REGULASI YANG MENGATUR SECARA KHUSUS TERKAIT PERLINDUNGAN DATA PRIBADI DI INDONESIA TENTANG HOAKS DAN KERAWANAN MEDIA SOSIAL (Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Yanti Kirana
E-mail : kiranas54321@gmail.com
STIH Painan, Banten

Abstrak

Perkembangan teknologi sangat cepat, utamanya di dunia internet karenanya masalah keamanan adalah hal utama yang sagat diperlukan bagi para penggunanya. Masa seperti saat ini sangat besar kemungkinan data–data dan sistem yang ada di internet dapat di curi oleh orang – orang yang tidak bertanggung jawab. Penyalahgunaan teknologi seperti ini dapat dikatakan sebagai Kejahatan Dunia Maya (Cyber Crime). Hasil penelitian ini menerangkan, 1). Mengapa dunia maya seringkali mengacu kepada aktivitas kejahatan dengan menggunakan komputer atau jaringan komputer ? dan 2). Apa yang mempengaruhi Faktor-faktor cyber crime ?. Di era teknologi yang semakin canggih, penting untuk menjaga keamanan data pribadi. Karena, korban kejahatan digital hingga pembobolan data pada sistem masih sering dijumpai. Kehadiran internet saat ini tidak hanya memberi kemudahan akses informasi, tetapi turut memunculkan berbagai aksi kejahatan. Salah satunya ialah kejahatan siber atau cyber crime. Kejahatan ini muncul sebagai salah satu dampak negatif pesatnya perkembangan internet. Perkembangan dalam bidang apapun tidak dapat dielakan, peran pemerintah dalam rangka menjerat pelaku yang memanfaatkan secara negative perkembangan tekhnologi dalam bentuk apapun harus dapat disentuh oleh hukum

Kata kunci : Perlindungan, Data Pribadi, Hoaks, dan Kerawanan ,Media Sosial**.**

PENDAHULUAN

Cyber crime terjadi bermula dari kegiatan hacking yang telah ada lebih dari satu abad. Pada tahun 1870-an, beberapa remaja telah merusak sistem telepon baru negara dengan merubah otoritas. Berikut akan ditunjukan seberapa sibuknya para hacker telah ada selama 35 tahun terakhir. Akhir 1980 Penipuan komputer dan tindakan penyalahgunaan memberi kekuatan lebih bagi otoritas federal.

Computer Emergency Response Team dibentuk oleh agen pertahanan Amerika Serikat bermarkas pada Carnegie Mellon University di Pittsburgh, misinya untuk menginvestigasi perkembangan volume dari penyerangan pada jaringan komputer. Pada usianya yang ke-25, seorang hacker veteran bernama Kevin Mitnick secara rahasia memonitor e-mail dari MCI dan pegawai keamanan Digital Equipment. Dia dihukum karena merusak komputer dan mencuri software dan hal itu dinyatakan hukuman selama satu tahun penjara.

Hukum dan Keadilan

Perkembangan teknologi sangat cepat, utamanya di dunia internet karenanya masalah keamanan adalah hal utama yang sagat diperlukan bagi para penggunanya. Masa seperti saat ini sangat besar kemungkinan data–data dan sistem yang ada di internet dapat di curi oleh orang – orang yang tidak bertanggung jawab. Penyalahgunaan teknologi seperti ini dapat dikatakan sebagai Kejahatan Dunia Maya (Cyber Crime).[1]

Di era teknologi yang semakin canggih, penting untuk menjaga keamanan data pribadi. Karena, korban kejahatan digital hingga pembobolan data pada sistem masih sering dijumpai. Beberapa waktu lalu Pemerintah Bersama DPR telah mengesahkan RUU Pelindungan Data Pribadi menjadi Undang-Undang. Aturan hukum tersebut memang sangat diperlukan mengingat serangan siber beberapa tahun terakhir melonjak drastis, ditambah antar lembaga saat ini Kementerian Komunikasi dan Informatika dan Badan Siber dan Sandi Negara (BSSN) saling lempar tanggung jawab.

