MAKALAH ETIKA PROFESI TEKNOLOGI DAN INFORMASI

DATA FORGERY

Diajukan untuk memenuhi nilai Ujian Akhir Semester (UAS)

Nama	NIM
DHENYS GARNESYAH	12180020

Program Studi Sistem Informasi

Fakultas Teknik dan Informatika

Universitas Bina Sarana Informatika

Jakarta

2021

KATA PENGANTAR

Alhamdulillah, Dengan mengucapkan puji syukur kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga pada akhirnya penulis dapat menyelesaikan tugas ini dengan baik. Tugas Makalah pada Etika Profesi Teknologi Dan Informasi ini penulis sajikan dalam bentuk buku yang sederhana. Adapun judul Tugas Makalah, yang penulis ambil sebagai berikut, **"Makalah Etika Profesi Teknologi Dan Informasi Data Forgery".**

Tujuan penulisan Tugas Makalah pada Etika Profesi Teknologi Dan Informasi ini dibuat sebagai salah satu syarat Ujian Akhir Semester (UAS). Sebagai bahan penulisan diambil berdasarkan hasil penelitian beberapa sumber literatur yang mendukung penulisan ini. Penulis menyadari bahwa tanpa bimbingan dan dorongan dari semua pihak, maka penulisan Tugas Makalah ini tidak akan berjalan lancar. Oleh karena itu pada kesempatan ini, ijinkanlah penulis menyampaikan ucapan terima kasih kepada:

1. Allah S.W.T yang memberikan Kesehatan dan kelancaran.
2. Bapak Fathur Rohman, S.Kom, MMSI selaku Dosen Etika Profesi Teknologi Dan Informasi.
7. Kakak tercinta yang telah memberikan dukungan moral maupun spiritual.
8. Orang tua tercinta yang telah memberi dukungan dan do'a.
9. Rekan-rekan mahasiswa kelas SI-6A.07.

Serta semua pihak yang terlalu banyak untuk disebut satu persatu sehingga terwujudnya penulisan ini. Penulis menyadari bahwa penulisan Tugas Akhir ini masih jauh sekali dari sempurna, untuk itu penulis mohon kritik dan saran yang bersifat membangun demi kesempurnaan penulisan di masa yang akan datang.

Akhir kata semoga Tugas Akhir ini dapat berguna bagi penulis khususnya dan bagi para pembaca yang berminat pada umumnya.

Jakarta, 22 Juni 2021
Penulis

Dhenys Garnesyah

DAFTAR ISI

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi dari waktu ke waktu menjadi semakin canggih dan simple, dulu menyimpan data hanya 3.75 Mb dengan alat yang besar sekarang 8.00 Tb hanya dengan alat yang kecil sekecil batu bata (*Harddisk*). Alat ini dinamakan *Harddisk,* alat tersebut berpotensi untuk menyimpan data

Data menurut Kuswadi dan E. Mutiara, data adalah kumpulan informasi yang diperoleh dari suatu pengamatan, dapat berupa angka, lambang, atau sifat. Sedangkan menurut Lia Kuswayatno, data adalah kumpulan kejadian atau peristiwa yang terjadi di dunia nyata yang berupa angka-angka, huruf-huruf, simbol-simbol khusus, atau gabungan dari semuanya. Berdasarkan pengertian tersebut , dapat ditarik kesimpulan bahwa data adalah sekumpulan fakta ataupun angka dan dapat diolah menjadi informasi yang berguna.

Data digital juga bisa diduplikat (copy) secara tidak sah atau memalsukan atau bisa disebut *Data Forgery*. *Data Forgery* adalah data pemalsuan atau dalam dunia *cybercrime Data Forgery* merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scripless document* melalui Internet.

Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan

menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan. Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet, Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web *database*.

1.2. Maksud dan Tujuan

Maksud pembuatan makalah ini yaitu :

Untuk memberi pengetahuan, pemahaman, dan pengertian tentang *Data forgery*

Tujuan pembuatan tugas makalah ini yaitu:

Untuk memenuhi nilai tugas mata kuliah etika

BAB II

LANDASAN TEORI

2.1. Cybercrime

Cybercrime merupakan kejahatan yang dilakukan oleh seorang atau pun kelompok yang mampu menggunakan teknologi informasi yang terkoneksi dengan internet sebagai alat kejahatan. Menurut Murti (2005) *cybercrime* adalah sebuah istilah yang digunakan secara luas untuk menggambarkan tindakan kejahatan dengan menggunakan media komputer ataupun internet. Gregory (2015) menggemukan *cybercrime* adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengekspolitasi komputer lain yang terhubung dengan internet.

2.1. Cyber Law

Cyber law adalah aspek hukum yang istilahnya berasal dari *cyberspace law*, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai “online” dan memasuki dunia *cyber* atau maya.

