KELOMPOK 5

1. **Moh Iqbal Maulidani (1910651150)**
2. **Muhammad Wildan Firdausi (1910651114)**
3. **Muhammad Asril Azim (1910651123)**
4. **Ridho Ananta B (1910651036)**
5. **Elvira Nugrah F P (1910651149)**

CYBER-THEFT

A. Pengertian Cyber-Theft

Pencurian data atau data theft merupakan tindakan ilegal dengan mencuri data dari sistem komputer untuk kepentingan pribadi atau dikomersilkan dengan menjual data curian kepada pihak lain.

1. Contoh kasus data theft adalah pembobolan jutaan data akun tokopedia beberapa waktu lalu.
2. Modus kejahatan dari cyber-Theft adalah penjahat biasanya mencuri informasi identitas orang lain seperti informasi kartu kredit, alamat, alamat email dan banyak lagi. Dengan informasi ini, mereka dapat berpura-pura menjadi orang lain dan membuat rekening bank baru.
3. Jenis kerugian dari cyber-theft adalah Biasanya, penyerang menargetkan bisnis untuk keuntungan finansial langsung atau untuk menyabotase atau mengganggu operasi. Mereka menargetkan individu sebagai bagian dari scam skala besar, atau untuk membahayakan perangkat mereka dan menggunakannya sebagai platform untuk aktivitas jahat.
4. Ruang lingkup kejahatan dari cyber-theft adalah Platform belanja online memang sangat digemari saat ini. Kemajuan teknologi menjadi salah satu ookan mengapa aplikasi belanja online semakin sering digunakan masyarakat. Banyak kemudahan yang diberikan oleh aplikasi belanja online yang membuat orang lebih nyaman dan lebih memilih aplikasi belanja tersebut dibandingkan berbelanja secara langsung di ook atau pasar.
5. Sifat kejahatan dari cyber-theft adalah ancaman keamanan cyber seperti rekayasa sosial, eksploitasi kerentanan perangkat lunak, dan serangan jaringan. Tetapi itu juga termasuk tindakan kriminal seperti pelecehan dan pemerasan, pencucian uang, dan banyak lagi.

CYBER-BREACH

B. Pengertian Cyber-Breach

pengertian dari data breach itu sendiri. Jadi data breach itu merupakan sebuah insiden dimana keamanan data dan informasi seseorang pengguna device telah diakses tanpa adanya otorisasi alias terjadi pembobolan ke dalam device untuk mencuri data dan informasimu.

Jika hal ini terjadi, maka akan banyak kemungkinan kerugian yang terjadi. Karena itulah data breach merupakan sebuah cyber crime yang dapat merusak kehidupan, bisnis sampai reputasi seseorang. File yang tercuri akibat data breach bisa disebarluaskan tanpa izin pemiliknya sehingga bisa merugikan banyak pihak.

1. Ruang Lingkup Kejahatan dari CYBER-BREACH adalah kejahatan konvensional, seperti pencurian, perampokan, pengeroyokan, dan sebagainya. Di lain sisi berbagai mass media seringkali menayangkan kosa kata “kejahatan siber” di headline-nya. Hal ini tentu akan menimbulkan bias interpretasi jika tanpa adanya upaya untuk lebih banyak memberikan “pencerahan” pada masyarakat umum terkait pengertian ataupun ruang lingkupnya yang dikemas dalam bahasa yang mudah dicerna oleh publik.

2. Sifat Kejahatan dari CYBER-BREACH adalah Pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer dengan cakupan pelanggaran adalah akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat.

3. Pelaku Kejahatan dari CYBER-BREACH adalah Secara teknis, mirip dengan *security breach*
atau pelanggaran keamanan, tapi berbeda tujuan. *Security breach* hanyalah
pembobolan, sedangkan data breach adalah aktivitas mencuri informasi. Analoginya,
security breach adalah seorang pencuri yang membobol jendela rumah Anda, sementara
data breach ketika si pencuri mengambil surat-surat penting atau laptop Anda.

4. Modus kejahatan dari CYBER-BREACH adalah

1. *phishing* yakni serangan manipulasi psikologis yang dirancang untuk mengelabui pengguna
agar menyerahkan data-data pribadi mereka.
2. penggunaan *software* ilegal untuk menebak kata sandi *device* milik pengguna.
3. *spyware* yang merupakan jenis malware dengan cara kerja mencuri data pribadi tanpa
terdeteksi sama sekali oleh pengguna.

5. Jenis kerugian yang ditimbulkan adalah Adanya cyber breach membuat banyak perusahaan kehilangan bisnis mereka. Menurut laporan *Teramind*, ada 231.354 catatan data hilang atau dicuri dalam periode 60 menit. Selain itu, jumlah pelanggaran data naik
54 persen dari tahun ke tahun, dan jumlah catatan yang terekspos melonjak sebesar 52 persen pada 2019.

CYBER-
OBSCENITY

C. Pengertian Cyber-Obscenity

Adalah kejahatan Kecabulan dunia maya adalah salah satunya. Pada dasarnya
'cabul' berarti tindakan atau bahasa seksual yang mengejutkan atau menyinggung
perasaan orang. Ketika kecabulan dilakukan melalui internet itu disebut sebagai "cabul

cyber". Kecabulan dunia maya adalah perdagangan materi ekspresif seksual di dalam ruang maya. Secara hukum, kecabulan dunia maya juga disebut sebagai 'pornografi'. Menurut Mahkamah Agung India yang terhormat-" Kecabulan memiliki kecenderungan untuk merusak dan merusak orang-orang, yang pikirannya terbuka untuk pengaruh tidak bermoral seperti itu". Kecabulan dunia maya dapat dilakukan melalui sastra, seni, musik, dll.

1. Ruang Lingkup Kejahatan dari CYBER-OBSCENITY adalah

Sifat Kejahatan dari CYBER-OBSCENITY

Eksploitasi Seksual sebagai kejahatan kesusilaan tidaklah dilihat dalam suatu pemahaman sempit mengenai bagaimana bentuk aktivitas seksual dan proses keterlibatan korban didalamnya. Aktivitas seksual yang dimaksud adalah bentuk konten yang dipertunjukan dimuka umum yang menggambarkan kecabulan dan melanggar norma kesusilaan. Ketentuan pidana mengenai Aktivitas Eksploitasi Seksual telah diatur dalam peraturan perundang-undangan yaitu Pasal 296 dan Pasal 506 KUHP, Pasal 4 dan Pasal 30 Undang-undang No 44 Tahun 2008, Pasal 1 dan Pasal 2 Undang-undang No 21 Tahun 2008 dan Pasal 27 dan Pasal 45 Undang-undang No 11 Tahun 2008. Apabila diantara aturan itu terdapat aturan umum dan khusus maka dikenakan adalah aturan khusus yang memuat ancaman paling berat berdasar pada Asas Concursus Idealis. Penelitian ini menggunakan Pendekatan undang-undang, Kasus dan Konseptual.

Pelaku Kejahatan dari CYBER-OBSCENITY

Sebagai contoh ; Pornografi anak melalui media digital kembali terkuak. Polda Metro Jaya dalam konferensi persnya bersama Asdep Perlindungan Anak dari kekerasan dan eksploitasi dari Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (KemenPPPA), bersama Kak Seto dan Ketua KPAI menjelaskan kronologi pengungkapan kasus pornografi anak melalui Skype yang terjadi di Kabupaten Kutai Kartanegara, Kalimantan Timur.

Direktur Reskrimsus Polda Metro Jaya Kombes Wahyu Hadiningrat mengungkapkan jika kasus tersebut telah diselidiki sejak April 2017. Pelaku melalui akun skype-nya tersebut membuat konten (foto dan video) tentang pornografi anak dan mentransmisikan gambar dan video yang bermuatan kesusilaan atau pornografi anak di bawah umur. Menjadi sorotan, sebab pelaku melakukan pelecehan seksual terhadap anak kandung dan keponakannya sendiri, dan disiarkan secara *live streaming* serta disebarkan ke grup *Whatsapp* dan *Telegram* lintas internasional.

“Komunitas ini terkuak setelah polisi mengidentifikasi seorang WNI melakukan kekerasan seksual terhadap anak kecil melalui platform *Skype*. Kemudian kami bekerja sama dengan US *Ice Homeland Security* (bidang khusus dalam *child pornografi* di AS), di mana data internasional yang didapat itu diinformasikan ke kami, sehingga tanggal 6 Mei kami berhasil menangkap pelakunya," ujar Wahyu.

KemenPPPA yang diwakili oleh Asdep Perlindungan Anak dari Kekerasan dan Eksploitasi, Rini Handayani menerangkan jika kejadian ini merupakan kasus eksploitasi seksual terhadap anak, karena dilakukan pelaku bukan

berdasarkan motif ekonomi. Tentu akan berdampak luarbiasa terhadap psikis para korban, karena rentan waktu terjadinya pelecehan dan kekerasan seksual dilakukan oleh pelaku sejak anaknya berusia 2 tahun.

“Kementerian Pemberdayaan dan Perlindungan Anak mengutuk dengan keras kejadian pornografi anak ini. Ini merupakan kasus *cyber* pornografi anak terbesar kedua di Indonesia yang berhasil diungkap. Apalagi kasus ini dilakukan oleh orang terdekat yakni ayah kandung, dimana orangtua seharusnya melindungi anak malah melakukan kejahatan seksual. Penegakan hukum harus benar-benar dilakukan, pelaku harus dihukum seberat-beratnya, dengan ancaman UU RI no.35 tahun 2014 tentang perubahan atas UU RI No.23 tahun 2002 tentang Perlindungan Anak, dengan ancaman hukuman mati,”

4. Modus kejahatan dari CYBER-OBSCENITY adalah
Jenis kerugian yang ditimbulkan

Dalam kegiatan aktivitas seksual pada Pornografi kemungkinan besar korban berangkat dari keinginan/kesadaran sendiri dan tidak dipaksa yang di latar belakangi banyak faktor, misal masalah ekonomi, ingin terkenal, jalan pintas untuk populer dan sebagainya. Berkembangluasnya eksploitasi sebagai bahan pornografi ditengah masyarakat juga mengakibatkan meningkatnya tindak asusila baik dalam bentuk eksploitasi ekonomi maupun eksploitasi seksual seperti pencabulan, pemerkosaan, prostitusi dan perdagangan orang yang keseluruhan adalah merupakan kejahatan kesusilaan. Tindak pidana eksploitasi seksual adalah kejahatan kesusilaan yang sudah menjadi satu konsep dalam Peraturan perundang-undang namun berdasarkan pengaturan dalam Undang-undang tersebut tidak didefinisikan dengan jelas dan tidak menempatkan eksploitasi seksual dalam suatu bab khusus. Aktivitas seksual dalam Eksploitasi yang dimaksud adalah bentuk aktivitas yang diperlihatkan atau dipertunjukan dimuka umum yang memuat kecabulan “sex related oriented” atau bentuk aktivitas yang menggambarkan ketelanjangan dan bentuk aktivitas yang melanggar norma kesusilaan