Bab 1

Profesionalisme di Bidang Teknologi Informasi

1.1 Pengantar

Bagian ini akan menjelaskan tentang profesionalisme di bidang teknologi informasi yang terkait dengan bagaimana seseorang mampu dalam mengelola secara utuh dan professional menjalankan perannya dalam pemanfaatan teknologi informasi dan komunikasi (TIK) di lingkungannya baik lingkungan pekerjaan sebagai pegawai atau pimpinan di perusahaannya ataupun sebagai personal dalam mengembangkan usaha secara mandiri atau wirausahawan. Oleh karena itu, perkembangan TIK ini tentu harus diiringi dengan peningkatan profesionalisme di bidang teknologi informasi, dimana sumber daya manusia sebagai pelaku utama dalam memanfaatkan TIK ini harus terus bertambah pengetahuannya dan mampu beradaptasi secara cepat agar dapat terciptanya keseimbangan antara perkembangan teknologi informasi dengan penggunaannya dalam upaya meningkatkan kinerja di bidang teknologi informasi.

Secara umum dapat dikatakan bahwa seseorang dikatakan profesionalisme di bidang teknologi informasi, jika pengetahuan tentang teknologi informasi dibidangnya yang dimilikinya secara mendasar dan kuat sehingga mengerti sekali tujuan, manfaat kegunaan dari keilmuan tersebut, juga harus

berdasarkan pengalaman dan hasil penelitian yang valid bukan hanya sekedar hasil membaca teori-teori yang ada, dan yang terakhir adalah mampu mengelolanya secara berkelanjutan dan berkembang terus mengikuti arah perkembangan teknologi informasi yang cepat ini. Hal lain yang perlu diperhatikan bagi seorang profesionalisme di bidang teknologi informasi adalah ketekunan, keseriusan, dan fokus dalam menjalani profesinya dan selalu meningkatkan kemampuan yang dimilikinya melalui program srtifikasi di bidang teknologi informasi.

Pendidikan secara formal di berbagai tingkatan sudah memberikan jalannya untuk pengembangan profesionalisme di bidang teknologi informasi ini, seperti program pendidikan sekolah menengah kejuruan bidang teknologi informasi, program pendidikan jenjang diploma jurusan teknik informatika atau manajemen informatika, dan program pendidikan tingkat sarjana atau pasca sarjana jurusan teknologi informasi. Sasaran pada masing-masing tingkatan pendidikan formal inipun berbeda-beda. Untuk pendidikan tingkat sekolah menengah kejuruan sasarannya adalah menghasilkan lulusan dengan kualifikasi tenaga teknolgi informasi yang siap pakai dalam bidang opersional, untuk pendidikan formal tingkat diploma sasarannya adalah menghasilkan lulusan secara professional siap pakai dan memiliki beberapa pengalaman proyek di bidang teknologi informasi. Sedangkan untuk tingkatan sarjana atau pasca sarjana sasarannya adalah menghasilkan lulusan yang terampil serta memiliki kemampuan yang kuat untuk melakukan analisis dan perancangan sistem dan teknologi informasi yang dapat diterapkan sampai diadopsi oleh perusahaan.

Profesionalisme di bidang teknologi informasi dapat didapat melalui program sertifikasi yang banyak diselenggarakan perusahaan bidang jasa pelatihan, diantaranya sertifikasi IC3 GS5 Computer Fundamental, yang dapat memberikan kemampuan: perangkat selular, perangkat keras,

arsitektur perangkat lunak komputer, backup dan restore, file sharing, cloud computing, dan keamanan sistem dan teknologi informasi (Schultz, 2021). Contoh yang lain adalah sertifikasi di bidang Information Technology Specialist in Databases, yang memberikan kemampuan dalam database design, database object management, data retrieval, data manipulasi, troubleshooting (Certiport, 2021).

1.2 Konsep Profesionalisme

Pengertian profesionalisme diawali dengan pemahaman tentang profesi dan profesional. Pengertian dari profesi dan profesional terkadang seperti sama namun memiliki pemahaman yang berbeda. Profesi lebih ditekankan pada seseorang yang memiliki keahlian khusus dalam bidangnya yang biasanya dijalankan untuk memenuhi kebutuhan hidupnya secara permanen, contohnya profesi guru/dosen, dokter, pengacara, polisi dan lain-lain. Sedangkan profesional adalah kemampuan atau keahlian yang dimiliki seseorang yang dijalankannya dengan penuh tanggungjawab dan fokus pada bidangnya, artinya tidak dijalankan hanya sambilan. Seorang profesional akan melakukan dan menjalankan profesinya dengan baik dan ada rasa bangga atas pekerjaannya tersebut (Isnanto, 2009).

Profesionalisme dapat bermakna mencerminkan suatu prilaku seseorang yang bermaksud untuk menerapkan profesinya dalam rangka bertujuan untuk mendapatkan atau berharap menghasilkan pekerjaan yang berkualitas di bidangnya, sehingga dapat bermanfaat bagi banyak orang atau masyarakat umum. Adapun profesionalisme ini dapat digambarkan melalui ciri-ciri khusus yaitu: (1) selalu berusaha meningkatkan kemampuan diri sesuai profesi yang dimilikinya secara professional dan berkelanjutan; (2) selalu fokus pada pekerjaannya sesuai profesinya dan tidak dijalankan hanya sesewaktu saja; (3) selalu berusaha mencari hasil terbaik dari hasil pekerjaannya dan tidak mudah menyerah ketika

mendapatkan kesuliatan-kesulitan dalam pekerjaannya; (4) selalu dijalankan dengan tujuan dan maksud yang baik tanpa ada rasa tuntutan terhadap imbalan apa yang diterimanya; (5) selalu berpikir positif dan terus menjaga kualitas pekerjaannya agar mendapatkan hasil pekerjaan yang lebih efektif (Suwinardi, 2017)

Profesionalisme dapat dicapai seseorang dengan cara meningkatkan kemampuan dirinya melalui sertifikasi yang diselenggarakan oleh pihak-pihak secara profesional. Ini adalah cara untuk menstandarisasikan sebuah profesionalisme. Sehingga sertifikasi ini akan menjadi sebuah simbol dari kemampuan seseorang secara profesionalisme yang disesuaikan dengan profesi masing-masing. Ketika seseorang sudah bekerja secara profesionalisme, maka dia akan mendapatkan pengakuan dari hasil pekerjaannya baik dari lingkungan internal pekerjaannya, masyarakat umum, organisasi profesi ataupun dari pemerintah pada level nasional atau internasional. Hal ini tentu akan berdampak pada peningkatan karir serta dapat meningkatkan kesejahteraan hidup atau pendapatannya sesuai dengan ketentuan yang berlaku.

Organisasi profesi merupakan bagian dari peningkatan profesionalisme seseorang, dimana ketika seseorang melaksanakan pekerjaannya dibawah naungan organisasi profesi maka ritme pekerjaannyapun dari awal sampai akhir akan mengacu pada standar dan kode etik profesinya. Oleh karena itu, seorang yang sudah profesionalisme menjalankan profesinya akan terlihat dari karakteristiknya, seperti: menjaga kredibilitas dan kode etik profesinya, berpengetahuan dan memiliki keterampilan sesuai bidang profesinya, mampu bekerja mandiri secara profesional, mampu bekerja secar kelompok atau berkolaborasi, serta selalu berpikir untuk peningkatan kemampuan diri secara berkelanjutan (Mustika, 2017).

1.3 Profesionalisme Bidang Teknologi Informasi

Perkembangan teknologi informasi yang semakin cepat menuntut ketersediaan sumber daya manusia yang adaptif dan profesional di bidang teknologi informasi. Tren kebutuhan sumber daya manusia di bidang teknologi informasi dan komunikasi pada berbagai sektor industri baik regional, nasional ataupun internasional sangat membutuhkannya secara profesionalisme. Beberapa fungsi area dari profesionalisme di bidang teknologi informasi dijelaskan pada dokumen Daftar Unit Kompetensi Okupasi dalam Kerangka Kualifikasi Nasional Indonesia (KKNI) bidang Teknologi Informasi & Komunikasi (TIK) (Bachtiar et al., 2018).

Terdapat 16 (enam belas) fungsi area secara profesionalisme bidang teknologi informasi dan komunikasi yang dilengkapi dengan kompetensi dari masing-masing area serta disesuaikan dengan kebutuhan regional, nasional, dan internasional, yaitu:

1. Data Management System;

   Area ini berhubungan dengan kemampuan seseorang dalam mendesign dan mengembangkan serta menerapkan sistem database baik secara struktur ataupun tidak terstruktur terhadap model data rasional ataupun objek.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Direktur data warehouse
   - Manajer data warehouse
   - Senior sistem analis
   - Supervisor manajemen data
   - Petugas entry data

2. Programming and Software Development;

   Area ini berhubungan dengan kemampuan seseorang dalam membangun sistem aplikasi baik aplikasi stand alone atau jaringan, yang dapat dikembangkan menggunakan beberapa Bahasa pemrograman dengan pendekatan terstruktur ataupun berorientasi objek.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Direktur Aplikasi Bisnis
   - Direktur Pemrograman Sistem
   - Programmer Senior
   - Manajer Pengembangan Sistem/Aplikasi
   - Manajer Rekayasa Perangkat Lunak
   - Database Programmer
   - Business Analyst
   - Program Documenter
   - Petugas Pengembangan Perangkat Lunak.

3. Hardware and Digital Peripherals;

   Area ini berhubungan dengan kemampuan seseorang dalam mengelola perangkat keras komputer termasuk notebook, tablet dan piranti digital lainnya.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Manajer Operasi Komputer
   - Analis Keamanan Jaringan
   - Pengawas Pemeliharaan Komputer
   - Pengawas Instalasi Perangkat Keras

- Staf Pemeliharaan Komputer, Petugas Pemeliharaan Komputer.

4. Network and Infrastructure;

   Area ini berhubungan dengan kemampuan seseorang dalam mengelola infrastruktur sistem jaringan komputer yang bsa beroperasi baik di darat, laut, maupun udara.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Direktur Infrastruktur TI
   - Direktur Layanan Jaringan
   - Manajer Jaringan
   - Manajer Aplikasi Cloud
   - Manajer Komunikasi Data
   - Administrator Jaringan
   - Desainer Jaringan
   - Administrator Layanan Jaringan
   - Teknisi Jaringan
   - Teknisi Dukungan Operasional
   - Petugas Dukungan Teknis.

5. Operation and System Tools;

   Area ini berhubungan dengan kemampuan seseorang dalam mengelola sistem operasi komputer yang dapat dijalankan baik secara stand-alone maupun dalam bentuk jaringan.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Direktur Operasi dan Teknologi
   - Manajer Operasi Komputer
   - Manajer Outsourcing TI

- Manajer Dukungan Desktop/Komputer
- Ahli Pengembangan Sistem Operasi
- Spesialis Teknisi Komputer Senior
- Supervisor Teknisi Komputer
- Spesialis Help Desk
- Teknisi Perbaikan Komputer
- Print Operator.

6. Information System and Technology Development;

   Area ini berhubungan dengan kemampuan seseorang dalam mengembangkan atau membangun sistem informasi dengan mengikuti metodologi pendekatan baik secara terstruktur ataupun berorientasi objek. Sistem informasi yang dibangun dapat digunakan untuk mendukung bisnis proses dalam perusahaan, misalnya sistem informasi keuangan, sistem informasi kepegawaian, sistem informasi inventori dan sebagainya.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Direktur Sistem Informasi
   - Manajer Arsitektur Informasi
   - Analis Perencanaan TI
   - Analis Sistem Senior
   - Analis Sistem
   - Administrator Sistem dan Teknologi Informasi.

7. IT Governance and Management;

   Area ini berhubungan dengan kemampuan seseorang dalam mengelola sebuah tata kelola sistem dan teknologi informasi dalam perusahaan. Tata kelola sistem dan teknologi

informasi ini meliputi 3(tiga) aspek utama, yaitu: People, Technology, dan Process.

Kompetensi yang termasuk dalam area ini, antara lain:

- Direktur Teknologi Informasi
- Direktur Pengembangan TI
- Direktur Perencanaan TI
- Manajer Pelatihan dan Dokumentasi
- Analis Indikator Kinerja Utama
- Supervisor Perencanaan Kapasitas
- Administrator Tata Kelola dan Manajemen TI.

8. IT Project Management;

   Area ini berhubungan dengan kemampuan seseorang dalam mengelola sebuah proyek sistem/teknologi informasi, meliputi pengelolaan sumber daya manusia, pengelolaan biaya, pengelolaan waktu, termasuk menjamin kualitas proyek sistem informasi dan mengendalikan risiko yang kemungkinan terjadi pada proyek sistem/teknologi informasi.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Manajer Proyek TIK
   - Layanan Teknis Jaringan Manajer Proyek
   - Manajer Proyek Sistem
   - Manajer Proyek Pelatihan TI
   - Administrator Kontrak Pemeliharaan TI
   - Pengawas Proyek TI
   - Staf Manajemen Proyek TI

- Administrator Manajemen Proyek TI.

9. IT Enterprise Architecture;

   Area ini berhubungan dengan kemampuan seseorang dalam merancang dan merencanakan sebuah arsitektur sistem/teknologi informasi perusahaan berupa arsitektur data, sistem/proses, dan teknologi.

   Kompetensi yang termasuk dalam area ini, antara lain:

   - Manajer Arsitektur Perusahaan
   - Analis Bisnis Manajemen Sumber Daya Perusahaan
   - Pemeta Arsitektur Aplikasi
   - Koordinator Desain Perusahaan TI
   - Staf Arsitektur TI.

10. IT Security and Compliance;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola sistem keamanan data, informasi dan sistem baik secara praktis ataupun konseptual serta menunjukkan bagaimana kesiapan organisasi/perusahaan dalam mematuhi peraturan-peraturan terkait keamanan teknologi informasi.

    Kompetensi yang termasuk dalam area ini, antara lain:

    - Direktur Keamanan Informasi
    - Manajer Keamanan Jaringan
    - Manajer Audit Teknologi Informasi
    - Manajer Keamanan Cyber
    - Manajer Keamanan Data
    - Administrator Keamanan Data
    - Administrator Keamanan Informasi

- Penguji Jaminan Kualitas Perangkat Lunak
- Staf Manajemen Keamanan TI
- Petugas Manajemen Keamanan TI.

11. IT Services Management System;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola sistem layanan di bidang teknologi informasi. Layanan tersebut meliputi: layanan terhadap ketersediaan sumber daya teknologi informasi dan layanan pada sistem help desk.

    Kompetensi yang termasuk dalam area ini, antara lain:

    - Direktur Layanan Teknis
    - Manajer Pusat Layanan Pelanggan
    - Manajer Dukungan Situs Pelanggan
    - Manajer Dukungan Pengguna
    - Manajer Dukungan Teknis
    - Manajer Layanan Perencanaan dan Integrasi
    - Manajer Shift Operasi komputer
    - Analis Meja Bantuan
    - Spesialis Dukungan Sistem
    - Koordinator Pengadaan TI
    - Staf Operasi Layanan IT
    - Petugas Manajemen Layanan TI.

12. IT and Computing Facilities Management;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola fasilitas sarana dan prasarana teknologi informasi.

Termasuk didalamnya adalah pengelolaan data center, server.

Kompetensi yang termasuk dalam area ini, antara lain:

- Kepala Staf Fasilitas TI
- Manajer Pusat Data
- Manajer Pendukung Fasilitas dan Peralatan
- Manajer Instalasi dan Pemeliharaan Telekomunikasi
- Administrator Fasilitas Pusat Data
- Teknisi Layanan Fasilitas Komputer
- Teknisi Pusat Data Muda
- Staf Operasi Pusat Data
- Administrator Manajemen Fasilitas TI
- Petugas Manajemen Fasilitas TI.

13. IT Multimedia;

Area ini berhubungan dengan kemampuan seseorang dalam mengola dan mendesain aplikasi komputer dengan berbasis multimedia yang friendly.

Kompetensi yang termasuk dalam area ini, antara lain:

- Direktur Multimedia
- Ahli Desain Grafis
- Video Editor
- Desainer Multimedia Utama
- Teknisi Audio Visual
- Petugas Manajemen Multimedia.

14. IT Mobility and Internet of Things;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola sistem teknologi informasi yang dapat diakses melalui perangkat-perangkat kebutuhan sehari-hari, misalnya handpone, televisi, jam tangan pulpen, dan lain sebagainya yang juga secara teknologi ditanam dalam peralatan tersebut (embedded).

    Kompetensi yang termasuk dalam area ini, antara lain:

    - Direktur Seluler dan IOT
    - Komputasi Awan keamanan
    - Manajer Sistem Internet
    - Manajer Konten Web
    - Pengembang Cloud Computing
    - Analis Web
    - Administrator Web
    - Perancang Situs Web
    - Komputasi Seluler Senior
    - spesialis e-niaga
    - Operator IOT
    - Petugas Pemrograman Seluler.

15. Integration Application System;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola sistem informasi secara terintegrasi yang dapat digunakan dalam mendukung bisnis proses perusahaan yang meliputi technolgi, human, dan process.

    Kompetensi yang termasuk dalam area ini, antara lain:

    - Direktur Sistem Aplikasi

- Manajer Proyek ERP
- Analis Keamanan ERP
- Administrator Infrastruktur ERP
- Pelatih ERP
- Pengembang ERP
- Pimpin Tim ERP
- Pimpin Teknis ERP
- Staf Manajemen Aplikasi
- Petugas Manajemen Aplikasi.

16. IT Consultancy and Advisory;

    Area ini berhubungan dengan kemampuan seseorang dalam mengelola teknologi informasi yang terkait dengan pelayanan-pelayanan, seperti help desk, training, consultant yang dapat membantu dalam proses peningkatan kemampuan di bidang teknologi informasi.

    Kompetensi yang termasuk dalam area ini, antara lain:

    - Konsultan TI
    - Pengawas Konsultasi TI
    - Koordinator Konsultan IT
    - Staf Konsultan TI

1.4 Penutup

Seseorang yang memiliki profesi tertentu haruslah menjalankan profesinya secara professional. Agar profesionalitas seseorang tersebut terus meningkat dan terjaga secara berkelanjutan, maka harus diimbangi dengan peningkatan kemampuan secara terus menerus dan selalu fokus pada bidangnya. Sehingga dengan demikian profesionalisme

seseorang dapat tercapai dan dapat diakui oleh masayarakat apapun dan dimanapun lingkungannya berada. Banyak cara untuk meningkatkan profesionalisme di bidang tertentu, namun harus dilewati dengan cara yang sehat, tidak dengan cara yang curang. Program sertifikasi dan masuk dalam suatu asosiasi profesi dapat dijadikan pilihan untuk meningkatkan profesionalisme.

