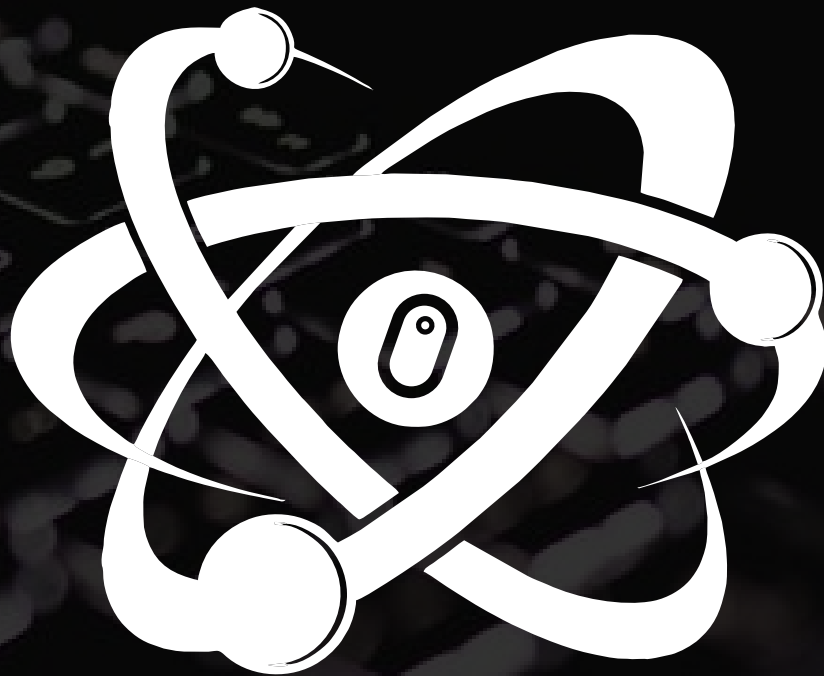


PATH

NEWS LETTER OF ALSA LC UNHAS



**CYBERCRIME MENGGURITA RAKYAT MENDERITA,
DIMANA REGULASI?**

Volume VIII

Rubrik Utama| Wawancara Khusus| Legal Opinion| Did You Know
Forum Bebas| ALSA Activity| Ga'de ALSA| Upcoming Events

DAFTAR

ISI

SEKAPUR SIRIH

Sambutan

1. Director ALSA LC Unhas
2. Project Officer PATH Vol. VIII

RUBRIK

5. Utama

11. Wawancara Khusus

15. Legal Opinion

DID YOU KNOW?

19.

FORUM BEBAS

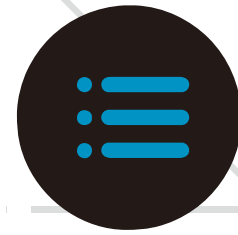
21.

ALSA ACTIVITY

23.

GA'DE ALSA

UP COMING PROJECT





Sekapur Sirih



Rubrik Utama



Wawancara Khusus



Legal Opinion



Forum Bebas



Did You Know?



ALSA Activity



GA'DE ALSA



Upcoming Events

FADIEL MUHAMMAD

—
Director ALSA LC Unhas
2016-2017



Assalamualaikum Wr. Wb.

Salam sejahtera untuk kita semua
Shalom. Om swastyastu. Namu budaya.

Puji syukur saya panjatkan kepada Allah SWT atas limpahan rahmat, karunia, dan izin-Nya sehingga ALSA LC Unhas dapat menerbitkan PATH: News letter of ALSA LC Unhas Volume VIII. Salawat serta salam tetap tercurahkan kepada junjungan Nabi Besar Muhammad SAW, semoga kita tetap istiqomah sebagai umatnya.

PATH: News letter of ALSA LC Unhas Volume VIII merupakan salah satu media yang dimiliki ALSA LC Unhas untuk bisa menyalurkan informasi dan berbagi pengetahuan yang berhubungan dengan hukum serta menyampaikan informasi mengenai Local Chapter Universitas Hasanuddin maupun ALSA secara umum.

PATH: News letter of ALSA LC Unhas Volume VIII kali ini mengangkat tema yang sangat menarik yaitu mengenai Cyber Crime, yang dimana pada saat ini sedang maraknya kasus cyber crime di tengah masyarakat ataupun lingkup pemerintah. Cyber Crime merupakan kejahatan yang sangat berbahaya sedangkan pengetahuan masyarakat masih sangat minim mengenai kasus tersebut. Oleh karena itu, kami dari ALSA LC Unhas berinisiatif untuk mengangkat permasalahan Cyber Crime sebagai tema dan pembahasan



ini didalam PATH: News letter of ALSA LC Unhas Volume VIII. Kami berupaya agar dapat mengupas lebih dalam mengenai cyber crime dan terintegrasikan melalui media ini.

Tidak lupa pula ucapan terima kasih dan apresiasi sebesar-besarnya untuk Technology, Information, and Multimedia Department, teman-teman tim redaksi, dan segenap orang yang telah berpartisipasi dan membantu dalam penerbitan PATH: News letter of ALSA LC Unhas Volume VIII.

Semoga PATH: News letter of ALSA LC Unhas Volume VIII dapat memberikan manfaat bagi kita semua, menambah pengetahuan serta wawasan bagi yang membacanya. Semoga dapat membawa ALSA ke tingkat lebih tinggi, khususnya ALSA LC Unhas.

Terima kasih
Wassalamualaikum Wr. Wb.
ALSA, Always Be One!



Sekapur Sirih.



FADLI GAFFAR

Project Officer PATH Vol. VIII

Ucapan terima kasih yang sebesar-besarnya saya sampaikan kepada tim redaksi PATH Vol. VIII yang telah membantu dengan sangat baik, telah memberikan ide, waktu, dan tenaganya sehingga tugas ini dapat terselesaikan. Tanpa bantuan dan kerja keras dari teman-teman tim redaksi, kita tidak dapat menyukseskan PATH Vol. VIII ini. Oleh karena itu, saya merasa ucapan terima kasih tidak akan mampu menggambarkan apresiasi saya akan kerja keras dan kesungguhan tim redaksi sekalian. Ucapan terima kasih juga saya sampaikan kepada keluarga besar ALSA Local Chapter Universitas Hasanuddin yang telah memberikan motivasi dan semangat yang luar biasa kepada kami.

Saya berharap PATH yang bertema "Cyber Crime Menggurita, Korban Menderita; Dimana Regulasi?" ini dapat menjadi referensi yang bermanfaat bagi para pembaca dalam meningkatkan ilmu pengetahuan. Semoga dapat menjadi bacaan yang menarik bagi teman-teman, dan semoga dapat bernilai ibadah bagi kita semua.

Terimakasih,
Akhir kata, wabillahi taufik wal hidayah
Wassalamualaikum Warahmatullahi
Wabarakatuh
ALSA, Always be One!

Assalamualaikum Wr.Wb

Salam sejahtera bagi kita semua
Shalom, om swastiastu namo budaya

Segala puji bagi Allah SWT yang telah melimpahkan rahmat-Nya kepada kita semua sehingga kita masih dapat merasakan nikmat kesehatan dan kesempatan yang tiada tara. Salam serta salawat semoga tetap tercurahkan kepada Nabi Besar Muhammad SAW. Nabi yang telah membawa manusia dari alam yang gelap gulita ke alam yang terang benderang.

