

Nanggroe : Jurnal Pengabdian Cendikia
Volume 5, Nomor 1, April 2026, Halaman 1-9
Licensed by CC BY-SA 4.0
e-ISSN: [2986-7002](https://doi.org/10.5281/zenodo.19733988)
DOI: <https://doi.org/10.5281/zenodo.19733988>

Sosialisasi Ruang Lingkup Kejahatan *Cybercrime* yang Terjadi di Masyarakat Pada Wilayah RT 007 RW 018 Kelurahan Kedaung Kecamatan Pamulang Kota Tangerang Selatan Provinsi Banten

Socialization of the Scope of Cybercrime Occurring in the Community in the Area of RT 007 RW 018, Kedaung Subdistrict, Pamulang District, South Tangerang City, Banten Province

Martahan Siburian

Mahasiswa Ilmu Hukum, Universitas Pamulang
Email: martahansiburian@outlook.com

Abstrak

Pemanfaatan dalam bidang teknologi Informasi, media, dan komunikasi telah membuat perilaku seseorang menjadi lebih baik dalam berperilaku dalam sebuah masyarakat. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tidak terhalang dengan batas dan norma yang ada sehingga dapat menimbulkan suatu perubahan dalam seluruh bidang missal bidang sosial, ekonomi, dan budaya secara cepat dan luas. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi factor penting dalam perbuatan melawan hukum. Perubahan ini juga memberikan dampak yang begitu besar terhadap transformasi nilai-nilai yang ada di masyarakat. Dampak yang ditimbulkan dari perkembangan teknologi bukan hanya dampak positif namun ada dampak negatif, perkembangan teknologi yang dimanfaatkan untuk tindak kejahatan yang biasa dikenal dengan *cybercrime*. *Cybercrime* mengacu kepada aktifitas kejahatan dengan komputer atau jaringan komputer yang menjadi alat atau tempat terjadinya kejahatan. Beberapa contoh dari *cybercrime* antara lain hacking, cracking, defacing, dll. Begitu juga dengan pembobolan ATM, judi online, dan pornografi termasuk dalam kejahatan dengan komputer.

Kata Kunci : *Cybercrime, Cyber Space, Cyber Law*

Abstract

The use of information technology, media, and communication has made a person's behavior better in behaving in a society. The development of information and communication technology has also caused world relations to be unhindered by existing boundaries and norms so that it can cause changes in all fields, such as social, economic and cultural fields, quickly and widely. Information technology is currently a double-edged sword because in addition to contributing to the improvement of welfare, progress, and human civilization, it is also an important factor in unlawful acts. This change also has a huge impact on the transformation of values in society. The impact caused by technological development is not only a positive impact but there is a negative impact, the development of technology that is used for crimes commonly known as cybercrime. Cybercrime refers to criminal activities with computers or computer networks that become tools or places of crime. Some examples of cybercrime include hacking, cracking, defacing, etc. Likewise, ATM break-ins, online gambling, and pornography are included in computer crime.

Keywords: *Cybercrime, Cyber Space, Cyber Law*

Article Info

Received date: 15 April 2025

Revised date: 20 April 2025

Accepted date: 24 April 2026

PENDAHULUAN

Kebutuhan akan teknologi Jaringan Komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui Internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar didunia bisa diketahui selama 24 jam. Melalui dunia internet atau disebut juga cyber space, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Tatkala pornografi marak di media Internet, masyarakat pun tak bisa berbuat banyak.

Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan yang disebut dengan "Cybercrime" atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus "Cybercrime" di Indonesia, seperti pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya Cybercrime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

METODE

Metode yang dipakai dalam kegiatan ini adalah metode sosialisasi berupa penyuluhan yang disampaikan oleh peserta pengabdian kepada warga RT 007 RW 018 Kelurahan Kedaung Kecamatan Pamulang Kota Tangerang Selatan Provinsi Banten dan disertai dengan tanya jawab dan diskusi yang melibatkan para pembicara dengan warga RT 007 RW 018 Kelurahan Kedaung.

HASIL

Peserta pengabdian dari Program Studi Ilmu Hukum Universitas Pamulang mengadakan sosialisasi tentang Ruang Lingkup Kejahatan Cybercrime yang terjadi di masyarakat pada wilayah RT 007 RW 018 Kelurahan Kedaung Kecamatan Pamulang Kota Tangerang Selatan Provinsi Banten pada hari minggu, 19 November 2023 bertempat di Aula Kelurahan Kedaung Kecamatan Pamulang Kota Tangerang Selatan. Sosialisasi dilakukan dengan cara melakukan penyuluhan kepada warga RT 007 RW 018 Kelurahan Kedaung dimana pemberian materi penyuluhan dibagi 2 (dua) sesi yaitu sesi pertama materi tentang cybercrime dan sesi kedua acara dilakukan diskusi dan Tanya jawab.



Gambar 1 Warga RT 007 RW 018 Kelurahan Kedaung mengikuti sosialisasi



Gambar 2 Pemberian Materi oleh Narasumber dari Team Pengabdian Kepada Masyarakat

Selama sosialisasi berlangsung para warga sangat memperhatikan konten materi yang diberikan oleh pembicara dari team atau peserta pengabdian, hal ini dikarenakan materi yang disampaikan sangat dekat dengan kehidupan social mereka di dunia maya dan cara penyampaian pembicara yang mudah dipahami oleh para warga.

Berdasarkan hasil wawancara yang dilakukan setelah pelaksanaan kegiatan pengabdian kepada masyarakat ini, terdapat beberapa hasil positif yang dapat terlihat dari kalangan warga yang menjadi peserta PKM kali ini. Menurut para warga, mereka mengakui baru kali ini mengetahui secara komprehensif mengenai ruang lingkup kejahatan yang terjadi di dunia maya (cybercrime). Setelah mengikuti kegiatan PKM yang dilaksanakan oleh Team Pengabdian dari mahasiswa/mahasiswi fakultas hukum Universitas Pamulang ini, para warga jadi lebih memahami tentang kejahatan yang dilakukan di dunia maya (cybercrime).

Selain para warga yang mendapatkan hal positif dari kegiatan PKM ini, pihak kelurahan pun mendapatkan hal yang positif dari kegiatan PKM ini. Hal ini dinyatakan oleh pihak kelurahan yang mengatakan bahwa dengan adanya kegiatan seperti ini sangat membantu para warga untuk mendapatkan pengalaman dan pengetahuan baru dalam hal kejahatan yang ada di dunia maya (cybercrime).

PEMBAHASAN

Pembicara dari Team Pengabdian Kepada Masyarakat, Martahan Siburian dihadapan para warga RT 007 RW 018 Kelurahan Kedaung mengatakan bahwa untuk mengetahui apa itu kejahatan yang dilakukan dunia maya (*cybercrime*) maka harus dipahami dulu apa itu cybercrime.

Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengidentikkan cybercrime dengan computer crime. The U.S. Department of Justice memberikan pengertian computer crime sebagai:

"...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".

Pengertian tersebut identik dengan yang diberikan Organization of European Community Development, yang mendefinisikan computer crime sebagai:

"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Adapun Andi Hamzah (1989) dalam tulisannya "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai:

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".

Dalam dua dokumen Kongres PBB mengenai The Prevention of Crime and the Treatment of Offenders di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal:

1. Cybercrime dalam arti sempit disebut computer crime, yaitu perilaku illegal atau melanggar secara langsung menyerang sistem keamanan suatu komputer atau data yang diproses oleh komputer
2. Cybercrime dalam arti luas disebut computer related crime, yaitu perilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan



Gambar 3 Mahasiswa Pengabdi Prodi Hukum sedang menjelaskan apa itu *cybercrime*

Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa cybercrime dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. Cybercrime ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.

Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa hardware/software maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya, seorang penyedia layanan/target Cybercrime harus mempunyai pengetahuan yang cukup tentang metode yang biasanya seorang cybercrime lakukan dalam menjalankan aksinya.

Karakteristik Cybercrime

Selama ini dalam kejahatan konvensional, dikenal adanya dua jenis kejahatan sebagai berikut:

1. Kejahatan Kerah Biru (Blue Collar Crime)
Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokan, pencurian, pembunuhan, dll.
2. Kejahatan Kerah Putih (White Collar Crime)
Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model diatas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal berikut :

- 1) Ruang lingkup kejahatan
- 2) Sifat kejahatan
- 3) Pelaku kejahatan
- 4) Modus kejahatan
- 5) Jenis-jenis kerugian yang ditimbulkan

Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka cybercrime dapat diklasifikasikan menjadi :

- 1) Cyberpiracy
Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
- 2) Cybertrespass
Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau individu.
- 3) Cybervandalism
Penggunaan teknologi computer untuk membuat program yang mengganggu proses transmisi elektronik, dan menghancurkan data dikomputer.

Jenis-Jenis Cybercrime

Berdasarkan motif kegiatannya, cybercrime dapat digolongkan sebagai berikut:

1. Cybercrime sebagai tindakan kejahatan murni
Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (spamming) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.
2. Cybercrime sebagai tindakan kejahatan abu-abu
Pada jenis kejahatan di internet yang masuk dalam wilayah "abu-abu", cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.
3. Cybercrime yang menyerang individu (Against Person)
Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, cyberstalking, dll
4. Cybercrime yang menyerang hak cipta / hak milik (Against Property)
Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.
5. Cybercrime yang menyerang pemerintah (Against Government)
Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan system pemerintahan, atau menghancurkan suatu Negara (Cyber Terrorism).

Berdasarkan modus atau jenis aktifitasnya cybercrime dapat digolongkan sebagai berikut:

1. Unauthorized Access
Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Probing dan port merupakan contoh kejahatan ini.
2. Illegal Contents
Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.
3. Penyebaran virus secara sengaja
Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
4. Cyber Espionage, Sabotage, and Extortion
Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
5. Cyberstalking
Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.
6. Carding
Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.
7. Hacking dan Cracker
Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari system komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.
8. 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.
9. 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.

10. Defacing

Defacing merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan/atau konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Sedangkan deface itu sendiri adalah hasil akhir dari kegiatan cracking dan sejenisnya, tekniknya adalah dengan membaca source codenya (ini khusus untuk konteks web hacking), kemudian mengganti image (misalnya), editing html tag dkk, dan lain-lain. Tindakan defacing ada yang sematamata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang untuk mencuri data dan dijual kepada pihak lain.

11. Phising

Phising merupakan kegiatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya. Phising biasanya dilakukan melalui e-mail spoofing atau pesan instan, dan sering mengarahkan pengguna untuk memasukkan rincian di sebuah website palsu yang tampilan dan nuansa yang hampir sama dengan yang aslinya.

Faktor Penyebab

Beberapa faktor yang menyebabkan kejahatan komputer (Cybercrime) adalah:

1. Akses internet yang tidak terbatas. Saling terhubungnya antara jaringanyang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya.
2. Kelalaian pengguna komputer.
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator komputer.
5. Kurangnya perhatian masyarakat dan penegak hukum
6. Sistem keamanan jaringan yang lemah.
7. Cybercrime dipandang sebagai produk ekonomi.

Perkembangan Cybercrime di Indonesia

Perkembangan cybercrime di Indonesia adalah kasus pornografi. Kegiatan yang termasuk pronografi adalah kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas. Saat ini di Indonesia sangat marak dan mudah mengakses konten pornografi di internet karena kurangnya perlindungan atau pembatasan konten-konten pornografi di Indonesia oleh pemerintah.

Contoh Kasus Cybercrime di Indonesia

1. Pada tahun 2008, Di Indonesia kasus pornografi yang terheboh baru-baru ini adalah kasusnya Ariel-Luna-Cut Tari. Kasus kejahatan ini memiliki modus yaitu agar video tersebut diketahui public dan untuk membuat para pemain yang di video itu agar malu, kasus video porno Ariel “PeterPan” dengan Luna Maya dan Cut Tari, video tersebut di unggah di internet oleh seorang yang berinisial ‘RJ’. Pada kasus tersebut, modus sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Penyelesaian kasus ini pun dengan jalur hukum, penunggang dan orang yang terkait dalam video tersebut pun turut diseret pasal-pasal sebagai berikut, Pasal 29 UURI No.44 th 2008 tentang Pornografi Pasal 56, dengan hukuman minimal 6 bulan sampai 12 tahun. Atau dengan denda minimal Rp 250 juta hingga Rp 6 milyar. Dan atau Pasal 282 ayat 1 KUHP.
2. Prita Mulyasari, Digugat dan dilaporkan ke Polisi oleh Rumah Sakit Omni Internasional atas tuduhan Pencemaran nama baik lewat millis. Kasus ini bermula dari surat elektronik yang dibuat oleh Prita yang berisi pengalamannya saat dirawat di unit gawat darurat Omni Internasional. Prita Mulyasari dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp.1 miliar.
3. EJA (38) inisial, atas dugaan pencemaran nama baik dan penyebaran berita bohong melalui system elektronik . EJA dijadikan sebagai tersangka karena mengirimkan e-mail kepada kliennya soal lima bank yang dilanda kesulitan likuiditas, EJA telah resmi ditahan. Informasi EJA itu katanya dikhawatirkan akan menyebabkan rush atau kekacauan. Dikatakan bahwa EJA mendengar rumor soal sejumlah bank kesulitan likuidasi dari para broker secara verbal. EJA lalu menginformasikan hal itu kepada para kliennya melalui e-mail dengan domain perusahaannya. Informasi inilah yang lalu tersebar luas. EJA dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar.

Penanggulangan Cybercrime

Untuk menanggulangi kejahatan internet yang semakin meluas maka diperlukan suatu kesadaran dari masing-masing negara akan bahaya penyalahgunaan internet. maka berikut adalah langkah ataupun cara penanggulangan secara global :

1. Modernisasi hukum pidana nasional berserta hukum acaranya diselarskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
2. Peningkatan standar pengamanan system jaringan computer nasional sesuai dengan standar internasional.
3. Meningkatkan pemahaman serta keahlian aparat hukum mengenai upaya pencegahan, inventigasi, dan penuntutan perkara-perkara yang berhubungan dengan cyber crime.
4. Meningkatkan kesadaran warga Negara mengenai bahaya cyber crime dan pentingnya pencegahan kejahatan tersebut.
5. Meningkatkan kerja sama antar Negara dibidang teknologi mengenai hukum pelanggaran cybercrime.

Jadi, secara garis besar untuk penanggulangan secara global diperlukan kerja sama antara negara dan penerapan standarisasi undang-undang Internasional untuk penanggulangan Cyber crime.

SIMPULAN

Simpulan yang dapat diambil dari pemaparan kegiatan Pengabdian Kepada Masyarakat Team Mahasiswa Prodi Ilmu Hukum Universitas Pamulang di wilayah RT 007 RW 018 Kelurahan Kedaung Kecamatan Pamulang Kota Tangerang Selatan Provinsi Banten adalah :

- a. Bahwa umumnya masyarakat masih sangat minim informasi mengenai kejahatan yang terjadi di dunia maya (cyberspace), hal ini disebabkan oleh karena kurangnya sosialisasi dari pemerintah

- kepada masyarakat supaya masyarakat mengerti dan paham apa saja kejahatan yang sering terjadi di dunia maya (cyberspace).
- b. Peran pemerintah sangat menentukan untuk pencegahan terjadinya kejahatan di dunia maya (cyberspace) seperti proteksi perlindungan data pribadi, keamanan internet, dan privasi individu.
 - c. Disamping peran pemerintah juga tidak kalah penting adalah peran orang tua untuk selalu memperhatikan anak-anak nya agar tidak menjadi pelaku maupun korban dari kejahatan dunia maya (cybercrime).

REFERENSI

- Raharjo, A. (2002). *Cybercrime (Pemahaman dan upaya pencegahan kejahatan berteknologi)*. PT Citra Aditya Bakti.
- Hamzah, A. (1987). *Aspek-aspek pidana di bidang komputer* (2nd ed.). Sinar Grafika.
- Makarim, E. (2005). *Pengantar hukum telematika*. PT Rajagrafindo Persada.
- Makarim, E. (2003). *Kompilasi hukum telematika*. PT Rajagrafindo Persada.
- Sunarso, S. (2009). *Hukum informasi dan transaksi elektronik*. PT Rineka Cipta.
- Muljono, W. (2012). *Pengantar teori kriminologi*. Pustaka Yustisia.
- Sahetapy, J. E. (2005). *Pisau analisis kriminologi*. PT Citra Aditya Bakti.
- Fajar, M., & Yulianto, A. (2013). *Dualisme penelitian hukum normatif dan empiris* (2nd ed.). Pustaka Pelajar.
- Nasution, D. A. F., Septiana, R., Syaputri, W., & Nurbaiti, N. (2023). Lingkup dunia cyber di Indonesia. *Comserva*, 2(11), 2477–2486.
- Djarawula, M., Alfiani, N., & Mayasari, H. (2023). Tinjauan yuridis tindak pidana kejahatan teknologi informasi (cybercrime) di Indonesia ditinjau dari perspektif Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik. *Jurnal Cakrawala Ilmiah*, 2(10), 3799–3806.
- Danuri, M., & Suharnawi, S. (2017). Trend cyber crime dan teknologi informasi di Indonesia. *Jurnal Ilmiah Infokam*, 13(2).
- Akbar, Y. R., Ikhsan, M. F., & Lubis, F. (2023). Analisis yuridis kejahatan mayantara dalam hukum pidana pencemaran nama baik di Indonesia. *Journal of Science and Social Research*, 6(1), 225–232.