Profesionalisme di bidang teknologi informasi cepat sekali berkembang sejalan dengan cepatnya perkembangan teknologi informasi itu sendiri. Orang-orang yang terlibat secara langsung dengan bidang teknologi informasi tidak bisa menutup mata dengan pertumbuhan yang cepat ini, bahkan harus semakin peka dengan banyaknya terjadi perubahan-perubahan teknologi informasi. Penerapan metode pembelajaran mulai dari siswa sekolah dasar sampai perguruan tinggi selalu melakukan penyesuaian dengan situasi dan kondisi dalam pemanfaatan teknologi informasi ini, termasuk juga proses-proses yang ada dalam kegiatan industri atau perusahaan, semuanya dituntut agar secara cepat dapat beradaptasi dengan perkembangan teknologi informasi ini. Tentu ini semua membutuhkan orang-orang yang profesionalisme di bidang teknologi informasi sebagai pelaku utamanya dalam pengelolaannya.

Bab 2

Etika Komunikasi di Ruang Digital

2.1. Pendahuluan - Apa itu Komunikasi Digital?

Tak dapat dipungkiri, dalam masa Revolusi Industri 4.0 dan Digital Society 5.0 ini, perkembangan dunia digital telah menyasar ke berbagai sisi kehidupan. Saat ini, rasanya hampir tidak ada sisi ruang manusia yang tidak terpengaruh proses digitalisasi. Informasi yang disajikan di ruang digital, benar-benar "overload". Tantangan utama pada masyarakat modern ini adalah termasuk diantaranya penggunaan internet dan media digital yang tidak hanya memberikan sisi manfaat positif bagi penggunanya, namun juga sangat dimungkinkan menimbulkan sisi negatif dan berbagai macam persoalan, kalau "etika komunikasi digital" diabaikan. Kita dihadapkan pada suatu urgensi bagaimana harus memiliki wawasan etik, dalam memilah informasi dan berkomunikasi di ruang digital.

Gambar 2.1. Ilustrasi Overload Informasi

Komunikasi adalah suatu proses dimana seseorang atau kelompok orang, organisasi atau masyarakat menciptakan dan menggunakan informasi agar terhubung dengan lingkungan dan orang lain. Dan, komunikasi digital merupakan salah satu jenis komunikasi yang berkembang sangat pesat saat ini, dimana komunikasi digital memungkinkan seseorang atau sekelompok orang untuk melakukan komunikasi dengan menggunakan media-media digital, yang bisa lebih efektif dan efisien. Melalui media-media tersebut, komunikasi bisa dilakukan tanpa harus tatap muka secara langsung dengan lawan bicara.

2.2. Etika Digital *(Digital Ethics)* dan Etika Komunikasi Digital?

Etika diperlukan bukan hanya dalam hal komunikasi langsung, tetap dalam komunikasi digital pun perlu adanya etika. Etika digital adalah serangkaian aturan dan prosedur yang dibuat untuk mengurangi kerugian yang ditimbulkan oleh penggunaan teknologi digital. Penetapan etika digital bersifat mempertahankan kenyamanan yang diberikan melalui penggunaan teknologi digital. Jadi Etika Digital *(Digital Ethics)*

adalah Kemampuan individu dalam menyadari, mencontohkan, menyesuaikan diri, merasionalkan, mempertimbangkan dan mengembangkan "Tata Kelola Etika Digital" dalam kehidupan sehari-hari.

Ada beberapa yang perlu diperhatikan dalam Etika Digital *(Digital Ethics), diantaranya:*

1. Kesadaran (Melakukan sesuatu dengan sadar atau memiliki tujuan)

   Media digital yang cenderung instan seringkali membuat penggunanya melakukan sesuatu dengan - 'tanpa sadar' sepenuhnya. Tindakan 'otomatis' begitu memegang

   gawai/gadget contohnya. Begitu bangun tidur langsung buka gawai/gadget. Begitu mendapatkan pesan, langsung berbagi *(share)* tanpa saring (misalnya)

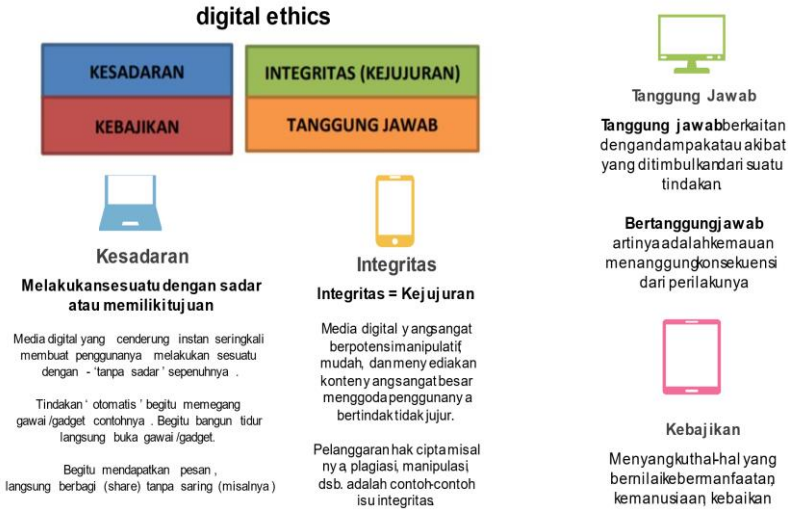
2. Integritas (Kejujuran).

   Media digital yang sangat berpotensi manipulatif, mudah, dan menyediakan konten yang sangat besar menggoda penggunanya bertindak tidak jujur. Pelanggaran hak cipta misalnya, plagiasi, manipulasi, dsb. adalah contoh-contoh isu integritas.

3. Kebajikan. Menyangkut hal-hal yang bernilai kebermanfaatan, kemanusiaan, kebaikan

4. Tanggungjawab

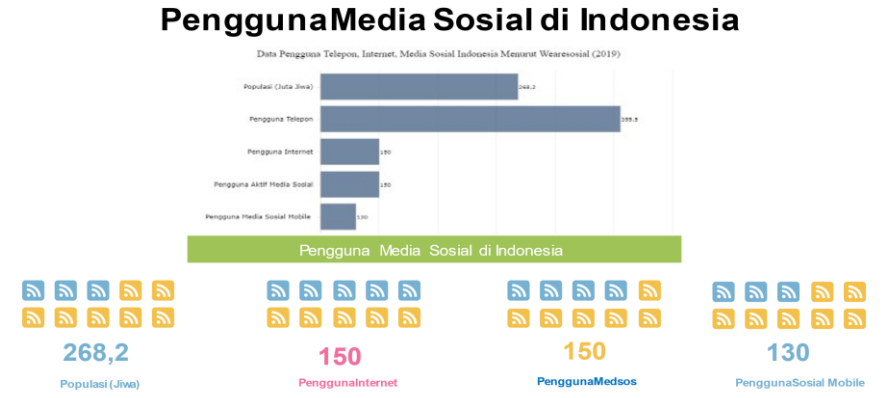
   Tanggung jawab berkaitan dengan dampak atau akibat yang ditimbulkan dari suatu tindakan. Bertanggungjawab artinya adalah kemauan menanggung konsekuensi dari perilakunya



Gambar 2.2 : Aspek-Aspek Etika Digital Digital Ethics

Sumber : Kominfo, Diolah Penulis

Dalam komunikasi digital, memungkinkan seseorang atau sekelompok orang untuk melakukan komunikasi dengan menggunakan media-media digital, seperti misalnya platform media sosial.



Sumber : Wearesosial. 2019 (diolah penulis)

2.3. Etika – Etiket

Sama seperti halnya sebuah komunitas, ruang forum digital juga mempunyai aturan dan tata tertib tertentu, dimana aturan ini menyangkut batasan dan cara yang terbaik dalam memanfaatkan fasilitas internet. Hal paling mendasar dari netiket adalah kita harus selalu menyadari bahwa kita berinteraksi dengan manusia nyata di jaringan yang lain, bukan sekedar dengan deretan karakter huruf di layar monitor, namun dengan karakter manusia sesungguhnya

1. Etika, Sistem nilai / norma moral yang menjadi pegangan bagi seseorang atau sekelompok orang dalam mengatur tingkah lakunya
2. Etiket, Tata cara individu berinteraksi dengan individu lain atau dalam masyarakat

Sumber : Komifo, 2021

Tanpa disadari, kita lebih banyak menggunakan internet dalam berkomunikasi seperti melalui media sosial *(whatsapp, facebook, instagram)* serta surat elektronik *(email)* dibanding berkomunikasi secara langsung, karena kita menganggapnya lebih efektif dan efisien.

Hampir 64 % penduduk di Indonesia sudah terkoneksi dengan jaringan internet. Kita berkomunikasi di dunia digital sama halnya seperti kita berkomunikasi di dunia nyata. Namun, Internet hadir bagai pisau bermata 2 yaitu dapat memberikan manfaat positif sekaligus memberikan dampak negatif sehingga diperlukan pengetahuan, kedewasaan serta etik.

Isu rendahnya etika komunikasi di ruang digital sangat berpeluang menciptakan ruang digital yang tidak "higienis" dan mungkin tidak akan menyenangkan, karena tanpa etika komunkasi dalam ruang digital, sangat dimungkinkan lahirnya konten-konten negatif. Etika termasuk hal yang kadang terlupakan dalam hal ini. Etika termasuk kedalam elemen-elemen komunikasi yang sangat penting. Tanpa adanya penggunaan etika pada saat kita berkomunkasi, ini akan menjadikan masalah tersendiri. Begitu pula dalam komunikasi digital, perselisihan dan konflik sangat dimungkinkan terjadi, karena seseorang melupakan etika didalamnya.

2.4. Penerapan Etika Komunikasi Digital

Etika komunikasi digital dibuat dengan tujuan untuk menjaga perasaan dan kenyamanan pengguna lain. Ada beberapa yang perlu diperhatikan dalam penerapan etika komunikasi diruang digital, diantaranya:

1. Hati-Hati dengan Tulisan atau Konten

   Tulisan merupakan bentuk perwakilan dari kita saat melakukan proses komunikasi digital. Dan bukan hanya sekedar tulisan saja, melainkan semua konten digital yang

kita bagikan dapat mewakili atau mencerminkan diri kita. Jangan menganggap bahwa tulisan atau konten yang kita buat atau bagikan di ruang digital, tidak akan dilihat atau dipehatikan oleh warganet, sehingga kita bebas membagikan tulisan atau konten kita.

2. Pentingnya mengendalikan Emosi

   Sebisa mungkin kita harus menghindari hal-hal yang akan membuat kita atau orang lain marah. Sebagai contoh dengan memberikan sebuah respon yang berapi-api, atau bahkan menyulut kebencian, adalah contoh yang kurang etis dalam berkomunikasi di ruang digital

3. Bersikap Sopan Santun

   Senantiasa bersikap sopan santun dalam komunikasi ruang digital, agar tidak menimbulkan masalah, bahkan memperkuat hubungan dengan orang lain menjadi lebih baik.

4. Bahasa dan Tulisan yang Jelas

   Bahasa dan Tulisan sangat krusial dalam komunikasi di ruang digital. Adalah suatu tindakan yang buruk, apabila kita tidak memperhatikan Bahasa dan Tulisan dalam proses komunikasi digital. Tulisan atau konten yang kita bagikan, akan mewakili siapa diri kita dan mempengaruhi penilaian orang lain pada kita

5. Menjaga privasi orang lain

   Apabila ingin membagikan informasi yang telah diberikan oleh orang lain, sebaiknya kita minta ijin terlebih dahulu. Membagikan informasi yang sensitif apalagi rahasia atau *privacy* orang lain adalah tindakan yang tidak etis.

6. Tidak memicu perselisihan atau perdebatan

   Tindakan yang kurang baik apabila kita bertujuan untuk mengadu domba atau memperburuk suasana dengan memberikan informasi yang tidak kita ketahui. Hal ini bisa menimbulkan perselisihan atau perdebatan di ruang digital.

2.5. Komunikasi - Interaksi, Partisipasi dan Kolaborasi di Ruang Digital

2.5.1. Komunikasi – Interaksi dalam Ruang Digital

Komunikasi adalah suatu proses dimana seseorang atau kelompok orang, organisasi atau masyarakat menciptakan dan menggunakan informasi agar terhubung dengan lingkungan dan orang lain. Dan Interaksi merupakan proses komunikasi dua arah antar pengguna terkait hal misalkan mendiskusikan ide, topik, dan isu dalam ruang digital. Dalam ruang digital, interaksi itu bersifat sosial. Hasil yang diharapkan adalah interaksi sehat dan menghangatkan seperti menjalin relasi atau pertemanan pada umumnya (Straubhaar et al., 2012). Bahkan dari proses interaksi ini dapat mendiskusikan ide, topik dan menghasilkan karya bersama. Contoh :

1. Menjalin pertemanan di Flatform Media Sosial : Pertemanan di Facebook, Twetter, saling "Follow" di Instragram, dll.
2. Menciptakan ide bersama membuat video atau konten yang dapat berpengaruh positif bagi orang lain.
3. Memunculkan ide *start-up* bersama melalui komunikasi secara digital, misalnya : mengadakan rapat secara daring, mengirim hasil diskusi melalui email, forum Whatsapp Group, atau menyimpan data melalui *Cloud Storage* / *Google Drive* / One Drive.

Namun, dengan kompleksitasnya informasi pada ruang digital, maka interaksi pun sangat dimungkinkan memunculkan

dampak negatif. Seperti memberikan komentar negatif terhadap berita, khususnya mengenai gosip selebriti di media sosial. Misal:

Pengikut beberapa akun Instagram populer memberikan kata-kata hujatan terkait selegram yang mengklarifikasi berita dirinya foto berdua yang dianggap selingkuh atau hal lain yang tidak pantas.

Komentar ini tentunya sebagai contoh bentuk interaksi yang "kurang pantas" di media sosial, karena lontaran-lontaran kata atau kalimat negatif dapat mempengaruhi persepsi orang lain dalam menyikapi berita tersebut. bahkan bisa memancing pembaca lain dan bahkan bagi yang tidak memberi komentar. memancing munculnya komentar negatif yang lain serta bisa menyakiti pihak-pihak yang terlibat.

Interaksi negatif lainnya adalah ujaran kebencian atau *hate speech. Hate Speech* adalah berbagai jenis komunikasi dalam bentuk lisan, tulisan maupun perilaku yang menggunakan bahasa merendahkan atau diskriminasi kepada orang atau kelompok tertentu berdasarkan agama, etnis, warga negara, RAS, warna kulit, keturunan, gender dan identitas lainnya.

Interaksi negatif ini dapat memiliki konsekuensi secara hukum, yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dengan ancaman pidana:

Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak 1 miliar.

Kemudian, selanjutnya kita bahas mengenai partisiapsi dan kolaborasi. Dimana berdasarkan kajian dan survey yang dilakukan oleh Japelidi (2019), kompetensi partisipasi dan kompetensi kolaborasi adalah kompetensi yang paling lemah diantara kompetensi lainnya seperti akses, seleksi, paham, distribusi, produksi, analisis, verifikasi dan evaluasi.

2.5.2. Partisipasi dalam Ruang Digital

Partispasi merupakan proses terlibat aktif dalam berbagai data dan informasi yang bermanfaat bagi diri sendiri dan orang lain. Proses partisipasi ini berakhir pada menciptakan konten kreatif dan positif untuk menggerakkan lingkungan sekitar. Kompetensi partisipasi dalam ruang digital dapat diartikan misalnya melibatkan diri dalam komunitas daring *(online)* sesuai kebutuhan, mengikuti kegiatan komunitas daring secara berkala dan rutin serta berkontribusi positif dalam komunitas daring secara berkelanjutan. Lebih lanjut, kompetensi partisipasi ini mengajak peserta untuk berperan aktif dalam berbagi informasi yang baik dan etis melalui ruang media sosial maupun kegiatan komunikasi daring lainnya (Kurnia, 2020). Sementara, terdapat pula partisipasi dari warganet yang bisa memicu polemik, seperti pernyataan yang menuai kontroversi dan membuat kegaduhan dimasyarakat. Kita dapat melihat fenomena ini dari berbagai informasi media masa maupun media elektronik.

2.5.3. Kolaborasi dalam Ruang Digital

Kolaborasi merupakan proses Kerjasama antar pengguna untuk memecahkan masalah bersama Monggilo, 2020). Kompetensi ini mengajak peserta untuk berinisiatif dan mendistribusikan informasi yang jujur, akurat dan etis dengan bekerjasama dengan kelompok masyarakat dan pemangku kepentingan lainnya (Kurnia, 2020). Lebih lanjut, kompetensi kolaborasi meliputi membuat dan mengelola forum komunitas

daring, serta mengelola topik dalam forum daring tersebut untuk mencapai suatu tujuan tertentu.

Berdasarkan catatan dari Kementerian Komunikasi dan Informatika (Kominfo), selama krisis pandemi, kurun waktu dari Maret 2020 sampai dengan Januari 2021, terdapat 1.387 hoaks beredar di dunia internet Indonesia. Dari fenomena ini, dibutuhkan kemampuan untuk berkolaborasi dengan berbagai komunitas dan berbagai elemen masyarakat untuk membantu mengurangi kasus tersebut. Kolaborasi positif, dapat menjadi sistem pendukung bagi kita dalam menghadapi berbagai serangan informasi di dunia internet. Sebaliknya, kolaborasi negatif dapat menjebloskan kita pada pusaran perspektif yang salah bahkan ranah hukum. Sebagai pengguna internet kita diharapkan memahami aturan hukum yang mengatur gerak-gerik kita di ruang digital. Aturan hukum tersebut tertuang dalam UU ITE.

2.6 Penerapan Etika dalam ber-Interaksi yang melahirkan Partisipasi dan Kolabarasi Positif di Ruang Digital

Pada dasarnya, konten pada media digital adalah produksi budaya, karena terdapat interaksi, partisipasi dan kolaborasi antar pengguna di dalamnya. Komunikasi - Interaksi yang positif akan melahirkan partisipasi dan kolaborasi yang positif, dan pada akhirnya, karya yang dihasilkan dapat dikatakan sebagai karya seni bersama. Contoh penerapan etika dalam berinteraksi, partisipasi dan kolaborasi, menurut Kominfo, Japelidi, Siberkreasi, 2021, terdapat beberapa pertanyaan yang menjadi pertimbangan, seperti:

1. Haruskah kita meminta ijin kepada pihak-pihak yang akan dicatut namanya, gambar atau videonya ? Mengapa ?
2. Bagaimana perasaan kita jika seseorang yang dicatut nama, gambar atau videonya kemudian menimbulkan masalah, karena membuat pihak tersebut dirugikan ?

3. Bagaimana jika kita melihat hasil karya kita sudah baik, namun orang lain melihatnya tidak layak ? Apakah yang membuatnya berbeda? Mengapa ?

Pertanyaan-pertanyaan tersebut adalah pertimbangan dasar kita dalam mengasah kemampuan berfikir kritis terkait hal etis yang patut dipertimbangkan sebelum menciptakan karya dalam ruang digital. Dan sebaiknya, pertanyaan ini dipakai sebagai refleksi awal sebelum berkarya.

2.7. Konsep Think dalam Komunikasi Digital

Kepanjangan akronim T.H.I.N.K. dalam etika digital adalah *True*, *Hurtful*, *Ilegal*, *Neccesary*, *Kind*. Pengertian konsep THINK adalah sebuah metode tata krama yang dimana akan berguna untuk menjadi kewargaan digital yang dimana akan dianggap menjadi baik dan juga benar sehingga kita akan memahami akan pentingnya kewargaan digital. Pada tata krama komunikasi sinkron ini sendiri akan memiliki sebuah ketersambungan dengan menggunakan sebuah konsep THINK pada saat kita sebelum memulai kegiatan komunikasi didalam sebuah dunia digital, baik itu dengan menggunakan email, facebook, Instagram, twitter, hingga blog dan forum.

Dengan menggunakan konsep T.H.I.N.K, kita mampu mempertahankan kepercayaan dan reputasi yang dimiliki oleh kita, bahkan kita mampu bertanggung jawab atas berita yang kita *share* atau bagikan.

1. True = Apakah ini benar? Apakah ini hanya issue yang memiliki ketidak jelasan akan sebuah sumber.
2. Hurtful = Apakah ini menyakitkan orang lain apabila saya menyebarkannya
3. Illegal = Apakah yang saya *post* ini merupakan tindakan yang illegal?

4. Necessary = Apakah yang saya post ini merupakan hal yang penting? Atau post yang dimana tidak penting dan akan mengganggu orang lain di internet?
5. Kind = Apakah ini menyebarkan kebaikan? Apakah kata-kata yang saya gunakan akan menyinggung orang lain ?

Bijaksanalah dalam menggunakan media sosial, selain Saring dulu baru Sharing, juga harus THINK memperhatikan aspek True, Hurtful, Illegal, Necessary dan aspek Kind.

Bab 3

Cybercrime dan Solusinya

3.1. Pengantar

Pesatnya perkembangan teknologi di era ini telah menyebabkan munculnya fenomena yang membuat interaksi publik antar individu dan kelompok menjadi lebih mudah. Ketika komputer pertama kali ditemukan, mereka hanyalah mesin besar dengan fungsionalitas terbatas. Dalam waktu yang relatif singkat, saat ini komputer telah mengalami evolusi yang signifikan baik dalam fungsi maupun ukuran. Frekuensi pemakaian komputer cenderung meningkat dikarenakan semakin banyak perusahaan maupun individu yang menggunakan komputer untuk mendukung kegiatan sehari-hari. Hal ini semakin diperkuat dengan adanya kemajuan yang sangat pesat pada seperempat abad kemudian setelah ditemukannya internet pada tahun 1969 lalu (Arifah, 2011).

Kehadiran internet menciptakan perubahan di berbagai aspek kehidupan manusia. Aktivitas komunikasi yang semula memiliki berbagai keterbatasan seperti hanya dapat dilakukan secara face to face, dapat berubah menjadi media komunikasi virtual yang menghubungkan setiap individu maupun kelompok kapanpun dan dimanapun tanpa adanya batas. Internet merupakan sebuah jaringan dari jutaan komputer yang saling terhubung satu sama lain dan menjembatani komunikasi berbagai orang dibelahan dunia hanya dengan menggunakan alat pendukung seperti keyboard dan mouse. Peningkatan

pengguna internet menciptakan sebuah grafik yang sangat tinggi mencapai 220 juta orang sampai saat ini (Fuady, 2005).

Teknologi tidak selalu memberikan dampak positif, ada berbagai aspek yang dapat menciptakan adanya dampak negatif dikarenakan penggunaan internet yang salah, salah satunya adalah cybercrime. Hal ini dikarenakan adanya ruang yang diberikan pengguna internet atas ketidakwaspadaan mereka. Penjahat cybercrime melakukan aksinya dengan menciptakan suatu link palsu yang berisi program jahat kemudian disebarkan dengan memanfaatkan jaringan pertemanan yang ada di internet. Hal ini didasari atas kecenderungan pengguna internet yang bisa percaya begitu saja atas link atau suatu konten yang mereka terima tanpa melakukan pengecekan terlebih dahulu. Hukum menjadi salah satu alat tumpuan untuk menjamin, mengamankan, dan melindungi pengguna internet demi memberikan kenyamanan dalam kelancaraan menggunakan internet. Hal ini sekaligus menindaklanjuti kejahatan cybercrime yang terjadi. Cybercrime dikategorikan kedalam borderless crime (kejahatan tanpa batas ruang dan waktu) dimana kejahatan tersebut dapat dilakukan kapan saja tanpa adanya batasan ruang sehingga diperlukan langkah khusus yang saling terkonsolidasi dari berbagai pihak (Arifah, 2011). Berbagai informasi dapat dengan mudah dan cepat didapatkan karena kemajuan teknologi. Sarana komunikasi yang cepat dan handal menandakan adanya globalisasi. Dalam hal ini mencakup dunia bisnis khususnya dalam dunia perdagangan. Pemanfaatan teknologi memperlihatkan dunia perdagangan yang mengalami perubahan signifikan karena aktivitas bisnis cenderung meningkat diberbagai negara (Handayani, 2013).

Cybercrime merupakan kejahatan yang dilakukan dengan berbagai macam tujuan. Seperti seseorang yang ingin menguji kemampuannya dalam dunia hacking, hingga kejahatan serius yang dapat merugikan pengguna lain baik secara finansial

ataupun mental. Kejahatan siber yang marak terjadi di Indonesia salah satunya adalah social engineering attack atau rekayasa sosial. Jenis kejahatan ini menggunakan teknik manipulasi yang memanfaatkan kesalahan user untuk mendapatkan akses masuk kedalam perangkat atau account miliknya sehingga pelaku bisa mendapatkan informasi pribadi dan data berharga milik user tersebut.

Kemajuan teknologi yang sangat pesat dari perkembangan internet, tentunya menimbulkan juga sisi negatif yang dimanfaatkan oleh oknum yang tidak bertanggung jawab untuk melakukan tindak pidana. Tindak pidana yang dapat dilakukan melalui internet seperti penyerangan kepada privacy seseorang, perjudian online, pornografi anak, perdagangan barang ilegal secara online, serta munculnya situs-situs yang dapat merugikan masyarakat (Putra, 2019).

3.2. Pengertian Cybercrime

Cybercrime merupakan bentuk kejahatan melawan hukum di dunia maya yang memanfaatkan kecanggihan komputer dan telekomunikasi melalui media internet. Kepolisian Inggris menuturkan, cybercrime adalah kejahatan internet dengan memanfaatkan teknologi digital yaitu komputer untuk kepentingan kriminal (Handayani, 2013). Perkembangan teknologi informasi yang semakin maju tentunya harus diiringi dengan pembentukan hukum teknologi informasi agar dapat menegakan hukum terkait kejahatan siber yang terjadi di Indonesia. Hal ini harus dijalankan oleh aparat penegak hukum untuk mencapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan masyarakat, golongan, kelompok, ras, suku dan agama di dalam suatu negara baik dalam hubungan di kawasan regional maupun internasional sehingga bisa menciptakan perlindungan yang baik terhadap kesejahteraan masyarakat Indonesia (Putra, 2019).

Dalam kejahatan konvensional¸ cybercrime memiliki beberapa karakterisik yaitu Blue collar crime dan White collar crime (Wahyono, 2009).

1. Kejahatan kerah biru (blue collar crime)

   Blue collar crime merupakan tindak kejahatan dimana pelaku berasal dari kelas bawah dengan ciri tidak terdidik dan berpenghasilan rendah dalam suatu lingkup masyarakat. Perampokan, pencurian, pembunuhan dan lain sebagainya merupakan tindak kejahatan kriminal yang biasa dilakukan secara konvensional. Para pelaku kejahatan ini ditandai dengan steorotip tertentu seperti masyarakat yang kurang terdidik (Galih, 2015).

   Blue collar crime merupakan salah satu jenis tindak kejahatan yang biasanya dilakukan atas dasar tuntutan ekonomi dari pelaku. Contoh kejahatan yang dilakukan seperti mencuri hewan peliharaan milik orang lain karena membutuhkan uang untuk memenuhi kebutahan hidup sehari-hari. Kebanyakan tindak kejahatan ini dilakukan tanpa adanya strategi tertentu sehingga pelaku dapat melakukan aksinya secara spontan. Blue collar crime mempunyai ciri khas yang melekat sehingga dapat dikenali dengan mudah. Ciri-ciri yang pertama yaitu tindak kejahatan ini biasanya dilakukan di ruang lingkup yang skalanya kecil, misalnya di area sekitar tempat tinggal pelaku. Selanjutnya, tindak kejahatan ini dilakukan demi keuntungan pribadi atau kelompok yang terlibat di dalamnya. Misalnya kejahatan yang dilakukan oleh sekelompok preman yang melakukan pemalakan atau geng motor suka mencari keributan (Merdeka, 2022). Setiap tindak kejahatan yang bisa merugikan dan membahayakan orang lain, tentunya pelaku tindak kejahatan dapat dijatuhi hukuman sesuai dengan undang-undang yang berlaku pada setiap negara (Hasjim & Erniwati, 2020).

2. Kejahatan kerah putih (white collar crime)

   White collar crime merupakan tindak kejahatan yang dilakukan kelas atas dengan karakteristik berpenghasilan tinggi, berpendidikan, memiliki kekuasaan diberbagai jenis lembaga dengan posisi yang dapat mempengaruhi kebijakan maupun keputusan dalam suatu bidang tertentu. Korupsi, kejahatan birokrat, kejahatan malpraktek, dan lain sebagainya merupakan tindakan kejahatan yang biasa mereka lakukan. Korupsi dikategorikan kejahatan yang paling besar. Korupsi adalah penyalahgunaan uang negara dengan cara melawan hukum dengan tujuan tertentu yang dilakukan oleh seseorang yang memiliki posisi tinggi dengan memanfaatkan kekuasaannya secara sewenang-wenang (Kamasa, 2014). White collar crime biasanya dilakukan oleh seseorang profesional dalam bidang bisnis yang mengacu pada kejahatan terkait masalah finansial. Kasus-kasus jenis kejahatan ini sulit untuk dilacak karena biasanya dilakukan oleh pejabat yang memiliki kekuasaan tinggi dalam penegakan hukum dan berperan penting dalam pembuatan keputusan.

   Dalam memahami jenis kejahatan ini, diperlukan pengetahuan terkait tipologi pelaku kejahatan tersebut. Pengertian Tipologi sendiri merupakan ilmu watak tentang bagian-bagian dalam diri manusia menurut corak wataknya masing-masing. Hal tersebut harus diketahui karena definisi terkait suatu tindak kejahatan dapat digolongkan ke dalam white collar crime atau tidak dapat dilihat berdasarkan tipologi pelakunya. Tipologi pertama dilihat dari status social pelaku, apakah berasal dari status "terhormat" atau tidak. Status terhormat dalam hal ini merupakan suatu jabatan yang dimiliki pelaku dalam instansi, baik negera maupun swasta, yang ia miliki. Selanjutnya, tipologi yang dapat dilihat adalah tindak kejahatan yang dilakukan memerlukan keahlian di

bidang komputerisasi atau tidak. Jika, iya, maka kejahatan yang dilakukan dapat digolongkan sebagai white collar crime dalam lingkup cybercrime. Terakhir, tindak kejahatan yang dilakukan pelaku bertujuan untuk menguntungkan individu atau kelompok. Melalui ini, dapat dilihat pola seleksi dan penggolongan dari kasus white collar crime yang terjadi. (Santi, 2017). White collar crime ditujukan kepada para aparat dan para petinggi negara, sedangkan blue collar crime ditujukkan kepada masyarakat kelas bawah yang memiliki kualitas serta kuantitas yang lebih rendah dari pada kejahatan white collar crime. Kejahatan white collar crime dibatasi dengan hukum di Indonesia mengenai pemberantasan kejahatan pencucian uang yang tertuang dalam UU NO.15 tahun 2003 yang diubah dengan UU No. 8 Tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang dengan harapan pelaku tidak melakukan kejahatan tersebut (Singal, 2021). Pada dasarnya kejahatan kerah putih ini dilakukan oleh orang-orang tertentu yang memiliki jabatan, kedudukan, dan kekuasaan yang penting dalam kehidupan bermasyarakat. Akan tetapi, hal tersebut tidak dijalankan sesuai dengan tanggung jawabnya masing-masing. Seharusnya para pelaku tindak kejahatan tersebut bisa memberikan tanggung jawabnya atas kepercayaan yang telah diberikan masyarakat kepada dirinya untuk melaksanakan tugasnya dengan baik dan benar (Buamona, 2019). Perbedaan dari kejahatan kerah biru dan kerah putih yaitu terdapat pada status sosial dari masing-masing pelaku. Jenis kejahatan kerah putih biasanya dilakukan oleh kaum elit yang memiliki status sosial tinggi di mata masyarakat, sedangkan jenis kejahatan kerah biru biasanya dilakukan oleh rakyat biasa yang memiliki golongan rendah dalam kehidupan bermasyarakat (Puspita, 2022).

3.3. Karakteristik Cybercrime

Cybercrime memiliki karakteristik unik yaitu: (Wahyono, 2009).

1. Ruang lingkup kejahatan yang bersifat global yang dilakukan secara transnasional, lintas batas antarnegara dan anonymous (tanpa identitas)
2. Kejahatan yang bersifat tanpa kekerasan (non violence)
3. Pelaku kejahatan berasal dari berbagai masyarakat secara umum, tidak terbatas usia dan memiliki ciri khas tertentu. Dengan kebanyakan dilakukan oleh remaja yang cerdas dan baik-baik.
4. Kejahatan dilakukan dengan penggunaan teknologi informasi.
5. Terjadinya kerugian material dan non-material.

Cybercrime memiliki karakter khusus jika dibandingkan dengan kejahatan konvensional yaitu: (Fuady, 2005)

1. Tindak kejahatan yang dilakukan secara ilegal, tanpa hak dan tidak etis yang terjadi di dunia maya (cyberspace), sehingga hal tersebut tidak dapat dipastikan yuridiksi terkait hukum negara mana yang berlaku terhadap pelaku tindak kejahatan.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materik maupun immateril (waktu, uang, nilai, jasa, barang, privasi, martabat) yang cenderung lebih besar dari kejahatan konvensional.
4. Pelakunya merupakan orang yang menguasai penggunaan internet dan bahasa komputer atau pemrograman.
5. Tindakan kejahatan tersebut biasanya dilakukan secara transnasional/melintasi batas negara.

Dari beberapa karakteristik diatas agar mempermudah penangannya maka cybercrime dapat diklasifikasikan menjadi Cyberpiracy, Cybertrespass, dan Cybervandals: (Ketaren, 2016)

1. Cyberpiracy

   Pemanfaatan teknologi komputer dalam mencetak ulang sebuah informasi.

2. Cybertrespass

   Pemanfaatan teknologi komputer dalam meningkatkan akses pada sistem komputer.

3. Cybervandalism

   Pemanfaatan teknologi komputer untuk membuat sebuah program yang dapat mengganggu proses transmisi elektronik menghancurkan data didalam komputer.

3.4. Jenis Cybercrime

Tergantung pada jenis aktivitas yang dilakukan, cybercrime dapat diklasifikasikan ke dalam beberapa kategori yaitu berdasarkan jenis aktivitasnya, motif kegiatannya, dan berdasarkan sasaran kejahatannya (Wahyono, 2009).

1. Berdasarkan jenis aktivitasnya:

   a. Unauthorized Access,

      Kejahatan yang disebabkan ketika seseorang yang tidak memiliki hak akses memasuki suatu sistem jaringan komputer secara tidak sah. Sebagai contoh Probing dan porting. Jenis kejahatan ini biasanya dilakukan dengan mensabotase atau menyusup masuk pada suatu sistem tanpa izin user. Hal tersebut dilakukan dengan tujuan untuk melakukan pencurian data dan informasi penting milik korban (Syifaudin, 2021). Unauthorized Access adalah perbuatan yang melanggar hukum dengan

memasuki ruang privasi milik seseorang seperti email untuk kepentingan tertentu (Surniandari, 2016) sehingga diperlukan sebuah tindakan khusus untuk mencegah kejahatan tersebut dengan mengamankan sistem jaringan komputer yang dimiliki seperti penggunaan hosting yang aman, mengupdate sistem secara continue, dan menerapkan fitur keamanan otentikasi dua fakor.

