MAKALAH

ETIKA PROFESI TEKNOLOGI

INFORMASI KOMUNIKASI

PERTEMUAN 13

"DATA FORGERY"

MAKALAH

Diajukan untuk memenuhi tugas mata kuliah EPTIK

Disusun oleh:

KALEB C MANURUNG 11191036

Program Studi Sistem Informasi Akuntansi

Fakultas Teknik dan Informatika

Depok

2022

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 ini penulis sajikan dalam bentuk yang sederhana. Adapun judul tugas yang penulis ambil sebagai berikut,"Makalah Data Forgery".Tujuan penulisan tugas ini dibuat untuk memenuhi nilai tugas mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi, juga menambah pengetahuan penulis mengenai DataForgery. Penulis menyadari bahwa tanpa bimbingan dan dorongan dari semua pihak, makapenulisan tugas ini tidak akan berjalan lancar. Penulis juga menyadari bahwa penulisanTugas Akhir ini masih jauh sekali dari sempurna, untuk itu penulis mohon kritik dan saranyang bersifat membangun demi kesempurnaan penulisan di masa yang akan

datang.Akhir kata semoga tugas ini dapat berguna bagi penulis khususnya dan bagi para pembacayang berminat pada umumnya.

Depok,18 juni 2022

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1.1.Latar Belakang

Di era kemajuan seperti saat ini semua aktivitas kita dituntut untuk serba cepatdan tepat. Salah satu fasilitas yang ada yang bisa kita gunakan untuk mendukungsemua aktivitas kita adalah dengan memanfaatkan jaringan internet. Dimana kita bisamempergunakan fasilitas internet tersebut agar terhubung dengan orang lain, untukmelakukan transaksi jual beli dan lain sebagainya. Akan tetapi fasilitas internet ituakan berujung pada dua hal nantinya yaitu internet bisa menjadi positif dan bisa jugamenjadi negatif. Fasilitas jaringan internet akan menjadi positif ketika dimanfaatkanuntuk hal- hal yang positif, begitu juga sebaliknya internet akan menjadi negatif ketikadipergunakan untuk hal-hal yang negatif dan bisa juga dibilang sebagai tindakkejahatan yang nantinya bisa merugikan orang lain.Kejahatan dalam dunia jaringan internet (dunia maya) biasa disebut dengan istilahcybercrime, dari segi bahasa cybercrime berasal dari kata cyber yang berarti duniamaya atau internet dan kata

crime yang berarti kejahatan. Jadi pengertian daricybercrime adalah segala bentuk kejahatan yang terjadi di internet (dunia maya).Cybercrime bisa juga didefinisikan sebagai tindak kriminal yang.dilakukan.dengan.menggunakan teknologi kecanggihan komput er sebagai alat kejahatan utama khususnya jaringan internet.

1.2 Maksud dan Tujuan

Adapun maksud dari pembuatan makalah ini yaitu:

1.Mengetahui apa yang dimaksud dengan Data Forgery

2. Menambah ilmu dan pengetahuan tentang Data Forgery.

3.Mengetahui contoh kasus Data Forgery yang pernah terjadi.Sedangkan tujuan dari pembuatan makalah ini untuk memenehi nilai tugas matakuliah etika profesi teknologi informasi dan komunikasi pada semester 6 di UniversitasBina Sarana Informatika.

1.3. Batasan Masalah

Dalam penulisan makalah ini, maka penulis akan membatasi masalah yaitum mengenai definisi Data Forgery dan contoh kasus Data Forgery yang pernah terjadidi Indonesia.

BAB II LANDASAN TEORI

2.1. Pengertian *Cybercrime*

Cybercrime merupakan kejahatan yang dilakukan dengan menggunakan jaringan computer atau jaringan nirkabel untuk melak

ukan kejahatan tersebut.Jaditanpa kontak fisik langsung seseorang bisa mengambil sesuatu dari korbannya.Takhanya digunakan untuk merampok,internet juga bisa digunakan untuk menyebarkan berita-berita palsu yang dapat mengancam kedamaian dunia (Eko Prabowo, 2020).

2.2. Klasifikasi Kejahatan *Cybercrime*

Berikut klasifikasi kejahatan cybercrime, diantaranya:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebutdilakukan dalam ruang/wilayah cyber sehingga tidak dapat dipastikanyuridiksi negara mana yang berlaku.