Regulasi yang mengatur secara khusus terkait perlindungan data pribadi di Indonesia sebetulnya sudah ada namun hanya sebatas pada peraturan Menteri dan belum mampu mengakomodir, mengingat kebocoran data masih terus terjadi dan meresahkan masyarakat.

Kehadiran BSSN tersebut merupakan bagian dari langkah strategis upaya negara untuk menjaga kedaulatan ruang siber negara melalui tata kelola pengamanan yang kuat. Penguatan di bidang keamanan siber adalah wujud usaha pemerintah untuk melahirkan keamanan nasional. Apabila mengingat tugas pokok dan fungsi atau tupoksi kelembagaan, berkaitan dengan kontrol pengawasan terkait dengan keamanan PDP idealnya menjadi tanggung jawab secara penuh BSSN sebagai penanggung jawab keamanan siber nasional. Tidak dapat dipungkiri teknologi informasi dan komunikasi menjadi ujung tombak era globalisasi.

Menurut Ashadi Siregar bahwa penggabungan computer dan telekomunikasi melahirkan suatu fenomena yang mengubah model konfigurasi komunikasi konvensional, dengan melahirkan suatu kenyataan dalam dimensi ketiga. Jika dimensi pertama adalah kenyataan keras dalam kehidupan empiris disebut dengan *hard reality*, dimensi kedua merupakan kenyataan dalam kehidupan simbolik dan nilai-nilai yang

[1] Cavazos Dan Morin, cyberspace and law, Lihat, Atip Latifulhayat, Cyber law" dan urgensinya bagi Indonesia (1), pikiran rakyat. 11 Januari 2001

dibentuk (dipadankan dengan istilah *soft reality*) dengan dimensi ketiga dikenal kenyataan maya (*virtual reality*) yang melahirkan suatu format masyarkat lainnya.[2]

Hanya saja memang perlu diperkuat dan lebih dipertegas kembali berkaitan dengan independensi lembaga untuk memperkuat tata kelola dan sektor publik tersebut agar kewenangan antar lembaga tidak terjadi tumpang tindih dalam menjalankan tugas masing-masing kelembagaan. Tujuannya agar upaya pencegahan dan penanganan tindak pidana siber lebih pasti dan optimal.

Kehadiran internet saat ini tidak hanya memberi kemudahan akses informasi, tetapi turut memunculkan berbagai aksi kejahatan. Salah satunya ialah kejahatan siber atau cyber crime. Kejahatan ini muncul sebagai salah satu dampak negatif pesatnya perkembangan internet. [3]

Berita bohong atau hoax bukan saja menjadi isu tetapi juga fakta, Kementerian Komunikasi dan Informatika (Kominfo) mengidentifikasi 425 isu hoax selama 3 bulan pertama pada tahun 2023.[4] Berdasarkan kategori, isu hoax paling banyak berkaitan dengan kesehatan, yakni sebanyak 2.256. Meskipun transisi ke endemi sedang berlangsung, ternyata masih banyak beredar isu hoax yang berkaitan dengan COVID-19, baik mengenai virus maupun vaksinasi. Selain itu ada banyak informasi yang menyesatkan terutama berkaitan dengan khasiat tanaman atau obat dan produk kesehatan.

Isu hoax yang berkaitan dengan kebijakan pemerintah juga tercatat paling banyak ditemukan. Secara kumulatif, sejak Agustus 2018, Kominfo menemukan 2.075 isu hoax dalam kategori pemerintahan. Paling banyak merujuk pada akun palsu pejabat pemerintah pusat dan daerah, ada pula yang mengenai kebijakan pemerintahterkini.

Sementara itu, pada urutan ketiga tertinggi temuan isu hoax, ada kategori penipuan. Kominfo mengidentifikasi sebanyak 1.823 isu hoax. Konten ini didominasi oleh tautan phising dan penipuan serta penipuan dengan menggunakan nomor ponsel.

---

[2] Ashadi Siregar, *Negara, Masyarakat dan Teknologi Informasi, makalh seminar Informasi, Pemberdayaan Masyarakat dan Demokrasi*, Dies Natalis FISIPOL UGM ke 46. 2001

[3] Wigrantoro Roes Setiadi, *Implikasi Multidimensional dari Kebijakan Tehnologi Informasi Indonesia* makalah Dies Natalis FISIPOL UGM Yogyakarta ke 46, 2001

[4] Septiaji Eko Nugroho, *Materi Potensi Kerawanan Media Sosial Jelang Pemilu 2024, Ketua Presidium MAFINDO*, 2023.

Kominfo sendiri dalam mengatasi hoax di internet ini mengklaim melakukan publikasi berupa klarifikasi atas isu hoax yang beredar di internet. Kominfo juga melakukan pemblokiran akses terhadap konten yang teridentifikasi sebagai isu hoax.

Dari latar belakang inilah yang membuat penulis tertarik untuk menulis jurnal dengan judul, **Regulasi Yang Mengatur Secara Khusus Terkait Perlindungan Data Pribadi Di Indonesia Tentang Hoaks dan Kerawanan Media Sosial" Dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)**

PEMBAHASAN PENELITIAN

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyber space Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet / elektronik yang dimulai pada saat mulai "online" dan memasuki dunia cyber atau maya. Apa yang Dimaksud dengan Cyber Crime ?

Cyber crime, atau kejahatan di dunia maya, adalah jenis kejahatan yang dilakukan melalui komputer dan jaringan. Komputer sendiri merupakan alat utama untuk melakukan cyber crime ini, tetapi seringkali komputer juga dijadikan sebagai target dari kejatahan ini. Biasanya, cyber crime membahayakan seseorang karena pencurian data hingga keuangan.[5]

Seiring dengan perkembangan zaman, manusia berhasil menemukan berbagai macam teknologi yang berguna untuk kehidupan sehari-hari. Telah banyak inovasi teknologi yang kini hadir di tengah masyarakat. Hal ini diciptakan semata-mata untuk memenuhi kebutuhan sehari-hari manusia.

Hadirnya teknologi juga memiliki pengaruh besar dalam kehidupan sehari-hari manusia. Hampir dapat dipastikan setiap orang kini juga telah bergantung dengan teknologi. Pasalnya, setiap hari kita memerlukan teknologi untuk menjalani aktivitas sehari-hari, tidak jarang ada oknum yang memanfaatkan perkembangan teknologi untuk melakukan tindak kejahatan atau yang biasa disebut dengan cyber crime.[6]

[5] https://www.cloudmatika.co.id/blog-detail/apa-itu-cyber-crime. diunggah tanggal 5 mei 2023
[6] http://Merdeka.com.Cyber Crime adalah Kejahatan Dunia Maya, Ketahui Jenis dan Cara Mencegahnya Minggu, 28 Februari 2021 14:01, diunggah tanggal 7 mei 2023, pukul 20.00 wib.

Kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain

Faktor-faktor yang mempengaruhi cyber crime adalah :

1). Faktor Politik.
Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi cyber crime yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku cyber crime, tapi penegakkan hukum tidak dapat berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang cyber crime belum ada. Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku cyber crime maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (lex specialist) bagi cyber crime. Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap cyber crime.

2). Faktor Ekonomi.
Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang menggunakan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi.

3). Faktor Sosial Budaya.
Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu:

a. Kemajuan teknologi Informasi.
Dengan teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena di situlah terdapat kebebasan yang seimbang, bahkan dapat mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya.

b. Sumber Daya Manusia.
Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali sebuah alat. Teknologi dapat dimanfaatkan untuk kemakmuran namun dapat juga untuk perbuatan yang mengakibatkan petaka akibat dari penyimpangan dan penyalahgunaan.

c. Komunitas Baru.
Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuk sebuah komunitas baru di dunia maya.

Ada beberapa jenis cyber crime yang kerap kali ditemui ketika beraktivitas di dunia maya, antara lain:[7]

1. Akses Ilegal

[7] Edmud Makarim, Kompilasi Hukum Telematika, divisi buku Perguruan Tinggi, Pt RajaGrafindo Persada, Jakarta, 2003

Akses ilegal adalah ketika pelaku memaksa masuk ke dalam akun korban tanpa sepengetahuan dan seizin dari korban. Hal ini memang merupakan salah satu jenis cyber crime yang paling umum. Bahkan, beberapa pelakunya terkadang tidak menyadari bahwa apa yang mereka lakukan termasuk ke dalam cyber crime.

Akun yang dimasuki secara ilegal tersebut dapat menyebabkan banyak sekali kerugian kepada korbannya. Pelaku bisa saja menyamar menjadi korban dan menipu orang lain dengan cara meminjam uang. Selain itu, informasi pribadi dari pemilik akun juga bisa tersebar luas ke khalayak umum.

2. Phising

   Phising adalah cara untuk melakukan penipuan dengan tujuan mencuri akun dari korban. Biasanya, pelaku mengincar korban melalui email atau pesan di dunia maya lainnya seperti pesan Facebook, Instagram, twitter, dan lain sebagainya.

   Phising juga dapat diartikan sebagai upaya untuk memperoleh informasi mengenai data seseorang dengan menggunakan teknik penipuan, biasanya dengan mengaku sebagai orang lain atau dengan mengirimkan sebuah link yang dapat mencuri informasi. Data dan informasi yang dimaksud adalah data pribadi seperti nama, umur, alamat, dan informasi akun tertentu atau bahkan data serta informasi keuangan.

3. Penipuan OTP

   OTP, atau On Time Password, adalah kode rahasia elektronik yang dikirimkan khusus kepada penggunanya. Biasanya, OTP akan dikirimkan ketika Anda hendak melakukan transaksi keuangan secara online untuk memastikan bahwa Anda adalah pengguna aslinya.

   Penipuan OTP ini adalah kejahatan yang dilakukan dengan cara mencuri kode rahasia elektronik tersebut. Biasanya, pelaku akan menyamar menjadi pihak dari suatu aplikasi di mana transaksi tersebut dilakukan agar korban dapat memercayainya dan memberikan kode OTP kepada pelaku.

4. Kejatahan Konten Ilegal

   Konten ilegal merupakan konten yang berisi data dan/atau informasi yang dianggap tidak benar, tidak etis, dan mengganggu ketertiban umum bahkan melanggar hukum. Nah, kejahatan kontel ilegal ini adalah ketilka pelaku membagikan konten tersebut ke khalayak umum.

   Biasanya, isi dari konten ilegal tersebut adalah informasi mengenai suatu topik yang bersifat tidak benar atau hoaks. Selain itu, konten yang bersifat SARA atau memiliki unsur tidak senonoh juga termasuk ke dalam konten ilegal.

5. Cyber Terrorism

   Cyber terrorism, atau terorisme siber, merupakan salah satu jenis cyber crime yang merugikan negara, bahkan mengancam keselamatan warga negara dan pemangku kepentingan yang mengatur jalannya pemerintahan. Aktivitas cyber terrorism ini mengacu pada serangan terhadap komputer, jaringan, dan sistem informasi suatu negara dengan tujuan untuk mengintimidasi dan menekan pemerintah untuk kepentingan tertentu.[8]

[8] Yahya Harahap, Op.cit., hlm 408

Beberapa ahli membagai cyber crime dengan beberapa jenis melihat perkembangan dan bidang, di antaranya :[9]

1. Carding, Adalah kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.dalam artian penipuan kartu kredit online.
2. Cracking, Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak system keamanan suatu system computer dan biasanya melakukan pencurian, tindakan anarkis begitu merekan mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identik dengan perbuatan negative, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.Sedang Cracker identik dengan orang yang mampu merubah suatu karakteristik dan properti sebuah program sehingga dapat digunakan dan disebarkan sesuka hati padahal program itu merupakan program legal dan mempunyai hak cipta intelektual.
3. Joy computing, yaitu pemakaian komputer orang lain tanpa izin.
4. Hacking, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
5. The trojan horse, yaitu manipulasi data atau program dengan jalan mengubah data atau intsruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau, dengan tujuan kepentingan pribadi atau orang lain.
6. Data leakage, yaitu menyangkut pembocoran data ke luar terutama mengenai data yang harus dirahasiakan.
7. Data diddling, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data atau output data.
8. To frustate data communication atau penyia-nyiaan data komputer.
9. Software piracy, yaitu pembajakan software terhadap hak cipta yang dilindungi Hak atas Kekayaan Intelektual (HaKI).
10. Cyber Espionage, Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.Biasaynya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai spyware.
11. Infringements of Privacy, Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.
12. Data Forgery, Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.

[9] https://www.kompas.com/skola/read/2022/04/25/100000169/cyber-crime--definisi-jenis-dan-contohnya.Kompas.com. Diunggah tanggal 5 April 2023

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

13. Unauthorized Access to Computer System and Service, Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.bagi yang belum pernah dengar, ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker.Kisah seorang mahasiswa fisipol yang ditangkap gara-gara mengacak-acak data milik KPU.dan masih banyak contoh lainnya.
14. Cyber Sabotage and Extortion, Merupakan kejahatan yang paling mengenaskan.Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyber-terrorism.[10]
15. Offense against Intellectual Property, Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.Dapat kita contohkan saat ini.Situs mesin pencari bing milik microsoft yang konon di tuduh menyerupai sebuah situs milik perusahaan travel online.
16. Illegal Contents, Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.Masih ingat dengan kasus prita mulyasari yang sampai saat ini belum selesai. Hanya gara-gara tulisan emailnya yang sedikit merusak nama baik sebuah institusi kesehatan swasta dia di seret ke meja hijau.

[10] M. Sarifal dkk, *Makalah Cyber Law & Cyber Crime*, BSI Tasikmalaya, 2015

2. Studi Kasus

[SALAH] Video "Cebong di Saudi Bisa Nyoblos Tanpa Identitas"

April 29, 2019 stefanus Fitnah / Hasut / Hoax 0

ini strategi PDIP yg bocor dari Arab Saudi!
Hallo @KPU_ID @bawaslu_RI jgn tangkap yg sebar video dong!!

#PrabowoSandiOkBanget

J.S. Prabowo

"Beredar video denga isi seorang pria yang mengajak wni di Saudi arabia untuk tetap datang mencoblos walaupun tanpa identitas dan hanya memiliki SPLP, diarahkan untuk tetap mencoblos setelah maghrib. Ketum Projo Budi Arie Setyadi, menekankan bahwa PDIP Saudi memperjuangkan hak pilih WNI yang hanya memiliki SPLP."

KLAIM: Di Saudi, pendukung tertentu bisa nyoblos tanpa identitas
FAKTA: Video ini berisi pernyataan Ketua DPLN PDIP Saudi Sharief Rachmat yang menekankan PDIP memperjuangkan hak pilih WNI yang hanya memiliki SPLP (Surat Perjalanan Laksana Paspor)

[SALAH] "Hasil perhitungan sementara diluar negri luarbiasa"

April 10, 2019 Adi Syafitrah Fitnah / Hasut / Hoax 0

4 jam

Cebong pasti bilang hoax...!!!
Link segera update harap bersabar...!!!
Pasti segera update sampai perhitungan selesai..!!!
Hasil perhitungan sementara diluar negri luarbiasa..!!
Saudi Arabia 01 : 25,6%. 02 : 65,4% suara
Yaman. 01 : 23,4% 02 : 66,6% suara
Belgia 01 : 17,1%. 02 : 82,2% suara
Jerman 01 : 12,3%. 02 : 87,7% suara
UEA. 01 : 22,7%. 02 : 61,3% suara
USA. 01 : 9,4% 02 : 89,9% suara
Ukraina. 01 : 3,4%. 02 : 96,6% suara
Papua Nugini 01 : 57,1% 02 : 42,3% suara
Taiwan 01 : 59,8% 02 : 40,2% suara
Hongkong 01 : 45,2% 02 : 46,8% suara
Korea Selatan 01 : 35,2% 02 : 64,8% suara

3 5 Komentar

KLAIM: Hasil Perhitungan Sementara Luar Negeri (Tertanggal 10 April 2019)
FAKTA: Perhitungan Luar Negeri akan dilakukan serentak pada tanggal 17 April 2029

[SALAH] "Dimalaysia sdah pencoblosan, Pak Prabowo menang telak, tapi kotak surat suara terbakar di jalan saat mau di bawa"

April 10, 2019 Adi Syafitrah Fitnah / Hasut / Hoax 0

Surat suara yang terbakar adalah surat suara yang belum dicoblos karena berdasarkan jadwal dari KPU RI, proses pemungutan suara di PPLN Kinabalu sendiri akan berlangsung pada Minggu, 14 April 2019 dan penghitungan suara untuk pemilu luar negeri di semua KBRI/KJRI baru dilaksanakan pada 17 April. Selengkapnya di bagian PENJELASAN dan REFERENSI!

KLAIM: Di Malaysia Prabowo Menang Telak, Tapi Surat Suara Terbakar di Jalan Saat Mau Dibawa
FAKTA: Kecelakaan yang Menyebabkan Surat Suara Terbakar Terjadi Sebelum Pencoblosan

- Tanggal 21 Maret 2019
- https://www.facebook.com/nicky.rindu.1
- Pada saat tulisan ini dibuat, dishare 1198 kali
- Hoax menyebutkan "Kecurangan KPU dan Rezim PKI Jokowi. Belum saatnya

Analisis Kasus

Hoax merupakan informasi, kabar, berita yang palsu atau bohong. Pada Kamus Besar Bahasa Indonesia (KBBI) hoax diartikan sebagai berita yang bohong. Hoax yaitu informasi yang dibuat-buat atau direkayasa untuk menutupi informasi yang sebenarnya.

Dengan kata lain, hoax diartikan sebagai upaya pemutarbalikan fakta menggunakan informasi yang seolah-olah meyakinkan akan tetapi tidak dapat diverifikasi kebenarannya.

Untuk dapat membedakan mana berita hoax dan berita benar, kita harus mengetahui cara untuk menangkal terjadinya hoax, diantaranya yaitu :

1. Cermati Alamat Situs
   Pastikan mendapatkan informasi atau berita yang bersumber dari situs-situs resmi dan telah terverifikasi kebenarannya.
2. Jangan Cuma Membaca Judul
   Judul provokatif biasanya dibuat untuk menambah viewer, meskipun isi dari informasi yang diberikan sering berbeda.
3. Periksa Fakta

Periksa kebenaran berita dengan cara melihat beberapa sumber lain agar mendapatkan beberapa referensi yang terpercaya.

4. Cek Keaslian Foto
   Pastikan selalu mengecek keaslian foto, Google Image dapat digunakan untuk mencari sumber-sumber foto yang asli.
5. Ikut Grup Diskusi
   Perbanyak pengetahuan tentang hoax dengan cara mengikuti beberapa grup diskusi.

HASIL PENELITIAN

Penebar Hoaks sebernarnya bisa saja dikenakan KUHP, Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang No.40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis, serta tindakan ketika ujaran kebencian telah menyebabkan terjadinya konflik sosial.