Suatu kebanggaan bagi saya dapat menjadi pimpinan redaksi PATH Vol. VIII yang tentunya menjadi suatu prestasi tersendiri bagi saya. PATH merupakan salah satu media publikasi untuk menyampaikan berbagai informasi yang berkaitan dengan dunia hukum maupun yang berkaitan dengan ALSA Local Chapter Universitas Hasanuddin.

OUR TEAM

—
WORK WITH
PASSION



Maghfirah Nasruddin

Manager of TIM Departement



Nurul Fadly Gaffar

Project Officer Path Vol. VIII

REPORTER



Aqiva Karenina, Amelia Parrangan, Syarifah Nurul



Galuh Triasny, Muh Naufal Syafiq, Ade Enaz M, Melkisedek M, Andi Megadara

LAYOUTER



Rian Nugraha, Huznul Faidzin, Satrio Aji Putra Wirabuana,
Brahmana M Ilman, Eti Kumala Putri

EDITOR

PHOTOGRAPHER



Reski Auliyah, Muthi Omar



Dimas Arya P, Indra Kurniawan

FUNDING



Ulfah Muthmainnah R, Annisa Mulya Rahman, St. Ratih Wardoyo



Rubrik Utama.

CYBERCRIME MENGGURITA, KORBAN MENDERITA; DI MANA REGULASI?

Perkembangan ilmu pengetahuan dan teknologi menghasilkan berbagai bentuk kejahatan, salah satunya di lingkungan cyber atau dunia komunikasi berbasis komputer, dan kemudian melahirkan istilah yang dikenal dengan cybercrime. Dokumen Kongres PBB tentang The Prevention of Crime and The Treatment of Offenders di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, memberikan definisi cybercrime sebagai computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network (setiap tindakan tidak sah yang terhubung melalui sistem komputer atau jaringan, termasuk kejahatan seperti harta benda tidak sah, penawaran atau distribusi informasi oleh sistem komputer atau jaringan).



Sementara itu Andi Hamzah (1989) dalam tulisannya *Aspek-Aspek Pidana di Bidang Komputer*, mengartikan kejahatan komputer sebagai kejahatan yang berhubungan dengan penggunaan komputer secara ilegal.

Dari beberapa pengertian di atas, secara ringkas dapat disimpulkan bahwa cybercrime didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi, komputer, dan telekomunikasi baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Oleh karena itu, fenomena cybercrime harus diwaspadai sebab kejahatan ini berbeda dengan kejahatan lain yang sifatnya konvensional (*streetcrime*). Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.

Sebagian besar dari perbuatan cybercrime dilakukan oleh seseorang yang sering disebut dengan hacker. Perbuatan hacking kali pertama terjadi pada tahun 1970-an saat beberapa remaja telah merusak sistem telepon negara dengan mengubah otoritas. Awal tahun 1970, John Draper membuat sebuah panggilan telepon jarak jauh secara gratis dengan meniupkan nada yang tepat ke dalam telepon lalu memberitahukan kepada sistem telepon agar membuka saluran. Draper kemudian ditangkap berulang kali untuk kasus pengrusakan telepon.

Sementara itu, munculnya cybercrime di Indonesia sulit ditelusuri kejadiannya, kapan, dan dalam kasus apa. Namun dapat dikemukakan bahwa era 1990-an adalah era awal masuknya fenomena cybercrime di Indonesia. Menilik putusan pengadilan, ada yang menyatakan bahwa kasus cybercrime yang kali pertama disidangkan di Indonesia adalah kasus pemakaian nama domain MustikaRatu.com di Pengadilan Negeri Jakarta Selatan. Perkara tersebut menyeret seorang terdakwa bernama Tjandra Sugijono dengan dakwaan pasal 382 bis KUHP dan 48 ayat (1) jo pasal 19 huruf b UU No. 5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Namun pada akhirnya terdakwa dibebaskan karena perbuatan yang didakwakan kepadanya tidak terbukti.

Instrumen Hukum Internasional publik yang mengatur masalah cybercrime yang saat ini paling mendapat perhatian adalah konvensi tentang kejahatan cyber (Convention on Cybercrime) 2001 yang digagas oleh Uni Eropa. Konvensi ini, meskipun pada awalnya dibuat oleh organisasi regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan cyber.



Sistem perundang-undangan di Indonesia sendiri belum mengatur secara khusus mengenai cybercrime. Namun, mengingat terus meningkatnya kasus-kasus cybercrime di Indonesia yang harus segera dicari pemecahan masalahnya, maka beberapa peraturan baik yang terdapat didalam KUHP maupun diluar KUHP tidak bisa dikesampingkan begitu saja.

Terdapat beberapa pasal didalam KUHP yang biasanya digunakan sebagai perumpamaan dan persamaan terhadap kasus cybercrime oleh para penyidik. Adapun pasal-pasal tersebut adalah: Pasal 378 KUHP untuk kasus penipuan; Pasal 311 KUHP untuk kasus pencemaran nama baik; Pasal 282 KUHP untuk kasus penyebaran pornografi; Pasal 378 dan 262 KUHP untuk kasus penipuan dengan kartu kredit; dan Pasal 406 KUHP untuk kasus hacking yang membuat sistem milik orang lain menjadi tidak berfungsi.



Hukum positif lain yang berlaku umum dan mengatur perbuatan-perbuatan yang dapat menjadi bentuk cybercrime, terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana melakukan kejahatan ialah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Selain mengatur cybercrime dari segi materil, UU ITE juga menentukan penegakan hukum

formil dari cybercrime tanpa mengesampingkan ketentuan dalam KUHP, khususnya dalam proses penyidikan. Ketentuan terkait penyidikan yang diatur secara khusus dalam UU ITE yaitu penyidikan dilakukan oleh Kepolisian Negara RI atau Kementerian Komunikasi dan Informatika dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data; dan penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat dengan menjaga terpeliharanya kepentingan pelayanan umum.





Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengklasifikasikan cybercrime ke dalam beberapa bentuk, yaitu Konten Ilegal; Akses Ilegal; Penyadapan Ilegal; Gangguan Data; Gangguan Sistem; Penyalahgunaan Perangkat; Penipuan dan Pemalsuan yang berkaitan dengan Komputer.

Tidak sedikit kasus cybercrime pernah terjadi di Indonesia, salah satunya adalah kasus sabotase terhadap fasilitas internet banking salah satu bank swasta sehingga transaksi-transaksi yang dilakukan oleh nasabah bank tersebut sudah dapat dipastikan tidak akan sesuai dengan permintaan nasabah atau dapat dikatakan sebagai transaksi palsu.


Hal-hal yang dapat menjadi modus pelaku cybercrime melakukan perbuatannya, yaitu: Unauthorized Access to Computer System and Service, merupakan kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah; Illegal Contents, merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang melanggar hukum; Data Forgery, merupakan kejahatan dengan memalsukan

data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet; Cyber Espionage, merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network sistem) pihak sasaran; Cyber Sabotage and Extortion, kejahatan ini dilakukan dengan membuat gangguan terhadap suatu data atau program komputer yang mana setelah kerusakan terjadi, pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data yang telah di sabotase dengan bayaran tertentu; Offense against Intellectual Property, kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet; Cracking, yaitu kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan dan biasanya melakukan pencurian saat mendapatkan akses; dan Carding, yaitu kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi melalui card credit orang lain.

Perkembangan teknologi informasi yang demikian pesatnya harus diantisipasi dengan hukum yang mengatur dengan lembaga kepolisian yang memegang peranan penting di dalam penegakan hukum, sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat terjadi kekacauan.