2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yangterhubung dengan internet.

3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterialyang cenderung lebih besar dibandingkan dengan kejahatan konvensional.

4. Pelakunya adalah orang yang menguasai penggunaan internet besertaaplikasinya.

5. Perbuatan tersebut sering dilakukan melintas batas negara

2.3.

Pengertian

Cyber Law

Cyber law

yang merupakan keseluruhan asas

–

asas, norma ataupun kaidahlembaga

–

lembaga, institusi

–

institusi dan proses yang mengatur kegiatan virtual yangdilaksanakan dengan menggunakan teknologi informasi, memanf aatkan kontenmultimedia dan infrastruktur telekomunikasi (Ramli et al., 2019)Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya) yangumumnya diasosiasikan dengan internet. Cyberlaw juga merupakan sebuah aspekhukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan meman faatkan teknologiinternet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya.Hukum dapat memberikan batasan-batasan yang jelas antara apa yang boleh dantidak boleh dilakukan oleh para pihak yang terlibat, hukum juga memberikankemungkinan-kemungkinan untuk diberikan sanksi atas pelanggaran yang dilakukandan memaksakan kehendak untuk mematuhi segala prinsip yang terkandung didalamnya.

disadari atau tidak olehsi pemilik data tersebut.

3.2.

Dasar Hukum

Data Forgery

Berikut ini merupakan dasar hukum dari kejahatan

data forgery

yang telah diaturdalam UU ITE Tahun 2008.A.

Pasal 301.

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukummengakses Komputer dan atau Sistem Elektronik milik Orang laindengan cara apa pun.

6

2.

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukummengakses Komputer dan atau Sistem Elektronik dengan cara apa pundengan tujuan untuk memperoleh Informasi Elektronik dan/atauDokumen Elektronik.3.

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukummengakses Komputer dan/atau Sistem Elektronik dengan cara apa pundengan melanggar, menerobos, melampaui, atau men9jebol sistem pengamanan.B.

Pasal 35Setiap orang dengan sengaja dan tanpa hak atau melawan hukummelakukan manipulasi, penciptaan, perubahan, penghilangan, p

engrusakanInformasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agarInformasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap

seolah‑olah data yang otentik

C.

Pasal 46

1.

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahundan/atau denda paling banyak Rp600.000.000,00 (enam ratus jutarupiah).

2.

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahundan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus jutarupiah).

3.

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun

dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus jutarupiah).D.

Pasal 51

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal35 dipidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00(dua belas miliar rupiah).

3.3.

Contoh Kasus

Data Forgery

1.

Kejahatan

Data Forgery

pada E-Banking BCAA.

Kronologi Kasus

Pada tahun 2001, internet banking diributkan oleh kasus pembobolaninternet banking milik bank BCA, Kasus tersebut

dilakukan oleh seorangmantan mahasiswa ITB Bandung dan juga merupakan salah satu karyawanmedia online (satunet.com) yang bernama Steven Haryanto. AnehnyaSteven ini bukan Insinyur Elektro ataupun Informatika, melainkan InsinyurKimia. Ide ini timbul ketika Steven juga pernah salah mengetikkan alamatwebsite. Kemudian dia membeli domain-domain internet dengan hargasekitar US$20 yang menggunakan nama dengan kemungkinan orang-orangsalah mengetikkan dan tampilan yang sama persis dengan situs

internet banking BCAKemudian dia membeli domain-domain internet dengan harga sekitarUS$20 yang menggunakan nama dengan kemungkinan orang-orang salahmengetikkan dan tampilan yang sama persis dengan situs internet bankingBCA, www.klikbca.com , seperti:

-

www.klikbca.com-

kilkbca.com-

clikbca.com-

klickbca.com-

klikbac.comOrang tidak akan sadar bahwa dirinya telah menggunakan situs aspaltersebut karena tampilan yang disajikan serupa dengan situs aslinya. Hackertersebut mampu mendapatkan User ID dan password dari pengguna yangmemasuki sutis aspal tersebut, namun hacker tersebut tidak bermaksudmelakukan tindakan criminal seperti mencuri dana nasabah, hal ini murnidilakukan atas- keingintahuannya mengenai seberapa banyak orang yangtidak sadar menggunakan situs klikbca.com, Sekaligus menguji tingkatkeamanan dari situs milik BCA tersebut.Steven Haryanto dapat disebut sebagai hacker, karena dia telahmengganggu suatu system milik orang lain, yang dilindungi privasinya.Sehingga tindakan Steven ini disebut sebagai hacking. Steven dapatdigolongkan dalam tipe hacker sebagai gabungan white-hat hacker dan black-hat hacker, dimana Steven hanya mencoba mengetahui seberapa besartingkat keamanan yang dimiliki oleh situs internet banking Bank BCA.Disebut white-hat hacker karena dia tidak mencuri dana nasabah, tetapihanya mendapatkan User ID dan password milik nasabah yang masuk dalamsitus internet banking palsu. Namun tindakan yang dilakukan oleh Steven, juga termasuk black-hat hacker karena membuat situs palsu d engan diam-diam mengambil data milik pihak lain. Hal-hal yang dilakukan Stevenantara lain scans, sniffer, dan password crackers.

9

Karena perkara ini kasus pembobolan internet banking milik bank BCA,sebab dia telah mengganggu suatu system milik orang lain, yang dilindungi privasinya dan pemalsuan situs internet bangking palsu. M aka perkara ini bisa dikategorikan sebagai perkara perdata. Melakuka n kasus pembobolan bank serta telah mengganggu suatu system milik orang lain, dan mengambildata pihak orang lain yang dilindungi privasinya artinya

mengganggu privasi orang lain dan dengan diam-diam mendapatkan User ID dan password milik nasabah yang masuk dalam situs internet banking palsu.

B.

Modus Pelaku Kejahatan

Modusnya sangat sederhana, si hacker memfotokopi tampilan websiteBank BCA yang seolah-olah milik BCA Tindakan tersebut dilakukan untukmengecoh nasabah sehingga pelaku dapat mengambil identitas nasabah

.

C.

Isi Surat Pernyataan Pelaku

Surat Steven Haryanto ke BCA 6 Juni 2001Dear BCA,Dengan ini saya: Nama: Steven HaryantoAlamat: (dihapus-red.), Bandung 40241Pembeli domain-domain internet berikut:

WWWKLIKBCA.COMKILKBCA.COMCLIKBCA.COMKLICKBCA.COMKLIKBAC.COM

Melalui surat ini saya secara pribadi dan tertulis menyampaikan permohonan maaf sebesar-besarnya. Saya menyesal dan mengakui telahmenimbulkan kerugian kepada pihak BCA dan

pihak pelanggan yangkebetulan masuk ke situs palsu tersebut. Namun saya menjamin bahwasaya tidak pernah dan tidak akan menyalahgunakan data tersebut.Bersama ini pula data user saya serahkan kepada BCA. Sejauh pengetahuan saya, data ini tidak pernah bocor ke tangan ketiga dan hanyatersimpan dalam bentuk terenkripsi di harddisk komputer pribadi saya.Mohon BCA segera menindaklanjuti data ini.Dengan ini juga saya ingin menjelaskan bahwa perbuatan ini berangkatdari rasa keingintahuan saja, untuk mengetahui seberapa banyak orangyang ternyata masuk ke situs plesetan tersebut. Tidak ada motif kriminalsama sekali. Alasan nyatanya, saya bahkan memajang nama dan alamatasli saya di domain tersebut, dan bukan alamat palsu. Sebab sejak awal pembelian saya memang tidak berniat mencuri uang dari rekenin g pelanggan.Saya tidak pernah menjebol, menerobos, atau mencoba menerobossistem jaringan atau keamanan milik BCA/Internet Banking BCA.Melainkan, yang saya lakukan yaitu membeli beberapa domain plesetandengan uang saya sendiri, dan menyalin halaman indeks dan halamanlogin http://www.klikbca.com ke server lain. Itu tetap suatu kesalahan,saya akui.