Berikut merupakan hal-hal yang menyebabkan maraknya kejahatan siber (unauthorized access) diantaranya yaitu:

1. Kebebasan user dalam menggunakan akses internet yang tidak ada batasnya
2. Kelalaian user dalam menggunakan komputer
3. Mudah dalam melakukan aksi kejahatan dan resiko yang kecil untuk dilacak
4. Pelaku umumnya merupakan orang yang ahli dalam dunia hacking dan memiliki rasa ingin tahu yang besar

b. Illegal Contents

Jenis kejahatan ini berkaitan dengan kejahatan tentang memasukan data dan informasi mengenai sesuatu hal yang tidak benar dan hal tersebut dianggap melanggar hukum (Syifaudin, 2021). Memasukkan dan menyebarkan data atau informasi yang tidak benar ataupun tidak etis di Internet tentang berbagai topik persoalan yang dapat memberikan kerugian diberbagai pihak karena dapat menyinggung ketertiban dan moral umum. Illegal Contents sama dengan penyuapan informasi. Menyebarkan video yang mengarah pada pornografi merupakan bentuk adanya penyuapan informasi. Tindakan yang harus dilakukan adalah lebih cerdas dalam memilih gambar atau foto pribadi yang

akan dipublikasikan agar tidak memancing si pelaku dalam melakukan kejahatan tersebut.

c. Penyebaran Virus Secara Sengaja

Kejahatan yang memanfaatkan media komunikasi seperti email dengan menyebarkan suatu virus yang sudah dimodifikasi sehingga pengguna yang terkena virus tidak menyadari hal tersebut. Penyebaran virus umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ketempat lain melalui emailnya. Contoh kasus: Virus Mellisa, I Love You, dan Sircam (Anggara, 2019). Kegiatan ini dilakukan dengan menyisipkan suatu virus yang bersifat merusak kedalam suatu file dan dapat terinstal secara otomatis pada device pengguna (Surniandari, 2016) untuk meminimalisir kejadian tersebut, dapat dilakukan dengan mengganti password secara berkala.

d. Data Forgery

Kejahatan yang dilakukan dengan memalsukan data dokumen penting di internet yang dimiliki oleh sebuah lembaga yang mempunyai database berbasis web. Kejahatan ini difokuskan pada dokumen-dokumen e-commerce seakan terdapat kesalahan yang pada akhirnya menguntungkan si pelaku (Abidin, 2015). Pemahaman yang cukup dalam mengenali modus atau trik kejahatan pelaku, memahami ciri-ciri pemalsuan dokumen dan karakter individu pelaku baik melalui tulisan ataupun tanda tangan dapat menjadi upaya untuk menghindari adanya pemalsuan dokumen (Suharto & Kurniawan, 2020).

e. Cyber Espionage, Sabotage and Extortion

Kejahatan ini dilakukan dengan tujuan untuk membuat gangguan, perusakan dan penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Cara yang dilakukan untuk melancarkan perbuatannya yaitu dengan menyusupkan logic bomb atau virus komputer kepada sistem sasaran sehingga sistem tersebut terjadi error dan tidak bisa berjalan sebagaimana mestinya (Bapenda Jabar, 2017). Sasaran dari kejahatan ini biasanya ditujukan terhadap saingan bisnis yang data-data pentingnya tersimpan dalam suatu sistem yang computerized (Yulianty, 2021). Kejahatan yang menggunakan internet untuk memata-matai pihak lain dengan cara membobol sistem jaringan komputer yang menjadi sasaran. Sabotage and Extortion adalah jenis kejahatan yang dilakukan melalui perusakan, atau penghancuran data, program komputer, atau sistem jaringan komputer yang terhubung ke Internet. Cyber espionage juga bisa diartikan dengan kejahatan yang menggunakan jaringan internet dengan cara meretas sistem jaringan komputer pihak yang dituju. Cara agar terhindar dari cyber espionage adalah dengan cara mengenali teknik serangan spionase siber, memantau sistem, dan mengubah password secara berkala.

f. Cyberstalking

Kejahatan yang dilakukan oleh seseorang untuk melecehkan orang lain dengan cara menguntit ataupun mengancam pihak yang dituju dengan memanfaatkan media komputer seperti melalui email. Cyberstalking merupakan tindakan kriminal yang ditujukan kepada seseorang dengan cara melecehkan, mengintimidasi, maupun meneror korbannya dengan cara memantau

aktivitasnya melalui internet. Selain itu, kejahatan ini mencakup aksi pelaku dalam membuat tuduhan palsu, pengancaman, menghina, serta mengganggu korban melalui sosial media, email, dan platform pribadi lainnya (Safira, 2020).

Hal yang biasa dilakukan oleh pelaku cyberstalking umumnya yaitu melakukan tindakan stalking dengan cara berkomentar pada status, foto atau unggahan dari korban dalam akun media sosialnya, bahkan pelaku mungkin saja mengirimi spam chat kepada korban sehingga bisa mengganggu kenyamanannya. Pelaku juga biasanya meneror rekan/teman dari korban dengan cara mengirim pesan kepada temannya untuk bisa mendapatkan informasi secara mendalam tentang korbannya (Ardiyanti et al., 2018).

Menggunakan proteksi akun pribadi serta menghindari publikasi pribadi di internet merupakan salah satu cara terbaik menangani masalah tersebut (Fazio & Sgarbi, 2012).

g. Carding

Carding adalah kejahatan yang dilakukan dengan memanfaatkan kartu kredit milik orang lain untuk melakukan transaksi dan berbelanja online di internet. Kejahatan ini menyebabkan kerugian bagi orang lain baik secara fisik maupun immaterial (Yulianty, 2021). Carder adalah istilah yang digunakan untuk menyebut pelaku penyalahgunaan informasi kartu kredit milik orang lain. Para carder (pelaku carding) biasanya menjual kembali barang yang telah dibeli secara online menggunakan kartu kredit milik korban tersebut dengan harga murah untuk mendapatkan uang (Legalku, n.d.).

Merahasiakan data pribadi kartu kredit, menggunakan internet pribadi serta memilih situs belanja yang terpercaya merupakan langkah yang dapat dilakukan untuk menghindari kejahatan tersebut.

h. Hacking dan Cracking

Hacking adalah kejahatan meretas program komputer milik orang lain tanpa melakukan pencurian atau perusakan data, sedangkan Cracking adalah kejahatan yang dilakukan dengan merusak suatu sistem komputer melalui pemanfaatan media teknologi komputer dengan tujuan melakukan pencurian dll (Agus & Riskawati, 2016). Pembajakan yang sering terjadi pada hacking dan cracking adalah pembajakan perangkat lunak (Abidin, 2015). Seorang hacker (pelaku hacking) sebenarnya memberikan manfaat bagi orang lain karena seorang hacker hanya melakukan tes pada keamanan sistem milik orang lain dan tidak akan merusaknya, sedangkan cracker (pelaku cracking) di internet memiliki lingkungan yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran yang dimana hal tersebut dapat merugikan pemiliknya (Anggara, 2019). Cara yang dapat dilakukan untuk mengatasinya yaitu memiliki password yang unik pada setiap website, menggunakan VPN, menghindari jaringan wifi public dan tidak menggunakan perangkat lunak bajakan.

i. Cybersquatting and Typosquating

Cybersquating merupakan jenis kejahatan yang dilakukan dengan mendaftarkan nama domain suatu perusahaan (penyerobotan domain name) sehingga domain tersebut tidak dapat digunakan oleh perusahaan (Singh, 2018), dengan mendaftarkan nama domain milik

perusahaan orang lain selanjutnya pelaku menjual domain tersebut dengan harga yang lebih tinggi ke perusahaan lain demi keuntungan pribadi. Typosquating merupakan kejahatan dengan membuat nama domain plesetan yang sudah dimodifikasi agar menyerupai nama domain pesaing perusahaan yang ditunjukkan. Menjual domain-domain palsu yang sudah dimodifikasi sehingga mirip dengan domain orang lain merupakan arti lain dari Cybersquatting and Typosquating (Siahaan, 2018). Cara terbaik yang dapat dilakukan untuk menghindari kejahatan ini adalah dengan cara jangan membuka email yang mencurigakan, menghilangkan kerentanan di OS dan aplikasi, menginstal perangkat lunak keamanan internet serta selalu update perangkat lunak.

j. Hijacking

Kejahatan yang dilakukan dengan sengaja untuk meraih keuntungan dengan cara melanggar hak cipta dari karya orang lain tanpa izin seperti pembajakan perangkat lunak. Pengertian lainnya dari hijacking yaitu suatu kegiatan yang berusaha untuk memasuki (menyelinap) kedalam sistem melalui sistem operasional lainnya yang dijalankan oleh seseorang (pelaku). Sistem ini dapat berupa server, jaringan/networking, LAN, atau MAN. situsweb, software, atau bahkan kombinasi dari beberapa sistem tersebut. Perbedaan hijacker dengan cracker adalah hijacker menggunakan bantuan software dalam melalukan pembajakan. Tujuannya adalah sama dengan cracker namun pada hijacker mengambil data dan informasi pendukung lain, tidak jarang sistem yang dituju juga diambil alih atau bahkan dirusak (Maulana et al., 2017). Metode untuk menghindari pembajakan tersebut adalah dengan menerapkan metode Cookie dan metode field tersembunyi.

k. Cyberterorism

Cyberterorism adalah kejahatan dengan cara mengancam berbagai pihak baik pemerintah maupun warga sipil. Seperti meretas web milik pemerintah dan militer. Cyberterorism adalah tindak kejahatan yang dilakukan oleh kelompok maupun perorang dengan cara mengancam kestabilan dan keamanan pemerintahan (Surniandari, 2016). Cara yang tepat untuk menghindari kejahatan ini adalah dengan mengamankan situs web pemerintah menggunakan sistem keamanan berlapis dan menggunakan pengacak IP agar tidak mudah diretas.

2. Berdasarkan Motif Kegiatannya

a. Cybercrime sebagai tindakan murni kriminal

Kejahatan yang dimana orang yang melakukan kejahatan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer (Bapenda Jabar, 2017). Contoh dari cybercrime sebagai tindakan murni kriminal adalah kejahatan carding, karena hal tersebut merugikan orang lain dengan membobol/mencuri kartu kredit milik korban.

b. Cybercrime sebagai kejahatan “abu-abu”

Kejahatan "abu-abu" adalah suatu tindakan yang sangat sulit untuk diindentifikasi apakah tergolong kejahatan atau bukan dikarenakan motifnya bisa jadi non-kriminal karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut (Illiyyin, n.d.). Contoh dari tindakan ini adalah probing atau pemindaian port. Probing atau portscanning 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 (Ketaren, 2016). Pengertian lainnya dari Probing adalah strategi yang dilakukan dengan penyelidikan dan pemeriksaan yang bertujuan untuk mendapatkan sebuah informasi.

3. Berdasarkan sasaran Kejahatannya

   a. Cybercrime yang menyerang individu (Against Person)

      Kejahatan yang dilakukan dengan memastikan seseorang yang memiliki ciri atau kriteria tertentu yang menjadi sasaran penyerangan. Cybercrime yang menyerang individu biasanya memiliki motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi (Yulianty, 2021). Contoh: pornografi, Cyberstalking, Cyber-Tresspass yang dimana sasaran dari kejahatan ini adalah perorangan atau individu yang sifatnya tertentu.

   b. Cybercrime Menyerang Hak Milik (Against Property)

      Kejahatan yang dilakukan dengan menyerang hak milik/hasil karya orang lain dengan contoh mengakses kepemilikan komputer atau kepemilikan informasi yang tidak sah, carding, cybersquatting, hijacking, data forgery dll (Mathilda, 2012). Biasanya kejahatan ini dilakukan dengan motif memasarkan, menggandakan, dan mengubahnya dengan tujuan untuk kepentingan pribadi sehingga mendapatkan keuntungan dari segi materi/nonmateri

c. Cybercrime Menyerang Pemerintah (Against Government)

Kejahatan ini termasuk kedalam cyberterorism karena merupakan tindakan yang mengancam pemerintah seperti membobol situs resmi milik pemerintah ataupun militer. Beberapa hal yang dapat memicu terjadinya cybercrime terhadap sistem pemerintahan adalah terjadinya cyberwar antar hacker dari negara lain sehingga menyebabkan saling serang terhadap sistem pemerintahan, hal tersebut dilakukan untuk menunjukan skill/kemampuan masing-masing hacker dalam melakukan cracking. Kejahatan yang dilakukan pada sistem pemerintahan sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan memiliki tujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu negara (Yulianty, 2021).

3.5. Penanggulangan Cybercrime

Beberapa langkah penting dapat diambil untuk memerangi penyebaran kejahatan di Internet yaitu mengamankan sistem, penanggulangan global, perlunya cyberlaw, dan perlunya dukungan lembaga khusus (Wahyono, 2009).

1. Mengamankan Sistem

   Keamanan sistem yang saling terintegrasi dapat menciptakan keamanan sistem yang handal. Sistem keamanan bertujuan untuk mencegah kerusakan jika terdapat pengguna yang tidak diinginkan membobol sistem tersebut. Membangun sistem yang saling terhubung dengan baik dapat menjembatani kesenjangan dalam meminimalisir tindakan jahat. Langkah awal yang perlu dilakukan oleh para pengguna teknologi internet dalam upaya penanggulangan

cybercrime adalah dengan mengamankan sistem komputer. Namun kesadaran masyarakat dalam tingkat pengamanan semakin tinggi, hal ini dapat kita lihat dari hasil survey yang dilakukan oleh CSI/FBI pada tahun 2003, menyatakan bahwa 99% dai 525 responden sudah menggunan perangkat lunak antivirus. Tujuan utama dari sebuah sistem keamanan adalah mencegah adanya perusakan bagian sistem sehingga orang lain tidak dapat merusaknya dengan mudah (Wahyono, 2009). Untuk mengamankan keamanan pribadi dapat menggunakan keamanan jaringan atau web server mulai dari tahap instalasi sistem hingga tahap pengamanan fisik. Langkah awal melindungi sistem adalah dengan mengamankan sistem komputer itu sendiri agar dapat mencegah adanya kerusakan pada setiap bagian sistem dari pengguna yang tidak diinginkan. Tidak menggunakan perangkat lunak bajakan serta rutin mengganti password berkala dapat menjadi langkah lanjutan agar terhindar dari kejahatan hacking.

2. Penanggulangan Global

   Cara yang dapat dilakukan untuk menyadarkan masing masing negara dalam menanggulangi kejahatan internet adalah diperlukannya keamanan sistem yang terintegrasi secara global untuk mencegah kerusakan pada bagian dalam sistem dari pengguna yang tidak sah. Menurut The Organization for Economic Cooperation and Development (OECD) ada beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime, yaitu; (Wahyono, 2009)

   a. Melakukan pembaruan hukum pidana nasional beserta hukum acaranya dan disesuaikan dengan konvensi internasional yang terkait dengan kejahatan tersebut.

b. Meningkatkan sistem pengamanan jaringan komputer berdasarkan standar internasional.

c. Meningkatkan pemahaman serta keahlian aparatur hukum mengenai upaya pencegahan, ivestigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.

d. Meningkatkan kesadaran warna negara akan pentingnya masalah cybercrime dan mencegah kejahatan tersebut.

e. Meningkatkan kerjasama antar negara, baik bilateral, ragional maupun multilateral sebagai upaya penanganan cybercrime yang dapat dilakukan melalui perjanjian ekstradisi dan mutual assistance treaties.

Masalah jurisdiksi cybercrime termasuk masalah yang sangat serius, Barbara Etter dalam (Marwin, 2013) mengidentifikasikan beberapa masalah kunci yang menyebabkan timbulnya masalah jurisdiksi berikut dalam konteks internasional, antara lain:

- Tidak adanya konsensus global mengenai jenis-jenis CRC (computer related crime) dan tindak pidana pada umumnya
- Kurangnya keahlian aparat penegak hukum dan ketidakcukupan hukum untuk melakukan investigasi dan mengakses sistem komputer
- Adanya sifat transnasional dari computer crime
- Ketidakharmonisan hukum acara/prosedural di berbagai negara
- Kurangnya sinkronisasi mekanisme penegakan hukum, bantuan hukum, ekstradisi, dan kerja sama internasional dalam melakukan investigasi cyber crime.

3. Perlunya Cyberlaw

Diperlukan adanya Cyberlaw atau hukum di dunia maya agar dapat membentuk perundang-undangan yang berkualitas untuk mengoptimalkan peranan hukum dalam perkembangan teknologi. Cyberclaw digunakan untuk mencegah kerusakan pada bagian dalam sistem oleh pengguna yang tidak sah sehingga memerlukan keamanan sistem yang terintegrasi secara global untuk meminimalisir kemungkinan kerusakan pada bagian dalam sistem tersebut.

Menurut Jonathan Rosenoer dalam (Ketaren, 2016) menyebutkan ruang lingkup cyberlaw yaitu:

1. Copy Right
2. Trademark
3. Defamation
4. Hate speech
5. Hacking, viruses, illegal access
6. Regulation internet resource
7. Privacy
8. Duty care
9. Criminal liability
10. Procedural issuses
11. Electronic contact
12. Pornography
13. Robbercy
14. Consumer protection
15. E-commerce, E-government

Oleh karena itu Cyberlaw sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, maupun penanganan tindak pidana. Cyberaw akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme (Nugraha, 2021).

4. Perlunya Dukungan Lembaga Khusus

Diperlukan sebuah upaya penanggulangan kejahatan internet dari lembaga lembaga khusus baik milik pemerintah maupun NGO (Non Government Organization). Sebagai contoh Amerika Serikat yang memilki Computer Crime and Intellectual Property Section (CCIPS) (Wahyono, 2009) sebagai sebuah divisi khusus dari U.S. Departement Of Justice merupakan Institusi informasi yang melakukan riset-riset khusus dalam penanggulangan cybercrime. Badan ini diperlukan untuk memberikan informasi mengenai kejahatan yang ada didunia maya kemudian menyebarkannya ke publik dan melakukan penyelidikan khusus tentang cara menanganinya. Akan tetapi di Indonesia masih mengalami kesulitan dalam menghadapi merebaknya cybercrime, beberapa penyebab diantaranya adalah keterbatasan Sumber Daya Manusia yang dimiliki penegak hukum. Oleh karena itu perlu adanya bimbingan khusus terkait cybercrime kepada anggota-anggota penegak hukum agar bisa menciptakan sumber daya manusia yang berkualitas supaya bisa membantu dalam menuntaskan kejahatan yang terjadi pada dunia maya. Diharapkan kedepannya Indonesia memiliki lembaga/anggota khusus yang bertugas di bidang cyber untuk membuktikan jejak-jejak para hacker, cracker dan phreacker dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer (Enggarani, 2012).

3.6. Cara Mencegah Cybercrime

Langkah sederhana yang dapat dilakukan untuk menghindari cybercrime: (Safira, 2020; Syifaudin, 2021)

1. Jangan pernah mengunduh file atau program apapun dari situs yang tidak terpercaya
2. Jangan mengklik link yang mencurigakan.
3. Jangan menggunakan aplikasi bajakan.
4. Gunakan kata sandi yang kuat dengan menggunakan kombinasi dari huruf, angka dan besar kecilnya huruf.
5. Gunakan fitur verifikasi 2 langkah pada akun google anda. Hal ini bertujuan untuk mengamankan akun anda dengan keamanan yang berlapis.
6. Bekali sistem dan jaringan Anda dengan security patches dan update software terbaru
7. Backup data Anda secara reguler untuk mencegah hilang maupun rusaknya data Anda
8. Selalu berhati-hati ketika menggunakan Wifi publik. Ada baiknya Anda menggunakan VPN untuk mengenkripsi data Anda.
9. Instal anti-virus atau anti-malware software untuk memindai, mendeteksi, dan menghapus segala ancaman siber pada perangkat Anda
10. Jangan memberikan data sensitif Anda, kecuali jika Anda telah meriset dan mengkonfirmasikan kebenaran identitas pihak yang meminta tersebut.
11. Bagi sebuah perusahaan, kembangkan kebijakan dan prosedur yang jelas untuk perusahaan maupun karyawan.

12. Tidak lupa juga untuk menguraikan setiap langkah keamanan yang telah ditempuh dan cari tau celah mana yang perlu ditingkatkan lagi keamanannya.
13. Selalu hati-hati dengan setiap email yang masuk, terlebih jika ada instruksi untuk transfer jumlah dana tertentu.
14. Untuk sebuah perusahaan terus latih karyawan Anda mengenai kebijakan dan juga prosedur keamanan serta beritahu mereka apa yang harus dilakukan jika ada terjadi pelanggaran keamanan.
15. Jaga keamanan website dengan menggunakan perangkat, software terbaru dan legal.
16. Buat backup data dan juga informasi secara teratur, agar mengurangi resiko data tersebut rusak karena serangan virus.
17. Anda juga bisa mengamankan perangkat anda dari serangan cyber crime dengan melengkapi keamanan terenkripsi pada media penyimpanan anda maupun di platform email yang anda gunakan. Anda juga bisa menggunakan VPN yang aman.

3.7. Penutup

Cybercrime merupakan kejahatan yang ditimbulkan karena adanya penyalahgunaan penggunaan teknologi internet bukan hanya terhadap komputer melainkan juga terhadap sistem jaringan komputer dan pengguna itu sendiri. Para pelaku cybercrime memiliki motif tersendiri dengan tujuan mendapatkan uang, politik hingga ajang membalas dendam. Tindakan ini dilakukan oleh seseorang yang memilki keahlian dan pengetahuan tinggi terhadap komputer dan jaringannya. Diperlukan adanya peraturan perundang-undangan tentang penggunaan teknologi untuk membatasi kejahatan dunia maya dan diperlukannya kerjasama dengan badan khusus untuk menanggulangi kejahatan cybercrime yang merugikan berbagai

pihak. Kejahatan tersebut didasari oleh beberapa faktor sehingga banyak terjadi di Indonesia seperti perekonomian, pergaulan, kesempatan yang ada, dan lain sebagainya. Faktor tersebut menimbulkan berbagai kejahatan - kejahatan seperti cybercrime yang bertujuan untuk memenuhi kebutuhan hidup. Oleh karena itu perlu adanya bimbingan atau pelatihan khusus kepada anggota penegak hukum untuk mencetak sumber daya manusia yang berkualitas sehingga aparat penegak hukum bisa membentuk badan khusus cybercrime di Indonesia yang bertugas untuk memberantas kejahatan-kejahatan yang terjadi di dunia maya yang disebabkan oleh oknum-oknum/pelaku yang merugikan banyak orang.

Bab 4

Cyber Law dan Implementasinya di Indonesia

4.1 Arti Kata Cyber

Kata Cyber berasal dari cybernetic yang berasal dari bahasa Yunani yang memiliki arti kata sifat terampil dalam mengarahkan/ mengatur. Kata Cyber digunakan dalam istilah cybersex, cyberporn, cyberspace dan istilah cyber yang lainnya. Istilah cyber digunakan untuk menggambarkan peristiwa yang terjadi di dunia maya. Istilah online juga menjadi salah satu kegiatan yang dilakukan di dunia maya. Dalam kamus.web.id «online» merupakan satu kegiatan yang terhubung melalui jarinngan komputer yang diakses melalui jaringan komputer lainnya. Seperti kegiatan di kehidupan nyata, dunia cyber mencakup banyak kegiatan yang ada di dunia nyata beralih ke dunia nyata. Jadi pembeda dengan dunia nyata adalah cara beraktivitas serta bertransaksi tidak dilakukan dengan tatap muka, tapi dilakukan melalui media internet tanpa harus bertatap muka (Munir, 2017).[1]

[1] Munir, N. (2017). *Pengantar Hukum Siber Indonesia* (Edisi Keti). PT RajaGrafindo Persada. Hal.

4.2 Istilah Hukum Cyber atau Hukum Telematika

Hukum Cyber (Cyber Law) merupakan istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum teknologi Informasi (Law of Information Technology), Hukum Dunia Maya (Virtual World Law) dan Hukum Mayantara. Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual. Istilah Hukum Siber (Hukum Cyber) dalam tulisan ini dilandasi pemikiran bahwa Siber jika diidentikkan dengan «dunia Maya» akan menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukumnya. Para penegak hukum menghadapi kesulitan jika harus membuktikan persoalan yang diasumsikan sebagai «maya», sesuatu yang tidak terlihat dan semu. (Pengantar Hukum Siber, Hal 26)

Di Indonesia istilah yang dimaksud sebagai terjemahan "Cyber Law", seperti Hukum Sistem Informasi, Hukum Informasi dan Hukum Telematika (Telematika dan Informatika). Secara Yuridis, kegiatan Siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum nyata. Kegiatan siber merupakan kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan sebagai orang yang telah melakukan perbuatan hukum secara nyata. (Pengantar Hukum Siber, Hal 26).

Hukum telematika atau cyber law secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi dan informasi. Hukum telematika merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi, hukum dunia maya, hukum mayantara. Istilah tersebut muncul ketika kegoatan yang dilakukan melalaui ssitem komputer dan

sistem komunikasi baik dalam lingkup lokal aupun global dengan memanfaatkan teknologi informasi berbasis sistem yang merupakan sistem elektronik yang dapat dilihat secara virtual (Maskun, 2013).[2]

Hukum dalam konteks sistem telematika merupakan satu tantangan baru dalam dunia hukum. Ketersediaan dan keterbatasan aturan hukum yang selama ini memaksa aparat penegak hukum dalam mengambil kebijakan untuk melakukan penemuan hukum di bidang ini keputusan yang berkaitan dengan masalah telematika dapat memenuhi aspek keadilan kemanfaatan dan kepastian hukum.

4.3. Pengertian Cyber Law

Definisi Cyber Law yang diterima semua pihak adalah milik Pavan Dugal dalam bukunya "Cyber Law The Indian Perspective" menurut Dugal, *Cyber Law is a generic term, which refers to all the legal and regulatory aspects of internet and the world wide web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others, in cyberspace comes within the amit of cyber law*. Disini Dugal mengatakan bahwa Hukum Siber (Cyber Law) adalah istilah umum yang menyangkut semua aspek legal dan peraturan internet dan juga World Wide Web.

Cyber Law (Hukum Siber) adalah hukum yang digunakan dalam dunia cyber (dunia maya) yang umumnya diassosiasikan dengan internet. Cyber Law dibutuhkan sebagai dasar dari hukum di berbagai negara yang mencakup 'ruang dan

---

[2] Maskun. (2013). Kejahatan Siber (Cyber Crime): Suatu Pengantar. Prenada Media Grup. Hal.

waktu', sementara disisi lain internet dan jaringan komputer mendobrak batasan ruang dan waktu ini.

Cyber Law juga didefinikan sebagai kumpulan peraturan perundang-undangan yang mengatur tentang berbagai aktifitas manusia di cyberspace dengan memanfaatkan teknologi informasi. Cyber Law (hukum siber) merupakan istilah yang berasal dari Cyberspace. Cyberspace berasal dari kata latin 'Kubernan' yang artinya menguasai atau menjangkau karena 'cyberspace'lah yang menjadi focus dari 'cyber law'.

Sebagaimana diuraikan diatas cyber law akan kita sebut sebagai hukum dunia maya. Dengan demikian pengertian hukum siber (cyber law) secara sederhana kita sebut sebagai hukum yang mengatur informasi di dunia maya dengan memanfaatkan teknologi informasi baik melalui telekomunikasi ataupun melalui telematika yang berakibat adanya hak dan kewajiban hukum. hal inilah yang membedakan cyber law dengan hukum lainnya karena adanya informasi didunia maya, sedangkan hukum lainnnya pada umumnya tidak menyangkut dunia maya. Hal ini dikarenakan hukum dunia maya tidak terlihat secara langsung tapi mempunyai akibat hukum yang berkaitan dengan hak-hak dan kewajiban hukum khususnya berlaku didunia cyber. (Pengantar hukum siber, hal 195)

4.4 Ruang Lingkup Cyber Law atau Hukum Telematika

Kedudukan hukum dalam ranah telematika jika ditelaah lebih jauh ternyata membawa implikasi bagi perubahan yang terjadi dalam masyarakat. Menurut Muchtar Kusumaatmadja, perubahan ketertiban dan keteraturan merupakan tujuan dari masyarakat yang sedang berubah atau membangun, Oleh sebab itu jika perubahan tidak dilakukan dengan tertib dan teratur maka hukum merupakan sarana yang tidak dapat diabaikan. Mengenai perubahan karakter sosial dan budaya masyarakat sebagai akibat perkembangan telematika tentu memiliki fakta

yang tidak dapat dihindarkan. Menurut Boele-Woelki berpandangan bahwa keterlibatan langsung pemerintah dan undang-undang dalam masalah cyberspace merupakan sesuatu yang dibutuhkan khususnya dalam menyelesaikan sengketa-sengketa yang timbul di bidang telematika. pandangan Senada juga dikemukakan oleh Tom Maddox, yang pada prinsipnya sepakat dengan Boele-Woelki, hanya saja berbeda dalam kaitan dengan sumber pengendalian (fungsi pengendalian).

Fakta menunjukkan bahwa penggabungan telekomunikasi dan Informatika telah melahirkan suatu fenomena yang telah mengubah konfigurasi model komunikasi konvensional dalam dimensi ke-3 Yang berimplikasi pada keterbatasan aturan-aturan hukum yang ada dalam mengejar perubahan yang begitu cepat. oleh karena itu, peran pemerintah sangatlah strategis dalam merumuskan aturan yang menjadi aturan main yang wajib ditaati oleh setiap aktor telematika

Berangkat pada deskripsi singkat tentang tertatih nya hukum mengejar kemajuan zaman maka Chris Reed merumuskan suatu kerangka telematika yang disebutnya sebagai hukum komputer. hukum ini dianggap sebagai cabang dari hukum yang berhubungan dengan teknologi informasi yang merupakan suatu perangkat aturan yang memiliki kelengkapan dalam menangani isu-isu yang dimunculkan dan dihasilkan oleh komputer. Hukum ini juga dianggap sebagai upaya dan usaha dari pembuat undang-undang dan penegak hukum dalam Bergerak bersama dalam menangani masalah teknologi yang kadang-kadang terlihat janggal.

Hal ini dapat dilihat pada beberapa kasus yang berkaitan dengan penyalahgunaan komputer seperti carding, hacking dan lain sebagainya. meskipun kebutuhan akan kerangka hukum di bidang telematika pada awalnya merupakan sesuatu yang harus segera dibuat, Ternyata hal tersebut tidak sepenuhnya direspon oleh para ahli hukum. beberapa ahli hukum menganggap bahwa

tidak diperlukannya suatu hukum khusus untuk memenuhi bidang baru ini khususnya di bidang informatika. menurut Peter Knight dan James Fitzsimons bahwa tidak ada yang disebut dengan hukum komputer. Hal Senada juga dikemukakan oleh beberapa pengacara (lawyer) yang mengatakan bahwa penting untuk membicarakan isu isu hukum yang relevan dengan komputer tetapi tidak terlalu jauh dari apa yang saat ini umumnya dikaitkan dengan label hukum komputer atau hukum teknologi informasi.

Pentingnya suatu aturan khusus di bidang telematika sangatlah disadari bahwa bidang baru ini terus berkembang dengan tingkat kompleksitas yang sangat tinggi tentunya memerlukan suatu payung hukum yang mengatur seluruh permasalahan di bidang telematika. oleh karena itu pembentukan kerangka hukumnya harus dilihat dari berbagai aspek seperti rule of law dan internet, yurisdiksi dan konflik hukum pengakuan hukum terhadap dokumen serta tanda tangan elektronik (electronic signature), perlindungan dan privasi konsumen, cybercrime, pengaturan konten, dan cara-cara penyelesaian sengketa domain. oleh karena itu keberadaan hukum telematika sebagai suatu pendekatan hukum interdisipliner yang dikaji berdasarkan perkembangan dan konvergensi telematika yang sebenarnya tidak hanya hidup dalam tataran wacana saja. melainkan keberadaannya adalah selaras dengan perbedaan hukum yang sesuai dengan dinamika masyarakat itu sendiri karena mempunyai tempat dalam sistem tata hukum.

Pendekatan hukum interdisipliner yang digunakan misalnya dapat dilihat pada beberapa aspek yang akan berkorelasi pada lahirnya kerangka hukum di bidang telematika seperti hukum telekomunikasi, hukum perlindungan data dan hak pribadi, hukum media, hukum perikatan, hak kekayaan

intelektual, hukum perlindungan konsumen, hukum pidana, dan hukum internasional (Maskun, 2013).(Munir, 2017)

4.5 Perbuatan Yang Dilarang Menurut UU ITE

Klasifikasi perbuatan yang dilarang dalam uu ite dijelaskan dalam pasal 27 hingga pasal 37. konstruksi pasal-pasal tersebut mengatur secara lebih detail tentang pengembangan modus-modus kejahatan tradisional sebagaimana yang tercantum dalam kitab undang-undang hukum pidana KUHP. pasal 27 misalnya mengatur masalah pelanggaran kesusilaan perjudian pencemaran nama baik dan tindakan pemerasan dan pengancaman. untuk lebih jelasnya dapat dilihat sebagai berikut:

Pasal 27

1. *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.*
2. *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian.*
3. *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.*
4. *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman.*

Konstruksi pasal 27 di atas menjelaskan perkembangan modus kejahatan dan garis miring atau pelanggaran dengan media komputer/internet dalam bentuk informasi/dokumen elektronik. hal tersebut sangatlah penting khususnya membantu para penegak hukum dalam memproses dan mengadili kasus-kasus yang telah menggunakan media informasi elektronik untuk memuluskan kejahatan/pelanggaran yang dilakukan.

Lebih lanjut pasal 28 mengatur tentang perlindungan konsumen dan aspek Sara. hal ini sangat beralasan mengingat banyak transaksi perdagangan yang dilakukan dengan menggunakan media komputer/internet di mana baik produsen maupun Konsumen tidak pernah bertemu satu sama lainnya. sehingga aspek kepercayaan (*trust*) memegang peranan penting dalam transaksi perdagangan.

Di sisi lain persoalan SARA adalah merupakan persoalan kebangsaan yang sangat rentan untuk menimbulkan konflik. Indonesia sebagai bangsa yang memiliki tingkat heterogenitas yang cukup tinggi telah menjadikan SARA sebagai salah satu produk konflik yang sangat mudah tersulut. Oleh karena itu perkembangan modus pengoptimalisasian cara sebagai produk yang rawan konflik harus diatur dengan penyesuaian perkembangan modus yang menggunakan media komputer/internet. Lebih jelasnya dapat dilihat dalam pasal berikut:

Pasal 28

1. *Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.*
2. *Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).*

Pasal 29 uu ite dapatlah dianggap sebagai suatu perkembangan yang sangat signifikan dalam pengaturan hukum mengenai adanya ancaman yang sering dilakukan dan garis miring atau dialamatkan kepada seseorang dengan menggunakan media informasi/ dokumen elektronik. perkembangan produk elektronik sangatlah memudahkan bagi seseorang untuk memuluskan langkah jahatnya dalam mencapai tujuan yang diinginkan. untuk lebih jelasnya sebagai berikut:

Pasal 29, setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30 UU ITE menyebutkan bahwa:

1. *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.*
2. *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.*
3. *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar menerobos melampaui atau menjebol sistem pengamanan.*

Konstruksi pasal 30 dengan jelas menyebutkan bahwa tindak ilegal yang dilakukan seseorang terhadap sistem elektronik orang lain dengan tujuan untuk memperoleh informasi/ dokumen elektronik dan/atau au upaya pembobolan, penerobosan dan penjebolan yang melanggar dan melampaui sistem pengamanan adalah sesuatu yang terlarang. beberapa kasus yang relevan dan telah terjadi dalam praktek dunia cyber

dapat dilihat pada kasus pembobolan kartu kredit pembobolan situs KPU 2004 penjebolan beberapa dokumen penting pada Departemen Pertahanan dan Keamanan pemerintahan Amerika Serikat dan masih banyak contoh kasus lainnya yang harus diselesaikan dengan menggunakan aturan hukum yang belum secara khusus mengatur tentang bentuk kejahatan/pelanggaran yang dimaksud.

Pasal 31 mengisyaratkan legalitas hukum tindakan penyadapan khususnya terhadap maraknya tindakan penyadapan yang dilakukan oleh lembaga penegak hukum lebih khusus lagi tindakan penyadapan yang dilakukan oleh Komisi Pemberantasan Korupsi KPK dalam memberantas kasus korupsi.

Dalam praktek negara-negara di dunia penyadapan hanya mungkin dilakukan oleh lembaga penegak hukum dalam konteks tugas yang diembankan kepadanya. akan tetapi uu ite belum secara khusus menyebutkan lembaga penegak hukum yang mana yang dapat melaksanakan otoritas tersebut. hal ini Tentunya berbeda dengan UU telekomunikasi yang secara terbatas telah menyebutkannya. Oleh karena itu amanah penentuan lembaga penegak hukum yang memiliki otoritas untuk melakukan penyadapan baik dalam uu ite ataupun UU telekomunikasi harus dirumuskan dan dikeluarkan dalam bentuk Peraturan Pemerintah PP yang hingga saat ini belum dikeluarkan. untuk lebih jelasnya pasal 31 dapat dilihat sebagai berikut:

Pasal 31

1. *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau Sistem elektronik tertentu milik orang lain.*
2. *setiap orang dengan sengaja dan tanpa hak dalam melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau*

dokumen elektronik yang tidak bersifat publik dari ke dan dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, Baik yang yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan penghilangan dan garis miring atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

3. *kecuali intersepsi sebagaimana dimaksud pada ayat 1 dan ayat 2 intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian Kejaksaan dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.*
4. *ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat 3 diatur dengan peraturan pemerintah.*

Pasal 32 dan 33 UU ITE mengatur tentang perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain maupun milik publik yang bersifat rahasia atau confidential untuk lebih jelasnya dapat dilihat sebagai berikut:

Pasal 32, Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah menambah mengurangi melakukan transmisi merusak menghilangkan memindahkan menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik. setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak. terhadap perbuatan sebagaimana dimaksud pada ayat 1 yang mengakibatkan terbukanya. Suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33, setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindak apapun yang mengakibatkan terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

Lebih lanjut pasal 34 hingga pasal 37 merupakan penekanan supporting idea terhadap bunyi pasal 27 hingga 33 yang merupakan kategori perbuatan yang dilarang dengan pengecualian pada Pasal 34 ayat 2 yang menyebutkan bahwa bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian pengujian sistem elektronik untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum. lebih jelasnya dapat dilihat sebagai berikut:

Pasal 34

1. *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi menjual mengadakan untuk digunakan mengimpor mendistribusikan menyediakan atau memiliki: perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33. Sandi lewat komputer kode akses atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33*
2. *Tindakan sebagaimana dimaksud pada ayat 1 itu bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian pengujian sistem elektronik untuk perlindungan sistem elektronik itu sendiri secara sah dan tidak melawan hukum.*

Pasal 35, Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi penciptaan perubahan penghilangan pengrusakan informasi elektronik dan atau dokumen elektronik dengan tujuan agar informasi elektronik

dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang autentik

Pasal 36, setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain.

Pasal 37, setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 36 di luar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia.(Munir, 2013)

Aturan hukum telematika atau hukum cyber berdasarkan perkembangan teknologi yang luar biasa cepat tidak sebanding dengan hukum telematika atau cyber yang mengakibatkan banyak terjadi kekosongan hukum. Para ahli hukum telematika juga terbatas, itupun lebih banyak yang memikirkan hukum pidana cyber atau aturan hukum telematika yang berkaitan dengan masalah pidana tetapi masih terbatas pemikiran tentang hukum perdata Cyber (Munir, 2017).

Bab 5

Inovasi Vs Etika

5.1 Pengantar

Saat ini banyak perusahaan-perusahaan yang bekolaborasi untuk menciptakan suatu inovasi bersama (co-creation) untuk memuaskan dan memanjakan konsumen. Sumber inovasi bukan hanya antar perusahaan saja, tetapi juga dapat berasal dari orang-orang yang ada di perusahaan ataupun di luar perusahaan itu sendiri, lembaga pemerintah, universitas atau Lembaga-lembaga Pendidikan, bahkan dari konsumennya. Schilling (2017) mendefinisikan inovasi sebagai implementasi praktis dari suatu ide yang ada di dalam suatu pikiran (imajiner) ke dalam perangkat atau proses baru atau karya baru dan bermanfaat.

Berdasarkan pembagian jenis yang dikemukakan oleh Schilling, maka jenis inovasi dapat dibagi ke dalam 4 jenis, yaitu:

1. Inovasi produk dan Inovasi Proses

   inovasi produk diwujudkan dalam bentuk produk atau barang (seperti smartphone yang dapat dilipat, robot dll), sedangkan inovasi proses diwujudkan dalam suatu cara baru organisasi dalam menjalankan bisnisnya (seperti cara memasarkan, cara produksi dll). Inovasi proses biasanya berorientasi pada peningkatan efektivitas atau efisiensi. Inovasi proses maupun inovasi produk biasanya terjadi

secara bersamaan, tetapi memang inovasi produk seringkali lebih terlihat.

2. Inovasi Radikal dan Inovasi Inkremenal

   inovasi radikal dapat dikatakan sebagai inovasi yang berbeda atau baru dibandingkan solusi (produk atau proses) yang ada sebelumnya atau hanya sedikit berbeda. Sehingga sebuah teknologi bisa jadi baru bagi dunia atau bagi industry atau bagi perusahaan atau bagi unit bisnis yang mengadopsinya. Seperti Teknologi IoT yang digunakan pada proses produksi menjadi proses produksi yang baru. Sedangkan inovasi incremental merupakan inovasi yang bukan sesuatu yang baru atau luar biasa, hanya melibatkan perubahan kecil, seperti aplikasi whatsapp yang menambahkan sistem keamanan ganda.

3. Peningkatan Kompetensi dan Penghancuran Kompetensi,

   inovasi dapat dikatakan sebagai peningkatan kompetensi jika inovasi dibangun atas dasar pengetahuan perusahaan yang ada, contohnya saja Microsoft yang membangun windows dari versi awal windows 1.0 hingga saat ini windows 11 yang dibangun berdasarkan generasi sebelumnya. Sedangkan sebaliknya, inovasi dikatakan sebagai penghancuran kompetensi adalah inovasi yang tidak dibangun dari pengetahuan perusahaan yang ada atau merupakan sesuatu yang baru, seperti kalkulator yang tidak dapat beralih ke teknologi baru.

4. Arsitektur dan Komponen

   Setiap produk dan proses merupakan sistem bersarang yang hirarkis, dimana terdiri dari sistem komponen, contohnya saja smartphone yang terdiri dari komponen software, kamera, speaker dll. Inovasi bisa saja memerlukan perubahan pada satu atau beberapa komponen, atau secara keseluruhan

arsitekturnya dimana komponen-komponen tersebut beroperasi. Sehingga, sebuah inovasi arsitektur memerlukan perubahan desain secara keseluruhan. Bagi perusahaan, untuk memulai atau mengadopsi inovasi arsitektur perlu untuk memahami setiap komponen dan integras di antara komponen-komponen tersebut untuk membentuk keseluruhan sistem. Perubahan arsitektur dapat merubah beberapa fitur sistem, yang pada akhirnya akan memicu perubahan dalam banyak fitur desain lainnya dari keseluruhan sistem atau komponen individual.

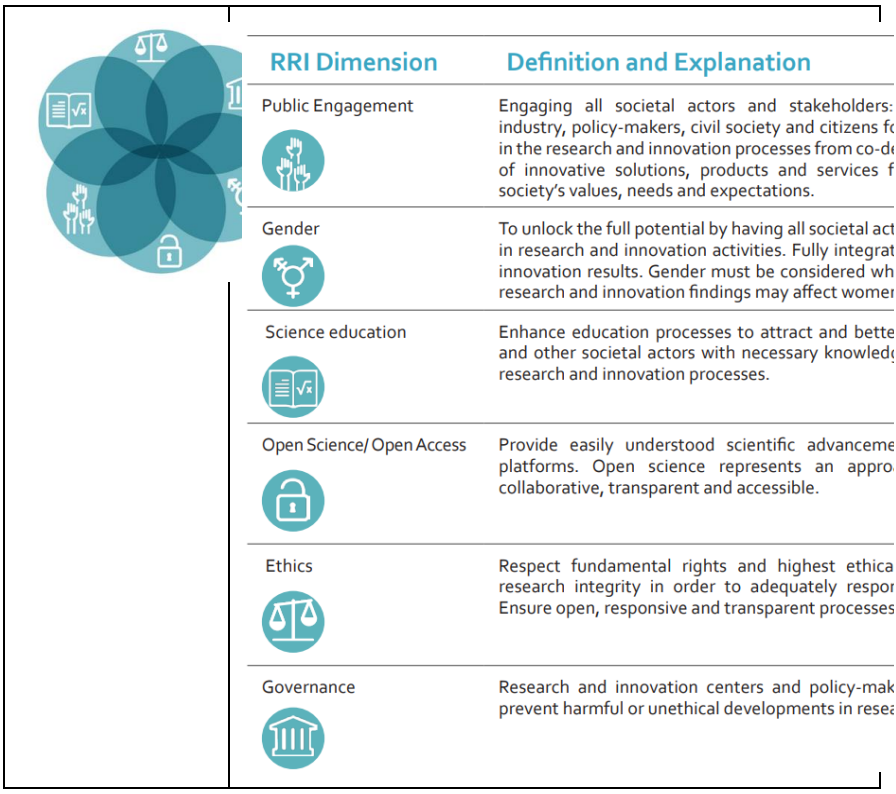
5.2 Inovasi yang Bertanggung Jawab

Penggunaan berbagai teknologi seperti penggunaan teknologi IoT, Blockchain, AI untuk menciptakan nilai (value) telah meningkatkan berbagai inovasi produk. Tentunya hal ini membuka berbagai resiko baru seperti resiko privasi dan perlindungan data, kekayaan intelektual dan kesenjangan digital. Tata Kelola penelitian menjadi semakin berkembang luas, yang telah dikemukakan oleh Stahl dkk. dari tahun 2014 yang disebut dengan penelitian dan inovasi yang bertanggung jawab (*Responsible Research and Innovation*/RRI).

RRI menurut Schneider (2019) merupakan suatu proses kerjasama antara masyarakat, peneliti, dan innovator secara aktif mendefinisikan, mendesain dan membangun solusi (produk atau jasa) yang dapat diterima secara sosial, berkelanjutan dan dapat menyelesaikan permasalahan social yang penting. Penerapan RRI pada bidang teknologi informasi dan komunikasi (TIK) membahas area yang lebih luas terhadap tata kelola ilmu pengetahuan, teknologi, dan inovasi. Sehingga RRI tidak fokus hanya pada TIK saja, tetapi juga berkaitan langsung dengan etika riset dan pengembangan teknologi. Hal ini tentunya akan mempersempit gap antara waktu fase mulai dirumuskannya penelitian sampai pada akhirnya individu dan organisasi

menggunakan produk dan layanan berdasarkan hasil penelitiannya tersebut.

Untuk menggunakan RRI, European Commission (Badan Eksekutif Uni Eropa) telah membuat RRI roadmap yang digambarkan ke dalam 6 dimensi yang saling berhubungan:



RRI Dimension	Definition and Explanation
Public Engagement	Engaging all societal actors and stakeholders: industry, policy-makers, civil society and citizens fo in the research and innovation processes from co-de of innovative solutions, products and services f society's values, needs and expectations.
Gender	To unlock the full potential by having all societal act in research and innovation activities. Fully integrat innovation results. Gender must be considered wh research and innovation findings may affect womer
Science education	Enhance education processes to attract and bette and other societal actors with necessary knowledg research and innovation processes.
Open Science/ Open Access	Provide easily understood scientific advanceme platforms. Open science represents an appro collaborative, transparent and accessible.
Ethics	Respect fundamental rights and highest ethica research integrity in order to adequately respor Ensure open, responsive and transparent processes
Governance	Research and innovation centers and policy-mak prevent harmful or unethical developments in resea

Gambar 5.1. Enam dimensi Roadmap RRI

[sumber: Schneider (2019)]

5.3 Permasalahan Etika TIK yang Muncul

Perkembangan sinkronisasi teknologi menjadikan setiap teknologi menjadi saling terhubung dan terintegrasi satu sama lain. Hal ini tentunya memunculkan berbagai teknologi baru yang dikenal dengan istilah emerging technologies, dimana

berbagai berbagai pengembangan teknologi dan aplikasi praktis yang melibatkan teknologi lama dan teknologi baru yang sebagian besar masih belum tereaslisasi. Stahl (2011) mengidentifikasi ada 11 teknologi yang dapat berdampak pada manusia secara sosial maupun sosio-teknis, yaitu:

1. affective computing, merujuk pada kemampuan teknologi untuk mengenali keadaan emosi penggunanya
2. ambient intelligence, teknologi tertanam yang memungkinkan banyak teknologi terintegrasi dan adaptif terhadap pengguna.
3. artificial intelligence, teknologi sistem komputer yang memiliki kecerdasan yang dapat meniru bentuk, sifat dan cara kerja manusia, sehingga mampu belajar, menyimpulkan dan mengkoreksi diri secara mandiri
4. bioelectronics, bidang ilmu yang mengintegrasikan penggunaan bahan dan arsitektur biologis dan elektronik untuk sistem pemrosesan informasi dan perangkat baru
5. cloud computing, metode pemanfaatan berbagai layanan melalui internet dengan sumber daya penyimpanan data, *server*, *database*, jaringan, dan perangkat lunak.
6. future internet, kegiatan-kegiatan penelitian yang berkaitan dengan arsitektur baru pada teknologi internet.
7. human-machine symbiosis, interaksi antara manusia dan komputer, dimana keterlibatannya memiliki hubungan yang erat antara manusia dan anggota elektroniknya
8. neuro-electronics, penelitian yang berkaitan dengan antarmuka neuron dari sistem saraf dengan perangkat elektronik.
9. quantum computing, pengembangan teknologi komputer dengan memanfaatkan fenomena pada fisika (kuantum) yang

berdampak pada perhitungan yang jauh lebih cepat dibanding komputer biasa.

10. Robotics, teknologi yang berhubungan dengan desain, konstruksi, operasi, disposisi struktural, pembuatan, dan aplikasi dari robot.
11. virtual/augmented reality, teknologi yang menggabungkan benda maya dua dimensi dan ataupun tiga dimensi ke dalam sebuah lingkungan nyata.

Meskipun perkembangan teknologi telah memberikan dampak pada munculnya berbagai produk yang digunakan manusia dalam mempermudah aktivitas dan sebagai sarana hiburan, permasalahan mengenai privasi, perlindungan data, kesenjangan digital selalu tetap ada dan menjadi satu hal yang tidak dapat lepas dari kebijakan aturan Lembaga pemerintah untuk dapat membuat suatu regulasi, serta norma-norma yang ada yang bertujuan untuk mengatasinya. Stahl (2011) mengidentifikasi berbagai masalah isu etika yang muncul seperti:

- Dampak secara individu (*Impact of Individual*) berkaitan dengan:
    a. **Perawatan manusia** (*treatments of human*), saat ini penerapan teknologi telah memungkinkan teknologi genetika, seperti kloning, terapi gen, manipulasi genetik dll terjadi. Hal ini telah menciptakan potensi besar bagi umat manusia untuk mempengaruhi dan mengubah kehidupan manusia. Berbagai tantangan timbul saat teknologi tersebut disalahgunakan dan bertentangan dengan etika, hukum, dan kebijakan sosial.
    b. **Privasi** (*privacy*), berkembangnya teknologi telah memunculkan berbagai jenis layanan yang saling terintegrasi dari satu aplikasi ke aplikasi lainnya. Berbagi

informasi antara pengguna di berbagai aplikasi menjadi semakin transparan. Hal ini tentunya menjadi tantangan bagi pelaku penyedia layanan untuk tetap menjaga data dan informasi privasi yang dimiliki oleh setiap individu yang ada di lingkungan layanan tersebut.

c. **Keamanan** (*security*), sama halnya dengan privasi, berbagai kejahatan di dunia maya semakin canggih seiring dengan meningkatnya berbagai layanan yang terintegrasi. Inovasi harus dapat memberikan jaminan keamanan bagi setiap pengguna produk atau layanan.

d. **Otonomi** (autonomy), berbagai inovasi telah melahirkan teknologi yang dapat berfungsi tanpa adanya perintah dari seseorang (teknologi otonomi), seperti mobil tanpa awak (driverless). Hal ini tentunya memiliki kerentanan jika terjadi serangan siber (cyberattacks) dibandingkan dengan mobil tradisional.

e. **Identitas** (*identity*), data pengguna teknologi baik media sosial dan berbagai aplikasi yang terintegrasi dengan aplikasi lainnya seperti marketplace, email dll. Memiliki kerentanan adanya pencurian identitas yang dapat disalahgunakan.

f. **Kepercayaan** (trust), ketergantungan suatu proses pada teknologi membuat penggunanya harus mempercayai apa yang dapat dilakukan oleh teknologi tersebut. Trus dalam teknologi menurut Asleigh (2002) seperti *quality of interaction, reliability, performance, understanding, communication, expectancy, confidence, proactively, ability, respect dan honestly.*

g. **Individu tertentu** (*specific individuals*),

Etika individu merujuk pada keyakinan akan apa yang benar dan salah. Teknologi memberikan pengaruh

terhadap etika individu untuk berperilaku dalam situasi tertentu, seperti dalam mengambil keputusan.

- Persepsi teknologi (*Perceptions of Technology*), berkaitan dengan:
  a. **Anthropomorphism**, yaitu penggunaan karakteristik manusia untuk menggambarkan atau menjelaskan objek non-manusia. Di dalam teknologi Cornelius dan Leidner (2021) menggunakan istilah Anthropomorphic Technology (AT) yang merupakan teknologi yang mirip manusia dalam desain dan memotivasi antropomorfisme, yang menurutnya masih menjadi perdebatan adanya penerimaan dan penolakan AT tersebut.
  b. **moral of status technology**, yaitu eksplorasi berbagai dimensi hubungan antara manusia dan teknologi). Pendekatan ini menjadikan status moral dengan memperlakukan teknologi sebagai sarana belaka yang bergantung pada nilai kepentingan manusia.
  c. **Overtaking humankind**, Huaihong (2019) dalam papernya menyatakan bahwa etika sosial tradisional selalu berhubungan dengan manusia, dimana saat ini etika modern berhubungan dengan manusia dan objek, dan etika di masa depan perlu menjelaskan hubungan antara manusia dan mesin cerdas. Sehingga melihat pada pembatasan pengembangan mesin cerdas untuk sarana dan kemampuan spesialisasi dan miniaturisasi dibandingkan dengan menetapkan penilaian nilai dari keramahan suatu mesin cerdas serta menjaganya dalam lingkup non-kekerasan
  d. ***Relationship Human-Machine***, secara tradisional hubungan manusia-mesin adalah manusia secara langsung mengendalikan mesin melalui suatu antarmuka. Pengendalian secara otomatisasi dilakukan

dengan menggunakan serangkaian instruksi. Berkembangnya teknologi kecerdasan buatan telah memungkinkan sistem untuk melaksanakan tugasnya tanpa instruksi khusus yang telah ditentukan sebelumnya. Kecerdasan mesin yang semakin canggih akan memunculkan hubungan baru antara manusia dan mesin.

- Dampak Konsekuensi Sosial (*Social Consequency*), berkaitan dengan:

  a. **Sifat masyarakat** (*Nature of society*), produk inovasi yang dibuat merujuk pada standar normatif perilaku manusia dan dipengaruhi oleh perasaan manusia.

  b. **Budaya** (*Culture*), inovasi tidak bertentangan dengan pengalaman, asumsi, dan harapan manusia untuk berperilaku tidak etis

  c. **Pengawasan** (*Surveillance*), inovasi yang terkendali, dan dikelola serta dipantau oleh berbagai lembaga agar tidak terjadi pelanggaran kode etik

  d. **Bertanggung jawab** (Responsibility), inovasi harus dapat dipertanggung jawabkan berdasarkan prinsip dan nilai dengan standar atau konteks tertentu

  e. **Tanggung jawab hukum** (Legal liability), inovasi dapat dipertanggungjawabkan secara hukum (bersifat legal), tidak melanggar aturan-aturan hukum yang ada

  f. Resiko (*Risk*), resiko berkaitan dengan konsekuensi negatif yang tidak terduga dari tindakan tidak etis akibat adanya teknologi baru.

  g. **keadilan social (***Equity/distribution*), prinsip-prinsip keadilan distributif berkaitan dengan teknologi yang dapat digunakan oleh seluruh masyarakat sesuai dengan tujuan produk tersebut.

h. **Kepemilikan** (*Property/ownership*), pemilik produk inovasi mendapatkan hak kepemilikan sesuai dengan aturan perundang-undangan.

i. **Kekuasaan/Hubungan** (*Power/relationships*), perlunya pengawasan agar penguasaan penelitian produk inovasi tidak hanya dikuasai oleh golongan tertentu, hal ini menuntut keterlibatan yang erat dari berbagai peneliti untuk memastikan pengetahuan yang dihasilkan tidak bias, atau berbahaya.

j. **Lingkungan/berkelanjutan** (*Environment/sustainability*), prinsip dasar dari suatu inovasi teknologi harus dapat berkeadilan, berkelanjutan, berkecukupan dan berpartisipasi.

k. **Bias gender** (*Gender biases*), suatu inovasi tidak menyebabkan adanya perlakukan yang berbeda berdasarkan identitas gender manusia.

l. **Meremehkan konsekuensi dari kecerdasan buatan** (AI) (*Underestimation of the consequences of AI*), dampak teknologi yang memiliki kemampuan AI memiliki resiko dan tantangan terkait etika yang harus disadari oleh setiap peneliti untuk dapat digunakan secara bertanggung jawab

m. **Hambatan rendah untuk terjadinya perang** (*Lower barriers for war*), suatu inovasi hendaknya tidak menyebabkan mudahnya terjadi peperangan.

5.4 Penutup

Teknologi akan selalu berkembang sesuai dengan aktivitas manusia dalam melakukan inovasi untuk memenuhi kebutuhan dan aktivitas manusia. Untuk menghasilkan inovasi yang bertanggung jawab perlu untuk mengelola penelitian atau eksplorasi teknologi dengan baik. Enam dimensi RRI dapat

digunakan untuk mengelola inovasi tersebut. Inovasi menghasilkan produk dan layanan yang baru yang memerlukan pertimbangan dan penetapan aturan berkaitan dengan isu-isu etika yang muncul baik dampak pada individu manusia, persepsi teknologi itu sendiri maupun terhadap konsekuensi sosial yang diperlukan untuk dapat menghasilkan inovasi yang bertanggung jawab bagi kehidupan manusia.

Bab 6

Etika Menggunakan Internet

6.1. Sekilas Tentang Internet di Indonesia

Siapa yang tidak kenal internet? Jaringan virtual satu ini sangat akrab di telinga dan aktivitas kita sehari-hari. Bahkan, bagi sebagian orang, internet sudah menjadi kebutuhan dasar yang digunakan setiap hari. Tapi apa sebenarnya internet itu?

Jika dilihat dari asal katanya, internet adalah akronim dari Bahasa Inggris, yakni *interconnection* dan *net.* Sementara itu, menurut Lister *et al,* dalam Fahrimal (2018:69) menyatakan bahwa internet adalah sebuah revolusi dari kumpulan jaringan yang menghubungkan begitu banyak server dan computer secara terperinci dan bersama-sama. Perkembangan dan penggunaan internet sudah meningkat begitu pesat sejak 20 tahun terakhir.

Di Indonesia sendiri, berdasarkan data yang dihimpun dari We Are Social (dalam Afriani & Azmi, 2020:332) menyatakan pengguna internet pada tahun 2019, naik sekitar 13 % dari tahun 2018 yakni mencapai 150 juta jiwa. Internet menjadi kian diminati karena memiliki karakteristik yang unik dan menarik, dibanding media massa konvensional terdahulunya, yakni media massa cetak (koran, tabloid, dan majalah) serta media massa elektronik (radio dan televisi). Karakteristik unik tersebut,

menurut Wood dan Smith (dalam Fahrimal, 2018:69) antara lain adalah karakteristik multimedia dan interaktif.

Multimedia maksudnya internet mampu menyedikan berbagai macam sarana bagi para pengguna untuk menikmati media, diantaranya membaca teks, menonton video, dan mendengarkan audio secara bersamaan. Hal ini sekaligus menjadi solusi dalam mengatasi kelemahan dan keterbasan yang dimiliki oleh media konvensional. Sementara itu, karakteristik unik kedua adalah interaktif, artinya para pangguna internet mampu untuk membuat, mengolah, dan menyebarluaskan pesan oleh diri mereka sendiri. Selain itu para pengguna internet pun mampu berinteraksi secara online dengan sesama pengguna.

Alasan lain, kenapa pada akhirnya internet menjadi candu bagi para penggunanya, menurut Riffie *et al* (dalam Fahrimal, 2018:69) adalah karena internet bisa menyampaikan informasi dengan begitu cepat, dalam, dan melimpah dengan biaya yang realatif murah. Hal lain, menurut Tapscot (dalam Fahrimal, 2018:69) yang menjadi daya Tarik internet adalah fitur kostumisasi yang memungkinkan setiap pengguna internet untuk bisa merasa *private* dan bebas melakukan *setting* atau pengaturan dalam setiap akun media sosial yang mereka punya sesuai dengan kebutuhan mereka masing-masing.

Pada akhirnya, internet menjadi ruang publik digital di mana masyarakat digital dari berbagai belahan dunia sangat dimungkinkan untuk saling berhubungan, berdiskusi, dan melakukan interaksi dalam bertukar pesan digital. Karena memiliki koneksi tanpa batas, maka Friedman (dalam Fahrimal, 2018:69) memberikan istilah internet sebagai sebuah dunia yang datar, hal ini terjadi karena perkembangan teknologi yang merujuk pada internet memungkinkan akses informasi dan komunikasi bisa diakses oleh siapapun, kapanpun, dan dimanapun dengan begitu mudah dan cepat, yang seolah-olah membuat seluruh manusia, kata Ibrahim (dalam Fahrimal,

2018:69) secara digital berkumpul dalam waktu bersamaan dalam "sebuah piring besar". Kondisi ini, menurut Flowe dan Christakis (dalam Fahrimah, 2018:69) disebut sebagai *hyperconnected*, yakni hubungan hubungan yang dibangun dari orang-orang yang berasal dari berbagai latar belakang geografi dan demografi memiliki relasi yang saling terikat.

Salah satu media yang sangat populer di internet adalah media sosial. Wellyana, dkk., (2020:115) menyebutkan bahwa kemunculan media sosial ini diawali oleh Friendster dan MySpace, era Facebook dan Twitter, serta yang terbaru Google Plus. Sementara itu, Kaplan dan Haenlein (dalam Mustika, 2018:44) mengelompokan media sosial menjadi enam jenis, yang akan diuraikan lebih terperinci seperti berikut ini:

Jenis yang pertama adalah *collaborative project*, yakni media sosial yang memungkinkan para penggunanya untuk membuat sebuah konten secara bersamaan, di mana konten tersebut dapat diakses oleh pengguna lainnya dari seluruh dunia. *Collaborative project* ini bermanfaat untuk mendukung citra sebuah *brand*, perusahaan, publik figur, atau hal lainnya. Yang termasuk dalam media sosial jenis ini adalah Wikipedia.

Jenis media sosial yang kedua adalah *microblogs* dan *blogs. Microblogs* dan *blogs* adalah sebuah aplikasi yang memfasilitasi para penggunanya untuk menulis berbagai macam hal yang diminati. Misalnya opini, berita, kegiatan sehari-hari, tips dan trik, pengalaman unik, atau hal lain dalam bentuk gambar, teks, video, atau kolaborasi dari ketiganya. Contoh dari media sosial ini adalah wordpress.com atau blogspot.com.

Kemudian, jenis media sosial yang ketiga adalah *content communities. Content Communities* adalah sebuah aplikasi yang memungkinkan pengguna internet untuk berbagi konten menarik seperti foto dan video secara virtual baik secara langsung maupun tidak langsung. Media sosial ini banyak

digunakan karena menarik banyak perhatian khalayak. Bahkan banyak perusahaan kini beralih dari media konvensial kepada media digital jenis ini untuk meningkatkan citra perusahaan atau melakukan sosialisasi dari produk barang dan jasa yang mereka tawarkan.

Lalu, jenis media sosial yang keempat adalah situs jejaring sosial atau yang populer dikenal dengan istilah *social networking sites,* yakni sebuah situs yang memungkinkan penggunakan untuk berhubungan dengan pengguna lain dengan cara membuat profil diri pada akun media sosial yang mereka miliki. Situs jejaring sosial ini sangat berperan dalam membentuk *personal branding* seseorang atau *brand image* sebuah produk atau perusahaan karena sifatnya yang interaktif dan sangat mudah digunakan sebagai sarana komunikasi dengan cara membagikan koleksi teks, foto, maupun video. Selain menyebarkan informasi yang bersifat umum, media sosial jenis ini juga memungkinkan penggunanya untuk saling berhubungan secara pribadi dengan pengguna lain melalui fitur *direct message* atau *inbox.* Contohnya Instagram, Facebook, dan Twitter.

Jenis media sosial yang kelima adalah *virtual social world,* yakni sebuah aplikasi yang memungkinkan para penggunanya untuk measarakansimulasi dunia nyata melalui internet. Aplikasi ini digunakan pada saat pemainnya menggunakan avatar dan berinteraksi dengan pengguna lainnya.

Terakhir, jenis media sosial yang keenam adalah *virtual game world,* yakni sebuah permainan *multiplayer* di mana ratusan pemain secara simultan dapat saling berinteraksi dan memberikan dukungan dalam bermain bersama. Salah satu fitur unik dari media sosial jenis ini adalah karena tampilannya yang menarik karena memiliki desain grafis yang mencolok dan permainan warna yang baik, sehingga menyajikan suguhan yang informatif dan interaktif.

6.2. Pentingnya Etika Dalam Menggunakan Internet

Kita sama-sama tahu bahwa pada saat mengakses internet kita harus menggunakan berbagai perangkat teknologi canggih, baik perangkat keras maupun perangkat lunak. Meski begitu, pada saat kita melakukan interaksi di internet dan media sosial, pengguna internet di belahan dunia sana adalah manusia juga. Maka seluruh transaksi informasi yang terjadi di internet maupun di media sosial tentu saja tidak terlepas dari aspek etika.

Maka dari itu, *cyber-ethic* atau yang populer dikenal sebagai *netiquette* atau netiket menjadi hal yang sangat penting dikaji dalam aktivitas interaksi di dunia maya. Sebelum jauh mengenal tentang netiket, ada baiknya kita uraikan dulu apa itu etika.

Secara etimologis, etika berasal dari Bahasa Yunani, yakni kata "*ethos*" yang artinya kebiasaan atau adat. Setiyani (dalam Mutiah, 2019:16) mengatakan bahwa etika adalah sebuah teori tentang perbuatan yang dilakukan oleh manusia yang pada akhirnya menjadi bahan pertimbangan bagi manusia untuk menentukan mana yang baik dan buruk bagi kehidupannya.

Hal yang sama juga diungkapkan oleh Rofadhilah, dkk (2018:27) menyatakan bahwa etika adalah sebuah ilmu yang mengkaji tentang hal-hal perkara buruk dan baik yang ditentukan berdasarkan akal pikiran. Terakhir adalah pendapat dari K.Bertens (dalam Kusmastuti, dkk., 2021:17) yang mendefinisikan bahwa etika adalah sistem norma moral dan nilai yang menjadi panduan bagi sekelompok orang atau seseorang dalam mengatur tingkah lakunya.

Dari beberapa pengertian mengenai etika di atas, kita bisa menarik kesimpulan bahwa etika berkaitan dengan hal-hal berikut ini:

a. Jika dilihat dari sudut pandang sumbernya, etika bersumber dari aka pikiran.

b. Kemudian jika dilihat dari fungsinya, etika berfungsi sebagai pedoman dan penentu dalam menetapkan hal yang baik dan buruk dalam tingkah laku manusia

c. Terakhir, jika dilihat dari objeknya, etika fokus pada kajian tentang perbuatan yang dilakukan oleh manusia.

Sementara itu, menurut Magnis-Suseno (dalam Fahrimal, 2018:72) etika dapat dibagi ke dalam beberapa bentuk, yaitu:

a. Etika individu adalah sebuah etika mengatur kewajiban manusia sebagai seorang individu. Artinya etika dalam lingkup ini mengatur mengenai perilaku manusia dengan dirinya sendiri dan manusia dengan Ilahi yang diperantarai oleh suara hati.

b. Etika yang kedua adalah etika sosial yakni sebuah kewajiban yang mengatur manusia dengan manusia lainnya. Karena sifat dasar dari manusia adalah sebagai mahluk sosial yang saling memiliki ketergantungan dan tidak bisa hidup seorang diri.

c. Etika yang ketiga adalah etika umum yakni yang mempersoalkan prinsip dasar perilaku manusia secara umum.

d. Sementara itu, etika yang terakhir adalah etika khusus, yakni sebuah prinsip yang mengatur manusia dengan lingkup khusus kehidupannya.

6.3. Netiket

Sadar atau pun tidak, pada saat melakukan penjelajahan di internet kita meninggalkan sebuah jejak yang dikenal sebagai jejak digital. Menurut Kusmastuti dkk., (2021:23) jejak digital ini terbagi menjadi dua jenis, yakni jejak digital aktif dan jejak digital

pasif. Jejak digital aktif adalah jejak digital yang dibuat secara sadar. Misalnya Ketika seseorang mendaftarkan diri dalam sebuah situ atau aplikasi media sosial. Kemudian dia membuat konten berupa teks, gambar, atau tayangan audiovisual yang di-*share* secara sadar dan dapat dilihat maupun dibagikan oleh pengguna lainnya.

Sedangkan jejak digital pasif adalah jejak digital yang muncul secara otomatis tanpa pengguna sadari. Misalnya *history* dari kata kunci yang seseorang tinggalkan di mesin pencari atau *cookis* berupa data kecil saat orang tersebut berkunjung ke dalam sebuah situs. Oleh sebab itu, meskipun berinteraksi di dunia digital, setiap pengguna wajib berpegang pada nilai dan norma yang berlaku di kalangan masyarakat, agar tidak terjebak pada pelanggaran etika yang akan merugikan dirinya atau pengguna lain.

Etika sangat penting diaplikasikan di dunia maya karena pada kenyataannya, berdasarkan hasil riset yang dilakukan oleh Andina (dalam Fahrimal, 2018:73) menyatakan bahwa media sosial Facebook menjadi aplikasi yang paling memiliki banyak dampak negatif bagi para penggunanya. Beberapa kasus seperti pembulian siber, penipuan, penculikan, prostitusi, perjudian online, dan konflik akibat beda pendapat dan pemikiran terjadi pada media sosial ini. Berdasarkan riset yang dilakukan oleh Kowalski dan Whittaker (dalam Fahrimal, 2018:73) pelaku yang melakukan berbagai tindak pelanggaran etika tersebut didominasi oleh kaum remaja. Mereka umumnya menyerang teman sebaya di fitur komentar media sosial.

Maka dari itu, diperlukan etika khusus dunia maya yang bisa dijadikan panduan internet bagi pengguna internet, agar mereka bisa berselancar di dunia maya dengan aman, nyaman, dan bertanggungjawab. Panduan etika di internet tersebut disebut dengan netiket. Menurut Mustika (2018:44) netiket adalah panduan bagi pengguna internet dalam berperilaku dan bersikap

sesuai dengan kaidah nilai dan norma yang berlaku di seluruh dunia.

Sependapat dengan Mustika, Tedre (dalam Fahrimal, 2018:72) menyatakan bahwa netiket adalah tata cara dan aturan penggunaan internet sebagai alat komunikasi yang baik dan benar. Sama seperti di dunia nyata, Monggilo (dalam Fahrimal, 2018:73) mengatakan bahwa netiket mendorong penggunya untuk patuh pada aturan moral dan etis (baik yang tertulis maupun tidak tertulis) yang berguna untuk menciptakan ruang digital yang damai, nyaman dan tentram.

Lalu sebenarnya seperti apa netiket itu harus diterapkan? Berikut beberapa hal yang Mustika (2018:44) tentang netiket yang menjadi panduan pengguna internet dalam berselancar di dunia maya:

1. Tidak semuanya yang ada di internet itu benar, maka jangan mudah percaya pada berbagai informasi yang disajikan di internet;
2. Menghargai dan menghormati pengguna internet lain dengan cara:
    a. Tidak melakukan plagiat
    b. Tidak mengganggu privasi oranglain
    c. Tidak menggunakan huruf kapital terlalu banyak, karena huruf kapital umumnya menjadi indikasi kemarahan
    d. Tidak hal-hal illegal di internet
    e. Tidak membagikan berita bohong atau informasi yang belum jelas kebenarannya
    f. Tidak mengunggah konten teks, foto, atau video tanpa menyebutkan sumber asli

g. Tidak membagikan konten dan berkomentar yang memiliki unsur pornografi dan melanggar unsur SARA

h. Tidak membagikan komentar atau berbagi konten yang merendahkan dan melecehkan oranglain

i. Tidak berkomentar yang sifatnya adu domba, memaki, menyalahkan, bersengketa, mencela, menyinggung, dan menimbulkan konflik

3. Menjaga kemanan data pribadi dengan cara:

a. Tidak menyebarkan informasi pribadi dan sensitif

b. Melakukan pengamanan terhadap diri sendiri dengan cara memasang antivirus agar perangkat keras dan perangkat lunak yang dimiliki tetap aman sehingga aktivitas berselancar di dunia maya bisa optimal;

Sementara itu, berdasarkan panduan dari Uncw.edu (dalam Fahrimal, 2018:74) berikut adalah hal-hal yang harus perhatikan ketika seseorang mengakses internet. Yang pertama adalah kesadaran bahwa tidak ada kebebasan yang bersifat mutlak di internet, maka dari itu masyarakat dunia maya atau netizen harus membatasi diri mereka dengan cara memilih mana yang layak ditampilkan dan mana yang perlu diabaikan, perilaku ini dikenal dengan istilah *freedom of speech may not exist*.

Prinsip yang kedua adalah *accept the views of others*. Artinya bahwa setiap orang memiliki pendapat sendiri-sendiri, maka dari itu pada saat melakukan interaksi di dunia maya media sosial akan terjadi pertukuran ide dan gagasan, maka dari itu, pengguna internet harus menghargai dan menghormati setiap pendapat yang ada.

Prinsip yang ketiga adalah *avoid flame*, artinya jangan membuat ketegangan dengan orang lain. Kalaupun terjadi silang pendapat, maka sebaiknya pengguna internet berdiskusi untuk menemukan jalan keluar. Kemudian prinsip yang keempat

adalah *be safe*, perilaku ini memastikan setiap unggahan pengguna internet harus membuat pengguna lain merasa nyaman baik secara fisik maupun secara emosional.

Prinsip yang keempat adalah *avoid "death by emoticons"*, artinya pengguna internet harus menggunakan *emoticon* yang tepat pada saat mengekspresikan emosi yang mereka miliki, jangan berlebihan menggunakannya. Prinsip yang kelima adalah *choose your words carefully*, artinya pengguna internet harus bijak dalam memilih kalimat dan kata-kata dalam mengomentari sesuatu di Internet.