Pada kasus cybercrime, baik korban maupun pelaku tidak berhadapan langsung dalam 1 (satu) tempat di mana kejadian perkara terjadi, bahkan dapat terjadi antar negara. Hal ini membuktikan bahwa cybercrime merupakan salah satu bentuk kejahatan lintas negara (transnational crime), tanpa batas (borderless), tanpa kekerasan (non violence), tidak ada kontak fisik (non physically contact) dan tiada nama (anonymity). Karakteristik cybercrime tersebut membuat pelaku sulit dilacak dan unsur-unsur pidananya sulit dibuktikan, apalagi adanya keterbatasan regulasi.

Keterbatasan sumber daya manusia kepolisian dan juga cyberlaw sering menyebabkan cybercrime yang telah terjadi dapat begitu saja terlepas dari pengawasan hukum, bahkan pelaku yang telah diduga melakukan cybercrime, akibat penyelidikan dan penyidikan yang kurang tepat sasaran atau kurang sempurna, maka pelaku dapat berkelit serta melakukan pembelaan terhadap tindak pidana yang telah dilakukannya. Bahkan, tidak sedikit kasus cybercrime yang telah masuk ke dalam tahap penyidikan dikarenakan kurangnya alat bukti dalam proses pembuktian, akan lolos dari jeratan hukum, sehingga menyebabkan pelaku akan bebas dari segala tuduhan dan yang paling menderita adalah korban atau akibat dari kejahatan tersebut yang dapat merugikan banyak pihak.



Saat ini, Indonesia belum memiliki peraturan khusus atau cyberlaw yang menjadi payung hukum cybercrime. Cybercrime merupakan suatu kejahatan tanpa batas dengan teknologi canggih sehingga untuk menjerat pelaku cybercrime di Indonesia tidak dapat menggunakan hukum pidana konvensional, tetapi hukum pidana khusus yang harus tetap diperbaharui sehingga dapat mengejar ketertinggalan kecanggihan dalam kejahatan ini.

Oleh karena itu, untuk menanggulangi kejahatan internet yang semakin meluas maka diperlukan peran pemerintah dalam sosialisasi agar masyarakat lebih berhati-hati dalam mengakses hal-hal yang berhubungan dengan dunia cyber, serta perlu adanya kesadaran masyarakat mengenai bahaya penyalahgunaan internet. Disamping itu, pemerintah juga perlu meningkatkan pemahaman serta keahlian aparat hukum mengenai upaya pencegahan, investigasi, hingga penuntutan perkara-perkara yang berhubungan dengan cybercrime. Di atas segalanya, Indonesia membutuhkan modernisasi hukum pidana nasional beserta hukum acara yang selaras dengan konvensi internasional terkait cybercrime.

Penanganan dan Penanggulangan Cyber Crime Melalui Penguatan Regulasi Cyber Law di Indonesia



**Teguh
Arifiyadi**

**Deputy Director For Cyber Crime
Investigation Kemkominfo RI**



Wawancara Khusus

Bagaimana perkembangan cyber crime di Indonesia ?

Tiga tahun terakhir, lonjakan pengaduan tentang cyber crime meningkat secara signifikan dan hal tersebut mencapai angka seratus persen. Pengaduan-pengaduan tersebut didominasi kasus seperti penipuan, kemudian illegal content seperti pornografi, judi, pencemaran nama baik, hatespeech, sara, bahkan ancaman. Sisanya kejahatan yang lebih advance seperti adanya hacking, tracking, intersepsi dan lain-lain.

Apakah penanganan cyber crime sudah cukup optimal sehubungan belum adanya regulasi yang cukup tegas dalam menangani masalah cyber crime di Indonesia ?

Jika membahas mengenai sisi regulasi, sebetulnya sudah sangat tegas bahkan terbilang cukup lengkap jika dibandingkan dengan negara lain khusus mengenai kasus cyber crime. Yang menjadi persoalan adalah masalah penegakan hukumnya, penegakan hukum membutuhkan resource yang banyak, butuh biaya yang tidak sedikit, waktu yang lebih lama, dan butuh orang-orang atau penyidik yang berkompeten. Hal-hal itulah yang membuat optimalisasinya tidak berjalan dengan baik. Namun, perlu diketahui bahwa hal tersebut terjadi di hampir semua negara, tidak hanya di Indonesia.



Apa solusi yang bisa ditawarkan untuk mengatur perlindungan cyber crime di Indonesia?

Solusinya adalah kerja sama lintas sektoral yakni aparat pemerintah, aparat penegak hukum, masyarakat, komunitas, dan akademisi. Kombinasi dari banyak stakeholder ini akan membuat struktur hukum menjadi kuat. Struktur hukum yang kuat, efek hukumnya bisa membuat penegakan hukum menjadi optimal. Penegakan yang optimal ini lama-lama akan menjadi sebuah culture atau budaya hukum. Sehingga kesadaran masyarakat terhadap hukum, terhadap modus dan terhadap pemahaman masyarakat terkait cyber crime juga ikut meningkat.

Apabila seorang WNI melakukan carding terhadap WNA yg berada di Indonesia, bagaimanakah pengaturan hukumnya?

Dalam undang-undang ITE dijelaskan bahwa korbannya bisa saja WNI, WNA maupun badan hukum, artinya bisa dialami oleh siapapun. Instrumen hukumnya bisa diberlakukan melalui hukum negara asing dengan cara melakukan ekstradisi tersangka dari Indonesia ke negara korban. Dapat juga menggunakan hukum Indonesia dengan cara korban melaporkan kasus tersebut ke Interpol Indonesia.

Bagaimana jika kedepannya terjadi cyber war antarnegara, sedangkan dalam hukum Indonesia tindakan cyber war itu merupakan salah satu bentuk cyber crime, apakah negara akan terpaksa memberdayakan para hacker untuk melawan negara musuh?

Dalam konteks peperangan semua hal bisa saja dilakukan, saat ini belum pernah terjadi cyber war dalam konteks sesungguhnya, yang ada adalah cyber tech tetapi tidak semua cyber tech itu dapat menjadi cyber war. Cyber

tech bisa terjadi meskipun antara dua negara, tetapi pelakunya dari negara lain, dan cyber tech tidak pernah dapat dibuktikan di pengadilan internasional bahwa tindakan tersebut dimobilisasi oleh negara. Dan mungkin apabila tindakan tersebut suatu saat terbukti dimobilisasi oleh negara maka hal itu dapat menjadi dasar pernyataan perang cyber untuk setiap negara

Bagaimana pandangan KEMINFO terkait pemberdayaan para hacker yang berbakat di Indonesia?

Sebetulnya dalam konteks positif, pemerintah sangat mendukung segala upaya dari para hacker yang memang memiliki niatan baik. Dari KEMINFO sendiri, ada program yang namanya born to protect, program tersebut yakni mengumpulkan para hacker berbakat untuk membantu negara ini. Namun, persoalannya adalah ketika mereka sudah mulai advance, maka kecil kemungkinan mereka mau bergabung dengan pemerintah karena adanya beberapa faktor, seperti: pendapatan, budaya kerja dan lain sebagainya. Sehingga hacker tidak bisa dipaksa untuk bergabung dengan pemerintahan.

Bagaimana langkah pencegahan yang baik agar tidak menjadi korban cyber crime?

Pencegahan utama kuncinya ada dua, yaitu: pertama, awareness atau kesadaran pengguna internet. Kesadaran pengguna internet berkaitan dengan budaya keamanan informasi dimana pengguna internet memahami apa yang boleh dan tidak boleh dilakukan di internet. Kedua, budayakan literasi. Dengan literasi yang baik, maka orang atau pengguna internet akan cenderung lebih imun terhadap upaya cyber crime yang menyangkut atau mengenai dirinya.



AKBP Edy Harto

**Kasubit 2 Ditreskrimsus
POLDA Sulsel**

Bagaimana perkembangan cyber crime saat ini?

Kasus cyber crime hampir setiap tahun mengalami peningkatan. Khusus di POLDA, pada tahun ini terdapat kurang lebih 80 - 90 pengaduan dan belum termasuk pengaduan yang di ajukan ke POLRES. Adapun kasus yang diajukan biasanya masalah penghinaan atau pencemaran nama baik dan transaksi online.

Bagaimana peran POLDA dalam melaksanakan penyidikan kasus cyber crime?

Terdapat 2 tahapan dalam proses penyidikan online, yaitu; Lidik-Sidik yang merupakan proses korban mengadu. Dalam Lidik -Sidik terdapat patroli cyber setiap harinya dimana terdapat petugas yang melakukan patroli tentang cyber.

Kasus cyber crime di internet biasanya didapatkan dari kicauan-kicauan pengaduan korban dari beberapa media sosial. Setelah itu kami menghubungi korban untuk menjelaskan kronologis kasusnya. Dalam proses penyidikan, setelah ada pengaduan maka korban akan dimintai keterangan dan mengumpulkan bukti-bukti yang ada. Setelah beberapa bukti telah terkumpul maka akan dilakukan analisis terhadap bukti-bukti tersebut.

Apa saja contoh kasus yang pernah di sidik sejauh ini oleh POLDA?

Sejauh ini kasus yang paling banyak ditangani yaitu kasus transaksi online, kemudian pencemaran nama baik dan kasus penghinaan. Misalnya pencemaran nama baik, biasanya terjadi oleh dua orang yang saling kenal hanya saja mereka menggunakan media elektronik sebagai



Penanganan dan Penanggulangan Cyber Crime Melalui Penguatan Regulasi Cyber Law di Indonesia



sarana untuk mendistribusikan atau mengkampanyekan sifat buruk seseorang dan korban tersebut merasa tidak terima. Kasus seperti ini cukup mudah di ungkapkan.

Apakah hukuman yang diberikan kepada pelaku cyber crime sudah cukup membuat jera dan menurunkan persentase kriminalisasi dalam cyber crime?

Sebetulnya belum memberi efek jera apalagi pelaku cyber crime tidak perlu kemana-mana karena dapat melakukan aksinya di mana saja dan kapan saja.

Bagaimana penerapan pendidikan positif cyber terhadap anak dibawah umur?

Saat ini setiap orang bisa menggunakan internet tanpa memandang strata sosial, sehingga pendidikan yang sangat diperlukan adalah pengawasan orang tua

dan bagaimana mengajarkan penggunaan internet yang bijak kepada anak dibawah umur.

Hambatan apa yang dialami dalam memberantas kasus cyber crime?

Banyak hambatan yang kami lalui, diantaranya pendukung fasilitas yang belum memadai, hal ini dikarenakan alatnya cukup mahal. Dan biasanya setiap POLDA hanya di sediakan satu alat. Diantaranya alat yang digunakan untuk melacak nomor telepon seseorang. Yang kedua yaitu apabila nomor telepon seseorang tidak aktif maka tidak dapat dilacak lagi. Sehingga penyidik akan kehilangan jejak dalam menyelesaikan kasus yang ada.

Legal Opinion.



UU ITE : Berpacu Ditengah Legalitas dan Modernisasi



Zul Kurniawan Akbar

Director ALSA LC Unhas 2014-2015

“The world is full of digital devices. Without them, society as we know it would probably collapse.” (Angus Marshall, Digital Forensics: Digital Evidence in Criminal Investigations). Perkembangan teknologi informasi telah menyediakan perubahan besar di seluruh dunia, baik itu untuk mempermudah segala urusan (positive effect) maupun menciptakan masalah karena menggunakan secara tidak cakap atau menggunakan dari dan untuk hal ilegal (Negative Effect).

Seperti halnya di negara ini, Indonesia telah menduduki Top 5 dalam deretan pemakai Internet terbesar di dunia. (Internet World Stats, Top 20 Countries With The Highest Number of Internet Users In June 2017). Tidak heran mengapa jumlah itu terus meningkat tiap tahunnya mengingat Indonesia merupakan negara dengan populasi yang sangat banyak dan

sebagian besar masih berperilaku konsumtif. Wajar saja jika Pemerintah perlu melakukan suatu tindakan yang perlu menjadi landasan sekaligus pijakan yang layak untuk mengawal perkembangan Teknologi Informasi.

Dengan semangat mendukung perkembangan Teknologi Informasi di Indonesia yang terbilang cepat dan masif ini, Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) lahir sebagai jawaban pemerintah dari segi infrastruktur hukum untuk menjadi langkah penindakan maupun pencegahan terhadap hal-hal yang menjadi Negative Effect dari perkembangan ini.



Seiring berjalannya waktu, ternyata pemberlakuan aturan tersebut masih menjadi polemik untuk sebagian penegak hukum. Penyebabnya diantara lain:

- Multitafsir dalam beberapa ketentuan Pasal maupun ayat
- Munculnya Tindak Pidana dengan modus yang lebih canggih.
- Besarnya potensi pelanggaran hak asasi manusia dalam proses penegakan hukum.
- Keabsahan alat bukti Elektronik yang masih debatable dalam proses persidangan.
- Minimnya penegak hukum yang memahami dan memanfaatkan teknologi informasi

Permasalahan itu datang secara beruntun dan telah menjadi bahan kajian bersama bagi pihak yang berwenang untuk segera melakukan revisi. Permasalahan itu tidak kurangnya datang dari beberapa kasus yang telah diputus inkracht maupun dari beberapa gugatan Judicial Review yang diajukan ke Mahkamah Konstitusi. Namun butuh waktu sekitar 8 tahun dari semenjak diberlakukan UU ITE tersebut, pemerintah akhirnya berani melakukan perubahan yang kemudian disahkan menjadi Undang-Undang No. 19 tahun 2016 tentang Perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pertimbangan utama perubahan ini ialah demi menjaminnya pengakuan serta penghormatan atas hak dan kebebasan orang lain untuk memenuhi tuntutan yang adil sesuai dengan

pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis agar terwujudnya keadilan, ketertiban umum dan kepastian hukum.

Adapun perubahan yang terdapat dalam Undang-Undang No. 19 Tahun 2016:

1. Menambahkan ketentuan Right to be Forgotten

Hal ini merupakan wujud dari banyaknya permintaan dari pihak korban yang dirugikan dari suatu informasi/dokumen elektronik yang telah terlanjut tersedia dalam suatu Sistem Elektronik. Ketentuan ini diatur dalam Pasal 26 yang mana pada intinya setiap Penyelenggara Sistem Elektronik wajib menghapus dan menyediakan mekanisme penghapusan Informasi/Dokumen Elektronik yang tidak relevan berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasar penetapan pengadilan.

2. Menambahkan penjelasan tentang "Mendistribusikan, mentransmisikan, dan membuat dapat diakses".

Demi mencegahnya multitafsir terhadap ketentuan larangan tersebut (pasal 27), maka "Mendistribusikan, mentransmisikan, dan membuat dapat diakses" diberikan batasan masing-masing agar jelas bila dilakukan pembuktian berdasarkan dari setiap unsur yang ada dalam pasal terkait.

3. Penegasan ketentuan Pasal Pencemaran nama baik/Penghinaan

Menegaskan ketentuan Pencemaran nama baik/Penghinaan (Pasal 27 ayat (3)) bahwa pada delik ini merupakan delik aduan bukan delik umum. Serta ketentuan ini dan ayat 4 juga mengacu pada ketentuan delik sejenis yang diatur dalam Kitab Undang-Undang Hukum Pidana.

4. Penurunan Ancaman Pidana.

Ancaman pidana yang diturunkan ada pada delik penghinaan/pencemaran nama baik (pasal 27 ayat (3)) dari maksimal 6 tahun dan/atau denda Rp. 1.000.000.000 menjadi maksimal 4 tahun dan/atau denda Rp. 750.000.000 yang dituang dalam pasal 45 ayat (3) dan delik ancaman elektronik (pasal 29) dari maksimal 12 tahun dan/atau denda Rp. 2.000.000.000 menjadi maksimal 4 tahun dan/atau denda Rp. 750.000.000. yang dituang dalam pasal 45B.

5. Pelaksanaan dari putusan Mahkamah Konstitusi

Merupakan hasil dari Judicial Review yang diajukan oleh Setya Novanto dengan Putusan No. 20/PUU-XIV/2016 tentang keberadaan penyadapan yang perlu batasan demi menjaga hak privasi individu yang dijaga oleh UUD. Hasil tersebut dituang dalam 2 ketentuan yaitu pertama, menambahkan penjelasan pada ketentuan pasal 5 ayat (1) dan (2) mengenai keberadaan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah. Terkhusus untuk informasi elektronik dan/atau dokumen elektronik yang didapatkan dari intersepsi atau penyadapan atau perekaman haruslah dilakukan dalam proses penegakan hukum dan memiliki izin dari pihak yang memiliki kewenangan untuk itu (kepolisian, Kejaksaan, dan institusi lainnya). Kedua, mengubah ketentuan pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam

Undang-undang.

6. Sinkronisasi ketentuan Hukum acara pada KUHAP

Pengegeledahan/Penyitaan (Pasal 43 ayat (5)) disesuaikan kembali dengan ketentuan dalam KUHAP serta Penangkapan/Penahanan (pasal 43 ayat (6)) juga disesuaikan kembali dengan ketentuan dalam KUHAP.

7. Penguatan Peran Penyidik Pegawai Negeri Sipil (PPNS)

Hal ini dijelaskan dalam ketentuan Pasal 43 ayat (5) yaitu adanya kewenangan membatasi/memutus akses terkait tindak pidana yang diatur dalam Undang-Undang ini. serta adanya kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana yang diatur dalam Undang-Undang ini.

8. Penguatan peran Pemerintah

Pemerintah dalam hal ini memberikan perlindungan dari segala jenis gangguan yang lahir dari penyalahgunaan Informasi dan Transaksi Elektronik. Adapun ketentuan yang ditambahkan dituangkan dalam Pasal 40 ayat (2a) dan ayat (2b) yang pada intinya Pemerintah wajib melakukan pencegahan dari penyebaran dan penggunaan Informasi/Dokumen Elektronik yang memiliki muatan yang dilarang serta metode pencegahan yang dilakukan dengan pemutusan akses oleh Penyelenggara Sistem Elektronik.

Perubahan ini telah berlaku diakhir tahun 2016, namun faktanya ada beberapa kasus yang sempat menjadi buah bibir di masyarakat Indonesia yang mencederai upaya Pemerintah dalam melakukan perubahan terhadap UU ITE ini. Terutama dalam hal Penyadapan/Intersepsi yang terbilang mempersulit ruang gerak penyidikan serta kedudukan/keabsahan Alat Bukti Elektronik yang dihadirkan dalam persidangan. Perubahan UU ITE ini seyogyanya menjadi solusi yang menjembatani antara modernisasi dan legalitas.

**KESIMPULAN:**

Teknologi Informasi akan terus berkembang dari waktu ke waktu yang telah menjadi bagian daripada peradaban manusia di zaman ini. Dari perkembangan tersebut, setiap Pemerintahan di dunia haruslah sudah menyiapkan segala kemungkinan terhadap hal-hal yang berada diluar dari fungsi perkembangan Teknologi Informasi. Indonesia sebagai penyumbang terbesar pemakai perangkat elektronik dan Internet perlu dikawal sebaik mungkin agar penyimpangan terhadap pemanfaatan Teknologi Informasi dapat diakomodir. Pemerintah mengeluarkan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai langkah konkrit untuk melakukan pencegahan serta penindakan dari dampak negatif perkembangan Teknologi Infomasi. Pemerintah kemudian mengeluarkan Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 Tahun 2008 (UU ITE) sebagai jawaban atas permasalahan yang dianggap belum atau tidak terakomodir pada ketentuan-ketentuan sebelumnya. Adapun Perubahannya berupa Penguatan terhadap Peran Penegak hukum dan Pemerintah, Penjelasan terhadap ketentuan-ketentuan yang multitafsir, Penambahan beberapa ketentuan yang sifatnya menguatkan ketentuan-ketentuan sebelumnya serta Pelaksanaan dari Putusan Mahkamah Konstitusi. Perubahan itu tidak serta-merta dapat menjawab permasalahan yang terjadi, tapi butuh waktu dan konsistensi dari penegak hukum dalam pelaksanaan Undang-undang ini. Sekiranya perubahan ini dapat dijadikan sebagai wujud tranformasi hukum yang sejalan dengan perkembangan zaman.

SARAN:

Penegak Hukum perlu lebih dalam lagi mengkaji tentang peraturan ini dan terus mempelajari perkembangan Teknologi infomasi agar tidak menjadi hambatan melainkan alat bantu yang memudahkan segala proses penegakan hukum yang telah diatur sebagaimana mestinya. Kesadaran Masyarakat umum juga diperlukan agar dapat memanfaatkan fungsi dari Teknologi Informasi tidak sekedar sebagai wujud mengikuti perilaku hidup yang dianggap kekinian, tetapi menjadi pemakai yang cerdas dan mengantar ke hal-hal yang sifatnya produktif untuk diri maupun untuk bangsa.

DASAR HUKUM:

Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
Kitab Undang-Undang Hukum Pidana
Putusan MK No.No.20/PUU-XIV/2016
Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
Kitab Undang-Undang Hukum Pidana
Putusan MK No.No.20/PUU-XIV/2016
Penegasan ketentuan Pasal Pencemaran nama baik/Penghinaan Menegaskan ketentuan Pencemaran nama baik/Penghinaan (Pasal 27 ayat (3)) bahwa pada delik ini merupakan delik aduan bukan delik umum. Serta ketentuan ini dan ayat 4 juga mengacu pada ketentuan delik sejenis yang diatur dalam Kitab Undang-Undang Hukum Pidana.



Did You Know ?

7 KASUS BESAR CYBER CRIME BERBENTUK MALWARE YANG PERNAH TERJADI DI DUNIA !!!

Ransomware Wannacry

Ransomware, secara sederhana, merupakan program jahat yang bertujuan untuk memperoleh uang tebusan atas penyanderaan atau penguncian data yang dilakukan program tersebut. Dalam laporan Reuters. Com disebutkan bahwa serangan ini telah menerjang hampir 100 negara di seluruh dunia. Perusahaan jasa pengiriman FedEx serta Departemen Kesehatan Inggris adalah contoh beberapa korban dari aktivitas malware ini.

1

My Doom

Malware ini muncul pada tahun 2004 dan terkenal sebagai malware terkejam karena membuat akses internet melambat dan dengan cepat menginfeksi sekitar satu juta komputer saat itu. Virus menyebar melalui email yang tampaknya seperti pesan yang memantul (bouncing email). Diperkirakan jumlah kerugian akibat virus ini sebesar 38 miliar dolar AS.

2



3

Agent.BTZ

Agent.BTZ, atau lebih dikenal dengan nama Autorun, adalah virus komputer yang menginfeksi USB flash drive dengan spyware. Pada tahun 2008 di sebuah pangkalan militer AS di Timur Tengah, USB flash drive yang terinfeksi Agent.BTZ dimasukkan ke dalam laptop yang terpasang pada Komando Pusat Amerika Serikat. Lalu virus tersebut menyebar tanpa terdeteksi ke sistem lain. Untuk menghentikan penyebaran virus tersebut Pentagon melarang penggunaan USB Drives serta media yang removeable. Pentagon menghabiskan waktu sekitar 14 bulan untuk membersihkan virus ini dari jaringan militer.

4

Stuxnet

Virus ini adalah virus komputer yang dirancang khusus oleh hacker yang umumnya digunakan untuk mengintai, mengganggu dan menyerang sistem kontrol industri. Malware menyebar melalui perangkat memori USB thumb drive yang terinfeksi, penyerangannya bertarget pada sistem SCADA (Supervisory Control and Data Acquisition). Pada Agustus 2010, Symantec mencatat bahwa 60% dari komputer yang terinfeksi di seluruh dunia berada di Iran dengan 62.867 komputer yang terinfeksi dan beberapa negara lainnya.

5

Black Shades

Virus jenis ini dapat menyusup secara diam-diam, mengubah file pada sistem, menginstal key-logger, mengakses kamera, membuat botnet yang bisa menyebabkan dDOS-attack, mengunduh file lain secara rahasia dan otomatis menjalankannya, hingga dapat menggunakan proxy server pada pengguna. Kemudian, "BlackShades" memungkinkan para peretas mencuri informasi pribadi, mencegat pesan penting dan membajak kamera pada komputer atau webcam untuk digunakan secara diam-diam demi kepentingan mereka. FBI mendeteksi lebih dari 500.000 komputer di lebih 100 negara di dunia terjangkau virus berbahaya ini.

6

Slammer

Slammer muncul pada tahun 2003, virus ini menyebabkan penolakan layanan pada beberapa host Internet dan secara dramatis melambatkan lalu lintas internet. Virus jahat ini menyebar dengan cepat dan menggandakan diri tiap 8.5 detik. Bank of America, panggilan 911, Maskapai Continental, hingga sebuah kawasan fasilitas di Ohio, Amerika Serikat pernah menjadi korbannya, dimana secara keseluruhan virus ini menginfeksi sekitar 200.000 komputer dan kerugiannya ditaksir mencapai 1,2 miliar dolar AS.

7

I LOVE YOU

Virus ini disebar oleh seorang mahasiswa bernama Onel de Guzman di Filipina pada tahun 2000. Cara penyebarannya melalui email ke email pengguna Microsoft Outlook dengan hadir sebagai lampiran pada email dengan nama file LOVE-LETTER-FOR-YOU-TXT.vbs. Ketika dibuka, virus I LOVE YOU akan menyerang sistem database pengguna komputer dan mencuri password akses internet pengguna. 55 juta unit komputer di seluruh dunia terjangkau oleh virus ini dan jumlah kerugiannya sekitar US\$10 miliar.

Menurut kamu, Bagaimana peran pemerintah menanggulangi berita hoax di dunia maya? Kalau belum maksimal, Apa saran mu?



Eflin Christy

ALSA LC Unair

Peran pemerintah dalam menanggulangi hoax belum maksimal, karena bisa dilihat berdasarkan kualitas berita yang disajikan dalam sosial media yang semakin gencar akan ketidaksesuaian dengan apa yang terjadi. Realita yang ada di Indonesia, ada sebuah website jika membuat berita hoax maka ada imbalan yang diperoleh berupa bayaran. Dapat dilihat dengan jelas bahwa peran pemerintah sangat kurang maksimal.

Saran untuk pemerintah khususnya Kementerian Komunikasi dan Informasi, lebih mengawasi lagi dalam hal memberantas berita hoax di sosial media. Sebab netizen saat ini lebih percaya hoax karena adanya beberapa website yang terpercaya, namun menyebar berita hoax yang akhirnya menyebabkan netizen percaya dan menimbulkan keresahan dalam masyarakat.



Mustabiqui Khair

Jurusan Elektro
Universitas Hasanuddin

Pihak pemerintah dengan serius telah melakukan kampanye-kampanye anti hoax, dan divisi siber POLRI telah sadar mengenai tugasnya untuk menangani kasus-kasus hoax yang meresahkan masyarakat. Dari pandangan saya, para engineer selalu berkompetisi menciptakan teknologi termutakhir sehingga dapat dinikmati oleh setiap lapisan masyarakat tetapi tidak diikuti dengan perkembangan kearifan masyarakat dalam menggunakannya, sehingga menciptakan "culture jetlag" pada masyarakat awam yang dengan polosnya mempercayai apapun yang ada di internet. Saya merasa perlu ada edukasi khusus dalam sekolah-sekolah mengenai bagaimana dunia IT itu dan bagaimana menyikapi hal-hal di dunia maya, sehingga masyarakat kedepannya tidak "awam" lagi jika menghadapi berita-berita yang tidak jelas resourcer-nya.



Andi M. Arie

ALSA LC Unsyiah

Saat ini perkembangan teknologi membawa banyak dampak positif maupun negatif. Seiring berjalannya waktu, dampak negatif dari perkembangan teknologi mulai terlihat, salah satunya tindak kejahatan di dunia maya atau lebih dikenal sebagai cyber crime.

Sesuai dengan UU No. 19 tahun 2016 perubahan atas UU No. 11 tahun 2008 tentang Internet dan Transaksi Elektronik, cyber crime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk didalamnya adalah penipuan, lelang secara online, pemalsuan cek, penipuan kartu kredit (carding), confidence fraud, penipuan identitas, pornografi anak, dan lainnya. Maka dibutuhkan sebuah payung hukum yang maksimal untuk mengawasi perkembangan ini, namun tanpa melebihi privasi yang masyarakat butuhkan dalam pengawasannya.



FORUM BEBAS

Saat ini pemerintah mulai melakukan upaya-upaya untuk menanggulangi isu-isu hoax yang sedang berkembang di masyarakat. Ketentuan mengenai hal tersebut telah diatur dalam UU ITE, dan UU Penghapusan Diskriminasi Ras dan Etnis. Selain itu, terdapat sosialisasi penanganan isu-isu radikalisasi dan hoax yang dilakukan oleh Kementerian Komunikasi dan Informatika (KOMINFO) serta terdapat Badan Siber & Sandi Nasional yang dibentuk guna menjamin terselenggaranya kebijakan dan program di bidang keamanan siber, yang salah satunya yaitu melawan penyebaran informasi yang menyesatkan. Namun, akan lebih baik apabila ditunjang dengan penegakan hukum yang lebih baik lagi. Saran untuk kedepannya yaitu lebih enforcement mengenai ketentuan terhadap hoax tersebut sehingga dapat ditanggulangi lebih cepat dan mengurangi dampak dari hoax bagi masyarakat. Selain itu, masyarakat harus lebih berhati-hati terhadap keakuratan informasi yang diterima, khususnya di dunia maya.



**Friliyanti
Putri**
ALSA LC UI

Peran pemerintah menanggulangi hoax di dunia maya meningkat dari tahun-tahun sebelumnya, namun belum ada perubahan yang signifikan dalam tersebarnya berita hoax. Berita hoax menyebar dengan sangat mudah karena semakin banyak pengguna media sosial. Agar peran pemerintah bisa lebih maksimal, pemerintah diharapkan dapat menggunakan situs resminya sebagai verifikator yang dapat mengklasifikasi berita-berita yang tersebar. Pemerintah juga dapat bekerjasama dengan akun-akun yang memiliki pengaruh di media sosial dan platform berpengaruh seperti Google, Facebook, Twitter atau Youtube.

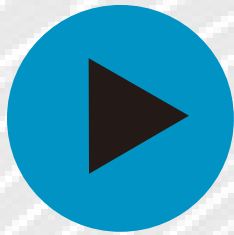


**Fakhraha
Rahmiani**
ALSA LC UGM

Seperti yg kita ketahui bahwa cyber crime merupakan bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Menurut saya, kemampuan pemerintah dan aparat kepolisian masih sangat minim dalam menangani kasus ini. Kendala utamanya yaitu borderless (tak terbatas) baik korban maupun tersangka sehingga perangkat hukum konvensional yang ada di Indonesia belum atau tidak bisa menjangkau secara efektif. diperlukan peralatan yang canggih guna pembuktian dan menyiapkan penyidik POLRI untuk di didik agar mampu menyidik cyber crime, serta kerjasama dengan penegak hukum yang ada di luar negeri. Aparat POLRI divisi siber diharapkan anggotanya bukan hanya dari jajaran kepolisian saja, tetapi sebaiknya membuka kesempatan atau merekrut orang-orang yang paham tentang kejahatan dunia maya. Karena hal ini sangat bermanfaat dalam mengungkap dan menanggulangi cyber crime, khususnya di Indonesia.



**Beyti Nur
Alimah**
ALSA LC Unsrat



ALSA Activity

Semworknas 2017

1

Seminar dan Workshop Nasional 2017 merupakan kegiatan nasional yang dilaksanakan oleh ALSA Indonesia setiap tahunnya. Acara ini terdiri dari serangkaian kegiatan, yaitu Seminar yang dibawakan oleh narasumber dari berbagai bidang hukum, diikuti dengan workshop, dan diakhiri dengan upacara penutupan serta city trip. Semworknas 2017 dilaksanakan di Jember pada tanggal 17-19 Juli 2017 dengan ALSA LC UJ sebagai tuan rumah.



2

ALSA Visit

ALSA Visit merupakan merupakan kegiatan tahunan ALSA LC Unhas yang bertujuan untuk meningkatkan hubungan sesama member ALSA LC Unhas di local chapter lain. ALSA Visit kali ini dilaksanakan pada tanggal 21-24 Juli 2017 di Universitas Udayana dengan ALSA LC Unud sebagai tuan rumah, ALSA Visit kali ini mengangkat tema "Creating Connection, Building Bridges Together".



Law Field Study

3

ALSA Law Field Study merupakan kegiatan magang / internship yang bertujuan untuk memberi pengalaman belajar secara langsung. Peserta magang ini ialah member/demisioner ALSA LC Unhas dan peserta IMCS 2017. Program kerja ini, ALSA LC Unhas bekerja sama dengan 7 instansi, yaitu: Kejaksaan Tinggi, Kejaksaan Negeri, Pengadilan Negeri, Kantor Notaris dan PPAT, Kementerian Lingkungan Hidup, PT. Bosowa Properti Indo, dan Otoritas Jasa Keuangan. Kegiatan ini dilaksanakan mulai tanggal 1-14 Agustus 2017.





ALSA ON VACATION

4



ALSA On Vacation merupakan program kerja dari Internal Affairs Department yang pada tahun ini dilaksanakan di Pulau Sanrobengi, Takalar pada tanggal 12-13 Agustus 2017. ALSA On Vacation bertujuan sebagai salah satu ajang bagi member untuk berlibur bersama sekaligus meningkatkan persaudaraan dan kekeluargaan diantara member ALSA LC Unhas

5

ALSA Cup



ALSA Cup adalah salah satu program kerja ALSA LC Unhas dalam rangka memperingati kemerdekaan Republik Indonesia, ALSA Cup kali ini bertemakan "Sportivity Strengthens Our Solidarity" yang dilaksanakan di Fakultas Hukum Universitas Hasanuddin pada tanggal 26 dan 27 Agustus 2017. Kegiatan ini menjadi salah satu media menjalin kekerabatan antar member ALSA LC Unhas.

Intensive Training

6



Intensive Training merupakan program kerja yang ditujukan untuk persiapan National Moot Court Competition XXI. Kegiatan dilaksanakan pada tanggal 14 Agustus sampai 3 September 2017. Intensive Training merupakan program kerja dari Moot Court Department. Setiap peserta akan diberikan pembelajaran mengenai materi serta praktik persidangan dari pemateri yang berpengalaman dan memiliki kemampuan yang handal di bidangnya.

7

Workshop NMCC MA



Workshop NMCC piala MA merupakan kegiatan yang ditujukan sebagai bentuk pelatihan dan pembekalan bagi member ALSA yang ingin mendaftarkan diri mengikuti kompetisi National Moot Court Competition piala MA XXI. Dalam kegiatan ini, para peserta akan dibekali ilmu dan keterampilan dari pemateri atau narasumber yg memiliki pengalaman dan prestasi di bidang peradilan semu.

GRADUATION DAY

8



Graduation Day merupakan kegiatan yang dilakukan oleh Alumni and Public Relation Department untuk alumni ALSA LC Unhas yang berhasil memperoleh gelar Sarjana dan Magister Hukum. Kegiatan ini dilaksanakan sekali per triwulan, dan bertujuan untuk mengikat tali silaturahmi antar member, pengurus, dan alumni ALSA LC Unhas.

9

ALSA Institutional Visit



ALSA Institutional Visit adalah salah satu kegiatan dari ALSA LC Unhas yang melaksanakan tur ke berbagai lembaga negara. ALSA Institutional Visit kali ini dilaksanakan pada tanggal 8 September 2017 dengan mengunjungi Badan Pemeriksa Keuangan RI Perwakilan Provinsi Sulawesi Selatan dan mengangkat tema "Independensi BPK dalam struktur ketatanegaraan Indonesia".

Kajian Malam

10



Kajian Malam merupakan kegiatan yang diadakan oleh HRD Department yang bertujuan untuk mengasah kemampuan member baru dari segi akademik. Kegiatan kajian pada malam hari ini dilaksanakan karena menimbang perlu adanya pengkajian kembali materi-materi serta isu-isu yang sedang hangat diperbincangkan di masyarakat.

11

Back To Society



Merupakan program kerja Legal Counseling Department yang bertujuan memberikan suatu pengalaman kerja nyata kepada member ALSA LC Unhas dalam hal pengabdian dan penanganan kondisi sosial yang terjadi di masyarakat. ALSA Back To Society kali ini bertema "Pengenalan dan Pendataan kartu Tanda Penduduk Warga Desa Toddolimae" dan dilaksanakan pada tanggal 15 - 17 september 2017, di Desa Toddolimae, Kabupaten Maros.



PALT 2017

12

Pra-Musyawah Nasional & ALSA Leadership Training XXIV merupakan salah satu program kerja dari ALSA Indonesia yang dilaksanakan setiap tahun. PALT ke XXIV ini dilaksanakan pada tanggal 25-28 September 2017 dengan ALSA LC Unair sebagai tuan rumah. PALT ini bertujuan untuk membahas progress tiap-tiap local chapter dan event-event nasional, serta melatih kepemimpinan member ALSA.



13

AECO 2017

ALSA English Competition (AECO) merupakan salah satu program kerja ALSA LC Unhas yang bertujuan untuk mewadahi peserta lomba untuk menyalurkan bakatnya dalam kompetisi bahasa Inggris, peserta kegiatan tersebut terdiri dari siswa(i) SMA serta Mahasiswa(i) dengan 4 item lomba yaitu, Debate, Speech, Newscasting, serta Story Telling. AECO dilaksanakan pada 20-22 Oktober 2017 dengan mengangkat tema "Raise Up The Champion, Lead The World Civilization".



Seminar Nasional

14

Seminar Nasional merupakan kegiatan ALSA LC Unhas yang kali ini mengangkat tema "CYBER LAW, INTERNET UNDERCOVER : Mengulas Cyber Crime di Tengah Masyarakat Urban". Seminar Nasional ini bertujuan untuk menambah wawasan dan membangun pandangan mahasiswa serta peserta seminar lainnya dalam memandang kasus-kasus hukum. Seminar Nasional kali ini dilaksanakan pada tanggal 3 November 2017 bertempat di Aula Prof. Amiruddin Universitas Hasanuddin.

Scrabble Competition

15



English Day merupakan salah satu program kerja dari English Department yang bertujuan untuk melatih dan menyesuaikan member ALSA LC Unhas dalam berbicara Bahasa Inggris sehari-hari (Daily Language) secara mudah dan aplikatif. English Day kali ini diadakan "Scrabble Competition" bagi internal ALSA LC Unhas.

16

Video Edukasi



Video Edukasi merupakan salah satu agenda kerja dari Technology, Information, and Multimedia Department yang bertujuan memberikan edukasi melalui menggunakan media video yang lalu selanjutnya diupload di media sosial ALSA LC Unhas. Video Edukasi dilaksanakan sekali dalam 3 bulan, dan saat ini telah ada 3 Video Edukasi, yakni Video Edukasi Ramadhan: Sahur On The Road, Video Edukasi II: Sarjana Hukum, Mau Jadi Apa?, dan Video Edukasi III: Haters di Sosmed.

ALSA Camp

17



ALSA Camp merupakan kegiatan atau program kerja dari Internal Affairs Department yang bertujuan meningkatkan rasa persaudaraan dan kekeluargaan para member ALSA LC Unhas. ALSA Camp diadakan di Villa Muallim, Camba kab. Maros. Kegiatan juga menjadi salah satu sarana liburan bagi member ALSA LC Unhas.

18

English Race



English Race merupakan program kerja dari English Department. Kegiatan English Race ini dilaksanakan di Camba Kab. Maros pada tanggal 12 November 2017. Pada kegiatan ini, member ALSA dibagi dalam beberapa kelompok secara acak, kemudian mengikuti berbagai games. Kegiatan ini ditujukan untuk melatih kekompakan serta keterampilan member ALSA dalam berbahasa Inggris yang dikemas dengan lebih menyenangkan.



ALSA Fun Day

19

ALSA Fun Day merupakan salah satu kegiatan ALSA LC Unhas yang diselenggarakan oleh Internal Department dengan tujuan untuk mempererat tali silaturahmi antar anggota ALSA LC Unhas.



20

English 101

English 101 adalah program kerja dari English Department yang dilaksanakan setiap bulan guna meningkatkan kemampuan berbahasa inggris member ALSA LC Unhas. Dalam pelaksanaannya, member ALSA akan diberikan materi atau bahan diskusi dari pemateri yang merupakan demisioner ataupun alumni ALSA LC Unhas yang handal di bidangnya.



Mootcourt Meeting

21

Merupakan kegiatan yang dilaksanakan untuk meningkatkan ilmu pengetahuan member ALSA dalam bidang peradilan semu. Kegiatan ini dilaksanakan sebulan sekali dengan menghadirkan fasilitator yang tentunya sangat memotivasi peserta dalam mengkaji pengetahuan di bidang peradilan.



22

ALSA Study Club

ALSA Study Club merupakan kegiatan bulanan yang diadakan oleh HRD Department dengan tujuan untuk meningkatkan pengetahuan member ALSA LC Unhas terkait isu yang sedang hangat di masyarakat dan melatih member ALSA untuk berfikir kritis dalam menghadapi isu tersebut.

ALSA Study Trip Japan

23



Salah satu program kerja yang diadakan oleh ALSA Nasional Chapter Jepang. Study Trip ini diikuti oleh beberapa negara yang tergabung dalam ALSA Internasional. Selain menikmati keindahan negara Jepang, para delegasi juga diajak mengunjungi Mahkamah Konstitusi Jepang dan melakukan table discussion untuk mengkaji masalah sosial dari sudut pandang negara masing-masing delegasi. Pada ALSA Study Trip Jepang ini, ALSA LC Unhas mengirimkan salah satu delegasinya, yakni Lavenia Budi Pratiwi Buce.

24

ALSA Forum



ALSA Forum merupakan salah satu program kerja yang dilaksanakan oleh ALSA International. Syarifah Fadliyah Nurul Hidayah sebagai delegasi dari ALSA LC Unhas bersama delegasi dari local chapter lainnya turut mewakili ALSA NC Indonesia di ALSA Forum 2017. ALSA Forum 2017 dilaksanakan di Singapura selama tujuh hari.

ALSA CLCC

25



ALSA Care and Legal Coaching Clinic merupakan program kerja turunan dari ALSA Indonesia yang diturunkan ke setiap local chapter dengan mengangkat tema mengenai Disabilitas, untuk ALSA LC Unhas sendiri memberi judul tema yakni "Raise the Sustainable Life, by Go Beyond Our (dis) Ability". Kegiatan ini berlangsung selama 2 hari yaitu tanggal 9-10 Desember. Kegiatan ini dirangkaikan dengan perayan HDI yang dihadiri oleh berbagai komunitas penyandang disabilitas.

Alone

We Can Do

So Little,

Together

We Can Do

So Much

Helen Keller

ALSA,

Always Be One !

GA'DE ALSA

Alsaian's merchandise



IDR 80 K
(sleeves + 10k)
available
S, M, L, XL

RECHT TEE



IDR 80 K
(sleeves + 10k)
available
S, M, L, XL
red & black

**LOADING SARJANA
HUKUM TEE**



For order & inquiries :

LINE andifadhillahdr
chiataaaa
epmrtha



ASIAN
LAW
STUDENTS'
ASSOCIATION
LOCAL CHAPTER
UNIVERSITAS HASANUDDIN

COMING SOON



Semworknas2018

“Find Your Rhythm of Harmony
Throughout The Nation”








Watturami Ke Makassar!



PATH

NEWS LETTER OF ALSA LC UNHAS

 www.alsalcunhas.org  [@alsalcunhas](https://twitter.com/alsalcunhas)  [Alsa Lc Unhas](https://www.facebook.com/Alsa.Lc.Unhas)  [Alsa Lcunhas](https://www.youtube.com/Alsa.Lc.unhas)  [alsalcunhas](https://www.instagram.com/alsalcunhas)