11

Saya tidak pernah mengkopi logo KlikBCA atau mengubahnya. Semuafile situs-situs gadungan, berasal dari server aslinya dihttp://www.klikbca.com/. yang dilihat pemakai, kecuali file halamandepan dan halaman loginSaya betul-betul mengharapkan apa yang telah saya perbuat ini LEBIHBERDAMPAK AKHIR POSITIF KETIMBANG NEGATIF.
Para pemakai dapat terbuka masalahnya dan menjadi lebih sadar akan isu

keamanan ini. Ingat iklan Internet Banking Anda? “Pengamanan

berlapis-

lapis. SSL 128 bit… Disertifikasi oleh Verisign…Firewalluntuk membatasi akses… Userid dan PIN.” Apakah seseorang

harusmenciptakan teknologi canggih, menyewa hacker jempolan, menjebolsemua teknologi pengaman itu untuk memperoleh akses ke rekening pemakai? Tidak. Yang Anda butuhkan hanyalah 8 USD. Ironis memang.Masalah TYPO SITE adalah MASALAH FUNDAMENTALdomain.com/.net/.org yang tidak mungkin dihindari (kita dapat melihatdatabase whois untuk melihat betapa banyaknya domain plesetan- plesetan yang dibeli pihak ketiga). Kebetulan dalam percobaan saya ini adalah klikbca.com. Semua situs-situs online sebetulnya terancam akan masalah ini, yaitu masalah pembelian domain salah ketik. Saat ini sayasendiri telah/akan terus berusaha untuk menjernihkan masalah ini kepadakhalayak ramai dan tidak bermaksud sama sekali merugikan pihak BCAmaupun customernya. Semua domain plesetan akan saya serahkankepada BCA tanpa perlu BCA mengganti biaya pendaftaran. Itu tidaksaya harapkan setimpal dengan kerugian yang mungkin telah sayatimbulkan, tapi hanya untuk menunjukkan rasa penyesalan dan

permohonan maaf saya. Demikian surat ini dibuat. Saya lampirkan juga kepada media massa sebagai permohonan maaf kepada publik dan akansaya taruh di situs master.web.id dan situs lain sebagai pengganti artikelsebelumnya yang telah diminta secara baik-baik oleh BCA untukditurunkan.Saya juga memohon kebijaksanaan para netter dan pembaca untuk tidakmengacuhkan forward email yang beredar dan bernada miring. Sepertiyang saya jelaskan inilah yang terjadi dan tidak pernah ada penyalahgunaan data atau pencurian data.

3.4.

Solusi Kasus

Data Forgery

Adapun cara untuk mencegah terjadinya kejahatan ini diantaranya :1.

Perlu adanya cyber law, yakni hukum yang khusus menangani kejahatan-kejahatan yang terjadi di internet. karena kejahatan ini berbeda darikejahatan konvensional.2.

Perlunya sosialisasi yang lebih intensif kepada masyarakat yang bisadilakukan oleh lembaga-lembaga khusus.3.

Penyedia web-web yang menyimpan data-data penting diharapkanmenggunakan enkrispsi untuk meningkatkan keamanan.4.

Para pengguna juga diharapkan untuk lebih waspada dan teliti sebelummemasukkan data-data nya di internet, mengingat kejahatan ini sering terjadikarena kurangnya ketelitian pengguna

BAB IVPENUTUP

4.1.

Kesimpulan

Berdasarkan dari kasus yang dibahas di atas, maka penulis dengan ini akanmenarik sebuah kesimpulan,

data forgery

merupakan sebuah kejahatan dalam duniamaya, dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada diinternet. Dokumen ini biasanya dimiliki oleh sebuah institusi atau lembaga yang milikisitus

web database

. Motif yang biasanya dilakukan oleh pelaku kejahatan ini biasanyaditujukan pada dokumen perusahaan

e-commerce

dengan membuat menjadi seolah-

olah terjadi “salah ketik” yang kemudian pada akhirnya akan menguntungkan pelaku

karena korban akan memasukkan data pribadi dan nomor kartu kredit yang nantinyadapat di salah gunakan.

4.2.

Saran

Berkaitan dengan

Data Forgery

tersebut maka perlu adanya upaya untuk pencegahannya, untuk itu yang perlu diperhatikan adalah :1.

Perlu adanya cyber law, yakni hukum yang khusus menangani kejahatankejahatan yang terjadi di internet. karena kejahatan ini berbeda dari kejahatankonvensional.2.

Penyedia web-web yang menyimpan data-data penting diharapkanmenggunakan enkrispsi untuk meningkatkan keamanan.3.

Para pengguna juga diharapkan untuk lebih waspada dan teliti sebelummemasukkan data-data nya di internet, mengingat kejahatan ini sering terjadikarena kurangnya ketelitian pengguna.

4.

Perlunya Penanggulangan Global, bahwa cybercrime membutuhkantindakan global atau internasional untuk menanggulanginya, mengingatkejahatan tersebut sering kali bersifat transnasional.5.

Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut