan, perekaman, pengkodean, pemeriksaan, pengecekan, konversi, atau pengiriman data. Ini adalah salah satu metode paling sederhana untuk melakukan kejahatan yang berhubungan dengan komputer, karena hampir tidak memerlukan keterampilan komputer sama sekali. Meskipun mudah dilakukan, biayanya bisa sangat besar.

m) Peretasan akun email: Email semakin banyak digunakan untuk interaksi sosial, komunikasi bisnis, dan transaksi daring. Sebagian besar pemegang akun email tidak mengambil tindakan pencegahan dasar untuk melindungi kata sandi akun email mereka. Kasus pencurian kata sandi email dan penyalahgunaan akun email selanjutnya menjadi sangat umum. Kata sandi akun email korban dicuri dan akun tersebut kemudian disalahgunakan untuk mengirimkan kode berbahaya (virus, worm, Trojan, dsb.) kepada orang-orang yang ada di buku alamat korban. Penerima virus ini percaya bahwa email tersebut berasal dari orang yang dikenal dan menjalankan lampirannya. Hal ini menginfeksi komputer mereka dengan kode berbahaya tersebut. Tersangka akan memasang keylogger di komputer umum (seperti warnet, lounge bandara, dsb.)

**Kejahatan Siber terhadap Pemerintah**

Terdapat beberapa tindak pidana yang dilakukan oleh sekelompok orang yang bermaksud mengancam pemerintah internasional dengan menggunakan fasilitas internet. Tindak pidana ini meliputi:

1) Terorisme Siber: Terorisme siber merupakan isu yang sedang hangat dibicarakan baik di dalam negeri maupun di dunia. Bentuk umum serangan teroris di internet adalah serangan penolakan layanan terdistribusi, situs web dan email kebencian, serangan terhadap jaringan komputer yang sensitif, dll. Aktivitas terorisme siber membahayakan kedaulatan dan integritas bangsa.

2) Perusakan web: Perusakan situs web biasanya berupa penggantian beranda asli situs web dengan halaman lain (biasanya bersifat pornografi atau pencemaran nama baik) oleh peretas.
3) Situs keagamaan dan pemerintah secara teratur menjadi sasaran peretas untuk menampilkan keyakinan politik atau agama. Dalam skenario ini, beranda situs web diganti dengan halaman pornografi atau pencemaran nama baik. Dalam kasus situs web pemerintah, hal ini paling sering dilakukan pada hari-hari simbolis (misalnya, Hari Kemerdekaan negara tersebut). Peretas dapat mengeksploitasi kerentanan sistem operasi atau aplikasi yang digunakan untuk menghosting situs web. Ini akan memungkinkannya untuk meretas server web dan mengubah beranda dan halaman lainnya. Atau, ia dapat meluncurkan serangan brute force atau dictionary untuk mendapatkan kata sandi administrator situs web. Ia kemudian dapat terhubung ke server web dan mengubah Halaman Web.
4) Perang Siber: Ini mengacu pada peretasan bermotif politik untuk melakukan sabotase dan spionase. Ini adalah bentuk perang informasi yang terkadang dianggap analog dengan perang konvensional meskipun analogi ini kontroversial karena akurasinya dan motivasi politiknya.
5) Penggunaan Internet dan Komputer oleh Teroris: Banyak teroris menggunakan media penyimpanan virtual maupun fisik untuk menyembunyikan informasi dan catatan bisnis terlarang mereka. Mereka juga menggunakan email dan ruang obrolan untuk berkomunikasi dengan rekan-rekan mereka di seluruh dunia. Tersangka membawa laptop tempat informasi yang berkaitan dengan aktivitas mereka disimpan dalam bentuk terenkripsi dan dilindungi kata sandi. Mereka juga membuat akun email menggunakan detail fiktif. Dalam banyak kasus, satu akun email digunakan bersama oleh banyak orang. Misalnya, seorang teroris menulis email dan menyimpannya di folder draft. Teroris lain masuk ke akun yang sama dari kota/negara lain dan membaca email yang disimpan. Ia kemudian menulis balasan dan menyimpannya di folder draft. Email tersebut sebenarnya tidak terkirim. Hal ini membuat pelacakan dan penelusuran email menjadi hampir mustahil. Untuk melakukan kejahatan ini, para teroris membeli perangkat penyimpanan kecil dengan kapasitas penyimpanan data yang besar. Mereka juga membeli dan menggunakan perangkat lunak enkripsi. Para teroris juga dapat menggunakan akun gratis atau berbayar dengan penyedia penyimpanan daring.
6) Distribusi perangkat lunak bajakan: Ini berarti mendistribusikan perangkat lunak bajakan dari satu komputer ke komputer lain dengan tujuan untuk menghancurkan data dan catatan resmi pemerintah.
7) Kepemilikan Informasi yang Tidak Sah: Sangat mudah bagi para teroris untuk mengakses informasi apa pun dengan bantuan internet dan memiliki informasi tersebut untuk tujuan politik, agama, sosial, dan ideologis.

**Kejahatan Dunia Maya terhadap Masyarakat Secara Luas**

Tindakan melawan hukum yang dilakukan dengan maksud untuk menimbulkan kerugian di dunia maya akan berdampak pada banyak orang. Tindak pidana ini meliputi:

a) Pornografi Anak: Melibatkan penggunaan jaringan komputer untuk membuat, mendistribusikan, atau mengakses materi yang mengeksploitasi anak di bawah umur secara seksual. Tindak pidana ini juga mencakup kegiatan yang berkaitan dengan pemaparan tidak senonoh dan kecabulan.
b) Perdagangan Dunia Maya: Bisa jadi perdagangan narkoba, manusia, senjata, dll. yang berdampak pada banyak orang. Perdagangan di dunia maya juga merupakan kejahatan yang paling serius.
c) Perjudian Daring: Penipuan dan kecurangan daring merupakan salah satu bisnis paling menguntungkan yang berkembang pesat di dunia maya saat ini. Ada banyak kasus yang terungkap, yaitu yang berkaitan dengan kejahatan kartu kredit, kejahatan kontrak, penawaran pekerjaan, dll.
d) Kejahatan Keuangan: Jenis tindak pidana ini umum terjadi karena ada pertumbuhan pesat dalam pengguna situs jejaring dan jaringan telepon di mana pelaku akan mencoba menyerang dengan mengirimkan surat atau pesan palsu melalui internet. Misalnya: Menggunakan kartu kredit dengan memperoleh kata sandi secara ilegal.
e) Pemalsuan: Berarti menipu banyak orang dengan mengirimkan surat yang mengancam karena transaksi bisnis daring menjadi kebutuhan kebiasaan gaya hidup masa kini.

## 2.3 PENYEBAB KEJAHATAN DUNIA MAYA

a. Kejahatan Dunia Maya Bermotif Ekonomi: Seperti halnya banyak kejahatan yang dilakukan di luar Internet, uang merupakan motivator utama bagi banyak penjahat dunia maya. Terutama karena bahaya kriminalitas kurang terlihat ketika Anda bersembunyi di balik jaringan, persepsi risiko rendah dan imbalan finansial yang sangat tinggi mendorong banyak penjahat dunia maya untuk terlibat dalam malware, phishing, pencurian identitas, dan serangan permintaan uang palsu. Business week memperkirakan bahwa kejahatan dunia maya yang menargetkan rekening perbankan daring saja, misalnya, menghasilkan hampir 700 juta dolar per tahun secara global.
b. Kejahatan Dunia Maya Bermotif Ideologi: Setelah perusahaan keuangan seperti Visa, MasterCard, dan PayPal menolak mengizinkan pemegang akun dan kartu memberikan sumbangan kepada WikiLeaks nirlaba yang kontroversial, kelompok "hacktivist" Anonymous mengoordinasikan serangkaian serangan bot pada server perusahaan, sehingga tidak dapat diakses oleh pengguna Internet. Jenis serangan ini dilakukan karena alasan etika, ideologi, atau moral yang dianggap merusak atau melumpuhkan peralatan dan jaringan komputer untuk menyampaikan keluhan terhadap individu, perusahaan, organisasi, atau bahkan pemerintah nasional.
c. Penyebab Struktural: Di luar penyebab yang memotivasi pelaku kejahatan, lingkungan tempat kejahatan siber dilakukan juga menjadi alasan maraknya fenomena tersebut. Meskipun semakin banyak informasi pribadi dan sensitif yang disimpan secara daring yang meningkatkan potensi keuntungan bagi pelaku kejahatan siber -- baik keamanan komputer maupun aplikasi seperti filter email tidak mengalami peningkatan yang signifikan dalam hal perlindungan. Misalnya, menurut produsen anti-virus Norton,

sebanyak 41 persen komputer tidak memiliki perlindungan keamanan terkini pada tahun 2012.

d. Kejahatan Siber yang Bermotif Pribadi: Pelaku kejahatan siber tetaplah manusia dan apa yang mereka lakukan, termasuk kejahatan mereka, sering kali merupakan penyebab emosi dan dendam pribadi. Mulai dari karyawan yang tidak puas yang memasang virus di komputer kantor hingga pacar yang cemburu yang meretas akun media sosial pacarnya atau remaja yang menutup situs web sekolah hanya untuk membuktikan bahwa ia mampu melakukannya, banyak kejahatan siber pada dasarnya adalah kejahatan yang dilakukan karena nafsu melalui Internet. Namun, banyak dari kejahatan ini masih dapat menimbulkan dampak yang sangat serius dan menyebabkan kerusakan properti yang cukup besar.

## 2.4 DAMPAK DAN EFEK KEJAHATAN DUNIA MAYA

Dampak dari satu serangan dunia maya yang berhasil dapat memiliki implikasi yang luas termasuk kerugian finansial, pencurian kekayaan intelektual, dan hilangnya kepercayaan dan keyakinan konsumen. Dampak moneter keseluruhan dari kejahatan dunia maya terhadap masyarakat dan pemerintah diperkirakan mencapai miliaran dolar per tahun. Kejahatan Dunia Maya selalu memengaruhi perusahaan dalam skala apa pun karena hampir semua perusahaan memperoleh kehadiran daring dan memanfaatkan kemajuan pesat dalam teknologi tetapi perhatian yang lebih besar harus diberikan pada risiko keamanannya. Dalam dunia dunia maya modern, kejahatan dunia maya merupakan masalah utama yang memengaruhi individu maupun masyarakat luas juga.

1) Hilangnya Pendapatan: Salah satu dampak utama kejahatan dunia maya terhadap perusahaan adalah hilangnya pendapatan. Kerugian ini dapat disebabkan oleh pihak luar yang memperoleh informasi keuangan sensitif, menggunakannya untuk menarik dana dari suatu organisasi. Hal ini juga dapat terjadi ketika situs e-commerce bisnis menjadi terganggu saat tidak dapat beroperasi, pendapatan yang berharga hilang ketika konsumen tidak dapat menggunakan situs tersebut.
2) Dampak Ekonomi Potensial: Karena konsumen saat ini semakin bergantung pada komputer, jaringan, dan informasi yang digunakan untuk menyimpan dan memeliharanya, risiko menjadi sasaran kejahatan dunia maya menjadi tinggi. Beberapa survei yang dilakukan di masa lalu menunjukkan sebanyak 80% perusahaan yang disurvei mengakui kerugian finansial akibat pelanggaran komputer. Karena ekonomi semakin bergantung pada internet, ekonomi pun terpapar pada semua ancaman yang ditimbulkan oleh penjahat dunia maya. Saham diperdagangkan melalui internet, transaksi bank dilakukan melalui internet, pembelian dilakukan menggunakan kartu kredit melalui internet. Semua contoh penipuan dalam transaksi tersebut berdampak pada kondisi keuangan perusahaan yang terdampak dan dengan demikian berdampak pada ekonomi.
3) Waktu yang Terbuang: Dampak atau konsekuensi utama lain dari kejahatan dunia maya adalah waktu yang terbuang ketika personel TI harus mencurahkan sebagian

besar waktu mereka untuk menangani kejadian tersebut. Alih-alih mengerjakan tindakan yang produktif untuk suatu organisasi, banyak anggota staf TI menghabiskan sebagian besar waktu mereka untuk menangani pelanggaran keamanan dan masalah lain yang terkait dengan kejahatan dunia maya.

4) Reputasi yang Rusak: Dalam kasus di mana catatan pelanggan dikompromikan oleh pelanggaran keamanan yang terkait dengan kejahatan dunia maya, reputasi perusahaan dapat mengalami pukulan besar. Pelanggan yang kartu kredit atau data keuangan lainnya dicegat oleh peretas atau penyusup lainnya kehilangan kepercayaan pada suatu organisasi dan sering kali mulai membawa bisnis mereka ke tempat lain. Dampak dari reputasi yang rusak dapat dipahami dengan jelas melalui contoh peretasan server Walmart yang menyebabkan hilangnya reputasi yang sangat besar bagi salah satu pengecer terbesar di AS dan Eropa.

**Studi Kasus Walmart**

Pada tahun 2006, WALMART menjadi korban pelanggaran keamanan serius di mana peretas menargetkan tim pengembangan yang bertanggung jawab atas sistem titik penjualan rantai tersebut dan menyedot kode sumber dan data sensitif lainnya ke server perusahaan di Eropa7.


KIM ZETTER SECURITY 10.13.09 7:00 AM

BIG-BOX BREACH: THE INSIDE STORY OF WAL-MART'S HACKER ATTACK

*Reproduced from Big Box Breach*

Wal-Mart memiliki sejumlah kerentanan keamanan pada saat serangan itu terjadi, menurut penilaian keamanan internal yang dilihat dan diakui sebagai asli oleh Wal-Mart. Misalnya, setidaknya data pembelian pelanggan selama empat tahun, termasuk nama, nomor kartu, dan tanggal kedaluwarsa, disimpan di jaringan perusahaan dalam bentuk yang tidak terenkripsi. Wal-Mart mengatakan bahwa pihaknya sedang dalam proses meningkatkan keamanan data transaksinya secara drastis, dan pada tahun 2006 mulai mengenkripsi nomor kartu kredit dan informasi pelanggan lainnya, dan membuat perubahan keamanan penting lainnya.

Wal-Mart benar-benar melakukan segala upaya untuk memisahkan data, membuat jaringan terpisah, mengenkripsinya sepenuhnya dari awal hingga akhir melalui transmisi, dan tidak hanya di satu area tetapi di berbagai penggunaan sistem kartu kredit. Penyelidik menemukan bahwa alat tersebut telah dipasang dari jarak jauh oleh seseorang yang menggunakan akun administrator jaringan generik.


Penyusup tersebut telah mencapai mesin tersebut melalui akun VPN yang diberikan kepada mantan pekerja Wal-Mart di Kanada, yang gagal ditutup oleh administrator setelah pekerja tersebut meninggalkan perusahaan. Pada hari server tersebut mogok, penyusup tersebut telah terhubung ke jaringan Wal-Mart selama sekitar tujuh jam, yang berasal dari alamat IP di Minsk, dokumen tersebut menunjukkan.

Ketertarikan penyusup terhadap sistem titik penjualan Wal-Mart konsisten dengan pelanggaran data besar yang terjadi di perusahaan lain sekitar waktu yang sama. Hal ini telah mengguncang kepercayaan konsumen dalam melakukan transaksi di Walmart dan selanjutnya telah mengurangi bisnis Walmart juga.

**Produktivitas yang Berkurang**

Karena berbagai tindakan yang harus diterapkan oleh banyak perusahaan untuk melawan kejahatan dunia maya, sering kali ada dampak negatif pada produktivitas karyawan. Hal ini karena, karena berbagai tindakan keamanan, karyawan harus memasukkan lebih banyak kata sandi dan melakukan tindakan lain yang memakan waktu untuk melakukan pekerjaan mereka. Setiap detik yang terbuang untuk melakukan tugas ini adalah detik yang tidak terpakai untuk bekerja secara produktif.

**Dampak pada kepercayaan konsumen**

Karena penyerang siber menyusup ke ruang orang lain dan mencoba merusak logika halaman, pelanggan akhir yang mengunjungi halaman terkait akan frustrasi dan enggan menggunakan situs tersebut dalam jangka panjang. Situs yang dimaksud disebut sebagai situs penipuan, sedangkan dalang kriminal yang mendalangi serangan tersembunyi tidak diakui sebagai akar penyebabnya. Hal ini membuat pelanggan kehilangan kepercayaan pada situs tersebut dan pada internet serta kekuatannya.

## 2.5 KEJAHATAN SIBER: BEBERAPA KEJADIAN BERSEJARAH

**1. Situs Web Resmi Pemerintah Maharashtra Diretas**

Pada bulan September 2007 di Mumbai, situs web resmi pemerintah Maharashtra diretas. Polisi Cabang Kejahatan Siber aktif menyelidiki masalah tersebut dan melacak para peretas. Selama sehari, situs web, *http://www.maharashtragovernment.in*, tetap diblokir.

Situs web pemerintah negara bagian tersebut berisi informasi terperinci tentang departemen pemerintah, surat edaran, laporan, dan beberapa topik lainnya. Pakar TI yang

bekerja untuk memulihkan situs web tersebut mengatakan bahwa mereka khawatir para peretas mungkin telah menghancurkan semua konten situs web tersebut. Menurut sumber, para peretas tersebut mungkin berasal dari Washington. Pakar TI mengatakan bahwa para peretas tersebut telah mengidentifikasi diri mereka sebagai "Peretas Al-Jazeera yang Keren" dan mengklaim bahwa mereka bermarkas di Arab Saudi. Mereka menambahkan bahwa ini mungkin merupakan upaya untuk mengecoh para penyelidik. Situs web resmi tersebut telah beberapa kali terkena virus di masa lalu, tetapi tidak pernah diretas. Pejabat tersebut menambahkan bahwa situs web tersebut tidak memiliki firewall.

**2. Situs Web Resmi IRCTC Diretas**

Kejadian kejahatan dunia maya lainnya dilaporkan ketika situs web resmi IRCTC diretas dan sekitar 1 crore detail pelanggan terancam8.


*Reproduced from Daily Bhaskar*

**3. Situs Web CBI Diretas**

Dalam sebuah kejadian, dilaporkan pada tahun 2013 bahwa situs web resmi CBI diretas selama beberapa jam9.


*Reproduced from Rediff News*

**4. Kasus Penipuan Bank ICICI - Pune**

Tiga orang dinyatakan bersalah dalam penipuan kartu kredit daring. Rincian kartu kredit nasabah disalahgunakan melalui sarana daring untuk memesan tiket pesawat. Para

pelaku ini tertangkap oleh Sel Investigasi Kejahatan Siber kota di Pune. Ditemukan bahwa rincian yang disalahgunakan adalah milik 100 orang. Bapak Parvesh Chauhan, pejabat Asuransi Jiwa Prudential ICICI telah mengajukan pengaduan atas nama salah seorang nasabahnya. Terkait hal ini Bapak Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale, dan Ahmead Sikandar Shaikh ditangkap. Lukkad bekerja di sebuah lembaga swasta, sedangkan Kale adalah temannya. Sheikh bekerja di salah satu cabang State Bank of India.

Menurut informasi yang diberikan oleh pihak berwenang, salah seorang nasabah menerima peringatan melalui SMS untuk pembelian tiket meskipun kartu kreditnya sedang dipegangnya. Nasabah waspada dan menyadari ada yang mencurigakan; ia bertanya dan mengetahui tentang penyalahgunaan tersebut. Ia menghubungi Bank terkait hal ini. Polisi mengamati keterlibatan banyak Bank dalam referensi ini. Tiket dipesan melalui sarana daring. Polisi meminta rincian log dan memperoleh informasi dari Lembaga Swasta. Penyelidikan mengungkapkan bahwa rincian tersebut diperoleh dari State Bank of India. Sheikh bekerja di departemen kartu kredit; karena ini ia memiliki akses ke rincian kartu kredit beberapa nasabah.

Dia memberikan informasi itu kepada Kale. Kale sebagai balasannya memberikan informasi ini kepada temannya Lukkad. Dengan menggunakan informasi yang diperoleh dari Kale, Lukkad memesan tiket. Dia biasa menjual tiket ini kepada pelanggan dan mendapatkan uang untuk itu. Dia telah memberikan beberapa tiket ke berbagai lembaga lainnya.

Cyber Cell terlibat dalam penyelidikan selama delapan hari dan akhirnya menangkap para pelakunya. Dalam hal ini berbagai Bank telah dihubungi; juga empat industri penerbangan dihubungi dan diberi tahu.

**5. Penipuan Pusat Panggilan Citibank Mphasis Pune**

Ini adalah kasus rekayasa sumber daya. Rp.35.000,000 dari rekening bank Kota milik empat pelanggan AS secara tidak jujur ditransfer ke rekening palsu di Pune, melalui internet. Beberapa karyawan pusat panggilan mendapatkan kepercayaan dari pelanggan AS dan memperoleh nomor PIN mereka dengan kedok membantu pelanggan keluar dari situasi sulit. Kemudian mereka menggunakan nomor-nomor ini untuk melakukan penipuan. Keamanan tertinggi berlaku di pusat panggilan di India karena mereka tahu bahwa mereka akan kehilangan bisnis mereka. Karyawan pusat panggilan diperiksa saat mereka masuk dan keluar sehingga mereka tidak dapat menyalin nomor dan karena itu mereka tidak dapat mencatatnya. Mereka pasti mengingat nomor-nomor ini, segera pergi ke kafe internet dan mengakses rekening Citibank milik nasabah. Semua rekening dibuka di Pune dan nasabah mengeluh bahwa uang dari rekening mereka ditransfer ke rekening Pune dan begitulah cara para penjahat dilacak. Polisi telah dapat membuktikan kejujuran pusat panggilan dan telah membekukan rekening tempat uang ditransfer.

**6. Kasus Serangan Parlemen**

Biro Penelitian dan Pengembangan Kepolisian di Hyderabad telah menangani beberapa kasus dunia maya teratas, termasuk menganalisis dan mengambil informasi dari laptop yang diambil dari sitaan milik dua teroris, yang ditembak mati ketika Parlemen dikepung pada 13 Desember 2001, dikirim ke Divisi Forensik Komputer BPRD. Laptop tersebut

berisi beberapa bukti yang mengonfirmasi motif kedua teroris tersebut, yaitu stiker Kementerian Dalam Negeri yang mereka buat di laptop dan ditempel di mobil duta besar mereka untuk memasuki Gedung Parlemen dan kartu identitas palsu yang dibawa salah satu dari kedua teroris tersebut dengan lambang dan stempel Pemerintah India. Lambang (tiga singa) tersebut dipindai dengan cermat dan stempel tersebut juga dibuat dengan licik beserta alamat tempat tinggal Jammu dan Kashmir. Namun, deteksi yang cermat membuktikan bahwa semua itu dipalsukan dan dibuat di laptop tersebut.

**7. Kasus Pajak Andhra Pradesh**

Pemilik perusahaan plastik di Andhra Pradesh ditangkap dan uang tunai sebesar Rs. 22 crore disita dari rumahnya oleh Departemen Pengawasan. Mereka meminta penjelasan darinya mengenai uang tunai yang tidak tercatat. Terdakwa menyerahkan 6.000 voucher untuk membuktikan keabsahan perdagangan, tetapi setelah pemeriksaan saksama terhadap voucher dan isi komputernya, terungkap bahwa semuanya dibuat setelah penggerebekan dilakukan. Terungkap bahwa terdakwa menjalankan lima bisnis dengan kedok satu perusahaan dan menggunakan voucher palsu dan terkomputerisasi untuk menunjukkan catatan penjualan dan menghemat pajak. Dengan demikian, taktik meragukan pengusaha terkemuka dari Andhra Pradesh terungkap setelah pejabat departemen tersebut memperoleh komputer yang digunakan oleh terdakwa.

**8. Gambar-gambar Menghina Prajurit Shivaji di Google - Orkut**

Seorang India memposting 'gambar-gambar menghina' prajurit-santo Shivaji yang dihormati di Google Orkut. Polisi India datang mengetuk pintu Google dan meminta alamat IP (IP mengidentifikasi setiap komputer di dunia secara unik) yang menjadi sumber citra negatif ini. Google, India menyerahkan alamat IP tersebut.

Insiden semacam itu di India tidak akan lengkap tanpa beberapa kesalahan administratif. Komputer dengan alamat IP tersebut menggunakan Airtel, India sebagai ISP untuk terhubung ke internet dan Orkut. Airtel memberikan nama orang yang tidak bersalah kepada polisi menggunakan alamat IP yang berbeda. Bagaimana dua alamat IP dapat tercampur dalam kasus polisi yang sensitif adalah dugaan siapa pun.

Seorang warga negara India yang tidak bersalah, Lakshmana Kailash K, ditangkap di Bangalore dan dijebloskan ke penjara selama 3 minggu. Akhirnya, ketidakbersalahannya terbukti dan ia dibebaskan pada bulan Oktober 2007.

Sejumlah media berita melaporkan insiden ini. Warga negara Amerika dan pecinta India Christopher Soghoian (halaman beranda *http://www.dubfire.net/chris/*) mempelajari Informatika di Universitas Indiana dan meneliti/menulis tentang keamanan, privasi, dan kejahatan komputer. Christopher membuat artikel yang bagus tentang topik ini untuk blog di grup media teknologi ternama CNET. Seperti semua penulis hebat lainnya, Christopher Soghoian memberikan daftar pertanyaan kepada Google, India agar ia dapat memberikan perspektif yang seimbang kepada jutaan pembaca CNET.

**9. Penipuan Kartu ATM Pertama di India**

Kepolisian Kota Chennai menangkap geng internasional yang terlibat dalam kejahatan dunia maya, dengan penangkapan Deepak Prem Manwani (22), yang tertangkap basah saat membobol ATM di kota itu pada bulan Juni lalu, seperti yang diketahui secara pasti. Dimensi pencapaian polisi kota dapat diukur dari fakta bahwa mereka telah menjaring seorang pria yang masuk dalam daftar buronan FBI Amerika Serikat yang tangguh.

Pada saat penahanannya, ia membawa serta uang senilai Rs 7,5 lakh (Rp. 150.000.000 ) yang diambil dari dua ATM di T Nagar dan Abiramipuram di kota itu. Sebelumnya, ia telah membawa kabur uang sebesar Rs 50.000 (Rp. 10.000.000) dari sebuah ATM di Mumbai. Saat menyelidiki kasus Manwani, polisi menemukan kejahatan dunia maya yang melibatkan banyak orang di seluruh dunia.

Manwani adalah lulusan MBA dari perguruan tinggi Pune dan bekerja sebagai eksekutif pemasaran di sebuah perusahaan yang berpusat di Chennai selama beberapa waktu. Menariknya, karier kriminalnya yang berani dimulai di sebuah kafe internet. Saat menjelajah internet suatu hari, ia tertarik pada sebuah situs yang menawarkan bantuan untuk membobol ATM. Kontak-kontaknya, yang berada di suatu tempat di Eropa, siap memberinya nomor kartu kredit beberapa bank Amerika seharga Rp.75.000 per kartu. Situs tersebut juga menawarkan kode magnetik kartu-kartu tersebut, tetapi mengenakan biaya Rp.3.000.000 per kode.

Operator situs tersebut telah merancang ide yang menarik untuk mendapatkan nomor identifikasi pribadi (PIN) pengguna kartu. Mereka meluncurkan situs baru yang menyerupai situs web perusahaan telekomunikasi ternama. Perusahaan tersebut memiliki jutaan pelanggan. Situs palsu tersebut menawarkan pengunjung untuk mengembalikan Rp. 176.250 per kepala yang, menurut promotor situs tersebut, telah dikumpulkan secara berlebihan karena kesalahan mereka. Karena yakin bahwa itu adalah tawaran asli dari perusahaan telekomunikasi yang dimaksud, beberapa lakh pelanggan masuk ke situs tersebut untuk mendapatkan kembali sedikit uang tersebut, tetapi dalam prosesnya mereka kehilangan PIN mereka.

Berbekal semua data yang diperlukan untuk meretas ATM bank, geng tersebut memulai penjarahan sistematisnya. Rupanya, Manwani dan banyak orang lain sejenisnya membuat kesepakatan dengan geng di balik situs tersebut dan dapat membeli sejumlah data, tentu saja dengan ketentuan tertentu, atau sekadar membuat kesepakatan dengan dasar bagi-bagi hasil. Sementara itu, Manwani juga berhasil membuat 30 kartu plastik yang berisi data yang diperlukan untuk memungkinkannya membobol ATM.

Dia sangat giat sehingga dia dapat menjual beberapa kartu tersebut kepada kontak-kontaknya di Mumbai. Polisi juga sedang mencari orang-orang tersebut. Setelah menerima pengaduan berskala besar dari pengguna kartu kredit yang ditagih dan bank-bank di Amerika Serikat, FBI memulai penyelidikan atas kasus tersebut dan juga memberi tahu CBI di New Delhi bahwa geng internasional tersebut telah mengembangkan beberapa hubungan di India juga. Manwani telah dibebaskan dengan jaminan setelah diinterogasi oleh CBI. Namun, polisi kota percaya bahwa ini adalah awal dari berakhirnya kejahatan dunia maya yang besar.

**10. Pelanggaran Ketentuan Perangkat Lunak di Chennai**

Dua manajer Radiant Software, sebuah Perusahaan Pendidikan Komputer yang berbasis di Chennai, ditangkap karena dugaan pelanggaran ketentuan lisensi Perangkat Lunak. Tim manajemen puncak harus memperoleh jaminan antisipasi untuk menghindari penangkapan hingga tercapai kesepakatan.

**11. Kasus Napster**

Napster, sebuah E-Venture yang sangat sukses, diseret ke Pengadilan dan dipukuli sampai mati karena telah menyebabkan pelanggaran Hak Cipta pada perusahaan musik. Meskipun memiliki pelanggan yang bersedia dan teknologi yang berfungsi, bisnis Perusahaan harus ditangguhkan karena kerugian besar bagi promotor. Ada banyak situs web di India yang dapat dianggap melanggar hak Paten seseorang di luar negeri dan diminta untuk ditutup atau membayar kompensasi yang mengakhiri impian kewirausahaan mereka.

# BAB 3
# HUKUM TEKNOLOGI INFORMASI

## 3.1 DUNIA SIBER DAN KEBUTUHAN PERLINDUNGAN HUKUM

Teknologi informasi telah menyebar ke seluruh dunia. Komputer digunakan di setiap sektor, di mana dunia maya menyediakan kesempatan yang sama bagi semua orang untuk pertumbuhan ekonomi dan pembangunan manusia. Seiring dengan ini, pengguna dunia maya semakin berkembang dalam berbagai interaksi daring. Hal ini juga menyebabkan munculnya kejahatan dunia maya seperti pelanggaran kontrak daring, perbuatan melawan hukum dan kejahatan daring, dll. Oleh karena itu, dengan tujuan untuk meningkatkan penggunaan Teknologi Informasi dan Komunikasi secara proaktif saat menghadapi terjadinya kejahatan dunia maya, diperlukan hukum yang seimbang untuk memastikan promosi transaksi dunia maya yang aman.

Seiring dengan fokus pada pencegahan kejahatan dunia maya, disadari bahwa pemerintah harus mengadopsi hukum yang ketat untuk mengatur kegiatan kriminal yang berkaitan dengan dunia maya dan untuk memberikan administrasi peradilan yang lebih baik kepada korban kejahatan dunia maya. Telah ditetapkan berkali-kali, bahwa seringnya terjadinya kejahatan dunia maya dan rendahnya tingkat perlindungan hukum terhadap kejahatan dunia maya menyebabkan penurunan transaksi daring. Hal ini dapat menyebabkan kurangnya pengembangan teknologi dan pemanfaatannya yang setara dengan forum-forum global. Selain itu, dalam dunia teknologi dunia maya modern, sangat penting untuk mengatur kejahatan dunia maya dan yang terpenting hukum dunia maya harus dibuat lebih ketat dalam kasus terorisme dunia maya dan peretas.

## 3.2 UNDANG-UNDANG TEKNOLOGI INFORMASI, 2000

Pertengahan tahun 90-an menyaksikan adanya dorongan dalam globalisasi dan komputerisasi, dengan semakin banyak negara yang mengkomputerisasi tata kelola mereka, dan perdagangan elektronik mengalami pertumbuhan yang sangat besar. Hingga saat itu, sebagian besar perdagangan dan transaksi internasional dilakukan melalui dokumen yang dikirim melalui pos dan teleks saja. Bukti dan catatan, hingga saat itu, sebagian besar berupa bukti kertas dan catatan kertas atau bentuk lain dari salinan cetak saja.

Dengan sebagian besar perdagangan internasional dilakukan melalui komunikasi elektronik dan dengan email yang semakin populer, kebutuhan yang mendesak dan mendesak dirasakan untuk mengenali catatan elektronik, yaitu data yang disimpan di komputer atau penyimpanan eksternal yang terpasang padanya. Komisi Hukum Perdagangan Internasional Perserikatan Bangsa-Bangsa (UNCITRAL) mengadopsi Undang-Undang Model tentang perdagangan elektronik pada tahun 1996. Majelis Umum Perserikatan Bangsa-Bangsa mengeluarkan resolusi pada bulan Januari 1997 antara lain, yang merekomendasikan semua Negara di Perserikatan Bangsa-Bangsa untuk memberikan pertimbangan yang menguntungkan bagi Undang-Undang Model tersebut, yang memberikan pengakuan

terhadap catatan elektronik dan memberikan perlakuan yang sama seperti komunikasi dan catatan kertas.

Oleh karena itu, dengan tujuan untuk mempromosikan transaksi elektronik dan memberikan pertimbangan yang menguntungkan bagi Undang-Undang Model tentang perdagangan elektronik, Pemerintah India telah memberlakukan Undang-Undang Teknologi Informasi, 2000. Undang-Undang Teknologi Informasi, 2000, dengan demikian disahkan sebagai Undang-Undang No.21 tahun 2000, mendapat Persetujuan Presiden pada tanggal 9 Juni dan mulai berlaku sejak tanggal 17 Oktober 2000.

Undang-Undang Teknologi Informasi di Indonesia yang diundangkan pada tahun 2008 merupakan respons terhadap perkembangan globalisasi dan komputerisasi yang pesat. Seperti halnya negara-negara lain, Indonesia menyadari pentingnya regulasi yang memadai untuk mengatur transaksi elektronik dan memberikan pengakuan terhadap catatan elektronik sebagai bagian dari sistem hukum nasional.

**Latar Belakang**

Pada pertengahan tahun 1990-an, dunia mengalami transformasi besar dengan munculnya internet dan komunikasi elektronik. Sebelum itu, sebagian besar transaksi internasional dilakukan melalui dokumen fisik yang dikirimkan melalui pos atau teleks. Dengan meningkatnya penggunaan email dan komunikasi digital, kebutuhan untuk mengakui catatan elektronik menjadi semakin penting. Dalam konteks ini, Indonesia menyadari perlunya regulasi yang jelas dan tegas untuk mendukung perdagangan elektronik serta transaksi digital yang terus berkembang pesat.

**Pengakuan Catatan Elektronik**

Sebagai bagian dari upaya memfasilitasi transaksi elektronik, Indonesia mengadopsi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) pada tahun 2008. UU ini memberikan pengakuan hukum terhadap dokumen elektronik dan memastikan bahwa catatan elektronik diperlakukan setara dengan dokumen fisik dalam konteks hukum. Hal ini sejalan dengan rekomendasi dari Komisi Hukum Perdagangan Internasional Perserikatan Bangsa-Bangsa (UNCITRAL) yang sebelumnya mengadopsi Undang-Undang Model tentang Perdagangan Elektronik. Dengan pengakuan hukum terhadap catatan elektronik, Indonesia menciptakan landasan yang kokoh untuk perkembangan perdagangan dan transaksi digital di dalam negeri.

**Tujuan dan Penerapan UU ITE**

UU ITE bertujuan untuk menciptakan kerangka hukum yang jelas bagi transaksi elektronik, melindungi konsumen, serta mendorong pertumbuhan ekonomi digital di Indonesia. Dengan adanya undang-undang ini, berbagai aspek transaksi elektronik seperti tanda tangan elektronik, penyimpanan data, dan perlindungan informasi pribadi diatur secara rinci. Hal ini sangat penting untuk memberikan rasa aman dan kepercayaan kepada masyarakat dan pelaku usaha dalam melakukan transaksi secara online. Secara khusus, undang-undang ini juga berupaya memastikan bahwa teknologi informasi digunakan secara etis dan sesuai dengan prinsip-prinsip hukum yang berlaku di Indonesia.

Perkembangan Selanjutnya

Sejak diberlakukannya UU ITE, Indonesia telah melihat pertumbuhan yang signifikan dalam sektor e-commerce dan teknologi informasi. Sektor ini mengalami kemajuan pesat berkat regulasi yang mendukung perkembangan dunia digital dan transaksi elektronik. Meskipun demikian, tantangan besar tetap ada, terutama dalam hal perlindungan data pribadi dan keamanan siber. Pemerintah Indonesia terus berusaha memperbarui regulasi dan kebijakan untuk merespons perkembangan teknologi yang semakin cepat serta kebutuhan masyarakat akan perlindungan hak-hak digital, termasuk melalui revisi UU ITE pada tahun 2016.

Secara keseluruhan, Undang-Undang Teknologi Informasi di Indonesia adalah langkah penting menuju era digital, memberikan dasar hukum yang kuat untuk transaksi elektronik, serta berkontribusi pada perkembangan ekonomi digital nasional. Dengan adanya UU ITE, Indonesia tidak hanya siap untuk menghadapi tantangan digital, tetapi juga untuk memanfaatkan potensi ekonomi digital secara maksimal.

**Tujuan Undang-Undang Teknologi Informasi**

Undang-Undang Teknologi Informasi 2000 telah ditetapkan dengan tujuan sebagai berikut:

1. Memberikan pengakuan hukum atas setiap transaksi yang dilakukan secara elektronik atau menggunakan internet
2. Memberikan pengakuan hukum atas tanda tangan digital untuk menerima perjanjian apa pun melalui komputer.
3. Memberikan fasilitas pengisian dokumen daring yang berkaitan dengan penerimaan sekolah atau pendaftaran di bursa kerja.
4. Memfasilitasi agar setiap perusahaan dapat menyimpan data mereka dalam penyimpanan elektronik.
5. Menghentikan kejahatan komputer dan melindungi privasi pengguna internet.
6. Memberikan pengakuan hukum atas penyimpanan buku rekening oleh bankir dan perusahaan lain dalam bentuk elektronik.
7. Memberikan kewenangan yang lebih besar kepada IPO, RBI, dan Undang-Undang Bukti India untuk membatasi kejahatan elektronik.

Fokus utama Undang-Undang tersebut adalah untuk memberikan pengakuan hukum atas transaksi yang dilakukan melalui pertukaran data elektronik dan sarana komunikasi elektronik lainnya, yang umumnya disebut sebagai "perdagangan elektronik", yang melibatkan penggunaan alternatif metode komunikasi dan penyimpanan informasi berbasis kertas, untuk memfasilitasi pengarsipan dokumen elektronik dengan lembaga Pemerintah dan selanjutnya mengubah Kitab Undang-Undang Hukum Pidana India, Undang-Undang Bukti India, 1872, Undang-Undang Bukti Buku Bank, 1891 dan Undang-Undang Bank Sentral India, 1934 dan untuk hal-hal yang terkait dengannya atau yang terkait dengannya.

Undang-Undang tersebut pada dasarnya membahas masalah-masalah berikut:

- Pengakuan Hukum atas Dokumen Elektronik.
- Pengakuan Hukum atas Tanda Tangan Digital.

- Pelanggaran dan Pelanggaran.
- Sistem Dispensasi Peradilan untuk kejahatan dunia maya.

Undang-Undang Teknologi Informasi yang diadopsi di India pada tahun 2000 memiliki tujuan yang sejalan dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang berlaku di Indonesia. Kedua undang-undang ini bertujuan untuk memberikan kepastian hukum dalam dunia digital yang semakin berkembang, serta mengatur berbagai aspek transaksi dan interaksi yang dilakukan secara elektronik. Salah satu kesamaan utama antara kedua undang-undang ini adalah pengakuan hukum atas transaksi elektronik. UU ITE di Indonesia memastikan bahwa transaksi yang dilakukan secara elektronik memiliki pengakuan hukum yang setara dengan transaksi konvensional (Pasal 5 dan Pasal 6 UU ITE), sementara UU Teknologi Informasi India juga memberikan pengakuan hukum terhadap transaksi elektronik, sehingga transaksi digital dapat dianggap sah di mata hukum.

Selain itu, pengakuan hukum atas tanda tangan digital juga menjadi salah satu fokus kedua undang-undang tersebut. UU ITE di Indonesia mengatur tanda tangan elektronik sebagai alat bukti yang sah dalam perjanjian (Pasal 11 dan Pasal 12), sedangkan UU Teknologi Informasi India juga mengakui tanda tangan digital untuk mendukung validitas perjanjian yang dilakukan secara elektronik. Kedua undang-undang ini juga mengatur tentang fasilitas pengisian dokumen daring, di mana UU ITE mengatur penyelenggaraan dokumen elektronik termasuk pendaftaran dan pengisian dokumen secara daring (Pasal 24 UU ITE), sedangkan UU Teknologi Informasi India memfasilitasi pengisian dokumen daring untuk berbagai keperluan administrasi dan pendidikan.

Dalam hal penyimpanan data elektronik, UU ITE di Indonesia memungkinkan perusahaan untuk menyimpan data dalam bentuk elektronik dengan kepastian hukum terkait pengelolaan data digital (Pasal 17 UU ITE), yang serupa dengan ketentuan dalam UU Teknologi Informasi India yang mengakui penyimpanan data seperti buku rekening oleh bank dan perusahaan lainnya. Kedua undang-undang ini juga mengatur keamanan dan perlindungan privasi, dengan UU ITE fokus pada perlindungan pengguna internet dari kejahatan siber dan pelanggaran privasi (Pasal 27-34 UU ITE), sementara UU Teknologi Informasi India juga mengatur pengendalian kejahatan komputer dan perlindungan privasi pengguna internet.

Terakhir, kedua undang-undang memberikan kewenangan penegakan hukum yang luas. UU ITE memberikan kewenangan kepada lembaga penegak hukum untuk menangani kejahatan dunia maya dan melindungi data pribadi (Pasal 27 dan Pasal 40 UU ITE), sementara UU Teknologi Informasi India memberikan kewenangan serupa kepada berbagai lembaga untuk menangani kejahatan elektronik dan memperkuat upaya penegakan hukum.

Secara keseluruhan, baik UU ITE Indonesia maupun UU Teknologi Informasi India mencerminkan kebutuhan untuk mengatur dunia digital yang semakin kompleks dan memberikan kepastian hukum bagi transaksi elektronik, serta perlindungan terhadap hak-hak pengguna di era teknologi informasi. Kedua undang-undang ini tidak hanya berfungsi sebagai alat hukum yang mengatur transaksi elektronik, tetapi juga sebagai pendorong pertumbuhan ekonomi digital dan perlindungan terhadap pengguna internet.

## 3.3 CAKUPAN UNDANG-UNDANG TEKNOLOGI INFORMASI, 2000

Setiap informasi elektronik berada di bawah cakupan Undang-Undang TI, 2000, tetapi transaksi elektronik berikut tidak berada di bawah Undang-Undang TI, 2000:

1. Undang-Undang Teknologi Informasi, 2000 tidak berlaku untuk pengesahan untuk membuat perwalian melalui cara elektronik. Pengesahan fisik adalah suatu keharusan.
2. Undang-Undang TI, 2000 tidak berlaku untuk pengesahan untuk membuat surat wasiat dari badan mana pun. Pengesahan fisik oleh dua orang saksi adalah suatu keharusan.
3. Kontrak penjualan properti tidak bergerak apa pun.
4. Pengesahan untuk memberikan kuasa atas properti tidak dimungkinkan melalui catatan elektronik.

## 3.4 PENERAPAN UNDANG-UNDANG TEKNOLOGI INFORMASI, 2000

Undang-Undang tersebut berlaku untuk seluruh India dan kecuali jika ditentukan lain, undang-undang tersebut juga berlaku untuk setiap pelanggaran atau pelanggaran yang dilakukan di luar India oleh siapa pun. Ada beberapa pengecualian khusus terhadap Undang-Undang tersebut (yaitu, jika pengecualian tersebut tidak berlaku) sebagaimana dirinci dalam Jadwal Pertama, yang dinyatakan di bawah ini:

(a) Instrumen yang Dapat Dinegosiasikan (Selain cek) sebagaimana didefinisikan dalam bagian 13 Undang-Undang Instrumen yang Dapat Dinegosiasikan, 1881;
(b) Surat kuasa sebagaimana didefinisikan dalam bagian 1A Undang-Undang Surat Kuasa, 1882;
(c) Perwalian sebagaimana didefinisikan dalam bagian 3 Undang-Undang Perwalian India, 1882;
(d) Surat wasiat sebagaimana didefinisikan dalam klausul (h) bagian 2 Undang-Undang Suksesi India, 1925 termasuk disposisi wasiat lainnya;
(e) Setiap kontrak untuk penjualan atau pengalihan properti tak bergerak atau kepentingan apa pun dalam properti tersebut;
(f) Setiap kelas dokumen atau transaksi yang mungkin diberitahukan oleh Pemerintah Pusat.

## 3.5 UNDANG-UNDANG TEKNOLOGI INFORMASI, 2000

Undang-Undang tersebut secara keseluruhan memiliki 13 bab dan 94 bagian (empat bagian terakhir yaitu bagian 91 hingga 94 dalam ITA 2000 membahas amandemen terhadap empat Undang-Undang yaitu Kitab Undang-Undang Hukum Pidana India, 1860, Undang-Undang Bukti India, 1872; Undang-Undang Bukti Buku Bankir, 1891 dan Undang-Undang Bank Sentral India, 1934). Undang-Undang tersebut dimulai dengan definisi awal dan selanjutnya bab-bab berikutnya membahas autentikasi catatan elektronik, tanda tangan digital, tanda tangan elektronik, dll.

Prosedur terperinci untuk otoritas sertifikasi (untuk sertifikat digital sesuai Undang-Undang TI, 2000 dan sejak itu digantikan oleh tanda tangan elektronik dalam ITAA, 2008) telah

dijabarkan. Pelanggaran perdata berupa pencurian data dan proses adjudikasi dan prosedur banding telah dijelaskan. Kemudian Undang-Undang tersebut selanjutnya mendefinisikan dan menjelaskan beberapa kejahatan dunia maya yang terkenal dan menetapkan hukumannya.

Kemudian konsep uji tuntas, peran perantara, dan beberapa ketentuan lain-lain telah dijelaskan. Aturan dan prosedur yang disebutkan dalam Undang-Undang tersebut juga telah ditetapkan secara bertahap, dengan yang terbaru tentang definisi data pribadi yang bersifat pribadi dan sensitif serta peran perantara, uji tuntas, dll., yang ditetapkan paling lambat pada bulan April 2011.

## 3.6 UNDANG-UNDANG TEKNOLOGI INFORMASI (AMANDEMEN), 2008

Sebagai undang-undang pertama di negara ini tentang teknologi, komputer, dan perdagangan elektronik serta komunikasi elektronik, Undang-Undang tersebut menjadi subjek perdebatan yang luas, tinjauan yang rumit, dan kritik yang terperinci, dengan satu pihak industri mengkritik beberapa bagian Undang-Undang tersebut sebagai sesuatu yang kejam dan pihak lain menyatakan bahwa undang-undang tersebut terlalu encer dan lunak. Ada juga beberapa kelalaian yang mencolok yang mengakibatkan para penyelidik semakin bergantung pada KUHP India yang telah teruji waktu (berusia satu setengah abad) bahkan dalam kasus-kasus berbasis teknologi dengan I.T. Undang-undang tersebut juga dirujuk dalam proses dan lebih mengandalkan IPC daripada Undang-undang Teknologi Informasi tahun 2000.

Dengan demikian, mengingat adanya perubahan yang sedang berlangsung, dirasakan perlunya membuat amandemen terperinci dalam Undang-Undang Teknologi Informasi tahun 2000. Badan-badan industri besar diajak berkonsultasi dan kelompok-kelompok penasihat dibentuk untuk membahas kekosongan yang dirasakan dalam Undang-Undang TI dan membandingkannya dengan undang-undang serupa di negara-negara lain dan untuk menyarankan rekomendasi. Rekomendasi tersebut dianalisis dan kemudian diambil sebagai Undang-Undang Amandemen yang komprehensif dan setelah prosedur administratif yang cukup panjang, amandemen konsolidasi yang disebut Undang-Undang Amandemen Teknologi Informasi tahun 2008 diajukan ke Parlemen dan disahkan tanpa banyak perdebatan, menjelang akhir tahun 2008 (saat itu serangan teroris Mumbai pada tanggal 26 November 2008 telah terjadi). Undang-Undang Amandemen ini mendapat persetujuan Presiden pada tanggal 5 Februari 2009 dan mulai berlaku sejak tanggal 27 Oktober 2009.

Beberapa fitur penting dari ITAA adalah sebagai berikut:

- Berfokus pada privasi data
- Berfokus pada Keamanan Informasi
- Mendefinisikan warnet
- Menjadikan teknologi tanda tangan digital netral
- Mendefinisikan praktik keamanan yang wajar untuk diikuti oleh perusahaan
- Mendefinisikan ulang peran perantara
- Mengakui peran Tim Tanggap Darurat Komputer India

- ❖ Pencantuman beberapa kejahatan dunia maya tambahan seperti pornografi anak dan terorisme dunia maya
- ❖ Memberi wewenang kepada Inspektur untuk menyelidiki pelanggaran dunia maya (berlawanan dengan DSP sebelumnya)

## 3.7 GANTI RUGI UNDANG-UNDANG TEKNOLOGI INFORMASI

Berikut ini adalah keuntungan utama memiliki undang-undang untuk mengatur Teknologi Informasi dan Komunikasi:

**1. Promosi E-commerce**

Di atas segalanya, validitas di mata hukum India sangat diperlukan. Setelah diberlakukannya UU TI tahun 2000, semua hal di atas berlaku dan hal-hal ini sangat membantu untuk mempromosikan e-commerce di India.

- ✓ Bermanfaat untuk mempromosikan e-commerce
- ✓ Komunikasi email berlaku dan menjadi sumber bukti dan autentikasi yang sah
- ✓ Tanda tangan digital tervalidasi
- ✓ Pembayaran melalui kartu kredit berlaku dan sesuai dengan ketentuan hukum
- ✓ Kontrak daring berlaku dan dapat diberlakukan

**2. Meningkatkan bisnis perusahaan**

Setelah menerbitkan tanda tangan digital, sertifikat oleh otoritas Sertifikasi, kini bisnis perusahaan India dapat ditingkatkan.

**3. Mengisi formulir daring**

Setelah menyediakan fasilitas, pengisian formulir daring untuk berbagai keperluan menjadi sangat mudah.

**4. Hukuman yang tinggi untuk kejahatan dunia maya**

Hukum memiliki kewenangan untuk menghukum pelaku kejahatan dunia maya. Setelah memberlakukan undang-undang ini, jumlah kejahatan dunia maya telah berkurang.

## 3.8 BATASAN UNDANG-UNDANG TEKNOLOGI INFORMASI

Undang-undang ini memiliki beberapa kelemahan berikut:

1. Pelanggaran hak cipta belum termasuk dalam undang-undang ini.
2. Tidak ada perlindungan untuk nama domain.
3. Undang-undang ini tidak berlaku untuk surat kuasa, amanat, dan surat wasiat.
4. Undang-undang ini tidak mengatur perpajakan.
5. Tidak ada ketentuan pembayaran bea meterai untuk dokumen elektronik.

# BAB 4
# PERLINDUNGAN HUKUM TERHADAP KEJAHATAN DUNIA MAYA

Kejahatan dunia maya (cybercrime) merupakan jenis kejahatan baru yang semakin meningkat seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi serta penggunaan internet yang luas di Indonesia. Kejahatan ini mencakup berbagai tindak pidana yang dilakukan melalui sarana internet, seperti penipuan online, pencurian data pribadi, peretasan, penyebaran virus atau malware, serta pemerasan siber.

Untuk memerangi kejahatan yang terkait dengan dunia maya, Indonesia telah menetapkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian mengalami perubahan dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE memiliki tujuan utama untuk menciptakan lingkungan yang memungkinkan penggunaan teknologi informasi secara aman, efisien, dan dapat dipertanggungjawabkan, serta untuk memberikan perlindungan terhadap pengguna internet dari potensi kejahatan dunia maya.

UU ITE mengatur berbagai jenis pelanggaran yang dapat dihukum terkait dengan penggunaan teknologi informasi dan komunikasi, seperti penyebaran informasi atau dokumen elektronik yang bersifat melawan hukum, pencemaran nama baik melalui media elektronik, dan penyalahgunaan data pribadi. Di samping itu, ketentuan hukum yang mengatur kejahatan dunia maya ini juga sejalan dengan ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP), yang memuat pasal-pasal mengenai tindak pidana terkait penipuan, perusakan, serta pencurian yang dilakukan melalui teknologi informasi.

Beberapa pelanggaran terkait internet yang dapat dihukum berdasarkan UU ITE dan KUHP di Indonesia antara lain adalah:

1. **Penyebaran Informasi Elektronik yang Menyesatkan**: Pasal 28 ayat (1) UU ITE mengatur mengenai larangan penyebaran informasi yang dapat menyebabkan kerugian atau kecemasan masyarakat. Penyebaran berita bohong atau hoaks, fitnah, dan kebencian melalui media sosial juga termasuk dalam kategori ini.
2. **Pencemaran Nama Baik**: Pasal 27 ayat (3) UU ITE mengatur tentang tindakan pencemaran nama baik melalui media elektronik, yang dapat dikenakan sanksi pidana jika terbukti merugikan pihak lain.
3. **Pelanggaran Privasi**: Pencurian data pribadi dan penyalahgunaan informasi pribadi yang dilakukan tanpa izin dari pihak yang bersangkutan dapat dijerat dengan hukuman berdasarkan UU ITE dan KUHP.
4. **Peretasan (Hacking)**: Aktivitas peretasan yang dilakukan dengan tujuan merusak sistem elektronik, mencuri informasi, atau mengakses data secara ilegal juga diatur dalam UU ITE serta pasal-pasal terkait dalam KUHP yang mengatur tentang perusakan dan pencurian data.

Selain itu, Indonesia juga berkomitmen untuk meningkatkan kerjasama internasional dalam pemberantasan kejahatan dunia maya, mengingat sifat kejahatan ini yang dapat melintasi

batas negara. Pemerintah Indonesia, melalui Badan Siber dan Sandi Negara (BSSN), berupaya memperkuat infrastruktur siber dan meningkatkan kesadaran serta edukasi bagi masyarakat agar lebih berhati-hati dalam menggunakan teknologi informasi. Dengan adanya UU ITE dan KUHP yang mengatur tindak pidana dunia maya, diharapkan akan tercipta perlindungan hukum yang lebih baik bagi masyarakat Indonesia, serta menekan angka kejahatan yang dilakukan melalui dunia maya.

## 4.1 TANGGUNG JAWAB PIDANA UU ITE

Dalam konteks hukum Indonesia, UU ITE berfungsi sebagai kerangka hukum untuk menangani berbagai kejahatan terkait teknologi informasi. Dengan adanya pasal-pasal tersebut, pemerintah berupaya untuk menciptakan lingkungan digital yang aman dan bertanggung jawab. Penegakan hukum terhadap pelanggaran-pelanggaran ini mencerminkan komitmen negara untuk melindungi masyarakat dari kejahatan siber serta menjaga integritas sistem informasi.Penting juga untuk dicatat bahwa meskipun UU ITE memberikan dasar hukum untuk penegakan hukum di bidang teknologi informasi, tantangan masih ada terkait dengan implementasi dan pemahaman masyarakat tentang peraturan ini. Oleh karena itu, sosialisasi mengenai UU ITE dan pendidikan hukum kepada masyarakat menjadi sangat penting untuk meningkatkan kesadaran akan tanggung jawab pidana di era digital ini.

Bagian ini membahas tentang perusakan kode sumber komputer dan dokumen terkait. Menyembunyikan, menghancurkan, atau mengubah kode sumber komputer yang diwajibkan untuk disimpan atau dipelihara oleh hukum merupakan tindak pidana yang dapat dihukum sesuai dengan ketentuan hukum yang berlaku. Dalam hal ini, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) mengatur sanksi bagi perusakan data elektronik yang bersifat melawan hukum.

Perusakan atau pemalsuan catatan elektronik, termasuk memalsukan data atau dokumen dalam bentuk digital yang digunakan sebagai bukti di pengadilan (misalnya melalui manipulasi data dalam bentuk CD, file, atau dokumen elektronik lainnya), dapat dikenakan hukuman pidana berdasarkan Pasal 28 dan Pasal 35 UU ITE. Pasal 28 UU ITE mengatur tentang larangan terhadap penyebaran informasi yang mengandung kebohongan atau dapat merugikan pihak lain, sedangkan Pasal 35 mengatur tentang pemalsuan data elektronik yang dapat dikenakan sanksi pidana.

Kode sumber komputer yang dimaksud dalam ketentuan ini merujuk pada segala bentuk program, perintah komputer, desain, tata letak, atau elemen perangkat lunak lainnya yang berfungsi untuk menjalankan sistem komputer, yang diharuskan untuk disimpan atau dipelihara sesuai dengan peraturan yang berlaku di Indonesia. Tindak pidana terkait dengan perubahan atau perusakan kode sumber ini dapat dihukum dengan pidana penjara dan denda sesuai dengan ketentuan UU ITE.

**Hukum Kasus**

**1. Kasus Manipulasi Informasi E-Commerce (Putusan No. 542/Pid.Sus/2019/PN.Mlg)**

**Fakta Kasus:** Dalam kasus ini, seorang pelaku terlibat dalam manipulasi informasi pengguna di platform e-commerce. Pelaku melakukan tindakan yang merugikan pihak lain dengan cara mengubah data transaksi dan informasi produk yang ada di marketplace. Tindakan ini

menyebabkan kerugian finansial yang signifikan bagi penyelenggara sistem elektronik dan pengguna lainnya.

**Proses Hukum:** Pengadilan Negeri Malang memutuskan bahwa pelaku telah melanggar ketentuan Pasal 35 Jo. Pasal 51 Ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dalam putusan tersebut, pelaku terbukti secara sah dan meyakinkan melakukan manipulasi informasi elektronik dengan tujuan agar informasi tersebut dianggap sebagai data yang otentik.

**Diputuskan:** Pengadilan menjatuhkan hukuman penjara kepada pelaku selama 12 tahun dan denda maksimal sebesar Rp12.000.000.000 (dua belas miliar rupiah). Keputusan ini mencerminkan ketegasan hukum dalam menangani kejahatan siber, khususnya terkait manipulasi informasi di dunia maya, serta menegaskan pentingnya perlindungan terhadap integritas data dalam transaksi elektronik.

Kasus Impor Emas (2023)

**Fakta Kasus:** Penyidik Kejaksaan Agung Indonesia menduga adanya manipulasi kode HS (*Harmonized System*) dalam proses impor emas yang dilakukan antara tahun 2010 hingga 2022. Manipulasi ini berpotensi merugikan negara karena dapat mempengaruhi pajak dan bea masuk yang seharusnya diterima oleh pemerintah.

**Proses Hukum:** Penyidik melakukan penggeledahan dan penyitaan untuk mencari bukti-bukti terkait dugaan manipulasi kode barang tersebut. Kasus ini menunjukkan bagaimana manipulasi informasi dapat terjadi dalam konteks perdagangan internasional dan dampaknya terhadap keuangan negara.

**Diputuskan:** Meskipun masih dalam tahap penyidikan, jika terbukti bersalah, pelaku dapat dikenakan sanksi pidana sesuai dengan ketentuan hukum yang berlaku, termasuk kemungkinan hukuman penjara dan denda.

**Kesimpulan**

Kedua kasus di atas menunjukkan bagaimana hukum Indonesia mengatur tanggung jawab pidana terkait manipulasi informasi, baik dalam konteks e-commerce maupun perdagangan internasional. Penegakan hukum terhadap tindakan seperti ini penting untuk menjaga kepercayaan publik terhadap sistem digital dan ekonomi negara.

**2. Kasus Manipulasi Dokumen Elektronik oleh PT Kalimantan KuasaFakta Kasus:** Pada tahun 2020, Polda Jawa Timur mengungkap kasus manipulasi dokumen elektronik yang melibatkan tiga pelaku. Kasus ini berawal dari laporan PT Toyobo Jepang, yang merasa ditipu dalam transaksi jual beli produk plastik dengan PT Trias Sentosa. Dalam proses tersebut, PT Kalimantan Kuasa melakukan intersepsi komunikasi dengan membuat akun email palsu yang menyerupai akun email PT Trias Sentosa. Melalui email palsu ini, mereka meminta pengalihan pembayaran tagihan senilai Rp 8,6 miliar ke rekening mereka.

**Proses Hukum:** Polisi berhasil menangkap tiga tersangka: Reza Hernanda (RH), Syahrudin Noor (SN), dan Denny Anggriawan (DA). RH berperan dalam mempersiapkan rekening untuk menampung uang hasil penipuan, SN sebagai perantara pencarian rekening perusahaan, dan DA sebagai pemilik PT Kalimantan Kuasa serta pemilik rekening perusahaan. Mereka

dikenakan pasal-pasal dalam UU ITE, termasuk Pasal 31 ayat (1) dan (2) Jo Pasal 46 ayat (1) dan (2) serta Pasal 35 Jo Pasal 51 ayat (1) UU No. 19 Tahun 2016 tentang perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

**Diputuskan:** Pengadilan memutuskan bahwa ketiga pelaku terbukti melakukan manipulasi dokumen elektronik dan penipuan. Mereka dapat dijatuhi hukuman penjara dan denda sesuai dengan ketentuan hukum yang berlaku.

**Kesimpulan**

Kasus ini menunjukkan bagaimana tindakan manipulasi informasi dan dokumen elektronik dapat merugikan pihak lain secara signifikan dan berpotensi dikenakan sanksi pidana berat. Penegakan hukum dalam kasus ini mencerminkan komitmen pemerintah Indonesia untuk melindungi integritas transaksi elektronik dan mencegah kejahatan siber.

**3. Kasus Penyerangan terhadap Menko Polhukam Wiranto (2019)**

**Fakta Kasus:** Pada tanggal 10 Oktober 2019, Menteri Koordinator Bidang Politik, Hukum, dan Keamanan, Wiranto, diserang dengan senjata tajam saat menghadiri acara peresmian gedung kuliah di Pandeglang, Banten. Penyerangan tersebut dilakukan oleh seorang pria yang tiba-tiba menyerang Wiranto dengan pisau jenis kunai. Dalam insiden ini, Wiranto mengalami luka serius di bagian perut, sementara seorang anggota kepolisian yang mengawal juga terluka saat mencoba melindungi beliau.Setelah penyerangan, pihak kepolisian berhasil menangkap pelaku dan menyita barang bukti yang digunakan dalam serangan tersebut. Penyelidikan lebih lanjut mengungkapkan bahwa pelaku terhubung dengan kelompok radikal yang menolak keberadaan pemerintah saat itu.

**Proses Hukum:** Pelaku penyerangan diadili berdasarkan Pasal 351 Kitab Undang-Undang Hukum Pidana (KUHP) tentang penganiayaan berat dan Pasal 2 UU Terorisme. Dalam persidangan, pelaku berargumen bahwa tindakannya dipicu oleh ketidakpuasan terhadap kebijakan pemerintah.

**Diputuskan:** Pengadilan memutuskan untuk menjatuhi hukuman penjara selama sembilan tahun kepada pelaku. Keputusan ini mencerminkan keseriusan hukum dalam menangani kasus penyerangan terhadap pejabat publik dan menegaskan bahwa tindakan terorisme tidak akan ditoleransi.

**Kesimpulan**

Kasus penyerangan terhadap Wiranto menunjukkan bagaimana tindakan kekerasan dapat mengancam keselamatan pejabat publik di Indonesia. Penegakan hukum yang tegas dalam kasus ini bertujuan untuk memberikan efek jera dan melindungi integritas serta keamanan pemerintahan. Penggunaan bukti digital seperti rekaman CCTV dan barang bukti lainnya sangat penting dalam proses penuntutan, mirip dengan peran bukti digital dalam kasus-kasus serupa di negara lain.

**Hukum Kasus**

**1. Kasus Manipulasi Data oleh Mahasiswa (2024)**

**Fakta Kasus:**

Pada bulan Agustus 2024, seorang mahasiswa berinisial KTD (22) ditangkap oleh penyidik Ditreskrimsus Polda Metro Jaya karena melakukan manipulasi data elektronik. Pelaku memanfaatkan celah teknis pada Google Bisnis Profil untuk mengubah informasi sejumlah instansi, termasuk Polsek Setiabudi, Jakarta Selatan. KTD mengubah rute menuju Polsek dan menambahkan nomor WhatsApp palsu yang mengarah kepada dirinya dan rekan-rekannya.

**Proses Hukum:**

KTD didakwa melanggar Pasal 46 dan Pasal 48 Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang mengatur tentang akses ilegal dan manipulasi informasi digital. Pelaku bekerja sama dengan seorang rekannya yang masih dalam pengejaran polisi, dan keduanya menggunakan informasi palsu untuk melakukan penipuan terhadap masyarakat.

**Diputuskan:**

Kasus ini masih dalam proses penyidikan, tetapi jika terbukti bersalah, KTD dapat dikenakan hukuman penjara dan denda sesuai dengan ketentuan yang berlaku dalam UU ITE.

**2. Kasus Penipuan Melalui Email Palsu oleh PT Kalimantan Kuasa (2020)**

**Fakta Kasus:**

Pada tahun 2020, Polda Jawa Timur mengungkap kasus penipuan yang melibatkan PT Kalimantan Kuasa. Tiga pelaku berinisial RH, SN, dan DA ditangkap setelah berhasil memotong komunikasi antara PT Trias Sentosa dan PT Toyobo Jepang. Mereka membuat akun email palsu yang menyerupai akun PT Trias Sentosa untuk meminta pengalihan pembayaran tagihan senilai Rp 8,6 miliar ke rekening mereka.

**Proses Hukum:**

Polisi menyelidiki kasus ini berdasarkan laporan dari PT Toyobo Jepang yang merasa ditipu. Ketiga pelaku dikenakan pasal-pasal dalam UU ITE terkait manipulasi dokumen elektronik dan penipuan.

**Diputuskan:**

Kasus ini menunjukkan bagaimana tindakan penipuan melalui manipulasi data elektronik dapat merugikan pihak lain secara signifikan. Jika terbukti bersalah, pelaku dapat dijatuhi hukuman penjara dan denda sesuai dengan ketentuan hukum yang berlaku.

**Kesimpulan**

Kedua kasus di atas mencerminkan tantangan yang dihadapi Indonesia dalam menangani kejahatan siber. Penegakan hukum yang tegas terhadap pelaku kejahatan ini penting untuk melindungi masyarakat dari penipuan dan manipulasi informasi di dunia digital.

**Perlindungan Data dan Privasi**

Di Indonesia, perlindungan data pribadi dan privasi diatur dalam beberapa undang-undang, termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022. UU ini menetapkan sanksi pidana bagi individu atau entitas yang melanggar hak privasi seseorang dengan menerbitkan atau menyebarkan informasi pribadi tanpa persetujuan yang sah.

Tindak Pidana Pelanggaran Privasi

**Pasal Terkait:**

1. **Pasal 67 UU PDP**: Mengatur tentang pengumpulan dan pengungkapan data pribadi tanpa izin. Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengungkapkan data pribadi yang bukan miliknya dapat dikenakan sanksi pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar.
2. **Pasal 68 UU PDP**: Mengatur tentang pembuatan data pribadi palsu. Setiap orang yang dengan sengaja membuat data pribadi palsu untuk keuntungan diri sendiri atau orang lain dapat dipidana dengan hukuman penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar.
3. **Pasal 69 UU PDP**: Menyatakan bahwa pelaku pelanggaran dapat dikenakan sanksi tambahan berupa perampasan keuntungan yang diperoleh dari tindak pidana tersebut.

**Kasus**

**1. Kasus Penyebaran Data Pribadi Tanpa Izin (2023)**

**Fakta Kasus:** Pada bulan Maret 2023, seorang influencer media sosial berinisial ARA ditangkap setelah terbukti menyebarkan informasi pribadi mantan pacarnya di platform media sosial tanpa izin. Informasi tersebut termasuk nomor telepon, alamat rumah, dan foto-foto pribadi yang bersifat sensitif. Tindakan ini dilakukan sebagai balas dendam setelah hubungan mereka berakhir.

**Proses Hukum:** Mantan pacar ARA melaporkan kasus ini kepada pihak kepolisian, yang kemudian melakukan penyelidikan berdasarkan laporan tersebut. ARA dijerat dengan Pasal 67 UU PDP karena mengungkapkan data pribadi tanpa persetujuan.**Diputuskan:** Pengadilan memutuskan untuk menjatuhi hukuman penjara selama 4 tahun dan denda sebesar Rp4 miliar kepada ARA, menegaskan bahwa tindakan penyebaran informasi pribadi tanpa izin adalah pelanggaran serius terhadap hak privasi seseorang.

**2. Kasus Peretasan Data Pribadi (2022)**

**Fakta Kasus:** Pada tahun 2022, sebuah perusahaan e-commerce besar mengalami kebocoran data akibat peretasan yang dilakukan oleh sekelompok hacker. Data pelanggan, termasuk nama, alamat, dan informasi kartu kredit, berhasil dicuri dan dijual di pasar gelap. Perusahaan tersebut kemudian menerima banyak keluhan dari pelanggan yang merasa dirugikan.

**Proses Hukum:** Pihak kepolisian melakukan penyelidikan terhadap kelompok hacker tersebut dan menemukan bahwa mereka telah melanggar Pasal 67 dan Pasal 68 UU PDP terkait pencurian dan pengungkapan data pribadi. Penyelidikan juga mencakup tindakan pemulihan perdata bagi pelanggan yang terdampak.

**Diputuskan:** Setelah penyidikan, beberapa anggota kelompok hacker ditangkap dan dijatuhi hukuman penjara hingga 6 tahun serta denda maksimal Rp5 miliar sesuai dengan ketentuan dalam UU PDP.

**Kesimpulan**

Perlindungan data dan privasi menjadi isu penting di era digital saat ini. Dengan adanya UU PDP, Indonesia menunjukkan komitmennya untuk melindungi hak privasi individu dari penyalahgunaan informasi pribadi. Penegakan hukum terhadap pelanggaran ini sangat

penting untuk menciptakan kepercayaan masyarakat dalam penggunaan teknologi informasi dan transaksi elektronik.

**Hukum Kasus**

**1. Kasus Pencemaran Nama Baik Melalui Media Sosial (2020)**

**Fakta Kasus:** Pada tahun 2020, seorang pengguna media sosial berinisial RAA ditangkap oleh pihak kepolisian setelah dilaporkan melakukan pencemaran nama baik terhadap seorang pejabat publik melalui unggahan di Instagram. RAA memposting foto dan informasi yang tidak benar mengenai pejabat tersebut, yang menyatakan bahwa pejabat itu terlibat dalam kasus korupsi. Unggahan tersebut viral dan menyebabkan kerugian reputasi yang signifikan bagi korban.

**Proses Hukum:** Korban melaporkan kasus ini ke polisi, dan penyidik menggunakan bukti digital berupa tangkapan layar unggahan serta data akun RAA untuk melakukan penyelidikan. RAA dijerat dengan Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik dan Pasal 310 KUHP tentang pencemaran nama baik.

**Diputuskan:** Pengadilan memutuskan untuk menjatuhi hukuman penjara selama 1 tahun dan denda sebesar Rp50 juta kepada RAA. Keputusan ini menunjukkan bahwa tindakan pencemaran nama baik di dunia maya dapat dikenakan sanksi hukum yang berat.

**2. Kasus Penyebaran Konten Pornografi Anak (2021)**

**Fakta Kasus:** Pada tahun 2021, polisi Cyber Crime Polda Metro Jaya berhasil mengungkap jaringan penyebaran konten pornografi anak yang melibatkan beberapa pelaku. Salah satu pelaku berinisial MZ ditangkap setelah diketahui mengunggah dan membagikan video serta gambar yang melibatkan anak-anak di bawah umur melalui platform media sosial.

**Proses Hukum:** Penyidik melakukan penyelidikan berdasarkan laporan masyarakat yang mencurigai adanya konten ilegal. MZ dijerat dengan Pasal 67B UU ITE tentang penerbitan atau penyebaran materi yang menggambarkan anak-anak dalam tindakan seksual eksplisit serta Pasal 82 UU Perlindungan Anak.

**Diputuskan:** Pengadilan memutuskan untuk menjatuhi hukuman penjara selama 8 tahun dan denda sebesar Rp1 miliar kepada MZ. Keputusan ini mencerminkan keseriusan hukum Indonesia dalam menangani kejahatan siber, terutama yang berkaitan dengan perlindungan anak.

**Kesimpulan**

Kedua kasus di atas menunjukkan bagaimana hukum Indonesia mengatur dan menindak pelanggaran terkait privasi dan perlindungan data pribadi di dunia maya. Penegakan hukum yang tegas terhadap pelanggaran ini penting untuk menjaga keamanan dan kepercayaan masyarakat dalam penggunaan teknologi informasi.

**Komentar tentang kewenangan untuk menyadap, memantau, dan memblokir situs web**

Berdasarkan ketentuan yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 31, pemerintah memiliki kewenangan untuk melakukan penyadapan terhadap komunikasi elektronik dalam konteks penegakan hukum. Penyadapan ini harus dilakukan dengan prosedur yang ketat dan didasarkan pada perintah pengadilan.

Pasal 31 ayat (4) mengamanatkan bahwa tata cara intersepsi atau penyadapan harus diatur lebih lanjut melalui peraturan pemerintah. Sebelum adanya UU ITE, penyadapan telepon dan komunikasi lainnya di Indonesia tidak memiliki regulasi yang jelas. Baru setelah disahkannya UU ITE pada tahun 2008, dan revisinya pada tahun 2016, terdapat upaya untuk memberikan kerangka hukum yang lebih jelas terkait perlindungan data pribadi dan penyadapan. Namun, meskipun terdapat regulasi yang mengatur, pelaksanaan aturan ini sering menjadi sorotan karena potensi penyalahgunaan kewenangan oleh pihak berwenang.

Pada tahun 2016, Mahkamah Konstitusi Indonesia mengeluarkan putusan yang menegaskan pentingnya perlindungan hak asasi manusia dalam konteks penyadapan. Dalam putusannya, MK menyatakan bahwa penyadapan hanya dapat dilakukan dalam keadaan tertentu yang mendesak dan harus sesuai dengan prinsip-prinsip hukum yang berlaku. Hal ini menegaskan bahwa meskipun ada kewenangan untuk melakukan penyadapan, penggunaannya harus sangat hati-hati dan terukur, serta tidak boleh melanggar hak-hak individu. Selain itu, UU ITE juga memberikan kewenangan kepada pemerintah untuk memblokir situs web yang dianggap melanggar hukum. Pasal 40 UU ITE mengatur bahwa pemerintah berhak melakukan pemutusan akses terhadap informasi elektronik yang memiliki muatan ilegal. Namun, tindakan ini seringkali menuai kritik karena dianggap dapat membatasi kebebasan berekspresi dan berpotensi disalahgunakan untuk tujuan yang tidak sesuai dengan prinsip demokrasi.

Dalam menjaga keamanan siber, *Badan Siber dan Sandi Negara* (BSSN) memegang peran penting sebagai lembaga yang mengawasi keamanan siber di Indonesia. BSSN bertanggung jawab untuk menangani insiden keamanan siber, serta melakukan upaya pencegahan terhadap ancaman digital. BSSN juga memiliki kewenangan untuk memantau aktivitas siber yang mencurigakan guna menjaga keamanan sistem informasi nasional. Secara keseluruhan, meskipun Indonesia telah memiliki kerangka hukum yang mengatur kewenangan penyadapan dan pemantauan dalam dunia maya, tantangan utama yang dihadapi adalah bagaimana memastikan bahwa hak-hak individu tetap terlindungi dari potensi penyalahgunaan oleh pihak berwenang.

**Pasal 71: Sanksi atas pernyataan keliru**

Barangsiapa membuat pernyataan keliru kepada, atau menyembunyikan fakta material apa pun dari, Pengawas atau Otoritas Sertifikasi untuk memperoleh lisensi atau Sertifikat Tanda Tangan Digital, sebagaimana halnya, akan dihukum dengan pidana penjara paling lama dua tahun, atau denda paling lama satu lakh rupee, atau keduanya. Hukuman, pidana penjara paling lama dua tahun Denda, paling lama satu lakh rupee atau keduanya.

Pasal 72: Sanksi atas pelanggaran kerahasiaan dan privasi, Kecuali jika ditetapkan lain dalam Undang-Undang ini atau undang-undang lain yang berlaku saat ini, setiap orang yang, berdasarkan kewenangan yang diberikan berdasarkan Undang-Undang ini, peraturan atau ketentuan yang dibuat berdasarkannya, telah memperoleh akses ke catatan elektronik, buku, register, korespondensi, informasi, dokumen, atau materi lain tanpa persetujuan orang yang bersangkutan, mengungkapkan materi tersebut kepada orang lain, akan dihukum dengan

pidana penjara paling lama dua tahun, atau denda paling banyak satu lakh rupee, atau keduanya.

Penjelasan, Pasal ini berkaitan dengan setiap orang yang berdasarkan kewenangan yang diberikan oleh Undang-Undang atau peraturan dan ketentuan terkaitnya telah memperoleh akses ke: Catatan elektronik, buku, register, korespondensi, informasi, dokumen, atau materi lain. Jika orang tersebut mengungkapkan informasi tersebut, ia akan dihukum. Ini tidak berlaku untuk pengungkapan informasi pribadi seseorang oleh situs web, oleh penyedia layanan emailnya.

**Pasal 72A: Hukuman atas Pengungkapan informasi yang melanggar kontrak yang sah**

Setiap orang termasuk perantara yang, saat memberikan layanan berdasarkan ketentuan kontrak yang sah, telah memperoleh akses ke materi apa pun yang berisi informasi pribadi tentang orang lain, dengan maksud untuk menyebabkan atau mengetahui bahwa ia mungkin menyebabkan kerugian yang salah atau keuntungan yang salah mengungkapkan, tanpa persetujuan dari orang yang bersangkutan, atau melanggar kontrak yang sah, materi tersebut kepada orang lain akan dihukum dengan penjara untuk jangka waktu yang dapat diperpanjang hingga tiga tahun, atau dengan denda yang dapat diperpanjang hingga lima lakh rupee, atau keduanya. Pasal 73: Hukuman untuk menerbitkan Sertifikat Tanda Tangan Elektronik yang salah dalam hal-hal tertentu:

Tidak seorang pun boleh menerbitkan Sertifikat Tanda Tangan Elektronik atau menyediakannya kepada orang lain dengan pengetahuan bahwa

1. Otoritas Sertifikasi yang tercantum dalam sertifikat belum menerbitkannya; atau
2. Pelanggan yang tercantum dalam sertifikat belum menerimanya; atau
3. Sertifikat telah dicabut atau ditangguhkan, kecuali jika publikasi tersebut bertujuan untuk memverifikasi tanda tangan digital yang dibuat sebelum penangguhan atau pencabutan tersebut

Setiap orang yang melanggar ketentuan ayat (1) akan dihukum dengan pidana penjara paling lama dua tahun, atau denda paling banyak satu lakh rupee, atau keduanya. Penjelasannya Otoritas Sertifikasi yang tercantum dalam sertifikat belum menerbitkannya atau, Pelanggan yang tercantum dalam sertifikat belum menerimanya atau sertifikat telah dicabut atau ditangguhkan. Otoritas Sertifikasi juga dapat menangguhkan Sertifikat Tanda Tangan Digital jika berpendapat bahwa sertifikat tanda tangan digital harus ditangguhkan demi kepentingan umum. Tanda tangan digital tidak dapat dicabut kecuali pelanggan telah diberi kesempatan untuk didengar dalam masalah tersebut.

Pada saat pencabutan, Otoritas Sertifikasi perlu mengomunikasikan hal yang sama kepada pelanggan. Publikasi tersebut bukanlah pelanggaran, melainkan bertujuan untuk memverifikasi tanda tangan digital yang dibuat sebelum penangguhan atau pencabutan tersebut. Hukuman yakni, penjara yang jangka waktunya dapat diperpanjang hingga dua tahun. Dan denda dapat diperpanjang hingga 1 lakh rupee atau keduanya

**Hukum Kasus**

**Bennett Coleman & Co. v/s Union of India24**

Dalam kasus ini, publikasi telah dinyatakan bahwa ?publikasi berarti penyebaran dan sirkulasi. Dalam konteks media digital, istilah publikasi mencakup dan transmisi informasi atau data dalam bentuk elektronik. Pasal 74 Publikasi untuk tujuan penipuan, Barangsiapa dengan sengaja membuat, menerbitkan, atau menyediakan Sertifikat Tanda Tangan Elektronik untuk tujuan penipuan atau melawan hukum apa pun akan dihukum dengan pidana penjara paling lama dua tahun, atau denda paling banyak satu lakh rupee, atau keduanya.

Pasal 75 Undang-undang untuk mengajukan tuntutan atas pelanggaran atau tindak pidana yang dilakukan di luar India Berpedoman pada ketentuan ayat (2), ketentuan Undang-undang ini juga berlaku untuk setiap pelanggaran atau tindak pidana yang dilakukan di luar India oleh siapa pun tanpa memandang kewarganegaraannya. Untuk tujuan ayat (1), Undang-undang ini akan berlaku untuk pelanggaran atau tindak pidana yang dilakukan di luar India oleh siapa pun jika tindakan atau perilaku yang merupakan pelanggaran atau tindak pidana tersebut melibatkan komputer, sistem komputer, atau jaringan komputer yang berlokasi di India.

**TABEL 4.1 KEJAHATAN DUNIA MAYA UMUM DAN KETENTUAN HUKUM YANG BERLAKU: GAMBARAN UMUM**

| S.No. | Kejahatan dunia maya | Ketentuan yang Berlaku |
|---|---|---|
| 1. | Pelecehan melalui profil publik palsu di situs jejaring sosial: Profil palsu seseorang dibuat di situs jejaring sosial dengan alamat, informasi tempat tinggal, atau detail kontak yang benar, tetapi dia dicap sebagai 'pelacur' atau orang yang 'berkarakter tidak senonoh'. Hal ini menyebabkan pelecehan terhadap korban. | Pasal 66A, Pasal 67 UU ITE dan Pasal 509 KUHP. |
| 2. | Komunitas Kebencian Online: Komunitas kebencian online dibuat dengan tujuan menghasut kelompok agama untuk melakukan tindakan | Pasal 66A UU ITE dan Pasal 153A & 153B KUHP. |
| 3. | Peretasan Akun Email : Jika akun email korban diretas dan email tidak senonoh dikirim ke orang-orang di buku alamat korban | Pasal 43, 66, 66A, 66C, 67, 67A, dan 67B Undang-Undang Teknologi Informasi. |
| 4. | Penipuan Kartu Kredit: Korban yang tidak menaruh curiga akan menggunakan komputer yang terinfeksi untuk melakukan transaksi daring. | Pasal 43, 66, 66C, 66D UU ITE dan pasal 420 KUHP. |
| 5. | Perusakan Web: Halaman beranda situs web diganti dengan halaman yang mengandung unsur pornografi atau pencemaran nama baik. | Pasal 43 dan 66 UU PPh dan Pasal 66F, 67 dan 70 UU PPh juga berlaku dalam beberapa kasus. |

| | | |
|---|---|---|
| | Situs pemerintah biasanya menghadapi amukan peretas pada hari-hari simbolis. | |
| 6. | Memperkenalkan Virus, Worm, Backdoor, Rootkit, Trojan, Bug: Semua hal di atas adalah beberapa jenis program jahat yang digunakan untuk menghancurkan atau mendapatkan akses ke beberapa informasi elektronik. | Pasal 43, 66, 66A UU ITE dan Pasal 426 KUHP. |
| 7. | Terorisme Dunia Maya: Banyak teroris menggunakan hard drive virtual (G-Drive, situs FTP) dan media penyimpanan fisik (USB) untuk menyembunyikan informasi dan catatan bisnis terlarang mereka. | Hukum terorisme konvensional dapat berlaku bersama dengan Pasal 69 UU IT. |
| 8. | Penjualan barang ilegal secara daring: Penjualan narkotika, obat-obatan terlarang, senjata, dan satwa liar yang difasilitasi oleh Internet | Umumnya hukum konvensional berlaku dalam kasus ini. |
| 9. | Pornografi Siber: Salah satu bisnis terbesar di Internet. Pornografi mungkin tidak ilegal di banyak negara, tetapi pornografi anak dilarang secara umum. | Bagian 67, 67A, dan 67B dari UU TI. |
| 10. | Phishing dan Penipuan Email: Phishing melibatkan upaya penipuan untuk memperoleh informasi sensitif dengan menyamarkan situs sebagai entitas tepercaya. (Misalnya, Kata Sandi, informasi kartu kredit) | Bagian 66, 66A, dan 66D UU ITE dan Bagian 420 KUHP |
| 11. | Pencurian Informasi Rahasia: Banyak organisasi bisnis menyimpan informasi rahasia mereka dalam sistem komputer. Informasi ini menjadi incaran para pesaing, penjahat, dan karyawan yang tidak puas. | Pasal 43, 66, 66B UU TI dan Pasal 426 KUHP. |
| 12. | Pencurian Kode Sumber: Kode sumber umumnya merupakan aset "permata mahkota" yang paling didambakan dan penting bagi sebuah perusahaan. | Pasal 43, 66, 66B UU IT dan Pasal 63 UU Hak Cipta. |
| 13. | Penghindaran Pajak dan Pencucian Uang: Pencuci uang dan orang-orang yang melakukan kegiatan bisnis ilegal menyembunyikan informasi mereka dalam aktivitas virtual maupun fisik. | Undang-Undang Pajak Penghasilan dan Undang-Undang Pencegahan Pencucian Uang. Undang-Undang TI dapat berlaku berdasarkan kasus. |
| 14. | Penipuan Perdagangan Saham Online: Investor kini diwajibkan untuk menghubungkan akun | Pasal 43, 66, 66C, 66D UU ITE dan Pasal 420 KUHP |

| | | |
|---|---|---|
| | demat mereka dengan akun perbankan online mereka yang umumnya diakses tanpa izin, sehingga menyebabkan penipuan perdagangan saham. | |

## 4.2 TANGGUNG JAWAB PERDATA BERDASARKAN UU IT, 2000

Konsep tanggung jawab yang masih harus dibayar hanya berlaku untuk hukum substantif dan tidak berlaku untuk hukum prosedural karena tidak seorang pun dapat mengklaim hak yang sah dalam prosedur tersebut. Di India, kami memiliki hukum substantif dan prosedural. Kitab Undang-Undang Hukum Pidana dan Undang-Undang Teknologi Informasi adalah hukum substantif sedangkan Undang-Undang Pembuktian, Kitab Undang-Undang Hukum Acara Pidana, dan Kitab Undang-Undang Hukum Acara Perdata adalah hukum prosedural. Dengan demikian, berdasarkan hukum retrospektif, prosedur tersebut dapat diubah, diubah, atau bahkan dicabut. Demikian pula, perlindungan Pasal 20(1) tersedia untuk dan dapat dicari terhadap masalah pidana saja dan tidak berlaku untuk masalah perdata. Dengan demikian, tanggung jawab perdata dapat ditingkatkan dengan efek retrospektif.

**Perlindungan Data**

Menurut Pasal: 43 siapa pun yang menghancurkan, menghapus, mengubah, dan mengganggu atau menyebabkan gangguan pada komputer mana pun dengan maksud merusak seluruh data sistem komputer tanpa izin dari pemilik komputer, akan dikenakan denda hingga 1 crore kepada orang yang terkena dampak sebagai ganti rugi. Pasal 43A yang disisipkan oleh ‘Undang-Undang Teknologi Informasi (Amandemen), 2008 menyatakan bahwa jika suatu badan hukum memelihara dan melindungi data orang-orang sebagaimana ditetapkan oleh pemerintah pusat, jika ada tindakan lalai atau kegagalan dalam melindungi data/informasi maka badan hukum tersebut akan dikenakan ganti rugi kepada orang yang terkena dampak.

Dan Pasal 66 mengatur tentang ‘peretasan dengan sistem komputer’ dan memberikan hukuman penjara hingga 3 tahun atau denda, yang dapat diperpanjang hingga 2 tahun atau keduanya. Pasal 43A UU TI membahas aspek kompensasi atas kegagalan melindungi data. Pemerintah Pusat belum menetapkan istilah 'data pribadi yang sensitif', dan juga belum menetapkan praktik keamanan yang standar dan wajar. Hingga ketentuan ini dibuat, data diberikan keamanan dan perlindungan hanya sebagaimana yang ditetapkan dalam perjanjian antara para pihak atau sebagaimana yang ditetapkan dalam undang-undang apa pun.

Namun, Penjelasan (ii) untuk Pasal 43A dirumuskan sedemikian rupa sehingga tidak ada kejelasan apakah bank (atau badan hukum mana pun) dapat membuat perjanjian yang menetapkan standar yang lebih rendah daripada yang ditetapkan oleh Pemerintah Pusat dan jika terjadi pertentangan (antara standar yang ditetapkan oleh Pemerintah Pusat dan yang ada dalam perjanjian) yang akan berlaku. Apakah kelalaian atau mala fide di pihak nasabah akan membuat lembaga keuangan bertanggung jawab tanpa kesalahannya atau apakah dengan memberikan terlalu banyak perlindungan kepada bank, nasabah dibuat menderita adalah dua situasi ekstrem.

Kebutuhannya adalah untuk mencapai keseimbangan antara perlindungan konsumen dan perlindungan bank dari tanggung jawab karena bukan kesalahan mereka. Selain memberikan perlindungan terhadap data pribadi (data pribadi yang sensitif - 43A), UU IT, 2000 juga menetapkan tanggung jawab perdata dan pidana (masing-masing Pasal 43 dan Pasal 66) kepada setiap orang yang tanpa izin dari pemilik atau orang lain yang bertanggung jawab atas komputer, sistem komputer, dll., antara lain, mengunduh, menyalin atau mengekstrak data apa pun atau merusak atau menyebabkan kerusakan basis data komputer apa pun, dll. Dalam konteks ini, Pasal 72 dan 72A dari UU IT yang diamandemen, 2000 juga relevan. Pasal 72 UU tersebut menetapkan hukuman jika setiap orang yang, sesuai dengan kewenangan yang diberikan berdasarkan UU IT, 2000, telah mengamankan akses ke catatan elektronik, informasi, dll.

Tanpa persetujuan dari orang yang bersangkutan mengungkapkan informasi tersebut kepada orang lain maka ia akan dihukum dengan penjara hingga dua tahun atau dengan denda hingga satu lakh atau dengan keduanya. Di sisi lain, Pasal 72A memberikan hukuman atas pengungkapan oleh siapa pun, termasuk perantara, yang melanggar kontrak yang sah. Cakupan Pasal 72A lebih luas daripada Pasal 72 dan mencakup pengungkapan informasi pribadi seseorang (tanpa persetujuan) saat memberikan layanan berdasarkan kontrak yang sah dan bukan sekadar pengungkapan informasi yang diperoleh berdasarkan kewenangan yang diberikan berdasarkan UU IT tahun 2000.

**Analisis Kritis: Yurisdiksi Komparatif**

Namun, upaya tersebut sangat terbatas dan sarat dengan kekurangan sehingga masih diperlukan undang-undang perlindungan data yang tepat. Mengingat usulan dimulainya skema UID, khususnya, ada kebutuhan mendesak akan undang-undang yang kuat dan cerdas dalam hal ini. Sebagian besar rezim negara lain dengan jelas melakukan setidaknya hal berikut:

1. Menetapkan dan mengklasifikasikan jenis data (misalnya, di sebagian besar negara Eropa, data pribadi adalah data yang mengidentifikasi seseorang, data pribadi sensitif adalah data yang mengungkapkan rincian etnis, agama, kesehatan, seksualitas, opini politik, dll.),
2. Menyempurnakan sifat perlindungan terhadap kategori data (misalnya, standar perawatan yang lebih besar terkait data pribadi sensitif),
3. Menerapkan secara setara pada data yang disimpan secara offline dan manual seperti pada data yang disimpan pada sistem komputer,
4. Membedakan antara pengendali data (yaitu, orang yang mengambil keputusan mengenai data) dan pemroses data (yaitu, orang yang memproses data berdasarkan instruksi pengendali data),
5. Menetapkan batasan yang jelas pada cara pengumpulan data (misalnya, harus diperoleh secara adil dan sah),
6. Memberikan pedoman yang jelas tentang tujuan penggunaan data tersebut dan oleh siapa (sering kali melibatkan persyaratan persetujuan yang memberikan individu tingkat kontrol yang lebih besar atas data mereka),

7. Memerlukan standar dan langkah-langkah teknis seputar pengumpulan, penyimpanan, akses, perlindungan, retensi, dan pemusnahan data,
8. Memastikan bahwa penggunaan data memadai, relevan, dan tidak berlebihan mengingat tujuan pengumpulannya,
9. Memenuhi rezim jenis opt-in dan opt-out, sekali lagi untuk memberi individu ukuran kontrol atas penggunaan data mereka bahkan setelah tahap pengumpulan awal (yang berdampak besar pada telemarketing invasif atau komunikasi tertulis yang tidak diminta),
10. Menetapkan persyaratan pengetahuan dan prosedur untuk memungkinkan individu mencari informasi tentang data apa yang disimpan tentang mereka, dan
11. Membuat perlindungan dan hukuman yang disesuaikan dengan baik untuk pelanggaran salah satu hal di atas.
12. Sayangnya, dan mungkin dapat dimengerti, ITA baru mulai menyentuh permukaan dari apa yang dimaksud dengan rezim perlindungan data yang baik. Ketentuan yang diperkenalkan (bagian 43-A dan 72-A) memiliki kekurangan yang mencolok, yaitu sebagai berikut:
13. Istilah data atau informasi pribadi yang sensitif digunakan tanpa pandang bulu tanpa definisi apa pun,
14. Ketentuan tersebut hanya mencakup data dan catatan elektronik, bukan data yang disimpan dalam sistem atau media non-elektronik,
15. Ketentuan tersebut tidak memberikan panduan tentang sebagian besar prinsip yang ditetapkan di atas seperti yang berkaitan dengan keakuratan, kecukupan, persetujuan, tujuan, dll.,
16. Jika tidak ada perbedaan antara pengendali dan pemroses, tanggung jawab dibebankan kepada orang-orang, yang tidak selalu berada dalam posisi untuk mengendalikan data, meskipun data tersebut ada dalam kepemilikan mereka,
17. Tanggung jawab perdata atas pelanggaran data hanya muncul jika ada kelalaian (misalnya, kegagalan untuk memiliki prosedur keamanan atau kegagalan untuk menerapkannya dengan benar tidak akan secara otomatis mengakibatkan kerugian kecuali kelalaian terbukti),
18. Demikian pula, tanggung jawab pidana hanya berlaku untuk kasus informasi yang diperoleh dalam konteks kontrak layanan, dan memerlukan unsur kesengajaan, atau pengungkapan tanpa persetujuan atau melanggar kontrak yang sah – ini adalah kewenangan yang sangat terbatas yang sebagian besar ditujukan untuk mencegah karyawan yang tidak puas atau tidak bermoral dalam menangani data perusahaan/pelanggan.

Selain kritik yang ditujukan pada ketentuan perlindungan data, sebagian besar kekhawatiran lainnya terkait dengan implikasi kebebasan sipil dari ITA. Ada beberapa kengerian yang diungkapkan di berbagai forum dan media tentang ITA yang berkontribusi pada pertumbuhan negara polisi, pembatasan berat kebebasan berbicara dan berekspresi, pelanggaran privasi, dan hukuman yang tidak proporsional untuk pelanggaran yang dilakukan di dunia maya

dibandingkan dengan kejahatan yang dilakukan di masa kini. Sayangnya, hal ini sebagian besar benar mengingat penanganan yang kikuk terhadap terorisme siber, pra-sensor yang tidak dapat ditoleransi yang dimungkinkan oleh pemblokiran situs web, pendekatan yang luas terhadap pemantauan dan pengumpulan data, dan kewajiban yang menuntut dari para perantara untuk bekerja sama dengan intersepsi, pemantauan, dan dekripsi data karena alasan yang tidak dijelaskan dengan baik.

Meskipun bab hak asasi Konstitusi kita, yang mengabadikan hak-hak dasar, demokratis, dan mendalam tertentu, mungkin tidak memiliki kosakata yang sama tentang proses hukum seperti yang kita lihat di AS, namun tetap saja hal itu mengharuskan pembatasan yang masuk akal. Preseden dan yurisprudensi yang lebih luas di bidang tersebut telah lebih jauh mengembangkan konsep checks and balances, perlindungan prosedural, dan legitimasi pembatasan yang harus diberikan oleh demokrasi yang berfungsi seperti India kepada rakyatnya. Dapat dikatakan bahwa beberapa ketentuan ITA menyebabkan ketegangan yang signifikan dengan hak atas kebebasan berbicara dan berekspresi, hak terhadap pembuktian diri sendiri, hak atas kesetaraan di hadapan hukum, dan hak untuk menjalankan perdagangan atau profesi.

**Privasi dan pengawasan**

Topik ini menyatukan berbagai masalah seputar pemantauan menyeluruh dan pengumpulan data atau informasi lalu lintas, penyadapan dan dekripsi (di bawah tekanan) oleh perantara (sekarang merupakan kumpulan besar ISP, mesin pencari, kafe internet, situs lelang daring, pasar daring, dll.) dan definisi luas terorisme dunia maya (yang secara menggelikan bahkan menjadikan pencemaran nama baik sebagai aktivitas teroris).

Beberapa masalah umum terkait dengan penyadapan, pemantauan, dan dekripsi dalam (bagian 69) adalah:

a) Tidak ada ketentuan tentang hubungan yang jelas antara perantara dan informasi atau sumber daya yang hendak dipantau atau disadap,
b) Pengecualian yang diakui secara internasional terhadap tanggung jawab hukum ketika perantara beroperasi murni sebagai penghubung dan tidak memiliki kendali atas data yang mengalir melalui jaringannya tidak dijabarkan dengan jelas,
c) Hukuman atas ketidak-kerjasamaan sangat berat, terutama mengingat tidak adanya a) dan b) di atas,
d) Hukuman yang berat ini dapat dikatakan melanggar Pasal 14 karena tampaknya sama sekali tidak proporsional. Pelanggaran dan upaya hukum serupa dalam Kitab Undang-Undang Hukum Acara Pidana atau Kitab Undang-Undang Hukum Pidana India menetapkan hukuman yang lebih ringan, dengan urutan besarnya yang sebenarnya. Jika satu-satunya perbedaan antara pelanggaran adalah media tempat informasi tersebut dimuat, maka tampaknya sewenang-wenang untuk menjatuhkan hukuman yang jauh lebih berat kepada perantara daring daripada kepada anggota masyarakat yang, misalnya, memberikan informasi palsu kepada polisi sehubungan dengan persidangan atau penyelidikan.

e) Aturan yang dibuat terkait pemantauan, penyadapan, dan dekripsi menawarkan sejumlah perlindungan prosedural, yaitu dengan memberlakukan batas waktu berapa lama arahan untuk penyadapan atau pemantauan dapat tetap berlaku, batasan berapa lama data dapat disimpan sebelum harus dimusnahkan, dll. Akan tetapi, efeknya sangat berkurang dengan pengecualian untuk persyaratan fungsional, dll. Ironi yang mengherankan adalah bahwa aturan 20 mengharuskan perantara untuk menjaga 'kerahasiaan yang ekstrem', 'kehati-hatian dan tindakan pencegahan yang sangat besar' dalam hal penyadapan, pemantauan, atau dekripsi informasi karena hal tersebut memengaruhi privasi warga negara.

Senada dengan itu, ada kekhawatiran seputar pemantauan dan pengumpulan data lalu lintas (Bagian 69B) karena bagian tersebut memuat daftar alasan pemantauan yang sangat panjang. Ini termasuk hal-hal yang sangat berlebihan seperti perkiraan insiden siber yang akan terjadi, pemantauan aplikasi jaringan dengan data lalu lintas atau informasi tentang sumber daya komputer, identifikasi dan penentuan virus/kontaminan komputer, dan hal-hal lain yang berkaitan dengan keamanan siber.

Terakhir, kritik utama terhadap pendekatan ITA terhadap terorisme siber adalah jaring yang sangat luas yang ingin dilemparnya, mencari permainan yang tidak ada hubungannya sama sekali dengan pelanggaran yang disebutkan. Di antara makhluk-makhluk yang tidak sengaja tertangkap selama ekspedisi penangkapan ikan ini, kami menemukan beberapa korban yang tidak terduga. Selain alasan pelanggaran yang biasa terhadap kedaulatan, keamanan nasional, pertahanan India, dll., yang telah kita lihat terkait dengan pasal-pasal lain, ITA menganggap hal-hal berikut sebagai tindakan terorisme siber secara umum, akses tidak sah ke informasi yang mungkin menyebabkan:

1. Kerugian terhadap kesopanan,
2. Kerugian terhadap moralitas,
3. Kerugian terkait penghinaan terhadap pengadilan, dan
4. Kerugian terkait pencemaran nama baik.

Hal ini hampir menggelikan jika alasan-alasan ini tidak ditetapkan menjadi undang-undang, yang mengancam kebebasan sipil karena keberadaannya. Negara-negara lain memiliki beberapa gagasan tentang ideologi politik, kasus agama, dll. dalam pandangan mereka tentang terorisme. Undang-Undang India tentang Teknologi Informasi dan Komunikasi telah dimasukkan ke dalam klausul yang memberlakukan hukuman terberat dalam seluruh ITA (penjara seumur hidup) yang bahkan lebih mengkhawatirkan.

## 4.3 TANGGUNG JAWAB PERDATA BAGI PERUSAHAAN

Tanggung jawab perdata bagi perusahaan dalam konteks perlindungan data di Indonesia sangat relevan dengan ketentuan yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Dalam hal ini, perusahaan memiliki kewajiban untuk mematuhi norma perlindungan data pribadi dan dapat dikenakan kewajiban untuk membayar kompensasi jika terjadi pelanggaran terhadap hak subjek data pribadi. Pasal 12 ayat (1) UU PDP mengatur bahwa subjek data

pribadi berhak menggugat dan menerima ganti rugi apabila terjadi kebocoran data pribadi. Selain itu, perusahaan juga diwajibkan untuk memberitahukan pengguna dan lembaga terkait dalam waktu maksimal 3x24 jam jika terjadi kebocoran data.

Kegagalan untuk memenuhi kewajiban ini dapat berakibat pada sanksi administratif dan kewajiban kompensasi. Selain itu, perusahaan juga harus memastikan perlindungan data pribadi dari akses, pengungkapan, dan pengubahan yang tidak sah, dan apabila perusahaan lalai dalam menjaga keamanan data hingga menyebabkan kebocoran, mereka dapat dimintai pertanggungjawaban secara perdata. UU PDP juga menetapkan sanksi administratif yang dapat berupa denda hingga 2% dari pendapatan tahunan perusahaan bagi yang melanggar ketentuan perlindungan data. Selain tanggung jawab perdata, perusahaan juga memiliki kewajiban untuk memperbaiki sistem keamanan mereka jika terjadi kebocoran data, termasuk dengan melakukan investasi pada teknologi keamanan dan pelatihan untuk karyawan. Dengan demikian, perusahaan harus sangat serius dalam mematuhi kewajiban-kewajiban ini karena kegagalan dalam melindungi data pribadi tidak hanya mengakibatkan konsekuensi finansial, tetapi juga dapat merusak reputasi perusahaan dan menurunkan kepercayaan publik.

Sebagaimana disebutkan di atas, setiap perusahaan yang gagal mematuhi norma perlindungan data dapat dikenakan kewajiban untuk membayar kompensasi jika:

a) Lalai dalam menerapkan dan memelihara praktik keamanan yang wajar, dan karenanya
b) Menyebabkan kerugian atau keuntungan yang tidak sah bagi siapa pun

## 4.4 KEJAHATAN DUNIA MAYA BERDASARKAN KUHP DAN UNDANG-UNDANG KHUSUS

**Kitab Undang-Undang Hukum Pidana India, 1860**

Biasanya disebut sebagai KUHP, ini adalah undang-undang yang sangat kuat dan mungkin yang paling banyak digunakan dalam yurisprudensi pidana, yang berfungsi sebagai KUHP utama di India. Awalnya ditetapkan pada tahun 1860 dan diamandemen berkali-kali sejak saat itu, KUHP mencakup hampir semua aspek substantif hukum pidana dan dilengkapi dengan ketentuan pidana lainnya. Di India yang merdeka, banyak undang-undang khusus telah ditetapkan dengan ketentuan pidana dan pidana yang sering dirujuk dan diandalkan, sebagai ketentuan hukum tambahan dalam kasus-kasus yang merujuk pada ketentuan KUHP yang relevan juga.

Kitab Undang-Undang Hukum Pidana India diamandemen dengan memasukkan kata 'elektronik' sehingga memperlakukan catatan dan dokumen elektronik setara dengan catatan dan dokumen fisik. Bagian yang mengatur tentang entri palsu dalam catatan atau dokumen palsu, dsb. Sejak saat itu telah diubah menjadi 'catatan elektronik dan dokumen elektronik' dengan demikian masuk dalam lingkup KUHP. Sekarang, catatan elektronik dan dokumen elektronik telah diperlakukan sama seperti catatan dan dokumen fisik selama dilakukannya tindakan pemalsuan atau pemalsuan catatan fisik dalam suatu tindak pidana. Setelah amandemen di atas, lembaga penyidik mengajukan kasus/surat dakwaan dengan mengutip bagian-bagian yang relevan dari KUHP berdasarkan pasal 463, 464, 468 dan 469 yang

dibacakan bersama dengan ITA/ITAA berdasarkan Pasal 43 dan 66 dalam pelanggaran serupa untuk memastikan bukti dan/atau hukuman dapat dicakup dan dibuktikan berdasarkan salah satu dari undang-undang ini atau berdasarkan kedua undang-undang tersebut.

1. Mengirim pesan yang mengancam melalui email - Pasal 503 KUHP
2. Mengirim pesan yang mencemarkan nama baik melalui email - Pasal 499 KUHP
3. Pemalsuan catatan elektronik - Pasal 463 KUHP
4. Situs web palsu, penipuan dunia maya - Pasal 420 KUHP
5. Pemalsuan email - Pasal 463 KUHP
6. Perampokan situs web - Pasal 383 KUHP
7. Penyalahgunaan email - Pasal 500 KUHP

**Kejahatan dunia maya berdasarkan Undang-Undang Khusus**

a) Penjualan Obat-obatan Terlarang secara daring - Undang-Undang Obat-obatan Terlarang dan Zat Psikotropika, 1985.
b) Penjualan Senjata secara daring – Undang-Undang Persenjataan, 1959.

**KUHP Pidana di Indonesia**

Kejahatan dunia maya di Indonesia diatur oleh berbagai perundang-undangan, terutama oleh Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Kedua undang-undang ini memberikan dasar hukum untuk menanggulangi berbagai jenis kejahatan yang terjadi di dunia maya. Dalam Kitab Undang-Undang Hukum Pidana (KUHP), beberapa pasal dapat diterapkan untuk menangani kejahatan dunia maya, meskipun tidak secara khusus mengatur mengenai kejahatan tersebut. Pasal 362 KUHP yang mengatur tentang pencurian, misalnya, dapat digunakan untuk menuntut pencurian data atau informasi yang dilakukan melalui internet. Pasal 378 mengenai penipuan juga relevan untuk menangani kasus penipuan online, seperti carding, di mana pelaku memanipulasi identitas untuk keuntungan pribadi. Selain itu, Pasal 406 KUHP yang mengatur tentang perusakan dapat diterapkan dalam kasus perusakan sistem komputer atau hacking yang merusak sistem milik orang lain. Namun, meskipun beberapa ketentuan dalam KUHP dapat diterapkan, banyak ahli hukum yang berpendapat bahwa hukum pidana konvensional tidak sepenuhnya memadai untuk mengatasi kompleksitas kejahatan siber yang terus berkembang, mengingat sifat kejahatan dunia maya yang sering kali tidak terdefinisi secara jelas dalam ketentuan yang ada.

Berbeda dengan KUHP, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) secara khusus mengatur tentang kejahatan dunia maya. UU ITE memberikan pengaturan yang lebih rinci dan spesifik mengenai berbagai bentuk kejahatan dunia maya, seperti penipuan elektronik, pencurian data, dan penyebaran konten ilegal. Pasal-pasal dalam UU ITE menetapkan definisi yang lebih jelas mengenai tindakan-tindakan tersebut, serta sanksi pidana yang sesuai, termasuk hukuman penjara dan denda. Sebagai contoh, Pasal 30 jo. Pasal 46 UU ITE mengatur mengenai pencurian data melalui sistem elektronik, sementara Pasal 32 jo. Pasal 48 mengatur penipuan dalam transaksi online. Meskipun demikian, mengingat perkembangan teknologi yang sangat cepat dan modus operandi kejahatan dunia maya yang terus berubah, UU ITE perlu diperbarui agar tetap efektif dalam menanggulangi kejahatan

siber. Rancangan revisi UU ITE dan pembaruan dalam konsep Kitab Undang-Undang Hukum Pidana (KUHP) baru tengah dibahas untuk menyesuaikan diri dengan tantangan hukum yang muncul akibat kemajuan teknologi.

Secara keseluruhan, kejahatan dunia maya di Indonesia diatur melalui kombinasi KUHP dan UU ITE, namun penegakan hukum di bidang ini menghadapi tantangan yang cukup besar. Penegak hukum perlu beradaptasi dengan perkembangan teknologi dan terus memperbarui kerangka hukum agar dapat lebih efektif dalam menangani kejahatan siber yang semakin kompleks dan beragam.

# BAB 5
# KEJAHATAN SIBER

## 5.1 PENDAHULUAN

Kejahatan siber merupakan salah satu isu yang semakin mendesak di era digital saat ini, di mana teknologi informasi dan komunikasi telah menjadi bagian integral dari kehidupan sehari-hari. Kejahatan siber mencakup berbagai tindakan kriminal yang dilakukan dengan memanfaatkan teknologi komputer dan jaringan internet, seperti penipuan online, pencurian identitas, peretasan, penyebaran virus, dan pelanggaran data. Dengan meningkatnya penggunaan internet dan perangkat digital, kejahatan siber telah berkembang menjadi ancaman serius bagi individu, perusahaan, dan bahkan negara.

Kejahatan ini tidak hanya merugikan secara finansial tetapi juga dapat mengancam privasi dan keamanan data pribadi. Dalam konteks hukum, penanganan kejahatan siber memerlukan kerjasama lintas negara karena sifatnya yang global dan kompleks. Di Indonesia, upaya untuk memberantas kejahatan siber dilakukan melalui berbagai regulasi dan undang-undang, termasuk Undang-Undang Informasi dan Transaksi Elektronik (ITE) yang bertujuan untuk memberikan perlindungan hukum terhadap pengguna internet serta menindak pelaku kejahatan siber. Namun, tantangan masih ada dalam hal penegakan hukum dan kesadaran masyarakat mengenai risiko serta dampak dari kejahatan siber. Oleh karena itu, edukasi dan peningkatan literasi digital sangat penting untuk mencegah terjadinya kejahatan siber di masa depan.

## 5.2 PUTUSAN KASUS DI BEBERAPA NEGARA

### 1. Kasus Pencurian Data dan Penipuan Online

**Latar Belakang Kasus**

Seorang karyawan di sebuah bank di Indonesia, yang memiliki akses ke sistem komputer bank, melakukan tindakan penipuan dengan memanipulasi data dalam sistem akuntansi. Karyawan tersebut menciptakan entri palsu dan menarik uang dari rekening bank menggunakan cek yang dipalsukan. Dalam prosesnya, ia berhasil menarik sejumlah uang yang cukup besar dari bank.

Pelanggaran Hukum

Kasus ini dapat dikenakan pasal-pasal berikut dalam KUHP dan UU ITE:

1. **Pasal 378 KUHP** - **Penipuan:**
   - Karyawan tersebut dapat dikenakan pasal ini karena telah melakukan penipuan dengan cara memalsukan dokumen dan menarik uang secara tidak sah dari bank.
2. **Pasal 362 KUHP** - **Pencurian:**
   - Tindakan karyawan yang mengambil uang dari bank tanpa izin dapat dikategorikan sebagai pencurian.
3. **Pasal 465 KUHP** - **Pemalsuan:**

- Dengan memalsukan cek dan dokumen lainnya, karyawan tersebut melanggar pasal ini.

4. **Pasal 30 UU ITE** - **Akses ilegal:**
   - Jika karyawan tersebut mengakses sistem komputer bank tanpa izin atau melampaui batas aksesnya, ia dapat dikenakan sanksi berdasarkan UU ITE.
5. **Pasal 32 UU ITE** - **Penipuan elektronik:**
   - Tindakan penipuan yang dilakukan melalui media elektronik juga diatur dalam UU ITE, sehingga pelaku dapat dikenakan sanksi sesuai dengan pasal ini.
6. **Pasal 65 UU ITE** - **Penghancuran data:**
   - Jika terdapat tindakan merusak atau mengubah data elektronik yang ada di sistem bank, pelaku juga dapat dikenakan pasal ini.

**Proses Hukum**

Setelah pengaduan diajukan oleh pihak bank, penyelidikan dilakukan oleh kepolisian. Bukti-bukti seperti rekaman transaksi, saksi-saksi dari pihak bank, dan dokumen pendukung lainnya dikumpulkan untuk membuktikan kesalahan pelaku. Jika terbukti bersalah, pelaku dapat dijatuhi hukuman penjara dan denda sesuai dengan ketentuan hukum yang berlaku.

**Kesimpulan**

Kasus pencurian data dan penipuan online ini menunjukkan bagaimana kejahatan dunia maya dapat merugikan institusi keuangan dan individu. Dengan adanya UU ITE dan KUHP, penegakan hukum terhadap kejahatan siber menjadi lebih terstruktur, meskipun tantangan dalam implementasi tetap ada. Penegak hukum harus terus beradaptasi dengan perkembangan teknologi untuk menangani kejahatan dunia maya secara efektif.

**2. Kasus Pelecehan Seksual Di Lingkungan Kerja**

Kasus nyata yang relevan di Indonesia yang mencerminkan isu eksploitasi seksual dan pelanggaran hukum terkait adalah kasus "Pelecehan Seksual di Lingkungan Kerja". Kasus ini melibatkan seorang pegawai negeri sipil (PNS) yang mengalami pelecehan seksual oleh atasan di tempat kerjanya. Kasus ini menunjukkan pelanggaran terhadap beberapa pasal dalam undang-undang yang berlaku di Indonesia.

**Pasal-Pasal yang Berlaku**

1. **Pasal 281 KUHP**: Mengatur tentang perbuatan cabul yang dilakukan oleh seseorang dengan cara memaksa orang lain untuk melakukan perbuatan cabul.
2. **Pasal 285 KUHP**: Mengatur tentang pemerkosaan, yang dapat dikenakan sanksi berat bagi pelaku.
3. **Pasal 6 Undang-Undang Nomor 23 Tahun 2004 tentang Penghapusan Kekerasan Dalam Rumah Tangga (PKDRT)**: Meskipun berfokus pada kekerasan dalam rumah tangga, pasal ini juga mencakup bentuk kekerasan seksual di luar rumah tangga.
4. **Pasal 8 UU No. 39 Tahun 1999 tentang Hak Asasi Manusia**: Menyatakan bahwa setiap orang berhak untuk tidak mengalami perlakuan diskriminatif, termasuk dalam konteks seksual.

5. **Pasal 32 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**: Mengatur tentang larangan penyebaran konten pornografi dan pelecehan seksual melalui media elektronik.

**Rincian Kasus**

Dalam kasus ini, korban melaporkan bahwa atasan melakukan tindakan pelecehan seksual secara verbal dan fisik selama periode tertentu. Setelah pengaduan diajukan, pihak berwenang melakukan penyelidikan berdasarkan laporan tersebut. Proses hukum kemudian berjalan melalui pengadilan, di mana terdakwa dihadapkan pada tuduhan berdasarkan pasal-pasal yang disebutkan di atas.Pengadilan memutuskan untuk memberikan sanksi kepada pelaku dengan mempertimbangkan bukti-bukti yang ada, termasuk kesaksian korban dan saksi lainnya. Kasus ini menyoroti pentingnya perlindungan hukum bagi korban kekerasan seksual dan penegakan hukum terhadap pelaku.Kasus ini juga mencerminkan tantangan dalam sistem peradilan Indonesia terkait dengan stigma sosial dan perlunya reformasi dalam penanganan kasus-kasus pelecehan seksual agar lebih sensitif terhadap kebutuhan korban.

**3. Kasus Penjualan Konten Ilegal di E-Commerce**

**Fakta Kasus:** Sebuah platform e-commerce di Indonesia, sebut saja "TokoOnline", menghadapi masalah ketika pengguna menjual barang-barang ilegal, termasuk barang-barang yang melanggar hak cipta dan konten pornografi. Salah satu produk yang terdaftar adalah video dewasa yang dijual secara daring.

**Masalah Hukum:**

- TokoOnline dituduh tidak mengambil tindakan cepat untuk menghapus konten ilegal setelah mendapat laporan.
- Pengacara dari pihak penuntut berargumen bahwa TokoOnline memiliki tanggung jawab untuk memantau dan menghapus konten yang melanggar hukum.

**Pertimbangan Pengadilan:**

- Pengadilan mempertimbangkan bahwa TokoOnline tidak secara langsung menerbitkan konten tersebut, mirip dengan pertimbangan dalam kasus Bajaj, di mana tidak ada bukti bahwa CEO secara langsung terlibat dalam publikasi materi cabul.
- TokoOnline menunjukkan bahwa mereka telah mengambil langkah-langkah untuk memperbaiki situasi dengan menghapus produk tersebut dalam waktu 24 jam setelah laporan diterima.

**Keputusan:**

Pengadilan memutuskan untuk memberikan jaminan kepada TokoOnline dengan syarat bahwa mereka harus lebih proaktif dalam memantau konten yang dijual di platform mereka dan wajib melaporkan setiap pelanggaran kepada pihak berwenang.

**4. Kasus Penyebaran Konten Fitnah Melalui Media Sosial**

**Fakta Kasus:** Seorang pengguna media sosial di Indonesia membuat postingan yang menyebarkan informasi palsu tentang seorang pejabat publik, yang menyebabkan kerugian reputasi bagi pejabat tersebut. Pengguna tersebut ditangkap berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (ITE).

**Masalah Hukum:**

- Apakah platform media sosial bertanggung jawab atas konten yang diposting oleh pengguna?
- Apakah pengguna media sosial harus bertanggung jawab penuh atas konten yang mereka bagikan?

**Pertimbangan Pengadilan:**

- Pengadilan menilai bahwa meskipun platform media sosial tidak menerbitkan konten secara langsung, mereka memiliki tanggung jawab untuk mengatur dan mengawasi konten yang diposting oleh pengguna.
- Dalam hal ini, pengadilan juga mempertimbangkan langkah-langkah yang telah diambil oleh platform untuk menghapus konten tersebut setelah menerima laporan.

**Keputusan:**

Pengadilan memutuskan untuk menjatuhkan hukuman ringan kepada pengguna tersebut, tetapi juga memberikan peringatan kepada platform media sosial untuk lebih aktif dalam memantau dan menangani konten ilegal.

**Kesimpulan**

Kedua contoh kasus di atas mencerminkan tantangan hukum yang serupa dengan kasus Avnish Bajaj. Baik dalam konteks e-commerce maupun media sosial, pentingnya tanggung jawab penyedia layanan dalam mengawasi dan menangani konten ilegal menjadi sorotan utama. Keputusan pengadilan menunjukkan bahwa meskipun penyedia layanan tidak selalu dapat dianggap sebagai penerbit konten, mereka tetap memiliki kewajiban untuk menjaga integritas platform mereka dan melindungi masyarakat dari potensi bahaya.

**5. Syed Asifuddin dan Ors. vs. Negara Bagian Andhra Pradesh dan 29 Lainnya**

**Fakta**: Karyawan Tata Indicom ditangkap karena memanipulasi nomor elektronik 32-bit (ESN) yang diprogramkan ke dalam telepon seluler yang secara eksklusif diwaralabakan ke Reliance Infocomm. Pengadilan memutuskan bahwa manipulasi tersebut sama dengan merusak kode sumber komputer sebagaimana diatur dalam pasal 65 Undang-Undang Teknologi Informasi tahun 2000.

**Kasus:** Reliance Infocomm meluncurkan skema di mana pelanggan telepon seluler diberi telepon genggam digital senilai Rs. 10.500/- serta paket layanan selama 3 tahun dengan pembayaran awal sebesar Rs. 3350/- dan pembayaran bulanan sebesar Rs. 600/-. Pelanggan juga diberikan garansi 1 tahun dan asuransi 3 tahun untuk telepon genggam tersebut. Syaratnya adalah telepon genggam tersebut dikunci secara teknologi sehingga hanya dapat digunakan dengan layanan Reliance Infocomm. Jika pelanggan ingin meninggalkan layanan Reliance, ia harus membayar sejumlah biaya termasuk harga sebenarnya dari ponsel tersebut. Karena ponsel tersebut berkualitas tinggi, respons pasar terhadap skema tersebut sangat fenomenal.

Orang-orang yang tidak dikenal menghubungi pelanggan Reliance dengan tawaran untuk beralih ke skema Tata Indicom dengan harga yang lebih rendah. Sebagai bagian dari kesepakatan tersebut, ponsel mereka akan "dibuka" secara teknologi sehingga ponsel Reliance yang eksklusif dapat digunakan untuk layanan Tata Indicom. Pejabat Reliance mengetahui tentang "pembukaan kunci" oleh karyawan Tata ini dan mengajukan Laporan

Informasi Pertama (FIR) berdasarkan berbagai ketentuan dalam Kitab Undang-Undang Hukum Pidana India, Undang-Undang Teknologi Informasi, dan Undang-Undang Hak Cipta.
Polisi kemudian menggerebek beberapa kantor Tata Indicom di Andhra Pradesh dan menangkap beberapa pejabat Tata Tele Services Limited karena memprogram ulang telepon genggam Reliance.

Orang-orang yang ditangkap ini mendatangi Pengadilan Tinggi dan meminta pengadilan untuk membatalkan FIR dengan alasan bahwa tindakan mereka tidak melanggar ketentuan hukum tersebut.
Masalah yang diajukan oleh Pembela dalam kasus ini:

1. Pelanggan selalu dapat berpindah dari satu penyedia layanan ke penyedia layanan lainnya.
2. Pelanggan yang ingin berpindah dari Tata Indicom selalu membawa telepon genggamnya ke penyedia layanan lain untuk mendapatkan layanan dan melepaskan layanan Tata.
3. Telepon genggam yang dibawa ke Tata oleh pelanggan Reliance mampu menampung dua jalur terpisah dan dapat diaktifkan pada telepon genggam penugasan utama (NAM 1 atau NAM 2). Aktivasi NAM 1 atau NAM 2 oleh Tata sehubungan dengan telepon genggam yang dibawa oleh pelanggan Reliance tidak dianggap sebagai tindak pidana apa pun.
4. Telepon genggam bukanlah komputer atau sistem komputer yang berisi pemrogram komputer.
5. Tidak ada undang-undang yang berlaku yang mengharuskan pemeliharaan "kode sumber komputer". Oleh karena itu, pasal 65 Undang-Undang Teknologi Informasi tidak berlaku.

**Pengamatan Pengadilan**

1. Sesuai pasal 2 Undang-Undang Teknologi Informasi, setiap perangkat elektronik, magnetik, atau optik yang digunakan untuk menyimpan informasi yang diterima melalui satelit, gelombang mikro, atau media komunikasi lainnya, dan perangkat yang dapat diprogram dan mampu mengambil informasi apa pun dengan memanipulasi impuls elektronik, magnetik, atau optik adalah komputer yang dapat digunakan sebagai sistem komputer dalam jaringan komputer.
2. Instruksi atau program yang diberikan ke komputer dalam bahasa yang dikenal komputer tidak terlihat oleh pengguna komputer/konsumen fungsi komputer. Ini dikenal sebagai kode sumber dalam bahasa komputer.
3. Sebuah kota dapat dibagi menjadi beberapa sel. Seseorang yang menggunakan telepon dalam satu sel akan terhubung ke pemancar pusat penyedia telekomunikasi. Pemancar pusat ini akan menerima sinyal dan kemudian mengalihkannya ke telepon yang relevan.
4. Ketika orang tersebut berpindah dari satu sel ke sel lain di kota yang sama, sistem, yaitu Mobile Telephone Switching Office (MTSO) secara otomatis mentransfer sinyal dari menara ke menara.

5. Semua penyedia layanan telepon seluler memiliki kode khusus yang didedikasikan untuk mereka dan ini dimaksudkan untuk mengidentifikasi telepon, pemilik telepon, dan penyedia layanan.
6. Kode Identifikasi Sistem (SID) adalah nomor unik 5 digit yang diberikan kepada setiap operator oleh pemberi lisensi. Setiap operator telepon seluler diharuskan untuk mendapatkan SID dari Pemerintah India. SID diprogram ke dalam telepon saat seseorang membeli paket layanan dan mengaktifkan telepon tersebut.
7. Nomor Seri Elektronik (ESN) adalah nomor unik 32-bit yang diprogram ke dalam telepon saat diproduksi oleh produsen instrumen. ESN merupakan bagian permanen dari telepon.
8. Nomor Identifikasi Seluler (MIN) adalah nomor 10 digit yang berasal dari nomor telepon seluler yang diberikan kepada pelanggan. MIN diprogram ke dalam telepon saat seseorang membeli paket layanan.
9. Saat telepon seluler dinyalakan, telepon akan mendengarkan SID pada saluran kontrol, yang merupakan frekuensi khusus yang digunakan oleh telepon dan stasiun pangkalan untuk saling berkomunikasi tentang hal-hal seperti pengaturan panggilan dan perubahan saluran.
10. Jika telepon tidak dapat menemukan saluran kontrol untuk didengarkan, telepon seluler akan menampilkan pesan "tidak ada layanan" karena berada di luar jangkauan.
11. Saat ponsel menerima SID, ponsel akan membandingkannya dengan SID yang diprogramkan ke dalam ponsel dan jika nomor kode ini cocok, ponsel akan tahu bahwa ponsel sedang berkomunikasi dengan sistem asalnya. Bersama dengan SID, ponsel juga mengirimkan permintaan registrasi dan MTSO yang melacak lokasi ponsel dalam basis data, mengetahui ponsel mana yang Anda gunakan, dan memberikan dering.
12. Agar sesuai dengan sistem penyedia ponsel, setiap ponsel berisi papan sirkuit, yang merupakan otak ponsel. Papan sirkuit adalah kombinasi beberapa chip komputer yang diprogram untuk mengubah analog ke digital dan konversi digital ke analog serta penerjemahan sinyal audio keluar dan sinyal masuk.
13. Ini adalah prosesor mikro yang mirip dengan yang umumnya digunakan dalam cakram padat komputer desktop. Tanpa papan sirkuit, instrumen ponsel tidak dapat berfungsi.
14. Saat pelanggan Reliance memilih layanannya, MIN dan SID diprogramkan ke dalam handset. Jika seseorang memanipulasi dan mengubah ESN, telepon genggam yang secara eksklusif digunakan oleh mereka dapat digunakan oleh penyedia layanan lain seperti TATA Indicom.

**Keputusan**

1. Telepon genggam adalah komputer sebagaimana dimaksud dalam Undang-Undang Teknologi Informasi.
2. ESN dan SID termasuk dalam definisi "kode sumber komputer" menurut pasal 65 Undang-Undang Teknologi Informasi.
3. Ketika ESN diubah, pelanggaran menurut Pasal 65 Undang-Undang Teknologi Informasi terjadi karena setiap penyedia layanan harus memelihara kode SID-nya

sendiri dan juga memberikan nomor khusus pelanggan untuk setiap instrumen yang digunakan untuk memanfaatkan layanan yang diberikan.

4. Apakah operator telepon genggam memelihara kode sumber komputer, merupakan masalah pembuktian.
5. Dalam Pasal 65 Undang-Undang Teknologi Informasi, 2000 kata pemisah "atau" digunakan di antara dua frasa-
    a. "ketika kode sumber komputer diharuskan untuk disimpan"
    b. "dipelihara oleh hukum yang berlaku saat ini"

**6. D'zine Garage Pvt. Ltd. yang diwakili oleh Direkturnya, Tn. Hari Sethuraman vs. D'zine Café FZE & D'zine Café FZE vs. D'zine Garage Pvt. Ltd. yang diwakili oleh Direkturnya, Tn. Hari Sethuraman30**

**Fakta Kasus**

Penggugat, pemilik terdaftar merek layanan 'D'zine', mengajukan gugatan untuk penyuntikan permanen terhadap Pemohon-Tergugat yang menggunakan merek 'D'zine' café sebagai merek layanan dan sebagai bagian dari nama perusahaan dan nama domain mereka 'www.Dzinecafe.com'- Termohon/Penggugat berpendapat bahwa Pemohon-Tergugat telah dengan sengaja mengadopsi merek layanan/nama dagang yang serupa, D'zine café, dalam upaya yang diperhitungkan untuk menguangkan reputasi dan niat baik yang dinikmati oleh Termohon/Penggugat dan untuk mendapatkan keuntungan yang tidak sah dan cepat tanpa melakukan upaya yang substansial.

Perintah sementara dikabulkan. Oleh karena itu, permohonan Tergugat untuk membatalkan perintah sementara dan untuk membatalkan gugatan dan menolak gugatan Pemohon-Tergugat berpendapat bahwa Tergugat-Penggugat tidak memiliki kantor di India dan karenanya Pengadilan saat ini tidak memiliki yurisdiksi untuk mengadili masalah tersebut dan oleh karena itu, gugatan tersebut dapat ditolak. Diputuskan bahwa untuk membenarkan Perintah penolakan gugatan, Tergugat akan diminta untuk menunjukkan kasus yang sangat kuat yang menguntungkannya dan kekuasaan akan dilaksanakan dengan hemat dan hanya dalam kasus-kasus pengecualian, karena akan bertentangan dengan hak pihak untuk melanjutkan persidangan untuk mendapatkannya secara sah dan sesuai dengan substansi kasusnya.

Kasus seperti itu belum dibuat oleh Tergugat dan diputuskan bahwa permohonan penolakan gugatan tidak dapat dipertahankan. Terdakwa meminta pembatalan putusan sementara dengan alasan bahwa pendaftaran hanya untuk logo dan bahwa 'D'zine' bukanlah kata yang diciptakan, itu adalah bentuk desain yang rusak dan umum digunakan lebih lanjut menyatakan bahwa, kafe D'zine cukup berbeda dan tidak mungkin menyesatkan dan banyak orang lain yang menggunakannya.

**Putusan**

Diputuskan, untuk memberikan putusan sementara, kesamaan fonetik tidak dapat diabaikan dan pengguna sebelumnya harus dibuktikan dan harus ada niat tidak jujur. Dalam kasus ini, ada kesamaan fonetik Lebih lanjut, 'D'zine bukan kata generik, tidak dapat dikatakan memiliki referensi khusus untuk perdagangan tertentu, menjadi publici jiris. Karena bisnis para

pihak hampir sama dan fakta bahwa yang satu adalah kafe 'Dzine' dan yang lainnya adalah garasi 'Dzine', klien cenderung tertukar dengan pengguna sebelumnya ditetapkan oleh Penggugat tidak ada penyangkalan khusus atas tuduhan bahwa Tergugat mengambil keuntungan dari merek penggugat. Penggunaan kata yang sama oleh orang lain dan orang lain dan itu adalah kata yang umum bukanlah pembelaan dalam tindakan untuk perintah sementara.

**7. Nirav Navinbhai Shah & ors. vs. State of Gujarat and Another31**

**Fakta Kasus**

Para pemohon, terdakwa asli dalam kejahatan I.C.R. No. 54 tahun 2004 tanggal 26.02.2004 yang terdaftar di kantor polisi sektor 7 Gandhinagar atas pelanggaran yang dapat dihukum berdasarkan pasal 381, 408, 415, 418, 420 dibaca dengan pasal 34 dan 120B dari Kitab Undang-Undang Hukum Pidana India dan pasal 66 dan 72 dari Undang-Undang Teknologi Informasi, 2000 (selanjutnya disebut sebagai 'Undang-Undang IT' untuk jangka pendek) telah mengajukan permohonan ini berdasarkan pasal 482 dari Kitab Undang-Undang Hukum Acara Pidana 1973 (selanjutnya disebut sebagai 'kode' untuk jangka pendek) untuk membatalkan FIR I.C.R. No. 54 tahun 2004 tanggal 26.02.2004 terdaftar di Kantor Polisi Sektor No. 7 Gandhinagar dan Kasus Pidana No. 54 tahun 2004 tanggal 26.02.2004 terdaftar di Kantor Polisi Sektor No. 7 Gandhinagar dan Kasus Pidana No. 3528 tahun 2004 yang dihasilkan masih menunggu keputusan Hakim Pengadilan Kelas Satu Gandhinagar, terutama atas dasar bahwa fakta dan tuduhan yang mengarah pada pengajuan FIR menunjukkan bahwa perselisihan yang sebenarnya adalah perselisihan perdata dan karena hal itu telah diselesaikan secara damai antara para pihak, tidak ada tujuan yang berguna untuk melanjutkan proses pidana, sebaliknya kelanjutannya akan menjadi kontraproduktif bagi kepentingan keadilan.

**Putusan**

Gugatan juga tidak mengandung unsur penting apa pun untuk mempertahankan proses pidana atas pelanggaran yang dituduhkan. Sebagaimana dinyatakan dalam argumen para penasihat hukum bahwa para pihak telah mengajukan gugatan perdata juga sehubungan dengan perselisihan yang sama. Seluruh perselisihan antara para pihak diselesaikan dengan penyelesaian secara damai. Peretasan yang dituduhkan dilakukan hanya pada sistem komputer Penggugat yang dikatakan memiliki data yang berkaitan dengan kliennya. Para Penasihat Hukum telah mengajukan bahwa di salah satu situs web data ini sudah tersedia.

Sengketa tersebut tampaknya bersifat pribadi. Pelanggaran yang dituduhkan tidak secara ketat mempengaruhi atau melanggar hak individu atau warga negara lain. Dengan demikian melihat pada sifat sengketa, dapat dikatakan bahwa kelanjutannya tidak sesuai dengan kepentingan keadilan. Diputuskan bahwa FIR 54 tahun 2004 yang terdaftar di Kantor Polisi sektor 7 Gandhinagar dan Kasus Pidana No. 3528 tahun 2004 yang tertunda di JMFC Gandhinagar layak untuk dibatalkan demi kepentingan yang adil dan dengan ini mereka dibatalkan. Aturan dibuat mutlak.

**8. SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra32**

**Fakta: Pencemaran Nama Baik di Dunia Maya**

Dalam kasus pencemaran nama baik di dunia maya pertama di India, Pengadilan Delhi mengambil alih yurisdiksi atas masalah pencemaran nama baik perusahaan melalui email dan mengeluarkan putusan pengadilan ex-parte yang penting. Dalam kasus ini, terdakwa Jogesh Kwatra yang merupakan karyawan perusahaan penggugat mulai mengirim email yang merendahkan, memfitnah, cabul, vulgar, kotor, dan kasar kepada atasannya serta kepada berbagai anak perusahaan perusahaan tersebut di seluruh dunia dengan tujuan untuk mencemarkan nama baik perusahaan dan Direktur Pelaksananya, Tn. R K Malhotra. Penggugat mengajukan gugatan untuk putusan pengadilan permanen yang melarang terdakwa melakukan tindakan ilegalnya dengan mengirim email yang merendahkan kepada penggugat.

Atas nama penggugat, dikemukakan bahwa email yang dikirim oleh tergugat jelas-jelas cabul, vulgar, kasar, mengintimidasi, mempermalukan, dan mencemarkan nama baik. Penasihat hukum lebih lanjut berpendapat bahwa tujuan pengiriman email tersebut adalah untuk mencemarkan nama baik penggugat di seluruh India dan dunia. Ia lebih lanjut berpendapat bahwa tindakan tergugat dalam mengirim email tersebut telah mengakibatkan pelanggaran hak hukum penggugat. Lebih lanjut, tergugat berkewajiban untuk tidak mengirim email tersebut. Penting untuk dicatat bahwa setelah perusahaan penggugat mengetahui bahwa karyawan tersebut terlibat dalam masalah pengiriman email yang kasar, penggugat menghentikan layanan tergugat.

**Putusan**

Setelah mendengarkan argumen terperinci dari Penasihat Hukum Penggugat, Hakim Pengadilan Tinggi Delhi mengeluarkan putusan sela ex-parte dengan menyatakan bahwa kasus prima facie telah diajukan oleh penggugat. Oleh karena itu, Pengadilan Tinggi Delhi melarang terdakwa mengirim email yang merendahkan, memfitnah, cabul, vulgar, memalukan, dan kasar baik kepada penggugat maupun kepada anak perusahaannya di seluruh dunia termasuk Direktur Pelaksana dan departemen Penjualan dan Pemasaran mereka.

Lebih lanjut, Hakim juga melarang terdakwa menerbitkan, mengirimkan, atau menyebabkan diterbitkannya informasi apa pun di dunia nyata maupun di dunia maya yang merendahkan, memfitnah, atau kasar kepada penggugat. Perintah Pengadilan Tinggi Delhi ini memiliki arti yang sangat penting karena untuk pertama kalinya Pengadilan India mengambil alih yurisdiksi dalam perkara yang menyangkut pencemaran nama baik dunia maya dan memberikan putusan ex-parte yang melarang tergugat melakukan pencemaran nama baik kepada penggugat dengan cara mengirimkan email yang merendahkan, mencemarkan nama baik, kasar, dan tidak senonoh baik kepada penggugat maupun cabangnya.

**9. Nasscom vs. Ajay Sood & Others**

**Fakta**

Dalam putusan penting dalam kasus National Association of Software and Service Companies vs Ajay Sood & Others, yang disampaikan pada bulan Maret 2005, Pengadilan Tinggi Delhi menyatakan bahwa 'phishing' di internet merupakan tindakan ilegal, yang memerlukan putusan pengadilan dan ganti rugi. Menguraikan konsep 'phishing', untuk menetapkan preseden di India, pengadilan menyatakan bahwa hal itu merupakan bentuk

penipuan internet di mana seseorang berpura-pura menjadi asosiasi yang sah, seperti bank atau perusahaan asuransi untuk mengambil data pribadi dari pelanggan seperti kode akses, kata sandi, dll.

Data pribadi yang dikumpulkan dengan cara tersebut dengan menyamarkan identitas pihak yang sah biasanya digunakan untuk keuntungan pihak yang mengumpulkan data. Pengadilan juga menyatakan, sebagai contoh, bahwa penipuan phishing yang umum melibatkan orang-orang yang berpura-pura mewakili bank online dan menyedot uang tunai dari rekening e-banking setelah menipu konsumen agar menyerahkan rincian perbankan rahasia.

**Putusan**

Pengadilan Tinggi Delhi menyatakan bahwa meskipun tidak ada undang-undang khusus di India yang menghukum phishing, pengadilan menganggap phishing sebagai tindakan ilegal dengan mendefinisikannya berdasarkan hukum India sebagai "salah penafsiran yang dilakukan dalam perdagangan yang menyebabkan kebingungan mengenai sumber dan asal email yang menyebabkan kerugian besar tidak hanya bagi konsumen tetapi juga bagi orang yang nama, identitas, atau kata sandinya disalahgunakan". Pengadilan menganggap tindakan phishing sebagai tindakan penipuan dan mencoreng citra penggugat. Penggugat dalam kasus ini adalah Asosiasi Nasional Perusahaan Perangkat Lunak dan Layanan (NASSCOM), asosiasi perangkat lunak utama India.

Para terdakwa mengoperasikan agen penempatan yang terlibat dalam perekrutan dan perekrutan karyawan. Untuk mendapatkan data pribadi, yang dapat mereka gunakan untuk tujuan perekrutan karyawan, para terdakwa membuat dan mengirim email ke pihak ketiga atas nama NASSCOM. Pengadilan tinggi mengakui hak merek dagang penggugat dan mengeluarkan putusan sementara ex-parte yang melarang para tergugat menggunakan nama dagang atau nama lain yang secara menipu mirip dengan NASSCOM. Pengadilan selanjutnya melarang para tergugat untuk menyatakan diri sebagai rekanan atau bagian dari NASSCOM.

Pengadilan menunjuk sebuah komisi untuk melakukan penggeledahan di tempat tinggal para tergugat. Dua hard disk komputer tempat para tergugat mengirim email palsu ke berbagai pihak ditahan oleh komisaris lokal yang ditunjuk oleh pengadilan. Email yang melanggar tersebut kemudian diunduh dari hard disk dan disajikan sebagai bukti di pengadilan. Selama proses kasus berlangsung, menjadi jelas bahwa para terdakwa yang namanya digunakan dalam pengiriman email yang melanggar tersebut adalah identitas fiktif yang dibuat oleh seorang karyawan atas instruksi terdakwa, untuk menghindari pengakuan dan tindakan hukum. Setelah tindakan penipuan ini ditemukan, nama-nama fiktif tersebut dihapus dari daftar pihak-pihak yang menjadi terdakwa dalam kasus tersebut.

Selanjutnya, para terdakwa mengakui tindakan ilegal mereka dan para pihak menyelesaikan masalah tersebut melalui pencatatan kompromi dalam proses gugatan. Menurut ketentuan kompromi, para terdakwa setuju untuk membayar sejumlah Rs. 1,6 juta kepada penggugat sebagai ganti rugi atas pelanggaran hak merek dagang penggugat. Pengadilan juga memerintahkan hard disk yang disita dari tempat tinggal para terdakwa untuk diserahkan kepada penggugat yang akan menjadi pemilik hard disk tersebut.

Kasus ini mencapai tonggak sejarah yang jelas: Kasus ini memasukkan tindakan "phishing" ke dalam lingkup hukum India bahkan tanpa adanya undang-undang khusus; Kasus ini menepis anggapan yang keliru bahwa tidak ada “budaya ganti rugi” di India atas pelanggaran hak kekayaan intelektual; Kasus ini menegaskan kembali keyakinan pemilik kekayaan intelektual terhadap kemampuan dan kemauan sistem peradilan India untuk melindungi hak kekayaan tak berwujud dan mengirimkan pesan yang kuat kepada pemilik kekayaan intelektual bahwa mereka dapat berbisnis di India tanpa mengorbankan hak kekayaan intelektual mereka.

**10. Negara Bagian Tamil Nadu vs. Suhas Kutti34**

**Fakta**

Asisten Komisaris Polisi, Sel Kejahatan Dunia Maya, C.C.B. Bahasa Indonesia: Egmore, Chennai mengajukan Laporan Akhir terhadap terdakwa, bahwa pada 7.2.04, malam di Cyber Café Hello World Centre, Sion, Mumbai yang memiliki I.P.61.11.10.99, terdakwa dengan maksud untuk merusak reputasi Penggugat Ibu R, membuat id pengguna atas nama dirinya dan menulis pesan cabul yang dimaksudkan agar dokumen tersebut digunakan untuk diposting di Grup Yahoo cabul yang berbeda, dengan maksud untuk membuat orang lain percaya bahwa dokumen tersebut dibuat olehnya, sehingga orang-orang yang melihat pesan cabul tersebut akan mengirim panggilan yang menyinggung kepadanya, dalam merusak reputasinya dan dengan menghina kesopanannya dengan kata-kata yang dipamerkan dalam email dan dalam transaksi yang sama, pada 7.2.04, malam di Cyber Café Hello World Centre, Sion, Mumbai, memiliki IP 61.11.10.99 Terdakwa memposting pesan cabul yang cabul dan juga memiliki efek untuk merusak orang-orang yang mungkin membaca dan melihat pesan cabul tersebut dan menyebabkan dipublikasikan di beberapa grup Yahoo yang tidak senonoh dan dalam transaksi yang sama.

Bahwa pada tanggal 9.2.04, pagi, di Cyber Café Heighten Advertising, Mahim, Mumbai, yang memiliki IP 202.88.165.53 terdakwa dengan maksud untuk merusak reputasi pengadu Ibu R memasukkan id pengguna. Bahasa Indonesia: yang dibuat olehnya atas nama penggugat dan membuat pesan cabul yang dimaksudkan agar dokumen tersebut digunakan untuk diposting di berbagai grup Yahoo cabul, dengan maksud agar orang lain percaya bahwa dokumen tersebut dibuat olehnya, sehingga orang yang melihat pesan cabul tersebut akan mengirim panggilan telepon yang menyinggung kepadanya, dalam rangka merusak reputasinya dan dengan menghina kesopanannya melalui kata-kata yang dipamerkan dalam email dan bahwa dalam transaksi yang sama, bahwa pada 9.2.04, pagi hari di warnet Heighten Advertising, Mahim, Mumbai, yang memiliki IP 202.88.165.53, terdakwa memposting pesan cabul yang mesum dan juga memiliki efek merusak orang yang mungkin membaca dan melihat pesan cabul tersebut dan menyebabkan dipublikasikan di berbagai grup Yahoo cabul dan dengan demikian terdakwa telah melakukan pelanggaran u/s 469 IPC, 67 I.T. Act. 469 & 509 IPC, dan 67 I.T. Act, 2000. P.W. 1 adalah putri tunggal dari P.W.2 dan P.W.3. P.W.2 adalah ayahnya, P.W.3 adalah ibunya.

Saat ini, P.W.1 bekerja sebagai Eksekutif senior (SDM) di sebuah Perusahaan multinasional di Chennai. Dia belajar Kursus MBA di Mumbai pada tahun 1997, terdakwa

belajar dengan P.W.1 dan dia adalah teman sekelasnya di Mumbai. Terdakwa berasal dari Mumbai. Pada 9.2.04, Dia membuka email Rediff-nya dan melihat tanda terima dua pesan cabul yang diunggah pada 7.2.04 dan 9.2.04. Dia mengambil hasil komputer dari pesan cabul yang diunggah pada 7.2.04, Ex P.1 adalah pesan cabul tersebut. Pesan cabul itu mencantumkan nomor telepon Kantornya dan ID email-nya. Nomor telepon rumah diberikan secara salah. Pesan cabul tersebut telah dikirim melalui situs web Yahoo ke 5 kelompok seks. Pesan cabul yang dicetak komputer yang diposting di grup pecinta @Radha adalah EX.P.2. Setelah melihat pesan tersebut, beberapa orang mengirim pesan balasan dan banyak orang mencoba menghubunginya melalui telepon. Seri Ex P3 adalah pesan balasan. Beberapa panggilan telepon masuk ke kantornya. P.W.1 memberi tahu masalah tersebut kepada orang tuanya. Pesan tersebut kemungkinan akan merusak reputasi dan moral.

P.W.1 telah menikah dengan Jaichand Prajapathi dari Uttar Pradesh pada tahun 2001. Kehidupan keluarga itu tidak bahagia dan dia memperoleh perceraian melalui pengadilan pada tahun 2003. Terdakwa dikutip sebagai saksi dalam petisi perceraian. P.W.1 mengingat satu kejadian dan mencurigai adanya keterlibatan Terdakwa. Selama masa kuliah di tahun 1997, terdakwa biasa bepergian dengan P.W.1 di kereta api di Mumbai. Pada salah satu kesempatan tersebut, Terdakwa menunjukkan coretan cabul dengan nomor telepon di kereta dan mengatakan kepada P.W.1 bahwa setelah melihat nomor telepon tersebut, banyak orang akan mencoba menghubungi nomor telepon tersebut dan ini adalah cara terbaik untuk merusak reputasi seorang wanita. Terdakwa bahkan menyatakan keinginannya untuk menikahi P.W.1, setelah pertunangan P.W.1 dengan Jaichand Prajapati berakhir. P.W.1 menolak lamarannya. Bahasa Indonesia: Pada tahun 2003, Terdakwa tinggal di rumah P.W.1 selama sekitar 10 hari dengan alasan harus menghadiri wawancara di Bangalore. Pada saat itu juga, terdakwa menawarkan diri untuk menikahi P.W.1 yang ditolak oleh P.W.1 dan orang tuanya. Setelah itu, P.W.1 setelah kembali ke Mumbai terbiasa menelepon, mengirim Pesan S.M.S. dan mengirim E-mail ke P.W.1 secara berkala. Oleh karena itu P.W.1 memblokir I.D. email terdakwa. Ex.P5 adalah keluaran Komputer untuk memblokir I.D. email terdakwa.

Setelah melihat pesan cabul tersebut, P.W.1 mendiskusikan masalah tersebut dengan P.W.2 dan P.W.3 dan meminta bantuan terdakwa melalui telepon. P.W.1 dan orang tuanya mengeluarkan pesan peringatan atas nama PW 2 dan PW 3 dengan membuat ID email yaitu. parant2003@yahoo.co.in dan mengirimkannya ke grup-grup yahoo. Dia mengirim pesan peringatan kepada orang-orang tersebut, yang kemudian mengirim pesan balasan dalam seri ExP.6. Salinan pesan peringatan juga dikirimkan kepada Terdakwa. P.W.1 mengajukan pengaduan pada 14/2/2004 bersama dengan Ex.P1 di Polisi Kejahatan Dunia Maya. Pengaduan tersebut adalah Ex. P.4 P.W.12 yang menerima pengaduan mengarahkan P.W.4 untuk mendapatkan detail header dan keterangan lain untuk mengetahui asal pesan. P.W.4 pergi ke Cyber Café di Kennath Lane, Egmore bersama dengan P.W. 1 dia mengunduh pesan tersebut, mencetaknya dengan menggunakan I.D. email Parant2003 @ Yahoo. Co.in Ex.P.9-Ex.P.12.

Dia mengekstrak dan menyimpan pesan dalam disket Mo.2. Setelah itu P.W.12 memberikan permintaan kepada Hathway Cable and Data Com. Pvt. Ltd; berdasarkan Ex.P.13,

yang dibalasnya dalam Ex. P.14. P.W.12 juga memberikan permintaan kepada Dishnet D.S.L. dalam Ex.P.13 dan balasan yang diberikan oleh Dishnet D.S.L adalah Ex.P.15. P.W.5 berbicara tentang Ex.P.13 dan Ex.P.14. P.W.6 berbicara tentang Ex.P.15.P.W.12 juga memeriksa P.W.11 dan memperoleh keterangan dalam rangkaian Ex. P.29 dan mengonfirmasi bahwa pesan tersebut berasal dari Mumbai. P.W.12- Petugas Investigasi mendaftarkan F.I.R. Ex.P.34 pada 20.2.04.

Selanjutnya, P.W.12 berangkat ke Mumbai pada 24.2.04, dan menangkap Terdakwa di Mumbai pada 25.2.04. Ia menyita Ponsel Mo.1 dari Terdakwa di bawah Mahazar Ex.P.8 P.W.8 dan P.W.9 yang menjalankan Pusat Penjelajahan di Mumbai, mengidentifikasi Terdakwa di hadapan P.W.12. Ia menyita Ex.P.23, 24 register dari mereka. P.W.8 berbicara tentang Terdakwa dan penyitaan Ex.P.22 dan pernyataan yang dibuat oleh P.W.12 dalam Ex.P.23, P.W. 9 berbicara tentang Terdakwa bahwa ia datang ke pusat penelusuran dan menandatangani Register Ex.P24 sebagai R. Ex.P.25 adalah kata yang ditulis oleh Terdakwa. P.W.12, membawa Terdakwa ke Chennai pada 28.2.04, setelah menghadirkan Terdakwa di hadapan Pengadilan Mumbai. Terdakwa memberikan pernyataan pengakuan di hadapan P.W.10 dan ia memberikan kata sandi “an rose”. Kata yang dimaksud adalah Ex.P.27. Informasi yang disimpan dalam Kartu SIM diambil dalam seri Ex.P.28 melalui Pembaca SMS. P.W.12 pergi ke kantor P.W.7 dan mengambil hasil cetak komputer dengan menggunakan kata sandi “an rose”. Ia menerbitkan sertifikat dalam Ex.P.21. Hasil cetak komputer adalah Ex. P 16-P.20. P.W.12 menyelesaikan penyelidikan dan mengajukan dakwaan terhadap Terdakwa atas pelanggaran u/s 67 UU TI dan u/s 469,509 KUHP.

**Putusan**

Pengadilan tidak cenderung menerima teori yang diajukan oleh Terdakwa bahwa pesan-pesan cabul itu dibuat oleh P.W.1, P.W.2, dan P.W.3 atau oleh Jaichand Prajapathi. Jelas bahwa Terdakwa sendiri yang telah membuat dan mengunggah pesan-pesan cabul dari pusat penelusuran P.W.8 dan P.W.9. Pengadilan ini berpendapat bahwa penuntutan telah membuktikan dakwaannya terhadap terdakwa tanpa keraguan yang wajar dan karenanya Terdakwa dapat dihukum.Terdakwa didengar mengenai pertanyaan tentang hukuman u/s 248 (2) Cr.P.C. Terdakwa memohon peringatan. Terdakwa bukanlah orang awam. Ia berpendidikan dan menempuh pendidikan hingga M.B.A. P.W.1 memegang jabatan penting di sebuah Perusahaan multinasional di Chennai. Terdakwa telah memilih untuk mengunggah pesan cabul itu karena alasan sederhana bahwa ia menolak untuk menikahinya.

Ia tidak berperilaku seperti orang terpelajar. Hanya seorang wanita yang sudah berkeluarga yang dapat menyadari penderitaan dan rasa sakit mental jika orang yang tidak dikenal menghubunginya melalui telepon dan email serta mengajaknya tidur. Penderitaan dan penghinaan mental yang dialami oleh P.W.1 tidak dapat dikompensasikan dalam bentuk uang atau kata-kata yang menenangkan. Tidak dapat dikatakan bahwa Terdakwa telah bertindak dalam keadaan emosi. Dua hari berulang kali ia telah mengirim pesan cabul—Sistem komputer dan pusat penjelajahan dimaksudkan untuk mempelajari berbagai hal dan memperbarui pengetahuan di berbagai bidang. Terdakwa telah menyalahgunakannya untuk membalas

dendam pada seorang wanita yang cerdas. Oleh karena itu, Terdakwa tidak pantas mendapatkan keringanan hukuman dan dapat dihukum.

Akibatnya, Terdakwa dinyatakan bersalah atas pelanggaran pasal 469,509 KUHP, dan pasal 67 UU TI. dan Terdakwa dinyatakan bersalah dan dijatuhi hukuman untuk menjalani pidana penjara yang ketat selama 2 tahun u/s 469 IPC, dan membayar denda Rs.500/- i/d, menjalani pidana penjara sederhana selama 1 bulan dan untuk pelanggaran u/s 509 IPC, dijatuhi hukuman menjalani pidana penjara sederhana selama 1 tahun dan membayar denda Rs.500/- i/d untuk menjalani pidana penjara sederhana selama 1 bulan dan untuk pelanggaran u/s 67 Undang-Undang Teknologi Informasi tahun 2000 untuk menjalani pidana penjara yang ketat selama 2 tahun dan membayar denda Rs.4,000/- i/d untuk menjalani S.I. selama 6 bulan. Semua hukuman akan dijalankan secara bersamaan. Periode yang dijalani oleh Terdakwa akan dikurangkan dari u/s 428 Cr.P.C.

**11. Google India Pvt. Ltd. vs. M/s.Visaka Industries Limited dan lainnya**

Pemohon/A-2 dituduh melakukan pelanggaran yang dapat dihukum berdasarkan Pasal 120-B, 500, 501/34 I.P.C dalam C.C. No.679 tahun 2009 pada berkas XI Additional Chief Metropolitan Magistrate, Secunderabad bersama dengan yang lainnya. Pemohon/A-2 adalah Google India Private Limited yang diwakili oleh Managing Director (Penjualan dan Operasional). Responden/penggugat pertama adalah Visaka Industries Limited, Secunderabad yang diwakili oleh penandatangan resminya yang merupakan Deputy Manager-Legal. Penggugat bergerak dalam bisnis manufaktur dan penjualan lembaran semen asbes dan produk terkait. Diduga bahwa A-1 yaitu Gopala Krishna adalah Koordinator "Ban Asbestos India", sebuah grup yang dihosting oleh A-2 dan menerbitkan artikel rutin di grup tersebut dan bahwa pada tanggal 21.11.2008 sebuah artikel diterbitkan di grup tersebut dan diberi judul "meracuni sistem; Hindustan Times" yang ditujukan pada satu produsen produk semen asbes yaitu penggugat dan nama-nama politisi terkenal negara tersebut G. Venkata Swamy dan Sonia Gandhi yang tidak ada hubungannya dengan kepemilikan atau pengelolaan perusahaan penggugat disebutkan dalam artikel tersebut.

Lebih lanjut diduga bahwa pada tanggal 31.07.2008 artikel lain diberi judul "Industri Asbestos Visaka memperoleh keuntungan" dan bahwa kedua artikel di atas berisi pernyataan yang mencemarkan nama baik penggugat dan tersedia di dunia maya dalam bentuk artikel untuk khalayak di seluruh dunia. Dalam pengaduan tersebut, rincian pernyataan yang bersifat mencemarkan nama baik yang dibuat dalam beberapa artikel lain yang diterbitkan oleh A-1 dalam kelompok A-2 diberikan secara rinci, yang mana rincian tersebut mungkin tidak diperlukan untuk tujuan pembuangan petisi pidana ini.

Penasihat hukum senior yang mewakili pemohon/A-2 berpendapat bahwa tindakan perantara seperti Google Inc., yang merupakan penyedia layanan yang menyediakan platform bagi pengguna akhir untuk mengunggah konten, tidak termasuk dalam publikasi hukum dan akibatnya pertanyaan tentang apakah perantara tersebut bertanggung jawab atas pencemaran nama baik tidak muncul. Penasihat hukum senior yang mewakili pemohon mengandalkan Pasal 79 Undang-Undang Teknologi Informasi Tahun 2000 (singkatnya, Undang-Undang) untuk mendukung sanggahan ini. Pasal 79 yang terdapat dalam Bab XII

Undang-Undang tersebut sebagaimana yang ditetapkan pada tahun 2000 berbunyi sebagai berikut:

**Bab XII- Penyedia Layanan Jaringan Tidak Bertanggung Jawab dalam Kasus Tertentu**

Pasal 79. Penyedia layanan jaringan tidak bertanggung jawab dalam kasus tertentu: Untuk menghilangkan keraguan, dengan ini dinyatakan bahwa tidak seorang pun yang menyediakan layanan apa pun sebagai penyedia layanan jaringan akan bertanggung jawab berdasarkan Undang-Undang ini, peraturan atau ketentuan yang dibuat berdasarkan Undang-Undang ini atas informasi atau data pihak ketiga yang disediakan olehnya jika ia membuktikan bahwa pelanggaran atau tindak pidana tersebut dilakukan tanpa sepengetahuannya atau bahwa ia telah melakukan semua upaya yang wajar untuk mencegah terjadinya pelanggaran atau tindak pidana tersebut. Penjelasan,Untuk tujuan pasal ini adalah ,penyedia layanan jaringan berarti perantara dan informasi pihak ketiga berarti informasi apa pun yang ditangani oleh penyedia layanan jaringan dalam kapasitasnya sebagai perantara.

Ketentuan tersebut membebaskan penyedia layanan jaringan dari tanggung jawab berdasarkan Undang-Undang, peraturan atau regulasi yang dibuat di bawahnya untuk informasi atau data pihak ketiga apa pun yang disediakan olehnya. Ketentuan tersebut tidak membebaskan penyedia layanan jaringan dari tanggung jawab apalagi tanggung jawab pidana atas pelanggaran berdasarkan undang-undang lain atau lebih khusus lagi berdasarkan Kitab Undang-Undang Hukum Pidana India. Lebih lanjut, ketentuan di atas membebaskan penyedia layanan jaringan dari tanggung jawab, hanya dengan bukti bahwa pelanggaran atau pelanggaran tersebut dilakukan tanpa sepengetahuannya atau bahwa ia telah melakukan semua upaya yang wajar untuk mencegah terjadinya pelanggaran atau pelanggaran tersebut. Bukti dalam hal itu dapat diberikan melalui bukti utama oleh terdakwa. Oleh karena itu, pertanyaan tersebut adalah pertanyaan fakta yang tidak dapat dibahas oleh Pengadilan ini dalam petisi yang diajukan berdasarkan Pasal 482 KUHAP. Bab XII Undang-Undang termasuk Pasal 79 diubah oleh Undang-Undang Teknologi Informasi (Amandemen), 2008 (10 tahun 2009) tertanggal 05.02.2009 dengan berlaku mulai 27.10.2009 dengan cara mengganti bab asli dengan yang berikut ini:

**12. Pengecualian dari tanggung jawab perantara dalam kasus tertentu:**

Meskipun ada ketentuan dalam undang-undang yang berlaku saat ini tetapi tunduk pada ketentuan ayat (2) dan (3), perantara tidak bertanggung jawab atas informasi, data, atau tautan komunikasi pihak ketiga yang disediakan atau dihosting olehnya. Ketentuan ayat (1) berlaku jika fungsi perantara terbatas pada penyediaan akses ke sistem komunikasi tempat informasi yang disediakan oleh pihak ketiga dikirimkan atau disimpan atau dihosting sementara atau perantara tidak memulai pengiriman, memilih penerima pengiriman, dan memilih atau mengubah informasi yang terdapat dalam pengiriman.

Perantara mematuhi uji tuntas saat menjalankan tugasnya berdasarkan Undang-Undang ini dan juga mematuhi pedoman lain yang mungkin ditetapkan oleh Pemerintah Pusat terkait hal ini. Ketentuan Sub-Bagian (1) tidak berlaku jika Perantara telah bersekongkol atau bersekongkol atau membantu atau membujuk baik dengan ancaman atau janji atau dengan cara lain dalam melakukan tindakan melawan hukum setelah menerima pengetahuan aktual,

atau setelah diberitahu melalui informasi, data atau tautan komunikasi yang berada di atau terhubung ke sumber daya komputer yang dikendalikan oleh perantara sedang digunakan untuk melakukan tindakan melawan hukum, perantara gagal untuk segera menghapus atau menonaktifkan akses ke materi tersebut pada sumber daya tersebut tanpa merusak bukti dengan cara apa pun.

Penjelasan, Untuk tujuan bagian ini, ungkapan "informasi pihak ketiga" berarti informasi apa pun yang ditangani oleh perantara dalam kapasitasnya sebagai perantara. Hal ini hanya berlaku berdasarkan amandemen tersebut; klausul non-obstenti dimasukkan dalam Pasal 79 yang menjaga penerapan hukum lain di luar lingkup dalam situasi fakta yang tercakup dalam ketentuan tersebut. Sekarang, setelah amandemen, perantara seperti penyedia layanan jaringan dapat mengklaim pengecualian dari penerapan hukum lain apa pun sehubungan dengan informasi, data, atau tautan komunikasi pihak ketiga yang disediakan atau dihosting olehnya; asalkan ia memenuhi persyaratan berdasarkan Sub-pasal (2) Pasal 79. Lebih lanjut, sebagaimana menurut Sub-pasal (3) Pasal 79 yang diamandemen, pengecualian berdasarkan Sub-pasal (1) tidak dapat diterapkan oleh Pengadilan mana pun dan tidak dapat diklaim oleh perantara mana pun jika perantara tersebut melakukan konspirasi apa pun sehubungan dengan hal tersebut.

Selain itu, perantara tidak dapat mengklaim pengecualian berdasarkan Sub-pasal (1) jika ia gagal dengan cepat menghapus atau menonaktifkan akses ke materi yang tidak menyenangkan atau aktivitas yang melanggar hukum bahkan setelah menerima pengetahuan aktual tentang hal tersebut. Dalam kasus ini, meskipun responden pertama mengeluarkan pemberitahuan yang membawa pemohon tentang penyebaran materi yang mencemarkan nama baik dan kegiatan yang melanggar hukum oleh A-1 melalui media A-2, pemohon/A-2 tidak menggerakkan jari kelingkingnya untuk memblokir materi tersebut atau menghentikan penyebaran materi yang melanggar hukum dan tidak menyenangkan tersebut.

Oleh karena itu, pemohon/A-2 tidak dapat mengklaim pengecualian apa pun baik berdasarkan Bagian 79 Undang-Undang sebagaimana yang berlaku pada awalnya atau Bagian 79 Undang-Undang setelah amandemen yang berlaku sejak 27.10.2009. Kasus saat ini di Pengadilan yang lebih rendah diajukan pada bulan Januari 2009 terkait dengan pelanggaran yang dilakukan sejak 31.07.2009 dan seterusnya, yaitu, sejak lama sebelum amandemen terhadap ketentuan tersebut. Tidak ada pengecualian terhadap pertanggungjawaban pidana apa pun terhadap perusahaan yang merupakan badan hukum dan tidak memiliki badan yang dapat dikutuk atau dicemooh.

Jika terbukti bersalah, perusahaan pemohon dapat diberi hukuman yang sesuai meskipun bukan hukuman fisik. Berdasarkan pandangan tersebut, saya tidak menemukan alasan dalam permohonan pidana ini. Dengan demikian, Permohonan Pidana ditolak.

**13. Microsoft Corporation vs. Yogesh Papat36**

**Fakta**

Kasus ini menyangkut pelanggaran hak cipta dalam perangkat lunak dan khususnya penafsiran Pasal 51 dan 55 Undang-Undang Hak Cipta, 1957. Microsoft Corporation, pemilik terdaftar merek dagang MICROSOFT, mengajukan permohonan putusan tetap yang melarang

terdakwa, direktur dan agennya untuk menyalin, menjual, menawarkan untuk dijual, mendistribusikan atau menerbitkan kepada publik versi palsu atau tidak berlisensi dari program perangkat lunak Microsoft dengan cara apa pun yang merupakan pelanggaran hak cipta Microsoft dalam program komputer, manual terkait, dan merek dagang terdaftar Microsoft.

Microsoft juga meminta agar terdakwa dilarang menjual dan mendistribusikan produk apa pun yang menggunakan merek dagang MICROSOFT atau varian apa pun dari merek dagang ini. Terdakwa tidak hadir di pengadilan, sehingga persidangan berlangsung secara ex parte. Pengadilan akhirnya memutuskan melawan terdakwa, yang mengunduh perangkat lunak Microsoft ke hard drive komputer yang kemudian dijual, tanpa lisensi atau izin dari Microsoft untuk melakukannya.

**Putusan**

Pengadilan memeriksa setiap bukti secara bergiliran dan, berdasarkan asumsi bahwa 100 komputer terjual setiap tahun dan bukti popularitas perangkat lunak, memutuskan bahwa Microsoft telah menderita kerugian laba total sebesar Rs. 1,98 juta, ditambah bunga sebesar 9% sejak tanggal putusan hingga tanggal pembayaran. Pengadilan, mengutip pernyataan Hakim Laddie di Pengadilan Tinggi Inggris dan Wales dalam Microsoft Corporation v.

Electrowide Ltd., memutuskan bahwa tindakan terdakwa merupakan ancaman umum untuk melanggar hak cipta dalam golongan perangkat lunak. Hakim Predeep Nandrajog, yang memimpin kasus ini, menyatakan bahwa: "Telah ditetapkan bahwa terdakwa telah melanggar hak cipta penggugat dengan membuat salinan ilegal dari perangkat lunak sistem operasi dengan secara terbuka menyalin sistem operasi apa pun yang saat ini dapat dijual."

**14. Autodesk, Inc. & Another vs. Tn. Prashant Deshmukh & Others37**

**Fakta**

Autodesk, Inc. (selanjutnya disebut “Penggugat 1”) adalah perusahaan perangkat lunak desain dan konten digital terkemuka yang berbasis di AS, yang menyediakan perangkat lunak desain untuk para profesional, memiliki beberapa pengecer resmi di India, dan juga mengklaim sebagai pemilik berbagai merek dagang di India, termasuk AUTODESK dan AutoCAD. Microsoft Corporation, (selanjutnya disebut “Penggugat 2”) memiliki perangkat lunak seperti Microsoft Windows dan Microsoft Office dan merupakan nama yang hampir dikenal luas terkait periferal komputer. Perusahaan ini juga memiliki anak perusahaan di New Delhi.

Para penggugat mengklaim bahwa perangkat lunak yang dikembangkan dan dipasarkan oleh mereka adalah program komputer sesuai dengan Bagian 2(ffc) Undang-Undang Hak Cipta, 1957 dan juga tercakup sebagai ‘karya sastra’ sesuai dengan Bagian 2(o) Undang-Undang Hak Cipta. Selain itu, hak-hak penulis dari negara-negara anggota Konvensi Berne dan Universal Copyright dilindungi berdasarkan hukum Hak Cipta India karena India dan AS merupakan penanda tangan kedua konvensi ini. Berdasarkan informasi mengenai penggunaan perangkat lunak bajakan/tanpa lisensi dalam skala besar oleh para tergugat, penggugat telah menduga adanya pelanggaran hak cipta dan hak merek dagang oleh para tergugat.

**Masalah yang diangkat dalam kasus ini**

Apakah para tergugat bersalah karena telah melanggar hak cipta dan hak merek dagang yang terkait dengan perangkat lunak milik para penggugat?

**Upaya hukum yang diminta oleh para penggugat**

Perintah yang melarang para tergugat untuk melanggar hak cipta dan merek dagang terdaftar milik penggugat, ganti rugi sebesar Rs.20 lakhs dan penyerahan akun serta pengiriman perangkat lunak bajakan/tanpa lisensi yang terdapat dalam hard disk, compact disk, disket, dll.

**Putusan**

Para tergugat tidak pernah mencoba untuk menentang gugatan tersebut dengan mengajukan pernyataan tertulis. Bukti menunjukkan bahwa terdakwa 1 dan 2 tidak memegang lisensi apa pun dari Penggugat 1, sementara terdakwa 3 (M/s Space Designers Syndicate) adalah pengguna berlisensi AutoCAD LT 2005. Tn. Devesh J. Tiwari, orang yang memberi tahu penggugat tentang pelanggaran tersebut, adalah seorang karyawan M&S Consultancy Services (salah satu terdakwa) sebagai teknisi layanan komputer. Ia mengungkapkan di pengadilan bahwa perusahaan tempatnya bekerja tidak memiliki perangkat lunak berlisensi resmi apa pun dan bahwa atasannya sepenuhnya mengetahui perangkat lunak bajakan tersebut, termasuk Sistem Operasi Microsoft Windows 95/98; Microsoft Office 97/2000 dan Auto CAD Versi 12, 14 dan 2000, dsb. yang digunakan dari CD cetak di dalam perusahaan.

Atas nama penggugat juga dikemukakan bahwa kata Microsoft telah digunakan secara terus-menerus dan ekstensif oleh Penggugat 2 sejak lama dan telah diidentifikasi dan dikenali secara eksklusif oleh Penggugat. Penanggung jawab Departemen TI dari Perwakilan Hukum perusahaan penggugat juga bersaksi bahwa sebagian besar lisensi yang digunakan oleh entitas komersial terkait produk penggugat dapat digunakan secara terus-menerus dan bahwa program perangkat lunak yang dibeli oleh suatu entitas kapan saja harus tercermin dalam basis data ringkasan pembelian produk yang dikelola oleh perusahaan penggugat. Tak perlu dikatakan lagi, nama-nama tergugat jelas tidak ada dalam basis data tersebut. Sehubungan dengan penerapan Undang-Undang tersebut pada karya yang pertama kali diterbitkan di wilayah mana pun di luar India seperti AS, pengadilan merujuk pada Bagian 40 Undang-Undang tersebut dan juga pada paragraf 2 dan 3 dari Perintah Hak Cipta Internasional, 1999 dan menyatakan ketentuan Undang-Undang tersebut, khususnya S.51 (yang mengatur pelanggaran tanpa adanya lisensi), berlaku terhadap hak-hak yang terkait dengan produk tergugat dalam kasus ini.

Lagi pula, sesuai dengan Pasal 14 UU tersebut, pengadilan yakin bahwa dengan menggunakan versi bajakan dari perangkat lunak yang dilindungi hak cipta oleh penggugat, tergugat pasti bersalah melakukan pelanggaran, selain juga menyebabkan pelanggaran merek dagang. Mengenai masalah ganti rugi punitif dalam kasus pembajakan dan pelanggaran hak cipta, disebutkan beberapa preseden seperti Time Incorporated vs. Lokesh Srivastava & Anr., 2005 (30) PTC 3 (Del), Hero Honda Motors Ltd. vs. Shree Assuramji Scooters, 2006 (32) PTC 117 (Del), Microsoft Corporation vs. Deepak Raval MIPR 2007 (1) 72, dan Larsen and Toubro

Limited vs. Chagan Bhai Patel MIPR 2009 (1) 194, yang semuanya mendukung pemberian ganti rugi punitif untuk mencegah pelanggar hak cipta, bahkan jika pelanggar hak cipta memutuskan untuk tidak hadir dalam proses gugatan sama sekali. Dinyatakan pula bahwa mengingat energi dan sumber daya yang dihabiskan oleh pemegang hak dalam litigasi pelanggaran, kegagalan untuk memberikan ganti rugi punitif hanya akan memicu dorongan untuk tindakan seperti pelanggaran dan pelanggaran hak cipta.

Pengadilan juga menyuarakan kekhawatiran tentang meningkatnya kasus pembajakan perangkat lunak dari perusahaan-perusahaan terkemuka seperti Microsoft dan AutoCAD di negara tersebut, yang dapat menyebabkan keputusasaan di antara para investor dalam pengembangan perangkat lunak tersebut karena kurangnya biaya lisensi yang semakin berkurang. Lebih jauh, penggunaan perangkat lunak bajakan untuk tujuan komersial daripada tujuan pribadi, menurut pengadilan, seharusnya lebih dikecam, dan oleh karena itu pengadilan memberikan penggugat putusan tetap yang diminta serta ganti rugi punitif sebesar Rs. 1 lakh terhadap Terdakwa No. 2.

**15. Travel India Times vs. India Times Travel38**

Fakta situasi dalam putusan Pengadilan Tinggi Delhi dalam Times Internet vs. M/s Belize Domian Whois Service Ltd. & Others merupakan contoh perampasan hak cipta di dunia maya. Putusan tersebut menegaskan kembali prinsip nama domain-merek dagang/passing off. Bertentangan dengan sengketa oktatabyebye.com di mana WIPO memutuskan mendukung Tata Sons yang mengharuskan portal perjalanan berbasis Gurgaon MakeMyTrip untuk mentransfer domain oktatabyebye.com ke Tata, passing off dalam kasus ini terbukti.

**Fakta**

Indiatimes.com adalah portal e-commerce yang dimiliki oleh perusahaan penggugat, Times Internet. Sejak tahun 2000, situs web tersebut menawarkan berbagai layanan termasuk layanan perjalanan melalui travel.indiatimes.com. Tergugat, M/s Belize Domain Whois Service Ltd. & Others mendaftarkan Indiatimestravel.com pada tahun 2005. Situs tersebut memuat beberapa tautan sponsor. Dengan menyatakan bahwa “indiatimestravel.com” secara menipu mirip dengan nama domain terdaftar penggugat "travel. indiatimes.com", penggugat mengajukan bahwa tergugat mencoba mengambil keuntungan dari nama mereknya. Penggugat, dengan mengutip angka pendapatan, mengajukan bahwa situs webnya memiliki reputasi dan menandakan layanan serta produk yang dipasarkan melalui situs web tersebut. Penggugat meminta putusan pengadilan yang melarang para tergugat melakukan cyber squatting, menggunakan nama lain yang identik atau mirip dan mengalihkan nama domain “indiatimestravel.com” kepada penggugat.

**Putusan**

Pengadilan merujuk pada putusan Mahkamah Agung dalam kasus Satyam Infoway Ltd. vs. Sifynet Solutions Pvt. Ltd. yang memiliki situasi fakta serupa. Dalam kasus ini, Mahkamah Agung mengamati bahwa nama domain dipilih sebagai instrumen perusahaan komersial tidak hanya karena memudahkan konsumen untuk menjelajahi Internet guna menemukan situs web yang mereka cari, tetapi juga pada saat yang sama, berfungsi untuk mengidentifikasi dan membedakan bisnis itu sendiri, atau barang atau jasanya, dan untuk menentukan lokasi

Internet daringnya yang sesuai. Akibatnya, nama domain sebagai alamat harus, tentu saja, bersifat khusus dan unik dan jika nama domain digunakan sehubungan dengan bisnis, nilai mempertahankan identitas eksklusif menjadi penting.

Dengan membandingkan nama domain dan merek dagang, Mahkamah Agung memutuskan bahwa nama domain dapat memiliki semua karakteristik merek dagang. Oleh karena itu, nama domain dapat dilindungi berdasarkan Undang-Undang Merek Dagang, 1999. Dalam kasus ini, Pengadilan Tinggi mengamati bahwa penggugat memiliki merek "indiatimes.com" jauh sebelum tergugat menciptakan merek "indiatimestravel.com". Lebih jauh, "indiatimes" yang merupakan komponen penting dari nama domain, digunakan oleh tergugat tanpa penjelasan apa pun. Hal ini dapat membingungkan warganet biasa dan dapat mengakibatkan pengaitan portal tergugat dengan portal perusahaan penggugat.

Penggunaan portal web yang dipermasalahkan oleh tergugat juga dapat membahayakan reputasi penggugat jika produk dan layanan yang diiklankan melalui situs web tersebut kurang berkualitas. Lebih jauh, karena tergugat tidak hadir di Pengadilan dan menentang klaim penggugat, tindakan tergugat dianggap sebagai mala fide. Mempertimbangkan aspek-aspek yang disebutkan di atas, sengketa ini dianggap sebagai kasus yang jelas tentang passing off. Karena penggugat dianggap memiliki hak tunggal untuk menggunakan kata-kata “indiatimes”, tergugat diarahkan untuk mentransfer “indiatimestravel.com” ke penggugat.

**16. Cubby, Inc vs. CompuServe, Inc.40**

Di mana CompuServe adalah perusahaan daring yang menyediakan akses ke lebih dari 150 forum minat khusus yang terdiri dari papan buletin elektronik, konferensi daring interaktif, dan basis data topikal. Buletin yang disebut Rumorville disediakan melalui papan buletin tersebut. Penggugat menggugat CompuServe atas pencemaran nama baik setelah pernyataan yang diduga mencemarkan nama baik disebarkan melalui buletin tersebut. Cubby berpendapat bahwa pengadilan harus menganggap CompuServe sebagai penerbit dari pernyataan yang diduga mencemarkan nama baik tersebut, dan dengan demikian menyatakannya bertanggung jawab atas pernyataan tersebut. Pengadilan memutuskan bahwa CompuServe tidak memiliki kendali editorial lebih besar atas publikasi tersebut daripada perpustakaan umum, toko buku, atau kios koran.

Sebaliknya, pengadilan menemukan CompuServe lebih mirip dengan distributor daripada penerbit. Dengan demikian, karena tidak dapat disangkal bahwa CompuServe tidak memiliki pengetahuan atau alasan untuk mengetahui pernyataan yang diduga bersifat mencemarkan nama baik yang dibuat dalam publikasi tersebut, terutama mengingat banyaknya publikasi yang dimuatnya dan kecepatan publikasi diunggah ke bank komputernya dan disediakan bagi pelanggan CompuServe, pengadilan memutuskan bahwa CompuServe tidak dapat dimintai pertanggungjawaban kepada Cubby atas pernyataan yang bersifat mencemarkan nama baik tersebut. Pengadilan mencatat bahwa memaksakan kewajiban CompuServe untuk memeriksa setiap publikasi yang dimuatnya untuk pernyataan yang bersifat mencemarkan nama baik akan memberikan beban yang tidak semestinya pada arus informasi yang bebas.

**15State Bank of India vs. Rizvi Exports Ltd.41**

State Bank of India (SBI) (Pemohon Banding) telah mengajukan kasus untuk menagih uang dari beberapa orang yang telah mengambil berbagai pinjaman darinya. Termohon: Rizvi Exports Ltd. Sebagai bagian dari bukti, SBI menyerahkan cetakan laporan rekening yang disimpan dalam sistem komputer SBI. Sertifikat yang relevan sebagaimana diamanatkan oleh Undang-Undang Buku Bukti Perbankan (sebagaimana diubah oleh Undang-Undang Teknologi Informasi) tidak dilampirkan pada cetakan ini. Pengadilan memutuskan bahwa dokumen-dokumen ini tidak dapat diterima sebagai bukti. Diputuskan pada: 01.10.2002

**17. Groff vs. America Online, Inc.42**

**Fakta**

Penggugat, seorang individu di Rhode Island yang berlangganan America Online, menggugat perusahaan tersebut di pengadilan negara bagian Rhode Island, dengan tuduhan pelanggaran undang-undang perlindungan konsumen negara bagian. Proses menjadi anggota AOL mencakup langkah di mana pemohon harus menyetujui persyaratan layanan AOL dengan mengeklik tombol "Saya Setuju". Persyaratan layanan "berisi klausul pemilihan forum yang secara tegas menyatakan bahwa hukum Virginia dan pengadilan Virginia adalah hukum dan forum yang tepat untuk litigasi antara anggota dan AOL."

AOL mengajukan permohonan untuk menolak gugatan ini dari Pengadilan Tinggi Rhode Osland karena tempat yang tidak tepat dengan alasan bahwa klausul pemilihan forum dalam kontrak para pihak mengamanatkan agar gugatan diajukan di Virginia, tempat basis operasi AOL berada. Pengadilan setuju, dan menolak gugatan tersebut.

**Putusan**

Pengadilan memutuskan bahwa penggugat menyetujui persyaratan layanan AOL secara daring dengan mengeklik tombol "Saya setuju". Persyaratan layanan tersebut mencakup klausul yang mengamanatkan agar gugatan terkait layanan diajukan di Virginia. Pelanggan AOL harus terlebih dahulu mengeklik tombol "Saya setuju" yang menunjukkan persetujuan untuk terikat oleh persyaratan layanan AOL sebelum mereka dapat menggunakan layanan tersebut. Tombol ini pertama kali muncul di halaman web tempat pengguna ditawari pilihan untuk membaca, atau sekadar setuju untuk terikat oleh, ketentuan layanan AOL.

Tombol ini juga muncul di bagian bawah ketentuan layanan, tempat pengguna ditawari pilihan untuk mengeklik tombol "Saya setuju" atau "Saya tidak setuju", yang dengannya ia menerima atau menolak ketentuan layanan. Pengadilan memutuskan bahwa kontrak yang sah ada, bahkan jika penggugat tidak mengetahui klausul pemilihan forum: "Pengadilan kami menyatakan aturan umum bahwa pihak yang menandatangani instrumen menyatakan persetujuannya terhadapnya dan tidak dapat kemudian mengeluh bahwa ia tidak membaca instrumen tersebut atau bahwa ia tidak memahami isinya. Di sini, penggugat secara efektif "menandatangani" perjanjian dengan mengeklik. "Saya setuju" tidak hanya sekali tetapi dua kali. Dalam keadaan ini, ia tidak boleh didengar untuk mengeluh bahwa ia tidak melihat, membaca, dll. dan terikat pada ketentuan perjanjiannya."

**18. Diebold Systems Pvt Ltd. vs. The Commissioner of Commercial Taxes43**

**Fakta**

Diebold Systems Pvt. Ltd. Pemohon banding memproduksi dan memasok Mesin Anjungan Tunai Mandiri (ATM). Diebold meminta klarifikasi dari Advance Ruling Authority (ARA) di Karnataka tentang tarif pajak yang berlaku berdasarkan Undang-Undang Pajak Penjualan Karnataka, 1957 atas penjualan Mesin Anjungan Tunai Mandiri.Pandangan mayoritas ARA adalah mengklasifikasikan ATM sebagai "terminal komputer" yang dikenakan pajak dasar sebesar 4% karena ATM termasuk dalam Entri 20(ii)(b) Bagian 'C' Jadwal Kedua Undang-Undang Pajak Penjualan Karnataka.

Ketua ARA tidak setuju dengan pandangan mayoritas. Menurut pendapatnya, ATM termasuk dalam deskripsi barang elektronik, suku cadang, dan aksesorinya. Dengan demikian, mereka akan menarik tarif pajak dasar sebesar 12% dan akan tergolong dalam Entri 4 Bagian 'E' dari Jadwal Kedua UU KST. Komisaris Pajak Komersial berpendapat bahwa putusan ARA keliru dan mengeluarkan perintah bahwa ATM tidak dapat diklasifikasikan sebagai terminal komputer. Temuan pengadilan:

1. Definisi "komputer" yang diperluas dalam Undang-Undang Teknologi Informasi tidak dapat digunakan untuk menafsirkan Entri berdasarkan undang-undang fiskal.
2. Mesin ATM adalah perangkat elektronik, yang memungkinkan nasabah bank untuk melakukan penarikan tunai, dan memeriksa saldo rekening mereka kapan saja tanpa perlu teller manusia.
3. ATM bukanlah komputer itu sendiri dan terhubung ke komputer yang melakukan tugas yang diminta oleh orang yang menggunakan ATM. Komputer terhubung secara elektronik ke banyak ATM yang mungkin terletak agak jauh dari komputer.

**Keputusan**

ATM bukanlah komputer, tetapi merupakan perangkat elektronik berdasarkan Undang-Undang Pajak Penjualan Karnataka tahun 1957.

**19. Manish Kathuria vs. State44**

Kasus cyberstalking pertama yang dilaporkan di India dan alasan amandemen Undang-Undang IT tahun 2008,5 kasus Manish Kathuria melibatkan penguntitan terhadap seorang wanita bernama Ritu Kohli. Kathuria mengikuti Kohli di situs web obrolan, melecehkannya dengan menggunakan bahasa cabul, lalu menyebarkan nomor teleponnya ke berbagai orang. Kemudian, dia mulai menggunakan identitas Kohli untuk mengobrol di situs web "www.mirc.com". Akibatnya, dia mulai menerima hampir empat puluh panggilan telepon cabul pada jam-jam aneh di malam hari selama tiga hari berturut-turut. Situasi ini memaksanya untuk melaporkan masalah tersebut ke Kepolisian Delhi.

Segera setelah pengaduan dibuat, Kepolisian Delhi melacak alamat IP dan menangkap Kathuria berdasarkan Pasal 509 KUHP India. Undang-Undang IT tidak digunakan dalam kasus tersebut, karena belum berlaku pada saat pengaduan diajukan. Meskipun tidak ada catatan tentang proses hukum selanjutnya, kasus ini membuat para legislator India menyadari perlunya undang-undang untuk mengatasi cyberstalking. Bahkan saat itu, baru pada tahun 2008 Pasal 66-A diperkenalkan. Akibatnya, sekarang kasus-kasus dilaporkan berdasarkan pasal ini dan bukan Pasal 509 KUHP India, seperti kasus seorang mahasiswa Universitas Delhi yang

ditangkap karena menguntit seorang wanita dari Goa dengan membuat profil palsu di situs jejaring sosial, mengunggah foto di sana, dan menyatakan wanita itu sebagai istrinya.

Diharapkan keputusan dalam kasus ini akan menguntungkan korban. Dalam kasus yang dikenal dengan nama Kasus Ritu Kohli, ini merupakan kasus pertama penguntitan siber di India. Ini merupakan pengungkapan penting dalam benak penguntit siber India. Seorang gadis muda India yang dikuntit siber oleh mantan kolega suaminya mengajukan tuntutan hukum terhadap penguntitan tersebut. Kasus Ritu Kohli menggemparkan India. Namun, kasus yang berhasil diungkap terjadi sebelum disahkannya Undang-Undang Siber India dan karenanya baru didaftarkan sebagai tindak pidana ringan menurut Kitab Undang-Undang Hukum Pidana India.

**20. Negara Bagian Maharashtra vs. Anand Ashok Khare45**

Kasus ini terkait dengan aktivitas insinyur Telekomunikasi berusia 23 tahun Anand Ashok Khare dari Mumbai yang menyamar sebagai peretas terkenal Dr Neuker dan melakukan beberapa upaya untuk meretas situs web Sel Siber kepolisian Mumbai.

**21. Firos vs. Negara Bagian Kerala46**

**Fakta**

Pemerintah Kerala mengeluarkan pemberitahuan u/s 70 Undang-Undang Teknologi Informasi yang menyatakan perangkat lunak aplikasi FRIENDS sebagai sistem yang dilindungi. Pembuat perangkat lunak aplikasi mengajukan petisi ke Pengadilan Tinggi terhadap pemberitahuan tersebut. Ia juga menggugat keabsahan konstitusional pasal 70 UU IT. Pengadilan menegakkan keabsahan pasal 70 UU IT dan pemberitahuan yang dikeluarkan oleh Pemerintah Kerala.

**Keputusan**

Tidak ada pertentangan antara ketentuan Undang-Undang Hak Cipta dan Pasal 70 Undang-Undang IT. Pasal 70 Undang-Undang IT tidak bertentangan dengan konstitusi. Saat menafsirkan pasal 70 Undang-Undang IT, diperlukan konstruksi yang harmonis dengan Undang-Undang Hak Cipta. Pasal 70 Undang-Undang IT tidak bertentangan tetapi tunduk pada ketentuan Undang-Undang Hak Cipta. Pemerintah tidak dapat secara sepihak menyatakan sistem apa pun sebagai "dilindungi" selain "karya Pemerintah" yang termasuk dalam pasal 2(k) Undang-Undang Hak Cipta yang hak cipta Pemerintahnya diakui berdasarkan Pasal 17(d) Undang-Undang tersebut.

**22. Negara Bagian Tamilnadu vs. Dr. L. Prakash47**

**Ringkasan kasus**

Negara Bagian Tamilnadu v/s Dr. L. Prakash adalah kasus penting di mana Dr. L. Prakash dijatuhi hukuman penjara seumur hidup dalam kasus yang berkaitan dengan kecabulan daring. Kasus ini juga menjadi tonggak sejarah dalam berbagai hal karena menunjukkan tekad penegak hukum dan peradilan untuk tidak membiarkan salah satu profesional India yang sangat terdidik dan canggih lolos begitu saja.

**23. Kasus Ayam Geprek Bensu vs. I Am Geprek Bensu**

**Fakta Kasus:** Ruben Onsu, pemilik brand Ayam Geprek Bensu, menggugat PT Ayam Geprek Benny Sujono yang menggunakan nama I Am Geprek Bensu. Kasus ini berfokus pada klaim pelanggaran merek dagang dan hak kekayaan intelektual.

**Masalah Hukum:**

- Ruben Onsu mengklaim bahwa penggunaan nama "I Am Geprek Bensu" oleh pihak lain dapat membingungkan konsumen dan merugikan reputasi mereknya.
- Pengadilan harus menentukan apakah penggunaan nama tersebut merupakan pelanggaran merek dagang yang sah.

**Keputusan Pengadilan:** Pengadilan Niaga Jakarta Pusat menolak gugatan Ruben Onsu dan mengakui PT Ayam Geprek Benny Sujono sebagai pemilik sah merek "I Am Geprek Bensu". Keputusan ini didasarkan pada fakta bahwa merek tersebut telah terdaftar lebih dahulu

**24. Ashcroft, Attorney General et al vs. Free Speech Coalition, et al.49**

**Fakta**

Mahkamah Agung AS menegaskan putusan Pengadilan Banding untuk Sirkuit Kesembilan bahwa larangan Pasal 2256 (8) (B) dan 2256(8) (D) berlebihan dan tidak konstitusional. Menjadi bagian dari Undang-Undang Pencegahan Pornografi Anak tahun 1996 (CPPA) S. 2256 (8) (B) melarang berbagai gambar eksplisit seksual, terkadang disebut pornografi anak virtual, yang tampak menggambarkan anak di bawah umur tetapi diproduksi dengan cara lain selain menggunakan anak-anak sungguhan, seperti melalui penggunaan orang dewasa yang tampak muda atau teknologi pencitraan komputer dan S.2256(8)(D) ditujukan untuk mencegah produksi atau distribusi materi pornografi yang disebut sebagai pornografi anak.

**Hakim Kennedy berpendapat:**

Kongres dapat mengeluarkan undang-undang yang sah untuk melindungi anak-anak dari pelecehan, dan itu telah terjadi. Prospek kejahatan. Namun, dengan sendirinya tidak membenarkan undang-undang yang menekan kebebasan bicara yang dilindungi. Sebagai prinsip umum, Amandemen Pertama melarang pemerintah mendikte apa yang dilihat atau dibaca atau diucapkan atau didengar. Kebebasan berbicara memiliki batasannya; itu tidak mencakup kategori ucapan tertentu, termasuk pencemaran nama baik, hasutan, kecabulan, dan pornografi yang diproduksi dengan anak-anak sungguhan. Pemerintah berpendapat bahwa pornografi anak virtual membangkitkan selera para pedofil dan mendorong mereka untuk terlibat dalam tindakan ilegal.

Alasan ini tidak dapat mendukung ketentuan yang dimaksud. Kecenderungan ujaran untuk mendorong tindakan ilegal saja tidak cukup menjadi alasan untuk melarangnya. Pemerintah secara konstitusional tidak dapat mendasarkan undang-undang pada keinginan untuk mengendalikan pikiran pribadi seseorang. Kebebasan Amandemen Pertama paling terancam ketika pemerintah berupaya mengendalikan pikiran atau membenarkan hukumnya untuk tujuan yang tidak diizinkan itu. Hak untuk berpikir adalah awal dari kebebasan, dan ujaran harus dilindungi dari pemerintah karena ujaran adalah awal dari pikiran.

**25. State vs. Amit Prasad 50**

State vs. Amit Prasad, merupakan kasus peretasan pertama di India yang terdaftar berdasarkan Pasal 66 Undang-Undang Teknologi Informasi tahun 2000. Kasus ini merupakan kasus dengan fakta yang unik, yang menunjukkan bagaimana ketentuan hukum siber India dapat ditafsirkan dengan cara apa pun, tergantung pada pihak yang dirugikan.

**26. R vs. Graham Waddon 51**

**Fakta**

Terdakwa didakwa dengan sejumlah tuduhan menerbitkan artikel cabul yang bertentangan dengan Pasal 2(1) Undang-Undang Publikasi Cabul Inggris tahun 1959. Terdakwa telah membuat gambar-gambar porno, yang ilegal berdasarkan Undang-Undang Publikasi Cabul Inggris. Ia mengelola serangkaian situs yang berbasis di AS, yang menghostingnya di penyedia layanan internet yang berbasis di AS. Gambar-gambar ini dapat diakses oleh siapa saja di dunia melalui internet yang menjadi pelanggan dengan memberikan rincian kartu kredit. Ia mengenakan biaya kepada pelanggan Inggris sebesar 25 pound per bulan untuk akses. Pelanggan diberi kata sandi dan dapat masuk ke berbagai situs web untuk mendapatkan gambar-gambar tersebut. Tergugat mengajukan bahwa, karena publikasi Internet tersebut telah terjadi di luar negeri, maka pengadilan saat ini tidak memiliki yurisdiksi.

Hardy Christopher, J. Berpendapat bahwa penerbitan artikel berdasarkan S. 1(3) (b) Undang-Undang 1959 mencakup data yang disimpan secara elektronik dan dikirimkan. Mengirimkan berarti mengirim dari satu tempat atau orang ke tempat atau orang lain. Dalam kasus saat ini, tindakan publikasi terjadi ketika data dikirimkan oleh tergugat atau agennya ke penyedia layanan, dan publikasi atau pengiriman tersebut pada dasarnya masih berlangsung ketika data diterima. Baik pengiriman maupun penerimaan terjadi dalam yurisdiksi pengadilan dan tidak relevan bahwa pengiriman tersebut mungkin telah meninggalkan yurisdiksi antara pengiriman dan penerimaan.

**27. Kasus Arzika51**

Pornografi dan konten elektronik cabul terus menarik perhatian masyarakat India. Kasus-kasus yang berkaitan dengan kecabulan daring, meskipun dilaporkan di media, sering kali tidak terdaftar. Kasus Arzika adalah yang pertama dalam hal ini.

**28. Air Force Bal Bharti School & Anr. vs. Delhi School Tribunal & Ors.52**

**Kasus**

Air Force Bal Bharti School menunjukkan bagaimana Pasal 67 Undang-Undang Teknologi Informasi, 2000 dapat diterapkan untuk konten cabul yang dibuat oleh seorang anak laki-laki yang bersekolah. Seorang anak laki-laki berusia 16 tahun ditangkap pada bulan April 2001 atas tuduhan membuat situs web pornografi yang berisi komentar cabul tentang beberapa guru perempuan dan anak perempuan di sekolahnya, Air Force Bal Bharati di Delhi. Ketika ia dibebaskan dengan jaminan, sekolah menolak untuk menerimanya kembali.

**29. Sri Prabhakar Singh vs. Union of India53**

P.R. Transport Agency melalui mitranya Sri Prabhakar Singh Vs. Union of India (UOI) melalui Sekretaris, Kementerian Batubara, Bharat Coking Coal Ltd. melalui Ketua, Kepala Manajer Penjualan Penjualan Jalan Raya, Bharat Coking Coal Ltd. dan Metal and Scrap Trading

Corporation Ltd. (MSTC Ltd.) melalui Ketua merangkap Direktur Pelaksana., Petisi Surat Perintah No. 58468 tahun 2005.

**Riwayat kasus**

Bharat Coking Coal Ltd. (BCC) mengadakan lelang elektronik untuk batu bara dalam beberapa lot. Penawaran P.R. Transport Agency (PRTA) diterima untuk 4000 metrik ton batu bara dari Tambang Batubara Dobari. Surat penerimaan diterbitkan pada tanggal 19 Juli 2005 melalui email ke alamat email PRTA. Berdasarkan penerimaan ini, PRTA menyetorkan jumlah penuh sebesar Rs. 81,12 lakh melalui cek yang ditujukan kepada BCC. Cek ini diterima dan dicairkan oleh BCC. BCC tidak mengirimkan batu bara tersebut kepada PRTA. Sebaliknya, BCC mengirim email kepada PRTA yang menyatakan bahwa penjualan dan lelang elektronik yang ditujukan kepada PRTA dibatalkan karena beberapa alasan teknis dan tidak dapat dihindari.

Satu-satunya alasan pembatalan ini adalah karena ada orang lain yang tawarannya untuk batu bara yang sama sedikit lebih tinggi daripada PRTA. Karena beberapa kelemahan pada komputer atau program atau pemasukan datanya, tawaran yang lebih tinggi tidak dipertimbangkan sebelumnya. Komunikasi ini ditentang oleh PRTA di Pengadilan Tinggi Allahabad. BCC menolak yurisdiksi teritorial pengadilan dengan alasan bahwa tidak ada bagian dari penyebab gugatan yang muncul di U.P.

**Masalah yang diajukan oleh BCC**

Pengadilan Tinggi di Allahabad (di U.P.) tidak memiliki yurisdiksi karena tidak ada bagian dari penyebab gugatan yang muncul di U.P.

**Masalah yang diajukan oleh PRTA**

1. Komunikasi penerimaan tender diterima oleh pemohon melalui email di Chandauli (U.P.). Oleh karena itu kontrak (yang menjadi sumber perselisihan) diselesaikan di Chandauli (U.P). Penyelesaian kontrak merupakan bagian dari "penyebab gugatan".
2. Tempat di mana kontrak diselesaikan dengan diterimanya komunikasi penerimaan adalah tempat di mana 'bagian dari penyebab gugatan' muncul.

**Pengamatan oleh pengadilan:**

1. Terkait kontrak yang dibuat melalui telepon, teleks, atau faks, kontrak dianggap lengkap saat dan di mana penerimaan diterima. Akan tetapi, asas ini hanya dapat diterapkan jika terminal pengirim dan terminal penerima berada di titik tetap.
2. Dalam kasus e-mail, data (dalam hal ini penerimaan) dapat dikirimkan dari mana saja oleh pemegang akun e-mail. Data tersebut masuk ke memori 'server' yang dapat berlokasi di mana saja dan dapat diambil oleh pemegang akun penerima dari mana saja di dunia. Oleh karena itu, tidak ada titik tetap baik pengiriman maupun penerimaan.
3. Pasal 13(3) Undang-Undang Teknologi Informasi telah mencakup kesulitan "tidak ada titik tetap baik pengiriman maupun penerimaan". Menurut pasal ini, "catatan elektronik dianggap diterima di tempat penerima berkantor."
4. Penerimaan tender akan dianggap diterima oleh PRTA di tempat-tempat ia berkantor. Dalam kasus ini, Varanasi dan Chandauli (keduanya di U.P.)

**Keputusan**

1. Penerimaan diterima oleh PRTA di Chandauli/Varanasi. Kontrak menjadi lengkap dengan diterimanya penerimaan tersebut.
2. Kedua tempat ini berada dalam yurisdiksi teritorial Pengadilan Tinggi Allahabad. Oleh karena itu, sebagian penyebab gugatan muncul di U.P. dan pengadilan memiliki yurisdiksi teritorial.

**30. Washington Post vs. Total News 55**

**Riwayat kasus:**

Di mana situs web "totalnews.com" menggunakan teknologi pembingkaian untuk menempatkan berita dari situs web lain dalam bingkai Total News secara keseluruhan dengan memblokir iklan banner dan fitur pembeda lainnya. Pengadilan Distrik AS Distrik Selatan New York mengeluarkan perintah penyelesaian yang menyatakan bahwa "para tergugat setuju secara permanen untuk menghentikan praktik pembingkaian situs web penggugat". Penggugat setuju bahwa Tergugat dapat membuat tautan dari situs web Totalnewa.com atau situs web lain ke situs web penggugat mana pun, dengan ketentuan bahwa:

1. Tergugat dapat membuat tautan ke situs web penggugat hanya melalui hyperlink yang terdiri dari nama-nama situs yang ditautkan dalam teks biasa, yang dapat disorot.
2. Tergugat tidak boleh menggunakan di situs web mana pun, sebagai hyperlink atau dengan cara lain, logo milik penggugat atau materi grafis, video, atau audio khas lainnya, dan tergugat juga tidak boleh membuat tautan dengan cara apa pun yang secara wajar dapat menyiratkan afiliasi dengan, dukungan, atau sponsor oleh penggugat mana pun, menyebabkan kebingungan, kesalahan, atau penipuan, mengencerkan merek penggugat atau melanggar hukum negara bagian atau federal dengan cara lain.
3. Setiap persetujuan penggugat untuk mengizinkan penautan oleh tergugat tetap dapat dibatalkan, dengan pemberitahuan 15 hari kerja, atas kebijakan masing-masing Penggugat. Pencabutan oleh penggugat mana pun tidak akan memengaruhi syarat dan ketentuan lain yang ditetapkan di sini. Jika tergugat menolak untuk menghentikan tautan setelah pemberitahuan, dan penggugat mengajukan gugatan untuk menegakkan haknya berdasarkan subparagraf ini, maka akan menjadi pembelaan tegas bahwa tindakan tergugat tidak melanggar atau menyalahi hak penggugat berdasarkan teori apa pun tentang kekayaan intelektual, persaingan tidak sehat, atau hukum lainnya.

# BAB 6
# HUKUM SIBER

## 6.1 TREN UU ITE DI INDONESIA

Tren hukum siber di Indonesia menunjukkan perkembangan yang signifikan, seiring dengan meningkatnya ancaman kejahatan siber dan kebutuhan untuk melindungi data serta privasi masyarakat. Jumlah kasus kejahatan siber di Indonesia terus meningkat, dengan laporan Badan Siber dan Sandi Negara (BSSN) mencatat lonjakan serangan siber sebesar 22% pada tahun 2022 dibandingkan tahun sebelumnya. Jenis serangan yang umum terjadi meliputi phishing, malware, ransomware, dan DDoS. Untuk menghadapi ancaman ini, Indonesia telah memperbarui regulasi hukum siber melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diamandemen dengan UU Nomor 16 Tahun 2019 dan UU Nomor 1 Tahun 2024.

Perubahan tersebut mencakup penambahan jenis tindak pidana baru terkait penyalahgunaan teknologi informasi serta peningkatan ancaman pidana untuk pelanggaran tertentu, seperti illegal access. Selain itu, dengan semakin banyaknya data pribadi yang diproses secara online, perlindungan data pribadi menjadi fokus utama, yang diwujudkan dalam pengesahan Undang-Undang Perlindungan Data Pribadi sebagai kerangka hukum untuk melindungi informasi pribadi individu dari penyalahgunaan dan kebocoran data. Meskipun kesadaran masyarakat tentang pentingnya keamanan siber semakin meningkat, masih terdapat kekurangan pemahaman tentang cara melindungi diri dari ancaman siber, sehingga upaya edukasi dan peningkatan kesadaran perlu terus diperkuat.

Peningkatan kasus kejahatan siber juga menjadi perhatian serius, dengan jenis kejahatan yang umum meliputi penipuan online, serangan malware, dan phishing. Kejahatan-kejahatan ini memanfaatkan teknologi untuk merusak sistem, mencuri data pribadi, dan merugikan korban secara finansial. Meskipun masyarakat semakin menyadari pentingnya keamanan siber, masih ada kekurangan pemahaman mengenai cara melindungi diri dari ancaman siber. Oleh karena itu, edukasi tentang keamanan informasi menjadi aspek penting yang harus terus digalakkan.

Meskipun ada kemajuan dalam regulasi, tantangan utama yang masih dihadapi adalah implementasi hukum yang efektif. Banyak pihak menganggap bahwa regulasi yang ada masih terlalu umum dan tidak cukup responsif terhadap perkembangan teknologi yang sangat cepat. Oleh karena itu, meskipun perubahan dalam UU ITE dan penguatan regulasi lainnya adalah langkah positif, Indonesia masih perlu terus beradaptasi dan memastikan bahwa hukum siber dapat efektif menghadapi ancaman yang semakin kompleks.

Dalam menghadapi kejahatan siber, kerjasama antara sektor publik dan swasta juga menjadi kunci, dengan pemerintah melalui BSSN bertanggung jawab untuk menjaga

keamanan siber, namun kolaborasi lebih lanjut antara semua pihak diperlukan untuk meningkatkan efektivitas penegakan hukum. Secara keseluruhan, tren hukum siber di Indonesia mencerminkan kebutuhan mendesak untuk memperkuat regulasi, meningkatkan kesadaran masyarakat, dan mendorong kolaborasi lintas sektor dalam menghadapi ancaman kejahatan siber yang terus berkembang, guna melindungi masyarakat dari dampak negatifnya.

**Tren Terkini dalam Hukum Siber di Indonesia**

1. **Peningkatan Kasus Kejahatan Siber**

Kejahatan siber di Indonesia, seperti penipuan online, pencurian data, dan serangan ransomware, terus meningkat. Laporan menunjukkan bahwa kejahatan ini telah menjadi salah satu isu utama yang dihadapi oleh masyarakat dan pemerintah. Dalam konteks ini, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi alat utama untuk menanggulangi masalah ini.

2. **Revisi UU ITE**

Revisi UU ITE yang disahkan pada tahun 2024 membawa sejumlah perubahan penting:

- **Penghapusan Pasal Kontroversial**: Pasal yang mengatur penghinaan dan pencemaran nama baik telah dihapus untuk mengurangi potensi penyalahgunaan.
- **Penambahan Ketentuan Baru**: Pengenalan pasal tentang larangan penyebaran berita bohong dan perlindungan data pribadi.
- **Wewenang Pemerintah**: Penambahan wewenang bagi pemerintah untuk mengatur penyelenggara sistem elektronik dalam rangka melindungi masyarakat dari kejahatan siber.

3. **Perlindungan Data Pribadi**

Pengesahan Undang-Undang Perlindungan Data Pribadi pada tahun 2022 memberikan kerangka hukum yang lebih jelas untuk melindungi informasi pribadi individu. Ini penting dalam konteks meningkatnya jumlah pelanggaran data yang terjadi.

**Tantangan dalam Implementasi Hukum Siber**

1. **Kesadaran Masyarakat yang Rendah**

Meskipun ada regulasi yang lebih baik, kesadaran masyarakat tentang keamanan siber dan hak-hak mereka di dunia maya masih rendah. Edukasi tentang cara melindungi diri dari ancaman siber perlu ditingkatkan.

2. **Sumber Daya Penegakan Hukum**

Aparat penegak hukum sering kali kekurangan sumber daya dan pelatihan yang diperlukan untuk menangani kasus-kasus kejahatan siber secara efektif. Modernisasi kepolisian dan peningkatan kemampuan investigasi diperlukan.

3. **Perlunya Kerjasama Internasional**

Kejahatan siber sering kali bersifat lintas negara, sehingga kerjasama internasional sangat penting. Indonesia perlu memperkuat hubungan dengan negara lain dalam hal pertukaran informasi dan strategi penanggulangan kejahatan siber.

**Langkah-Langkah Mengatasi Kejahatan Siber**

1. **Peningkatan Kapasitas Penegakan Hukum**

Pemerintah telah berupaya meningkatkan kapasitas aparat penegak hukum melalui pelatihan dan penyediaan alat teknologi yang memadai untuk menangani kejahatan siber.

2. **Edukasi Masyarakat**

Program-program edukasi tentang keamanan siber mulai diperkenalkan di sekolah-sekolah dan komunitas untuk meningkatkan kesadaran masyarakat akan risiko di dunia maya.

3. **Kerjasama dengan Sektor Swasta**

Pemerintah bekerja sama dengan perusahaan teknologi dan penyedia layanan internet untuk menciptakan sistem keamanan yang lebih baik dan berbagi informasi tentang ancaman siber.

**Kesimpulan**

Tren hukum siber di Indonesia menunjukkan adanya kemajuan dalam regulasi dan penegakan hukum terkait kejahatan siber. Namun, tantangan seperti kesadaran masyarakat yang rendah, kekurangan sumber daya penegakan hukum, dan perlunya kerjasama internasional masih perlu ditangani secara serius. Dengan langkah-langkah yang tepat, diharapkan Indonesia dapat menciptakan lingkungan digital yang lebih aman bagi semua warganya.

## 6.2 TREN UU TI, 2000 DI INDIA

Undang-Undang Teknologi Informasi, 2000 (UU TI 2000) masih mengatur hukum siber India dan isu-isu terkait. UU TI, 2000 telah menjadi hukum yang berlebihan dan kejam yang perlu dicabut. Hukum telegraf dan siber India tetap ketinggalan zaman, kolonial, dan kejam pada tahun 2014 juga. India harus memastikan langkah-langkah hukum teknologi untuk mengatur dunia siber India. Demikian pula, peraturan dan pedoman untuk investigasi kejahatan siber yang efektif di India juga dibutuhkan saat ini. Pemerintah India telah memastikan pada tahun 2014 bahwa UU TI, 2000 dapat diamandemen untuk mengakomodasi masalah e-commerce.

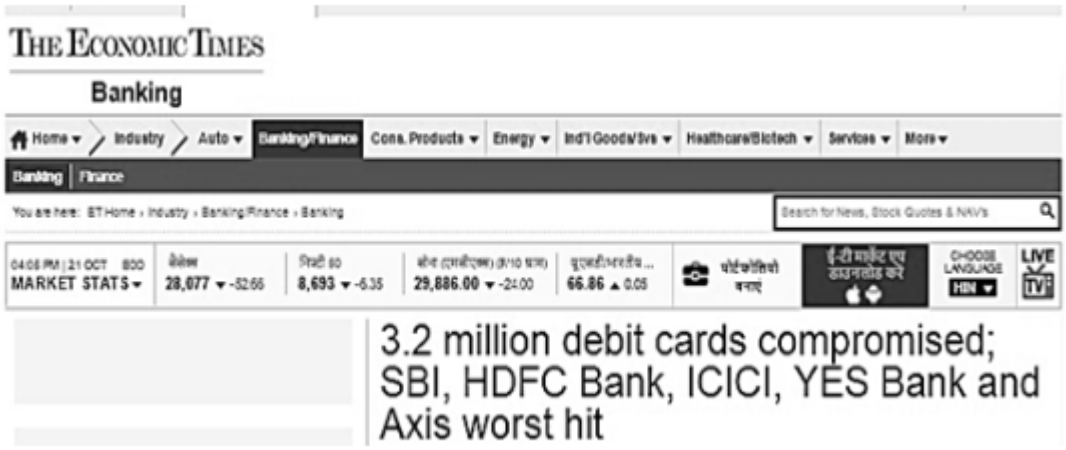
Perkembangan teknologi telah melahirkan dunia siber yang membentuk ruang siber. Ruang siber mengalami kemajuan yang cukup besar dengan peningkatan pesat dalam teknologi informasi. Selalu sulit untuk menentukan atau memprediksi sesuatu di masa depan secara akurat. Ada kemungkinan untuk mengkonsolidasikan kemajuan teknologi di masa lalu. Pengguna internet meningkat pesat setiap tahun dan pada saat yang sama juga terjadi peningkatan jumlah orang yang menggunakan ponsel dan telepon pintar.

**Tren dan perkembangan hukum siber di India adalah sebagai berikut:**

1. Strategi Pencegahan Kejahatan Siber: Kejahatan siber telah meningkat secara signifikan di India dalam beberapa tahun terakhir. Menanggapi hal yang sama, Pemerintah India kini telah memutuskan untuk merumuskan strategi pencegahan kejahatan siber untuk India. Namun, hingga saat ini, strategi yang diusulkan belum dirumuskan.
2. Pelatihan Investigasi Kejahatan Siber: Dengan meningkatnya kejahatan siber di India, dirasakan perlunya memberikan pelatihan investigasi kejahatan siber kepada lembaga penegak hukum India. India perlu meningkatkan kemampuan investigasi kejahatan siber sehingga kejahatan siber dapat ditangani secara efektif. Demikian pula,

modernisasi kepolisian India sangat dibutuhkan dengan fokus khusus pada pengembangan keterampilan teknis hukum bagi mereka.

3. Undang-Undang Enkripsi: Hampir enam tahun yang lalu Komite Tetap Teknologi Informasi menarik Departemen Telekomunikasi (DOT) atas masalah enkripsi. Undang-undang dan peraturan enkripsi di India perlu diperjelas. Risiko hukum bagi perusahaan pengembangan situs web di India juga akan meningkat karena penggunaan enkripsi yang tidak tepat untuk situs web tersebut. Kebijakan enkripsi khusus India dan undang-undang enkripsi teknis di India sangat dibutuhkan saat ini.
4. ATM Bank Dibobol: Baru-baru ini, pada tanggal 20 Oktober 2016, dilaporkan bahwa sekitar 3,2 juta kartu debit nasabah bank dibobol. Di antara banyak yang terkena dampak, SBI, HDFC Bank, ICICI, YES Bank, dan Axis Bank adalah yang paling parah terkena dampaknya. Bank-bank di India akan mengganti atau meminta pengguna untuk mengubah kode keamanan untuk lebih dari 3,2 juta kartu debit.




*Reproduced from The Economic Times*

**Gambar 6.1 Kartu Debit dari SBI, HDFC, ICICI, YES Bank, dan Axis Bank Terancam dalam Insiden Keamanan Data**

5. Investigasi Penipuan Korporat: Meskipun Undang-Undang Perusahaan, 2013 telah dirumuskan untuk mengekang penipuan korporat, namun peraturan khusus tentang MLM yang bersifat penipuan sangat dibutuhkan saat ini. Kewenangan Kantor Investigasi Penipuan Serius (SFIO) juga ditingkatkan sehingga mereka dapat secara efektif menangani penipuan dan kejahatan korporat di India. SEBI juga telah memberitahukan Peraturan Dewan Sekuritas dan Bursa India (Prosedur Penggeledahan dan Penyitaan), 2014.
6. Asuransi Siber: Asuransi siber di India menjadi kenyataan pada tahun 2014 dan banyak perusahaan dan individu telah mulai mengambil polis asuransi siber di India. Namun, bisnis asuransi siber akan menimbulkan banyak masalah hukum teknologi baru dalam hal ini yang harus dipersiapkan dengan baik oleh semua pemangku kepentingan.

7. Komputasi Awan: Masalah hukum komputasi awan di India masih belum jelas dan hal ini mengakibatkan terbatasnya adopsi komputasi awan di India. Persyaratan hukum dan peraturan komputasi awan di India untuk bisnis dan pengusaha harus dianalisis terlebih dahulu sebelum meluncurkan proyek. Penyedia layanan komputasi awan di India adalah perantara internet dalam pengertian Undang-Undang TI tahun 2000 dan mereka juga diharuskan untuk mematuhi persyaratan uji tuntas hukum siber.
8. Kebijakan Surel: Kebijakan surel India masih belum diterapkan meskipun ada peringatan keras dari Pengadilan Tinggi Delhi. Situasinya sangat buruk sehingga Pengadilan Tinggi Delhi menuduh pemerintah pusat ikut campur dalam kebijakan surel India. Pengadilan Tinggi Delhi juga telah memerintahkan Pemerintah Pusat untuk mengeluarkan pemberitahuan mengenai tanda tangan elektronik berdasarkan Undang-Undang Teknologi Informasi tahun 2000. Kebijakan enkripsi India juga belum ada hingga saat ini meskipun itu sangat dibutuhkan. Namun, Madhya Pradesh telah memberikan pengakuan hukum terhadap komunikasi surel di antara Departemen Pemerintah.
9. Pembayaran Daring: Pembayaran daring dan seluler mengalami peningkatan di India dalam dekade terakhir. Namun, berbagai penyedia pembayaran seluler di India tidak menganggap serius masalah hukum dan peraturan. Ada banyak masalah hukum e-commerce di India yang harus dipatuhi oleh berbagai penyedia layanan pembayaran daring India. Pengadilan tersebut telah menetapkan persyaratan uji tuntas hukum siber untuk Paypal dan transfer pembayaran daring di India. Demikian pula, kami juga telah menguraikan kepatuhan hukum e-commerce dan bisnis daring untuk pasar pembayaran daring di India. Lebih jauh, penyedia layanan gerbang pembayaran dan terminal POS juga harus mengingat persyaratan uji tuntas hukum siber di India.
10. Perjudian Daring di India: Undang-undang perjudian daring di India masih ditangguhkan. Perjudian daring di India masih dapat dihukum dalam hampir semua kasus dengan beberapa pengecualian selektif. Masalah ini masih menunggu keputusan Mahkamah Agung India dan telah merujuk masalah tersebut untuk mendapatkan pendapat dari Pemerintah Pusat. Namun, Pemerintah Pusat belum memberikan pendapat konklusif tentang masalah ini sejauh ini.
11. Pemblokiran Situs Web di India: Pemblokiran situs web di India merupakan perkembangan lain yang juga mengakibatkan banyak protes. Misalnya, situs web Tamil Savukku diperintahkan untuk diblokir oleh Pengadilan Tinggi Madras. Namun, segera setelah pemblokiran situs web Savukku, situs tersebut tersedia melalui server proxy sehingga pemblokiran menjadi tidak diperlukan lagi. Pada tahun 2013, Pemerintah India memblokir 39 situs Internet atas dasar pornografi. Mahkamah Agung India juga meminta tanggapan Pemerintah India terkait hal ini pada tahun 2013. Akan tetapi, Penyedia Layanan Internet (ISP) India memberi tahu Mahkamah Agung bahwa mereka tidak dapat memblokir situs web pornografi secara sepihak dan sukarela.
12. Bitcoin: Legalitas bitcoin di India menjadi pertanyaan besar pada tahun 2014. Direktorat Penegakan Hukum (ED) menggeledah dan menggerebek beberapa bursa

Bitcoin untuk melihat apakah mereka melanggar hukum India atau tidak. ED yakin bahwa Bitcoin dapat digunakan untuk kegiatan kriminal termasuk pencucian uang, transaksi hawala, dan pendanaan kegiatan teroris. Indian Laxmicoin bahkan telah meminta klarifikasi dari otoritas regulasi India sebelum peluncurannya. Serangan siber juga menargetkan pengguna Bitcoin dan Bursa Bitcoin pada tahun 2014. Menurut beberapa laporan, situs web Bitcoin Mt. Gox menghilang karena serangan siber canggih dan pencurian Bitcoin. RBI memberi tahu bahwa mereka tidak dapat mengatur Bitcoin.

13. Aplikasi Seluler: Aplikasi seluler juga mengalami peningkatan luar biasa di India dalam beberapa tahun terakhir. Namun, sebagian besar pengembang aplikasi seluler melanggar Hukum India dan dapat dituntut di masa mendatang.
14. Uji Tuntas Hukum Siber: Persyaratan Uji Tuntas Hukum Siber di India diabaikan oleh berbagai pemangku kepentingan. Pemerintah India tetap acuh tak acuh sementara persyaratan Uji Tuntas Hukum Siber dilanggar oleh Perusahaan Telekomunikasi, Situs Web E-commerce, dll.
15. Tanggung Jawab Perantara Internet: Tanggung Jawab Perantara Internet di India terkait erat dengan Kepatuhan Uji Tuntas Hukum Siber. Karena banyak pemangku kepentingan gagal memastikan Kepatuhan Uji Tuntas Hukum Siber, mereka melanggar Peraturan Teknologi Informasi (Pedoman Perantara) India tahun 2011.
16. Pelanggaran Perusahaan Telekomunikasi: Tata Teleservices Limited (TTL) dan Airtel Melanggar Hukum Siber India dan Peraturan Perantara Internet India. Keluhan terhadap Tata dan Airtel sudah tertunda di Departemen Telekomunikasi dan Otoritas Regulasi Telekomunikasi India (TRAI).
17. Persyaratan E-Discovery: Kebutuhan E-Discovery bagi perusahaan-perusahaan India telah meningkat secara signifikan dan bahkan akan terus meningkat di tahun-tahun mendatang. Ketidakpatuhan Hukum Siber telah menimbulkan peningkatan permintaan untuk E-Discovery di India.
18. Penipuan Korporasi di India: Investigasi Penipuan Korporasi di India telah menjadi multidisiplin. Selain penipuan korporat tradisional, kini Kejahatan Siber dan Penipuan Teknologi juga telah menjadi bagian dari Investigasi Penipuan Korporasi di India.
19. Kerjasama Kejahatan Siber Indo-Amerika: Jaringan peringatan, pengawasan, dan pengawasan Indo-Amerika untuk berbagi informasi waktu nyata dalam Kasus Kejahatan Siber telah dibentuk untuk menangani kasus Kejahatan Siber yang termasuk dalam yurisdiksi India dan Amerika.
20. Uji Tuntas Terkait Korupsi dan Teknologi: Selain Uji Tuntas Hukum Siber, cakupan uji tuntas terkait Korupsi dan Teknologi India dan Asing di India juga telah meningkat. Dengan disahkannya Undang-Undang Lokpal dan Lokayuktas, 2013 oleh Parlemen India, tekanan pada lingkungan bebas korupsi telah dibuat. Bahkan izin Pemerintah Pusat tidak lagi diperlukan oleh CBI untuk menuntut birokrat senior atas kasus korupsi yang dipantau oleh Mahkamah Agung India.

21. Pelecehan dan Penguntitan Siber: Kasus Pelecehan dan Penguntitan Siber telah meningkat di India. Situs web seperti OLX menjadi tempat berkembang biaknya Pelecehan dan Penguntitan Siber. Lebih jauh, tuduhan penjualan barang curian juga dilayangkan kepada OLX.
22. Kepatuhan terhadap E-Commerce: Situs web yang menyediakan layanan E-Commerce di India tidak mematuhi Hukum India. Situs web e-Commerce harus diatur di India karena beroperasi dengan sangat mengabaikan Hukum India. Meskipun Pemerintah India telah menjamin bahwa E-Commerce di India akan diatur oleh pedoman yang komprehensif, namun hingga saat ini belum ada tanda-tanda seperti itu yang ditunjukkan oleh Pemerintah.
23. Legalitas Bitcoin: Kegilaan Bitcoin akhirnya mulai memudar karena Bank Sentral India (RBI) mengeluarkan Peringatan terhadap penggunaan Bitcoin di India dengan alasan Keamanan Siber dan Risiko Hukum. Direktorat Penegakan Hukum (ED) juga menggeledah kantor dan situs web Seven Digital Cash LLP untuk penjualan dan pembelian Bitcoin di India. Legalitas Bitcoin di India selalu diragukan. Banyak negara seperti Tiongkok, Prancis, Thailand, Norwegia, dll. telah mengatur penggunaan Bitcoin atau melarangnya sepenuhnya di wilayah hukum mereka.
24. Konflik Hukum di Dunia Maya: Masalah lain yang tidak ingin diselesaikan Pemerintah India berkaitan dengan Konflik Hukum di Dunia Maya India. Selama ini, Perusahaan seperti Google, Facebook, dll. telah melanggar Hukum India. Pemerintah India belum mengambil sikap tegas terhadap Perusahaan Asing tersebut yang meskipun beroperasi di India untuk mencari keuntungan tetapi tidak mematuhi Hukum India. Misalnya, G-Mail mendukung dan mendorong terjadinya berbagai Kejahatan Dunia Maya di India tetapi Pemerintah India telah mengizinkannya beroperasi sejauh ini.
25. Kebijakan Email India: Tidak ada Kebijakan Email India yang operasional. Pengadilan Tinggi Delhi sedang menganalisis Kebijakan Email India dan mekanisme pengaduan ke Facebook. Pengadilan Tinggi Delhi juga telah memerintahkan Pemerintah Pusat untuk mengeluarkan Pemberitahuan mengenai Tanda Tangan Elektronik berdasarkan Undang-Undang Teknologi Informasi tahun 2000. Sebuah Imbauan oleh Pemerintah Maharashtra untuk menggunakan Email Resmi telah dikeluarkan. Bahkan Kebijakan Email India sedang dalam proses.
26. Kejahatan Dunia Maya dan Satwa Liar: Para penjahat dunia maya tidak menyia-nyiakan kesempatan untuk terlibat dalam Kejahatan Dunia Maya di India. Para penjahat dunia maya mencoba membobol Kalung Satelit GPS Iridium milik seekor Harimau. Upaya membobol kalung tersebut dilakukan dari Pune sedangkan harimau yang memakai kalung tersebut berada di tempat yang sangat jauh di cagar alam harimau Madhya Pradesh. Biro Pengendalian Kejahatan Alam Liar (WCCB) juga baru-baru ini melacak sedikitnya 200 situs web di seluruh negeri, yang digunakan oleh orang-orang untuk memperdagangkan bagian-bagian tubuh hewan. Jadi Kejahatan Dunia Maya di India terus berkembang dan Badan Penegak Hukum India harus diperlengkapi dengan baik untuk menangani Kejahatan tersebut.

27. Gangguan Pornografi Anak: Pornografi Anak di India menjadi gangguan besar. Sebuah Nasihat dari Kementerian Dalam Negeri India tentang Pencegahan dan Pemberantasan Kejahatan Dunia Maya terhadap Anak-anak di India juga telah dikeluarkan. Baru-baru ini Interpol membantu India dalam melacak peselancar pornografi anak. Kita juga memerlukan Kerangka Kerja Hukum Teknologi semacam itu sehingga pornografi anak dapat dikekang semaksimal mungkin di India.
28. Perjudian Daring di India: Meskipun kita tidak memiliki Undang-Undang Perjudian Daring khusus di India, perjudian daring diatur secara adil di India berdasarkan berbagai Undang-Undang. Dengan terlibat dalam perjudian secara daring dan luring, orang atau perusahaan yang bersangkutan akan melanggar Hukum India. Banyak pemerasan perjudian daring yang digagalkan pada tahun 2013 dan Pemerintah India harus mempertimbangkan secara serius regulasi Perjudian Daring di India.
29. Apotek Daring di India: Apotek Daring di India berada di bawah pengawasan regulasi di seluruh dunia, termasuk India. Penjualan obat resep daring di India pada umumnya tidak diatur dan terbuka untuk penyalahgunaan. Faktanya, penjualan obat resep daring yang ilegal dan tidak diatur di India berkembang pesat seperti wabah. Pemerintah India harus memikirkan dengan serius bidang ini. Sementara itu, berbagai pemangku kepentingan harus memahami berbagai aspek Hukum Telemedicine dan Apotek Online di India serta implikasi hukum dan tanggung jawabnya.
30. Penipuan Perusahaan MLM: Penipuan Pemasaran Bertingkat (MLM) telah meningkat secara signifikan di India. Pemerintah India bahkan telah mempertimbangkan pemblokiran situs web perusahaan MLM di India yang terlibat dalam perilaku penipuan. Diperlukan kejelasan lebih lanjut dalam hal ini.
31. Perlindungan Kebebasan Sipil di Dunia Maya: Perlindungan Kebebasan Sipil di Dunia Maya semakin penting di India dan di seluruh dunia. Bahkan di Perserikatan Bangsa-Bangsa (PBB), Perlindungan Kebebasan Sipil di Dunia Maya dipertimbangkan. Perserikatan Bangsa-Bangsa bahkan mengeluarkan resolusi yang menyetujui Hak Privasi di Era Digital. Namun, India tidak berminat untuk mematuhi Resolusi tersebut.
32. E-Surveilans di India: E-Surveilans di India telah meningkat pesat meskipun ada Resolusi PBB. India telah meluncurkan Proyek Ilegal dan Inkonstitusional seperti Aadhar, Central Monitoring System (CMS), National Intelligence Grid (Natgrid), Crime And Criminal Tracking Networks and Systems (CCTNS), Internet Spy System Network And Traffic Analysis System (NETRA), dll tanpa Pengawasan Parlemen dan Kerangka Hukum apa pun. E-Surveillance, Perlindungan Kebebasan Sipil di Dunia Maya, dan Konflik Hukum merupakan beberapa isu penting yang harus dipertimbangkan oleh Perserikatan Bangsa-Bangsa dan India sebagai prioritas.
33. Tata Kelola Internet dan India: Mengingat meningkatnya kekhawatiran India terhadap Keamanan Siber, India telah memutuskan untuk menantang kendali pemerintah AS atas Internet dan memastikan bahwa trio AS, Rusia, dan Tiongkok tidak mengabaikan kekhawatiran India saat mengembangkan Rezim Internasional untuk Tata Kelola

Internet. India juga akan mendorong penyimpanan semua Data Internet dan Layanan VoIP di dalam Negara, selain memastikan kontrol dan pengelolaan server.

34. Perlindungan Nama Domain Gratis ICANN di India: Kebijakan dan Perjanjian Internet Corporation for Assigned Names and Numbers (ICANN) secara aktif melanggar Hukum India. Dengan demikian, Perlindungan Nama Domain di India harus bebas dari pengaruh ICANN dan harus dinilai secara independen dari Kebijakan dan Perjanjian ICANN.
35. Tantangan dalam Hukum Seluler: Saat ini, ada banyak aktivitas dalam ekosistem seluler. Meningkatnya persaingan telah memperkenalkan model-model baru ponsel, asisten digital pribadi, tablet, dan perangkat komunikasi lainnya di pasar global. Penggunaan perangkat seluler secara intensif telah memperluas ekosistem seluler dan konten yang dihasilkan kemungkinan akan menimbulkan tantangan baru bagi yurisprudensi hukum siber di seluruh dunia. Tidak ada undang-undang khusus yang mengatur penggunaan perangkat komunikasi dan platform seluler baru ini di sejumlah yurisdiksi di seluruh dunia karena penggunaan perangkat seluler untuk aktivitas input dan output meningkat dari hari ke hari. Dengan meningkatnya kejahatan seluler, ada kebutuhan yang semakin meningkat untuk memenuhi tantangan hukum yang muncul dengan penggunaan perangkat seluler dan memastikan perlindungan dan privasi seluler.
36. Masalah hukum Keamanan Siber: Tren hukum siber lain yang muncul adalah perlunya memberlakukan kerangka hukum yang tepat untuk menjaga, mempromosikan, dan meningkatkan keamanan siber. Insiden keamanan siber dan serangan terhadap jaringan meningkat pesat yang menyebabkan pelanggaran keamanan siber yang kemungkinan akan berdampak serius pada negara. Namun, tantangan di hadapan pembuat undang-undang bukan hanya untuk mengembangkan rezim hukum yang tepat yang memungkinkan perlindungan dan pelestarian keamanan siber, tetapi juga untuk menanamkan budaya keamanan siber di antara pengguna internet. Fokus dan penekanan baru adalah untuk menetapkan ketentuan wajib yang efektif yang akan membantu perlindungan, pelestarian, dan promosi keamanan siber dalam penggunaan komputer, sumber daya terkait, dan perangkat komunikasi.
37. Komputasi awan dan hukum: Dengan pertumbuhan teknologi internet, dunia bergerak menuju komputasi awan. Komputasi awan membawa tantangan baru bagi para pembuat undang-undang. Tantangan yang berbeda mungkin termasuk keamanan data, privasi data, yurisdiksi, dan masalah hukum lainnya. Tekanan pada legislator dan pemangku kepentingan siber adalah untuk menyediakan kerangka hukum yang tepat yang dapat menguntungkan industri dan memungkinkan penyelesaian yang efektif jika terjadi insiden komputasi awan.
38. Privasi & Perlindungan Data: Seiring dengan semakin banyaknya komputasi yang dapat diakses 24x7 ke berbagai jenis sumber daya dan perangkat komunikasi, privasi daring dan perlindungan data akan terus menjadi topik penting sejauh menyangkut pertumbuhan yurisprudensi hukum siber. Berbagai negara kemungkinan akan

membuat kerangka kerja yang memungkinkan mereka sendiri agar tidak hanya menjaga dan melindungi privasi daring tetapi juga menyediakan metodologi yang ketat untuk melindungi data dalam ekosistem digital dan seluler.

39. Media sosial & masalah hukum: Media sosial mulai memberikan dampak sosial dan hukum akhir-akhir ini yang menimbulkan masalah dan tantangan hukum yang signifikan. Sebuah studi terbaru menunjukkan bahwa situs jejaring sosial bertanggung jawab atas berbagai masalah. Sejak lembaga penegak hukum, lembaga intelijen menargetkan situs media sosial; mereka adalah tempat penyimpanan semua data yang disukai. Penggunaan media sosial yang tidak tepat menimbulkan kejahatan seperti pelecehan siber, penguntitan siber, identitas, pencurian, dll. Privasi di media sosial akan sangat terganggu meskipun ada upaya dari pemangku kepentingan terkait. Tantangan bagi legislator siber adalah mengatur penyalahgunaan media sosial secara efektif dan memberikan ganti rugi kepada korban kejahatan media sosial. Litigasi Media Sosial juga cenderung meningkat terkait dengan hubungan atau kaitan dengan keluaran media sosial. Litigasi terkait pencemaran nama baik, tindakan perkawinan semakin populer dan dengan data, informasi yang ada di jejaring media sosial, ada tren munculnya berbagai litigasi lain di tahun-tahun mendatang.
40. Undang-undang spam: Terjadi peningkatan spam yang cukup besar dalam email dan ponsel. Banyak negara telah menjadi titik panas untuk menghasilkan spam. Seiring dengan meningkatnya jumlah pengguna internet dan ponsel, para spammer menggunakan metode inovatif untuk menargetkan pengguna digital. Oleh karena itu, diperlukan ketentuan legislatif yang efektif untuk menangani ancaman spam. Berikut ini adalah beberapa tren dalam Hukum Siber yang didasarkan pada analisis yurisprudensi hukum siber yang sedang berkembang. Dengan semakin pesatnya perkembangan teknologi, mungkin tidak mungkin untuk mengesampingkan tren baru apa pun dalam teknologi yang mungkin berdampak langsung atau tidak langsung pada Hukum Siber. Dengan terus berkembangnya teknologi, tren yang lebih baru pasti akan muncul. Hal ini menciptakan tanggung jawab yang besar untuk memperbarui perlindungan hukum dan regulasi masalah siber ini agar setara dengan standar global.

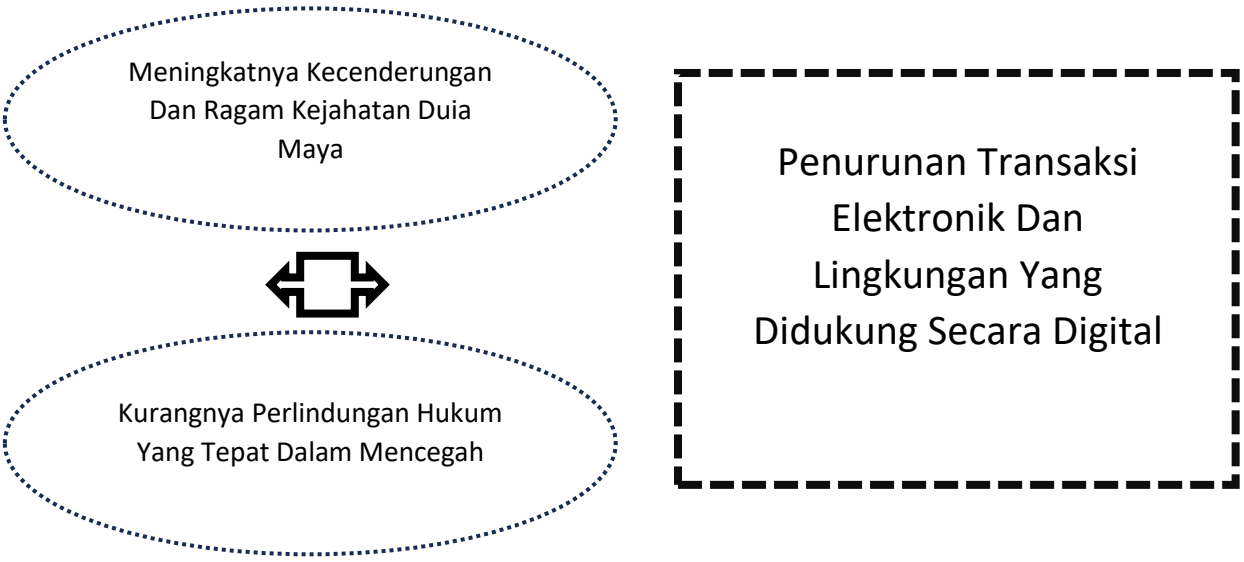
# BAB 7
# KESIMPULAN DAN REKOMENDASI

## 7.1 HUKUM SIBER: PERLU DITINJAU KEMBALI

Dari pembahasan di atas, tampak cukup jelas bahwa dengan kemajuan Teknologi Informasi dan Komunikasi, frekuensi kejahatan siber juga meningkat. Dengan kemajuan teknologi yang terus berlanjut, berbagai kejahatan siber pun terjadi. Kategori baru kejahatan siber mulai dari peretasan email hingga pembajakan perangkat lunak, dari cyber stalking hingga terorisme siber terjadi di dunia teknologi informasi dan komunikasi yang berkualitas.

Berulang kali dilaporkan bahwa rata-rata kejahatan melalui dunia siber meningkat pada tingkat 1,4% setiap tahun. Yang mengejutkan adalah bahwa sebagian besar kejahatan siber dilakukan oleh orang-orang yang berkualitas. Dari kasus penipuan Bank Pune hingga kasus pencemaran nama baik siber di Bangalore, teknisi yang berkualitas dalam teknologi ini ditandai sebagai terdakwa. Mereka cenderung melakukan kejahatan karena mereka sangat memahami prinsip dan etika komputer untuk menggunakannya dengan benar atau menyalahgunakannya untuk merusak kedamaian masyarakat.

Isu-isu yang dibahas dalam berbagai kasus oleh pengadilan di India membatasi fakta bahwa hukum India tentang Teknologi Informasi tidak kuat dan keraguan yang tersisa dalam ketentuan tersebut menjadi alasan pelarian terdakwa. Undang-Undang Teknologi Informasi mengobjektifikasi promosi transaksi elektronik daripada pencegahan penyalahgunaan dunia maya. Baru pada tahun 2008 ketika Undang-Undang Amandemen tahun 2008 memasukkan beberapa kategori khusus kejahatan dunia maya.




**Gambar 7.1**

Gambar di atas memperjelas bahwa 1) Meningkatnya frekuensi dan variasi Kejahatan Dunia Maya ditambah dengan 2) Rendahnya tingkat perlindungan dalam mencegah dan mengatur

kejahatan dunia maya yang muncul sama dengan 3) menurunnya pertumbuhan transaksi elektronik dan lingkungan yang mendukung secara digital. Hal ini juga dapat berdampak buruk pada pertumbuhan inklusif negara kita.

Cukup jelas bahwa meningkatnya kecenderungan kejahatan dunia maya tanpa adanya upaya hukum merugikan pertumbuhan transaksi elektronik di negara kita yang setara dengan standar global. Oleh karena itu, undang-undang yang seimbang tentang pencegahan dan pengaturan kejahatan dunia maya sangat dibutuhkan saat ini. Undang-undang tentang kejahatan dunia maya harus kuat untuk mencegah kejahatan dunia maya di masa mendatang. Undang-undang harus mengubah upaya hukumnya untuk memastikan lingkungan komputasi yang aman, terjamin, dan dapat dipercaya.

Hal ini penting tidak hanya untuk kesejahteraan nasional kita, tetapi juga untuk keamanan dan ekonomi nasional kita. Meskipun India telah mengambil banyak langkah untuk menghentikan kejahatan dunia maya, tetapi undang-undang dunia maya tidak boleh statis, undang-undang harus berubah seiring dengan perubahan zaman.

## 7.2 REKOMENDASI

Oleh karena itu, untuk memerangi kejahatan dunia maya secara efektif dan efisien sejalan dengan tren hukum dunia maya yang sedang berkembang, berikut ini adalah rekomendasi yang diajukan:

**Rencana Nasional untuk Memerangi Kejahatan Dunia Maya**

Disarankan agar pemerintah India, seperti halnya negara-negara maju, juga memulai Rencana Nasional untuk memerangi kejahatan dunia maya. Rencana nasional ini harus bertujuan untuk mencapai tujuan dan prioritas utama berikut:

1. Mendidik Masyarakat untuk Melindungi Diri Sendiri;
2. Bermitra dengan industri untuk mengatasi masalah berbagi Kejahatan Dunia Maya;
3. Membina pendekatan yang dipimpin oleh Intelijen dan berbagi informasi;
4. Meningkatkan kapasitas dan kapabilitas lembaga untuk menangani kejahatan dunia maya;
5. Meningkatkan kerja sama internasional dalam kejahatan dunia maya;
6. Memastikan Sistem Peradilan Pidana yang efektif

**Panduan Pencegahan Kejahatan Dunia Maya untuk Pengguna**

Benarlah bahwa pencegahan lebih baik daripada pengobatan, oleh karena itu, disarankan agar pemerintah mengeluarkan pedoman pencegahan kejahatan dunia maya kepada masyarakat luas sehingga pengguna dapat mengikuti pedoman dalam melindungi diri dari Kejahatan Dunia Maya. Praktik terbaik untuk mencegah Kejahatan Dunia Maya harus mencakup petunjuk berikut kepada pengguna:

a. Memperbarui sistem komputer secara berkala
b. Memilih kata sandi yang kuat dan tidak mudah ditebak. Sebaiknya hindari penggunaan kata sandi seperti tanggal lahir, tanggal ulang tahun pernikahan, dan sejenisnya
c. Terus ganti kata sandi secara berkala
d. Melindungi komputer dengan perangkat lunak keamanan dan firewall fisik

e. Melindungi informasi pribadi
f. Mengawasi pesan email palsu
g. Keluar secara berkala dari akun dan transaksi daring
h. Menghindari berbagi detail kartu kredit dan kartu debit
i. Berhenti menanggapi email dan pesan yang meminta informasi pribadi
j. Memperhatikan kebijakan privasi
k. Menjaga alamat email
l. Secara berkala meninjau laporan bank dan kartu kredit dan sejenisnya

**Undang-Undang Komprehensif tentang Kejahatan Dunia Maya**

Undang-Undang tentang Teknologi Informasi saat ini harus diamandemen secara komprehensif dengan mempertimbangkan perubahan terkini dan perubahan prospektif di arena dunia maya. Kategori-kategori yang mungkin dari kejahatan dunia maya harus didefinisikan dengan baik dengan variabel-variabel yang merupakan kejahatan, kemungkinan pencegahan dan demarkasi yang jelas tentang hukuman untuk kejahatan dunia maya. Ini akan memudahkan pengadilan untuk memberikan keadilan dengan cepat dan hukuman yang jelas akan mencegah orang melakukan kejahatan.

**Badan Khusus untuk Menyelidiki Kejahatan Dunia Maya**

Penyelidikan memainkan peran penting dalam mendapatkan pelaku sebenarnya untuk dihukum atas perbuatannya. Kejahatan Dunia Maya sebagai kejahatan khusus dan intelektual membutuhkan para ahli dalam menyelidiki kejahatan tersebut. Oleh karena itu, disarankan agar dibentuk badan khusus yang bertugas menyelidiki kejahatan tersebut sehingga korban bisa mendapatkan keadilan yang setara.

**Mempromosikan Literasi Siber**

Terakhir, pemerintah harus memulai kampanye untuk mempromosikan literasi tentang dunia siber dan kejahatan siber, khususnya untuk membuat masyarakat lebih sadar tentang penggunaan dan penyalahgunaannya. Lebih lanjut, direkomendasikan agar literasi siber dimulai dari tingkat akar rumput; lembaga, pusat komputer, sekolah, dan individu. Kecuali masyarakat menyadari kekuatan Teknologi Informasi dan Komunikasi dalam pembangunan dan pembangunan bangsa serta dampak buruk penyalahgunaannya dalam menghancurkan pembangunan inklusif masyarakat secara keseluruhan, tidak ada hukum yang dapat mengatasi nuansa kejahatan dunia maya. Oleh karena itu, selain memperkuat perlindungan hukum terhadap kejahatan dunia maya, pemerintah harus meningkatkan kesadaran masyarakat tentang penggunaan dan penyalahgunaan Teknologi Informasi dan Komunikasi serta balasan dan dampaknya dalam pembangunan inklusif bangsa secara keseluruhan. Ini pasti akan membawa kita menuju "India Digital" yang sesungguhnya.

# DAFTAR PUSTAKA


Akrich, M., & Lascoumes, P. (2018). The regulation of digital security risks: Between technological determinism and legal frameworks. Routledge.

Albar, A. (2016). Hukum siber di Indonesia: Perspektif, tantangan, dan implementasi. PT. Elex Media Komputindo.

Alhajj, R., & Sadiq, S. (2018). Cybersecurity risk management: Principles and practices. Wiley.

Amazon Web Services. (n.d.). What is cybersecurity? https://aws.amazon.com/id/what-is/cybersecurity/

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610–613. https://doi.org/10.1126/science.1130993

Arora, A., & Telang, R. (2005). Optimal security investment in the presence of externalities. Information Economics and Policy, 17(3), 301-316.

Bada, A., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Journal of Cybersecurity, 1(1), 1-10. https://doi.org/10.1093/cybsec/tyv003

Binns, M. (2017). Cybersecurity and the law: Protecting the connected world. Taylor & Francis.

Blakley, B., & Krutz, R. (2019). Cybersecurity: Protecting critical infrastructures from cyber threats. Elsevier.

Bradley, J., & Baker, S. (2016). International cybersecurity law: Current challenges and emerging issues. Oxford University Press.

Broadhurst, R. (2017). Cybercrime, law enforcement and the internet. Springer.

Bruce, D. (2020). Cybersecurity law and policy for global operations. Routledge.

Campbell, C., & Gregory, L. (2022). Digital privacy laws in the age of cybersecurity threats. Palgrave Macmillan.

Chertoff, M., & Simon, T. (2018). The impact of cybersecurity laws on innovation. In Cybersecurity and privacy protection in the digital age (pp. 51-67). Springer.

CIPS Indonesia. (n.d.). Perlindungan keamanan siber di Indonesia. Center for Indonesian Policy Studies. https://www.cips-indonesia.org/publications/perlindungan-keamanan-siber-di-indonesia?lang=id

Clough, J. (2010). Principles of cybercrime law (2nd ed.). Cambridge University Press.

Cohen, F. (2018). The ethics of hacking: A comparative approach to the law. Edward Elgar Publishing.

Deibert, R. (2017). Black code: Surveillance, privacy, and the dark side of the internet. McClelland & Stewart.

Denning, D. E. (2014). The information warfare doctrine: A legal and operational perspective. ACM Press.

Derler, J., & Langer, M. (2021). Legal challenges in data protection and cybersecurity. Journal of Technology Law & Policy, 25(2), 135-156.

Dettmer, C., & O'Brien, J. (2019). Cybersecurity risk assessment and mitigation: A comprehensive guide. Wiley.

Diskominfo Kotim. (n.d.). Kepala BSSN ungkap upaya pemerintah Indonesia dalam menghadapi ancaman siber. Dinas Komunikasi dan Informatika Kabupaten Kotawaringin Timur. https://diskominfo.kotimkab.go.id/kepala-bssn-ungkap-upaya-pemerintah-indonesia-dalam-menghadapi-ancaman-siber/

Dormehl, L. (2019). The cybersecurity dilemma: Hacking, panic, and the law of unintended consequences. Viking.

ELSAM. (2020). Mengurai permasalahan kebijakan keamanan siber di Indonesia: Ruang lingkup dan kelembagaan. Lembaga Studi dan Advokasi Masyarakat. https://www.elsam.or.id/bisnis-dan-ham/mengurai-permasalahan-kebijakan-keamanan-siber-di-indonesia-ruang-lingkup-dan-kelembagaan

Ghernaouti-Hélie, S. (2013). Cybersecurity: The beginner's guide. Springer.

Goodwin, A. (2018). The role of international law in cybersecurity regulation. Journal of International Law and Politics, 50(1), 1-29.

Gorman, L. (2014). Cybersecurity law and policy. John Wiley & Sons.

Green, P., & Smith, R. (2020). Cybersecurity in a hyper-connected world: Legal frameworks and protection mechanisms. Springer.

Grimes, R. A. (2019). Hacker's guide to cybersecurity law. Routledge.

Haggerty, K. D. (2015). Surveillance and security: Technological politics and the transformation of privacy. Wiley.

Hardt, M., & Negri, A. (2012). Empire and the law of cybersecurity. Harvard University Press.

Harvey, W. (2020). Emerging cybersecurity threats and the law. Cambridge University Press.

ID-SIRTII. (n.d.). Pengantar strategi keamanan siber Indonesia. https://idsirtii.or.id/halaman/tentang/pengantar-strategi-keamanan-siber-indonesia.html

Jøsang, A., & Pope, S. (2005). A survey of trust and reputation systems for online service provision. International Journal of Electronic Commerce, 9(3), 37-56. https://doi.org/10.1080/10864415.2005.11044394

Kalin, D. (2014). The law of cybersecurity. West Academic Publishing.

Kementerian Komunikasi dan Informatika. (2016). Kebijakan keamanan dan pertahanan siber. https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/

Kesan, J. P., & Hayes, C. R. (2005). Cybersecurity and the role of government. Journal of Legal Studies, 34(2), 345-373.

Klieger, M. (2021). Regulating cybersecurity risks in the digital economy. Edward Elgar Publishing.

Kroll, C., & Sormunen, K. (2021). Data protection laws and their impact on cybersecurity strategies. Springer.

Kshetri, N. (2013). Cybersecurity management: The role of public policy. Technology in Society, 35(4), 276-284. https://doi.org/10.1016/j.techsoc.2013.07.001

Langer, M., & Finkelstein, M. (2019). Cybercrime and the evolving legal landscape. International Journal of Information Security, 18(3), 199-213. https://doi.org/10.1007/s10207-019-04573-1

Maughan, M. (2017). Data breach and the law. Oxford University Press.

Membangun pertahanan dan keamanan siber. (2020). Neliti. https://media.neliti.com/media/publications/359981-membangun-pertahanan-dan-keamanan-siber-cd7ec38a.pdf

Naylor, R. T. (2018). Cybersecurity and the criminal justice system. Routledge.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Owens, L., & Dhanaraj, P. (2021). An introduction to global cyber laws and policies. Journal of Global Governance, 15(3), 209-229.

Pomerance, D. (2008). Cybersecurity and international law: The new frontier. Routledge.

renner, S. W. (2001). Defining cybercrime: A review of state and federal law. In R. D. Clifford (Ed.), Cybercrime: The investigation, prosecution and defense of a computer-related crime (pp. xx-xx). Carolina Academic Press.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.

Setkab. (n.d.). Penerapan zero trust sebagai upaya pelindungan dari ancaman serangan siber. Sekretariat Kabinet Republik Indonesia. https://setkab.go.id/penerapan-zero-trust-sebagai-upaya-pelindungan-dari-ancaman-serangan-siber/

Shostack, A. (2017). Threat modeling: Designing for security. Wiley.

Sitompul, J. (2012). Cyberspace, cybercrimes, cyberlaw: Tinjauan aspek hukum pidana. PT. Tatanusa.

Soghoian, C., & Soltani, A. (2017). The risks of surveillance technologies in the modern era. MIT Press.

Stewart, R. (2018). Law enforcement and cybersecurity: An international approach. Routledge.

Sutherland, E. H. (2016). Principles of criminology (12th ed.). Free Press.

Taylor, R. (2020). Cybersecurity regulations in the global landscape: A comparative study. International Journal of Cybersecurity Law, 7(2), 153-177.

Thomas, J. (2019). Internet governance and the law of cybersecurity. Palgrave Macmillan.

Tufekci, Z. (2017). Twitter and tear gas: The power and fragility of networked protest. Yale University Press.

U.S. Department of Homeland Security. (2021). Cybersecurity overview. Retrieved from https://www.cisa.gov/cybersecurity-overview

Van Oosterhout, T., & Jaquet-Chiffelle, D. (2020). Legal frameworks in cybersecurity: A global perspective. Springer.

Wallace, D. R., & Webber, L. M. (2019). The law of cybercrimes and their investigation. Elsevier.

Wang, F., & Li, B. (2015). Cybersecurity governance in organizations: A comprehensive framework. Journal of Information Privacy and Security, 11(2), 85-103. https://doi.org/10.1080/15536548.2015.1079324

Wiggins, A. (2021). The regulatory framework for digital identity and cybersecurity. Springer.

Williams, M. (2020). Cybersecurity governance and risk management. Elsevier.

Wong, T., & Yoon, D. (2022). International cybersecurity law and human rights. Cambridge University Press.

Wright, J. R. (2020). Cybersecurity law: Protecting the networked world. West Academic Publishing.

Zeng, S., & Leung, T. (2018). Cybersecurity and data protection: Legal challenges in the digital era. Edward Elgar Publishing.

Zetter, K. (2016). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown Publishing Group.

Zhang, L., & Zheng, Z. (2020). Legal principles in cybersecurity protection: A global approach. Springer.

Dr. Agus Wibowo, M.Kom, M.Si, MM.

# Hukum Siber
## dan
# Keamanan Informasi

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

# Hukum Siber dan Keamanan Informasi

Dr. Agus Wibowo, M.Kom, M.Si, MM.

## BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen, ilmu sosiologi dan ilmu hukum. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik), Ilmu Perpajakan.

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM ) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

**PENERBIT :**
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-49-6 (PDF)

9 786238 642496