Dalam Pasal 40 ayat (2) Undang-Undang No.19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 40 ayat (2a) Undang-Undang No.19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pasal 40 ayat (2b) Undang-Undang No.19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sampai Peraturan Menteri Komunikasi dan Informatika No.19 Tahun 2014 tentang Penanganan Situs Bermuatan Negatif. Secara garis besar Persoalan hoax itu ada dua hal, yaitu :

i. Berita bohong harus punya nilai subyek obyek yang dirugikan.
ii. Melanggar Pasal 28 ayat 2 Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 28 ayat 2 itu berbunyi, "Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukkan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA)"

Penegakan hukum adalah usaha untuk melaksanakan hukum sebagaimana mestinya, mengawasi pelaksanaannya agar tidak terjadi pelanggaran. Dan jika terjadi pelanggaran usaha lain untuk memulihkan hukum yang dilanggar itu agar ditegakkan kembali. Pengertian penegakan hukum itu dapat pula ditinjau dari sudut obyeknya, yaitu dari segi hukumnya.[11]

KESIMPULAN

1. Teknologi informasi dan Komunikasi telah berkembang demikian pesat. cyber (komputer) telah melahirkan internet yang membawa fenomena baru di bidang media massa yang bisa dengan mudah digunakan untuk aktivitas kejahatan.
2. Faktor Politik, faktor ekonomi dan faktor sosial budaya dan untuk menghindari kerugian yang lebih besar akibat tindakan pelaku cyber crime maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (*lex specialist*) bagi cyber crime.

[11] Yanti Kirana. SH., MH, *Modul Kuliah UU ITE Dalam Sistem Hukum Nasional*, 2023

SARAN

1. Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (cyber crime). Sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.

2. Perkembangan dalam bidang apapun tidak dapat dielakan, peran pemerintah dalam rangka menjerat pelaku yang memanfaatkan secara negative perkembangan tekhnologi dalam bentuk apapun harus dapat disentuh oleh hukum, untuk mengurangi dampak Keamanan Negara yang dapat mengakibatkan Kurangnya kepercayaan dunia terhadap Indonesia, Berpotensi menghancurkan negara dan Keresahan masyarakat pengguna jaringan komputer.

DAFTAR PUSTAKA

BUKU

Ashadi Siregar, *Negara, Masyarakat dan Teknologi Informasi, makalh seminar Informasi, Pemberdayaan Masyarakat dan Demokrasi*, Dies Natalis FISIPOL UGM ke 46. 2001

Cavazos Dan Morin, *cyberspace and law*, Lihat, Atip Latifulhayat, Cyber law" dan urgensinya bagi Indonesia (1), pikiran rakyat. 11 Januari 2001

Edmud Makarim, *Kompilasi Hukum Telematika*, divisi buku Perguruan Tinggi, Pt RajaGrafindo Persada, Jakarta, 2003

M. Sarifal dkk, *Makalah Cyber Law & Cyber Crime*, BSI Tasikmalaya, 2015

Septiaji Eko Nugroho, *Materi Potensi Kerawanan Media Sosial Jelang Pemilu 2024, Ketua Presidium MAFINDO*, 2023.

Teknik Penulisan Skripsi stih Painan, 2017/2018

Wigrantoro Roes Setiadi, *Implikasi Multidimensional dari Kebijakan Tehnologi Informasi Indonesia* makalah Dies Natalis FISIPOL UGM Yogyakarta ke 46, 2001

Yanti Kirana. *Modul Kuliah UU ITE Dalam Sistem Hukum Nasional*, 2023

Yahya Harahap,Op.cit., hlm 408

INTERNET

https://www.kompas.com/skola/read/2022/04/25/100000169/cyber-crime--definisi-jenis-dan-contohnya.Kompas.com. Diunggah tanggal 5 April 2023

https://www.cloudmatika.co.id/blog-detail/apa-itu-cyber-crime.Di unggah tanggal 5 mei 2023.

http://Merdeka.com.Cyber Crime adalah Kejahatan Dunia Maya, Ketahui Jenis dan Cara Mencegahnya. Minggu, 28 Februari 2021 14:01, diunggah tanggal 7 mei 2023, pukul 20.00 wib.