Keamanan Siber

Pertemuan # IT & Cyberlaw

Always The First

Pengantar Cyber Law

- Definisi dan Ruang Lingkup
  - Cyberlaw mencakup segala aturan hukum yang mengatur aktivitas manusia di internet
- Pentingnya Cyber Law
  - Melindungi hak pengguna internet
  - Menyediakan landasan hukum untuk pelanggaran di dunia maya

Cyber Law di Indonesia

- Terminologi di Indonesia
  - Istilah seperti Hukum Sistem Informasi dan Hukum Telematika digunakan sebagai padanan
- Tantangan Implementasi
  - Sifat internet yang lintas batas mempersulit yurisdiksi dan penegakan hukum
- Perspektif Internasional
  - Perkembangan Global
    - Banyak negara mengembangkan Cyberlaw untuk menangani kejahatan online
  - Peran Perjanjian Internasional
    - Perjanjian seperti Konvensi Budapest penting untuk kasus lintas negara

Area Kunci

- Perlindungan HAKI
  - Melindungi hak cipta dan merek dagang
- Privasi dan Perlindungan Data
  - Menjaga privasi pengguna
  - Mencegah penyalahgunaan data
- Kebebasan Berekspresi
  - Menjaga kebebasan berbicara di internet

Aspek Hukum

- Definisi dan Evolusi
  - Cyber crime adalah kejahatan yang dilakukan melalui internet
- Jenis Cyber Crime:
  - Kategori offline
  - Kategori semi-online
  - Kategori online

Jenis-jenis Cyber Crime

- Motif Intelektual vs Ekonomi
  - Intelektual dilakukan untuk kepuasan
  - Ekonomi untuk keuntungan
- Contoh Kejahatan
  - Hacking
  - Pencurian identitas
  - Pembobolan data

Tantangan Yurisdiksi

- Masalah Yurisdiksi Internasional
  - Dunia maya tidak memiliki batasan teritorial
- Kekhawatiran Transnasional
  - Kejahatan lintas negara menghadapi tantangan penegakan hukum
- Tanggung Jawab Pidana
  - Konsep Tanggung Jawab Pidana: Bergantung pada niat pelaku dan dampak
  - Pengaruh Niat dan Kerugian: Mempengaruhi proses penuntutan dalam cyber law

Cyber Crimes dalam Sistem Keuangan

- Penipuan Kartu Kredit:
  - Banyak penipuan melibatkan pencurian informasi kartu kredit melalui metode seperti phishing, keylogging, atau penggunaan malware.
  - Setelah data dicuri, pelaku dapat melakukan transaksi ilegal atau menjual informasi di pasar gelap.
  - Tindakan pencegahan termasuk pengenalan teknologi seperti chip EMV pada kartu kredit dan penggunaan OTP (One-Time Password) untuk transaksi online.
- Keamanan E-Banking:
  - E-Banking memungkinkan pengguna untuk melakukan transaksi keuangan melalui internet, namun sering menjadi target cybercrime.
  - Metode serangan umum meliputi pembuatan situs palsu (typosquatting), peretasan akun melalui brute force, dan penggunaan malware untuk mencuri kredensial.
  - Banyak bank menerapkan autentikasi multi-faktor dan enkripsi data untuk meningkatkan keamanan, serta menyediakan edukasi untuk menghindari situs palsu.
- Modus Operandi Umum:
  - Phishing: Upaya menipu korban agar memberikan informasi pribadi melalui situs web atau email palsu.
  - Keylogging: Penggunaan perangkat lunak untuk merekam penekanan tombol pada keyboard, mencuri informasi login pengguna.
  - Man-in-the-Middle (MitM): Serangan di mana pelaku mencegat komunikasi antara pengguna dan bank, memungkinkan pelaku mencuri atau mengubah data.

Pencegahan Cyber Crime

- Upaya Nasional dan Internasional
  - Kolaborasi antara pemerintah, swasta, dan masyarakat
- Strategi Keamanan
  - Enkripsi data dan sertifikat digital membantu mencegah kejahatan

Implementasi di Indonesia

- Kerangka Legislatif:
  - Di Indonesia, Cyber Law mulai diatur melalui berbagai peraturan, seperti UU ITE (Undang-Undang Informasi dan Transaksi Elektronik), yang bertujuan mengatur aktivitas di dunia maya serta memberikan perlindungan hukum bagi masyarakat.
  - UU ITE mencakup berbagai aspek, termasuk pencemaran nama baik, privasi, dan transaksi elektronik, serta hukuman bagi pelaku cyber crime.
  - Selain UU ITE, terdapat upaya untuk mengembangkan peraturan baru dan menyesuaikan peraturan lama yang terkait dengan teknologi informasi.
- Model Pengaturan (Triangle Regulation):
  - Model regulasi ini menitikberatkan pada pengaturan tiga aspek utama: transaksi online, perlindungan privasi, dan pengendalian cyber crime.
  - Transaksi Online: Regulasi ini mengatur agar transaksi elektronik memiliki landasan hukum yang kuat dan dapat dipercaya.
  - Perlindungan Privasi: Aspek ini menggarisbawahi pentingnya menjaga data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.
  - Pengendalian Cyber Crime: Menyediakan kerangka hukum bagi aparat penegak hukum untuk menangani kejahatan siber, termasuk aturan prosedural untuk penyelidikan dan pembuktian.

Proposal Hukum Cyber di Indonesia

- Pembuatan UU Khusus vs Amandemen KUHP
  - Membuat UU khusus atau memperbarui KUHP
- Pendekatan Transaksi Internet
  - Regulasi untuk transaksi internet yang aman dan etis

Cyber Crime dan Pembuktian

- Jenis Bukti dalam Cyber Crime
  - Bukti elektronik
  - Kesaksian ahli
  - Data digital
- Tantangan Pembuktian
  - Pembuktian rumit karena melibatkan teknologi baru

Jenis Yurisdiksi dalam Cyber Law

- Yurisdiksi
  - Legislasi
  - Penegakan hukum
  - Peradilan
- Asas Yurisdiksi
  - Universality dan territoriality untuk menentukan otoritas hukum

Teori Yurisdiksi

- Uploader-Downloader Theory
  - Negara dapat mengatur aktivitas upload/download dalam wilayahnya
- The Law of the Server
  - Server lokasi data menentukan yurisdiksi hukum

Instrumen Hukum Internasional

- Panduan PBB (Perserikatan Bangsa-Bangsa):
  - PBB telah mengeluarkan berbagai resolusi untuk membantu negara-negara dalam menangani cyber crime, mendorong kolaborasi global untuk menghadapi ancaman lintas batas.
- Kerjasama Internasional melalui Konvensi Budapest:
  - Konvensi Budapest tentang Cyber Crime, diadopsi oleh Dewan Eropa, adalah kerangka hukum pertama yang mengatur tentang kejahatan dunia maya secara internasional.
  - Tujuan utama konvensi ini adalah untuk memfasilitasi kerja sama antar negara dalam penyelidikan dan penuntutan kejahatan cyber, termasuk akses ilegal, penyadapan ilegal, dan penyalahgunaan data.
- Manfaat Kerjasama Internasional:
  - Kerjasama internasional memungkinkan pertukaran informasi yang lebih efisien antar negara, mempercepat proses investigasi, dan meningkatkan kemungkinan menangkap pelaku kejahatan.
  - Konvensi ini juga memungkinkan negara-negara yang tidak tergabung dalam Uni Eropa untuk berpartisipasi, memperluas cakupan globalnya.
- Tantangan dalam Implementasi:
  - Meskipun banyak negara telah mengadopsi Konvensi Budapest, beberapa negara masih belum memiliki kerangka hukum yang mendukung kerjasama ini.
  - Adanya perbedaan undang-undang dan yurisdiksi dalam setiap negara membuat proses harmonisasi peraturan menjadi sulit.

Studi Kasus

- Pelanggaran HAKI (Hak Kekayaan Intelektual):
  - Kasus: Pelanggaran HAKI seperti pembajakan karya digital (musik, film, perangkat lunak) sering terjadi. Negara tertentu menuntut pelaku secara pidana atau denda finansial tinggi.
  - Penanganan: Teknologi DRM (Digital Rights Management) membantu perlindungan digital. Cyber Law memberi hak gugatan jika HAKI dilanggar.
- Penipuan Finansial (Financial Fraud):
  - Kasus: Penipuan kartu kredit adalah contoh umum. Data kartu kredit dicuri dan digunakan untuk transaksi ilegal.
  - Penanganan: Bank menggunakan OTP (One-Time Password) dan sertifikat digital untuk keamanan data. Penanganan lintas negara butuh kolaborasi internasional.
- Masalah Yurisdiksi dalam Studi Kasus:
  - Tantangan Yurisdiksi: Kasus lintas negara sulit ditangani karena aturan yurisdiksi berbeda. Penegakan hukum jadi rumit.
  - Solusi Kolaboratif: Konvensi internasional seperti Konvensi Budapest mendukung kolaborasi antarnegara untuk penanganan cyber crime.

Masa Depan Cyber Law

- Perkembangan Teknologi
  - Cyberlaw harus selalu diperbarui sesuai teknologi.
- Tren Baru
  - Perlindungan data pribadi
  - Regulasi AI membutuhkan perhatian hukum.

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First