Cyber law menurut Sunarto (2006) adalah upaya untuk melindungi secara hukum yang berkaitan dengan dunia maya atau internet. Tujuan dari dibentuknya *cyber law* sendiri menurut Sunarto (2006) adalah :

1. Melindungi data pribadi.
2. Menjamin kepastian hukum.
3. Mengatur tindak pidana cyber crime

BAB III

PEMBAHASAN

3.1. Motif

Motif pelaku kejahatan di dunia maya (*cybercrime*) pada umumnya dapat dikelompokkan menjadi dua kategori, yaitu :

1. Motif intelektual, yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individual.

2. Motif ekonomi, politik, dan kriminal, yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi. Dan dibawah ini berdasarkan motif kegiatannya :

    a. Cybercrime sebagai tindak kejahatan murni

        Dimana orang yang melakukan kejahatan yang dilakukan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

b. Cybercrime sebagai tindakan kejahatan abu-abu

   Dimana kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

c. Cybercrime yang menyerang hak cipta (Hak milik)

   Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.

d. Cybercrime yang menyerang pemerintah

   Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu negara.

e. Cybercrime yang menyerang individu

   Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermaikan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, *cyberstalking*, dan lain-lain.

3.2. Penyebab

Pada tahun 2002 diperkirakan terdapat sekitar 544 juta orang terkoneksi secara online. Meningkatnya populasi orang yang terkoneksi dengan internet akan menjadi peluang bagi munculnya kejahatan komputer dengan beragam variasi kejahatannya. Dalam hal ini terdapat sejumlah tendensi dari munculnya berbagai gejala kejahatan komputer, antara lain:

1. Permasalahan finansial

   Cybercrime adalah alternatif baru untuk mendapatkan uang. Perilaku semacam carding (pengambil alihan hak atas kartu kredit tanpa seijin pihak yang sebenarnya mempunyai otoritas), pengalihan rekening telepon dan fasilitas lainnya, ataupun perusahaan dalam bidang tertentu yang mempunyai kepentingan untuk menjatuhkan kompetitornya dalam perebutan market, adalah sebagian bentuk *cybercrime* dengan tendensi finansial.

2. Adanya permasalahan terkait dengan persoalan politik, militer dan sentiment Nasionalisme

   Salah satu contoh adalah adanya serangan hacker pada awal tahun 1990, terhadap pesawat pengebom paling rahasia Amerika yaitu Stealth Bomber. Teknologi tingkat tinggi yang terpasang pada pesawat tersebut telah menjadi lahan yang menarik untuk dijadikan ajang kompetisi antar negara dalam mengembangkan peralatan tempurnya.

3. Faktor kepuasan pelaku, dalam hal ini terdapat permasalahan psikologis dari pelakunya.

   Terdapat kecenderungan bahwasanya seseorang dengan kemampuan yang tinggi dalam bidang penyusupan keamanan akan selalu tertantang untuk menerobos berbagai sistem keamanan yang ketat. Kepuasan batin lebih menjadi orientasi utama dibandingkan dengan tujuan finansial ataupun sifat sentimen.

3.3. Penanggulangan

Beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah:

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*
d. Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi

e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties

BAB IV

PENUTUP

4.1. Kesimpulan

Di dunia ini banyak hal yang memiliki dualisme yang kedua sisinya saling berlawanan. Seperti teknologi informasi dan komunikasi, hal ini diyakini sebagai hasil karya cipta peradaban manusia tertinggi pada zaman ini. Namun karena keberadaannya yang bagai memiliki dua mata pisau yang saling berlawanan, satu mata pisau dapat menjadi manfaat bagi banyak orang, sedangkan mata pisau lainnya dapat menjadi sumber kerugian bagi yang lain, banyak pihak yang memilih untuk tidak berinteraksi dengan teknologi informasi dan komunikasi.

Sebagai manusia yang beradab, dalam menyikapi dan menggunakan teknologi ini, mestinya kita dapat memilah mana yang baik, benar dan bermanfaat bagi sesama, kemudian mengambilnya sebagai penyambung mata rantai kebaikan terhadap sesama, kita juga mesti pandai melihat mana yang buruk dan merugikan bagi orang lain untuk selanjutnya kita menghindari atau memberantasnya jika hal itu ada di hadapan kita.

4.2. Saran

Cybercrime adalah bentuk kejahatan yang mestinya kita hindari atau kita berantas keberadaannya. *Cyberlaw* adalah salah satu perangkat yang dipakai oleh suatu negara untuk melawan dan mengendalikan kejahatan dunia maya (*cybercrime*)

khususnya dalam hal kasus *cybercrime* yang sedang tumbuh di wilayah negara tersebut. Seperti layaknya pelanggar hukum dan penegak hukum.

DAFTAR PUSTAKA

e-jurnal.peraturan.go.id. PRINSIP-PRINSIP CYBER LAW PADA MEDIA, dari https://e-jurnal.peraturan.go.id/index.php/jli/article/download/485/pdf