Prinsip yang keenam adalah *be constuctive*, yakni sebuah sikap yang menunjukkan komentar positif dan membangun untuk orang lain. Dan prinsip terakhir adalah *remember, we're all human*, yakni ingatan bahwa seluruh pengguna internet adalah manusia yang punya perasaan yang harus dihargai dan dihormati.

Bab 7

Prosedur Pendirian Usaha di Bidang Teknologi Infomasi

7.1 Pengantar

Revolusi industry 4.0 merupakan revolusi industri yang dapat dikatakan berbeda dengan revolusi industry sebelumnya. Semua disiplin ilmu, industri, ekonomi dan pemerintah dipengaruhi oleh kemajuan teknologi baru yang mengintegrasikan dunia fisik, digital dan biologis. Sehingga kekuatan digital adalah hal yang saat ini paling dibutuhkan dalam menghadapi era 4.0 ini. Dengan lahirnya teknologi digital yang berdampak kuat pada kehidupan manusia di seluruh dunia merupakan puncak dari revolusi industri. Didalam semua proses aktivitas melalui sistem otomatisasi pada revolusi industri terkini atau generasi keempat. Seperti yang di sampaikan oleh Presiden Joko Widodo, perubahan-perubahan yang mungkin tak terduga sebelumnya telah terjadi pada revolusi industri 4.0. Seperti menyaksikan pertarungan antara taksi online versus taksi konvensional atau ojek online versus ojek pangkalan. Pada akhirnya semua itu berdampak kepada publik, dimana dalam hal ini publik diuntungkan dengan menjadi lebih mudah untuk mendapatkan layanan transportasi dan bahkan dengan harga yang sangat terjangkau.

Tidak dipungkiri bahwa salah satu skill terpenting yang harus dikuasai masyarakat pada umumnya adalah teknologi informasi, sehingga ini yang mendorong untuk mendirikan usaha dibidang teknologi informasi, misalnya lembaga pendidikan dan pelatihan.

Sampai saat ini, peluang usaha untuk kursus komputer masih memiliki prospek bisnis yang cukup bagus dan profitable. Sehingga dapat menjadi kran pengisi rekening keuangan yang bisa diandalkan dari profit usaha jasa kursus komputer. Salah satu alasan memilih lembaga kursus komputer sebagai tempat belajar yang nyaman adalah kebutuhan untuk penguasaan aplikasi komputer dengan sistem belajar yang fleksibel dan *friendly* terutama bagi mereka yang sudah bekerja. Sampai saat ini, prospek kursus komputer masih sangat menjanjikan. Meskipun penguasaan aplikasi komputer sudah banyak diajarkan di sekolah-sekolah formal, akan tetapi kebutuhan untuk menguasai aplikasi tertentu dengan durasi waktu belajar lebih singkat dan jam belajar yang lebih fleksibel menjadikan lembaga kursus komputer tetap dicari banyak orang.

Pemilihan wilayah padat penduduk dan lingkungan industry menjadi nilai tersendiri dalam mendirikan kursus komputer. Sehingga tidak dipungkiri bahwa kebutuhan akan penguasaan IT sungguh sangat dibutuhkan. Apalagi usaha dan bisnis yang berkembang sangat membutuhkan dunia IT untuk melakukan marketing dengan target penaikan omset penjualan. Selain itu pemilihan wilayah dengan banyak sekolah dan kampus yang menjadi target dan peluang pasar juga menjadi penilaian untuk dijadikan target marketing nantinya.

7.2 Profil Bisnis

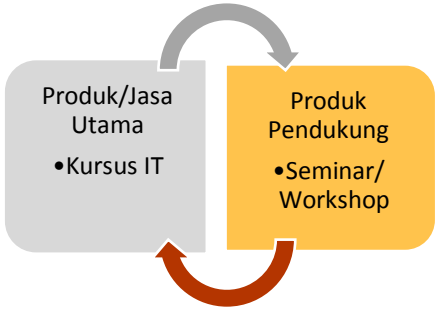
Profil bisnis atau *business profile* merupakan sebuah deskripsi atau penggambaran secara singkat sebuah perusahaan yang berisi mengenai sejarah pendirian, status dan tujuan jangka

pendek dan jangka panjang yang hendak dicapai. Intinya, profil bisnis akan berisi tentang semua informasi penting yang berkaitan dengan bisnis yang dijalankan oleh perusahaan. Profil bisnis berfungsi untuk identitas usaha yang bertujuan untuk membuat calon klien atau pihak yang akan bekerjasama semakin tertarik dengan perusahaan. Profil bisnis sebagai bentuk deskripsi atau penggambaran perusahaan berisi tentang nama, *tagline*, visi dan misi dari bisnis hingga target besar yang akan dicita-citakan sebagai arah dan tujuan yang akan dicapai kedepannya.

Dalam menentukan gambaran umum usaha, pemilihan nama, lokasi, rencana berdiri, registrasi perusahaan, dan lingkup bisnis merupakan bagian yang harus di tentukan terlebih dahulu. Selanjutnya menentukan visi dan misi usaha. Hal ini juga sejalan dengan *tagline* yang akan diusung perusahaan. Kemudian, target jangka pendek dan jangka panjang harus ditetapkan sehingga akan menentukan arah jalannya usaha.

7.3 Detail Produk dan Jasa

Bagian penting dari sebuah bisnis di bidang IT adalah produk atau jasa yang ditawarkan. Sebagai contoh, produk yang utama dijalankan adalah pada bagian pelatihan dan kursus dibidang IT. Semua sub-sub yang berada dibawah IT diupayakan untuk dibuka sesuai dengan kemampuan SDM yang sudah di rencanakan.



Gambar 7.1. *Produk Utama dan Pendukung*

Untuk melaksanakan pelatihan di bidang IT dapat dikategorikan menjadi beberapa kategori, diantaranya:

1. *Programming,* terdiri atas pemrograman berbasis web, *mobile, desktop* serta *Internet of Thing*
2. Komputer dan Jaringan, terdiri atas perakitan dan *maintenance PC, Mikrotik,* dan *CISCO*
3. *Digital Marketing*, terdiri atas internet *marketing* dan Teknik SEO
4. Multimedia, terdiri atas desain grafis, *editing video,* animasi,
5. Aplikasi Perkantoran, terdiri atas aplikasi komputer akuntansi, ERP dan *Microsoft Office*

Untuk produk pendukung, seperti mengadakan seminar dan workshop merupakan peluang pasar yang cukup menjanjikan. Kesesuaian topik yang diangkat dan tren saat ini memegang peranan penting dalam jenis bisnis ini.

7.4 Analisis Pasar dan SWOT

Saat hendak memulai bisnis, melakukan analisis pesaing adalah hal yang harus dilakukan. Pasalnya, dengan begini dapat mengidentifikasi ancaman, kesempatan, atau permasalahan strategi yang akan terjadi. Analisis pesaing adalah bidang analisa

strategis yang spesialisasinya dalam pengumpulan dan analisis informasi tentang perusahaan pesaing. Ini merupakan taktik penting untuk mengetahui apa yang di lakukan oleh pesaing dan jenis ancaman apa yang mereka hadirkan bagi kesejahteraan finansial bisnis.

1. Kenali para pesaingmu, seperti apa mereka? Pesaing Langsung / Pesaing Tidak Langsung
2. Monitor strategi media sosial pesaing kamu
3. Analisa bagaimana pesaing memasarkan produk
4. Perhatikan struktur **SEO** pesaing
5. Mengetahui harga produk pesaing
6. Lakukan analisa **SWOT**

Gunakan beberapa pertanyaan sebagai pemandu, seperti:

1. Apa hal yang membuat pesaing lebih baik (dalam hal produk, pemasaran konten, media sosial, dan lain-lain)
2. Di mana letak keunggulan pesaing yang tidak di miliki?
3. Apa kelemahan pesaing?
4. Pada hal apa kamu lebih unggul?
5. Di bidang apa kamu akan menganggap pesaing ini sebagai ancaman?
6. Apakah ada peluang di pasar yang diidentifikasi pesaingmu?

Analisis ini didasarkan pada logika yang dapat memaksimalkan kekuatan (**Strengths**) dan peluang (**Opportunities**), namun secara bersamaan dapat meminimalkan kelemahan (**Weaknesses**) dan ancaman (**Threats**).

Gambar 7.1 *Contoh analisis SWOT*

7.5 *Marketing* dan Pengembangan

Dalam memulai usaha perlu adanya marketing yang sesuai, sehingga target kita bisa terpenuhi. Marketing di bidang IT ini bisa dilakukan dengan beberapa cara, misalnya *marketing* dengan cara pembuatan website dan *email marketing*, *marketing* melalui sosial media, seperti Instagram, Facebook dan WhatsApp, sebar brosur-brosur, dan penawaran langsung ke sekolah dan instansi melalui proposal.

7.6 Operasional dan Manajemen

Dalam pelaksanan operasional bisnis, perlu dilakukan perencanaan dalam memilih tempat, produk, tim/SDM dan alur operasional dari system. Pada memilihan lokasi, harus dijelaskan kelebihan dan kekurangan lokasi sebagai tempat usaha. Pada pemilihan produk dan peralatan, harus dijelaskan produk utama yang akan diproduksi/dijalankan beserta peralatan dan kebutuhannya, lengkap dengan flowchart proses bisnis usaha yang diangkat. Dalam hal SDM, ini meliputi struktur organisasi dari usaha yang dijalankan seperti (CEO,

CFO, CTO, HRD, Keuangan, Programmer, dan lain sebagainya) mencakup *job description* masing-masing bagian.

7.7 Rencana Keuangan

Keuangan bisnis harus dipahami ketika menjalankan bisnis. Untuk memulai suatu usaha, perencanaan keuangan harus diperjelas dari awal. Perencanaan keuangan memegang peranan penting untuk menjelaskan target pendapatan sesuai dengan produk atau jasa yang ditawarkan. Pengelolaan perencanaan keuangan dan pendanaan yang kurang tepat dapat membuat kegagalan dalam mulai berbisnis. Pengelolaan keuangan harus menyeluruh agar dapat bermanfaat dalam usaha dan dapat membantu seluruh komponen usaha dalam mengambil keputusan usaha bersama. Beberapa manfaat dalam merencanakan keuangan bisnis antara lain:

1. Mengetahui pertumbuhan penghasilan
2. Mengetahui pertumbuhan arus kas
3. Membantu dalam investasi
4. Menciptakan asset
5. Meraih tujuan jangka panjang

Rencana keuangan ini dapat dibuat berupa simulasi pendapatan perbulan dan pertahun. Contoh simulasi target pendapatan tahun pertama dapat dilihat pada Gambar 3. Simulasi taget pendapatan ini sebaiknya dibuat per bulan selama beberapa tahun sehingga dapat di simulasikan pembagian hasil dan simulasi resiko.

Simulasi Target Pendapatan TAHUN 1

Simulasi Target Pendapatan Perbulan

Target Estimasi Pendapatan Tahun 1											
PROGRAM	SUB-PROGRAM	KELAS	EST. JAM	EST. BULAN	HARGA PAKET	HARGA BULAN	TARGET PESERTA	TARGET PENDAPATAN	BIAYA PENGAJAR	Marketing Fee	TARGET OMSET
MULTIMEDIA	Desighn Graphics	Basic(SD,SMP,SMA)	18	2,25	1.500.000	666.667	2	1.333.333	600.000	66.667	666.667
		Advance(SMA, Umum)	18	2,25	2.000.000	888.889	2	1.777.778	600.000	88.889	1.088.889
	Editing Audio Video	Advance(SMA, Umum)	18	2,25	2.000.000	888.889	2	1.777.778	600.000	88.889	1.088.889
	Animasi	Basic(SD,SMP,SMA)	18	2,25	1.000.000	444.444	3	1.333.333	600.000	66.667	666.667
		Advance(SMA, Umum)	18	2,25	1.500.000	666.667	2	1.333.333	600.000	66.667	666.667
	Coding For Kids	Reguler(SD,SMP)	18	2,25	1.000.000	444.444	2	888.889	600.000	44.444	244.444
	Auto Cad	Reguler	12	1,5	1.500.000	1.000.000	2	2.000.000	600.000	100.000	1.300.000
KOMPUTER JARINGAN	Mikrotik	Reguler	12	1,5	1.500.000	1.000.000	3	3.000.000	600.000	150.000	2.250.000
	Cisco	Reguler	12	1,5	2.000.000	1.333.333	2	2.666.667	600.000	133.333	1.933.333
	Perakitan & Maintencan PC	Reguler	12	1,5	1.500.000	1.000.000	3	3.000.000	600.000	150.000	2.250.000
PROGRAMMING	Pemograram Web	Basic(SD,SMP, SMA)	18	2,25	1.500.000	666.667	3	2.000.000	600.000	100.000	1.300.000
		Advance(SMA, Umum)	18	2,25	2.000.000	888.889	3	2.666.667	600.000	133.333	1.933.333
		Framework (SMA,UMUM	18	2,25	2.500.000	1.111.111	3	3.333.333	600.000	166.667	2.566.667
	Pemograman Android	Basic(SD,SMP)	18	2,25	1.500.000	666.667	2	1.333.333	600.000	66.667	666.667
		Advance(SMA, Umum)	18	2,25	2.000.000	888.889	2	1.777.778	600.000	88.889	1.088.889
	Pemograman Desktop	Basic(SD,SMP)	18	2,25	1.500.000	666.667	2	1.333.333	600.000	66.667	666.667
		Advance(SMA, Umum)	18	2,25	2.000.000	888.889	2	1.777.778	600.000	88.889	1.088.889
	Internet of Things	Reguler	18	2,25	1.500.000	666.667	2	1.333.333	600.000	66.667	666.667
OFFICE	Aplikasi Office	Basic(SD,SMP,SMA)	12	1,5	1.000.000	666.667	2	1.333.333	600.000	66.667	666.667
		Advance(SMA, Umum)	12	1,5	1.500.000	1.000.000	2	2.000.000	600.000	100.000	1.300.000
	Computer Akuntasi	Reguler	12	1,5	1.500.000	1.000.000	2	2.000.000	600.000	100.000	1.300.000
DIGITAL MARKETING	Toko Online	Reguler	8	1	1.000.000	1.000.000	2	2.000.000	600.000	100.000	1.300.000
	InterneT Marketin & SEO	Reguler	8	1	1.000.000	1.000.000	2	2.000.000	600.000	100.000	1.300.000
BIMBINGAN SKRIPSI	Bimbingan Skripsi	Reguler	10	1,25	500.000	400.000	2	800.000	600.000	40.000	160.000
Total							54	44.800.000	14.400.000	2.240.000	28.160.000

Gambar 7.3 *Simulasi Target Pendapatan Tahun Pertama*

Untuk pembagian hasil dan resiko, dapat dibuatkan rencana capaian omset per tahun. Dalam simulasi pada Gambar 4, dibuatkan juga perkiraan pengeluaran, investasi awal, kebutuhan dana awal dan simulasi resiko.

Simulasi Pembagian Hasil Dan Simulasi Resiko

Simulasi Target Pendapatan vs Pengeluaran dan Analisa Resiko

Detail Omset - Pengeluaran	Tahun 1	Tahun 2	Tahun 3	Tahun 4
Laba Kotor/bulan	28.160.000	31.326.667	35.295.556	35.760.000
Pengeluaran				
1 Biaya Marketing	2.000.000	1.500.000	1.300.000	1.200.000
2 biaya pemeliharaan	1.500.000	1.000.000	1.000.000	1.000.000
3 payroll (3 sales, 1 admin)	8.000.000	8.000.000	8.000.000	8.000.000
4 biaya operasional	1.500.000	1.200.000	1.200.000	1.200.000
5 biaya penyesutan	1.000.000	1.000.000	1.000.000	1.000.000
6 biaya listrik	1.000.000	1.000.000	1.000.000	1.000.000
7 biaya air	100.000	100.000	100.000	100.000
8 biaya internet	500.000	500.000	500.000	500.000
Total Pengeluaran	15.600.000	14.300.000	14.100.000	14.000.000
Omset Bersih/Bulan	12.560.000	17.026.667	21.195.556	21.760.000

Investasi Awal	100.000.000	setor	kas
Omset Bersih Tahun 1	45.216.000	31.651.200	9.495.360
Omset Bersih Tahun 2	61.296.000	42.907.200	12.872.160
Omset Bersih Tahun 3	76.304.000	53.412.800	16.023.840
Omset Bersih Tahun 4	78.336.000	54.835.200	16.450.560
Total Dana Kembali 4 Tahun	261.152.000	182.806.400	54.841.920

no	Simulasi Resiko	total aset	setor	kas	kembali
1	Tahun 1	30.000.000	31.651.200	9.495.360	71.146.560
2	Tahun 2	20.000.000	74.558.400	22.367.520	116.925.920
3	Tahun 3	15.000.000	127.971.200	38.391.360	181.362.560
4	Tahun 4	10.000.000	182.806.400	54.841.920	247.648.320

Kebutuhan Dana Awal				
no	Item	qty	price	total
1	Meja	6	550.000	3.300.000
2	Kursi	12	100.000	1.200.000
3	AC	2	3.500.000	7.000.000
4	Infocus	2	5.000.000	10.000.000
5	Laptop Second+acc	5	2.200.000	11.000.000
6	Biaya Sewa	1	35.000.000	35.000.000
7	renov	1	5.000.000	5.000.000
8	perijinan	1	5.000.000	5.000.000
9	marketing	1	10.000.000	10.000.000
10	Operasional	1	12.500.000	12.500.000
Total				100.000.000

Simulasi Omset Tahun Ke-1					
Bulan ke	laba bersih	Investor	Setor	Kas	Pengelola
		30%	70%	30%	70%
1	12.560.000	3.768.000	2.637.600	791.280	8.792.000
2	12.560.000	3.768.000	2.637.600	791.280	8.792.000
3	12.560.000	3.768.000	2.637.600	791.280	8.792.000
4	12.560.000	3.768.000	2.637.600	791.280	8.792.000
5	12.560.000	3.768.000	2.637.600	791.280	8.792.000
6	12.560.000	3.768.000	2.637.600	791.280	8.792.000
7	12.560.000	3.768.000	2.637.600	791.280	8.792.000
8	12.560.000	3.768.000	2.637.600	791.280	8.792.000
9	12.560.000	3.768.000	2.637.600	791.280	8.792.000
10	12.560.000	3.768.000	2.637.600	791.280	8.792.000
11	12.560.000	3.768.000	2.637.600	791.280	8.792.000
12	12.560.000	3.768.000	2.637.600	791.280	8.792.000
	150.720.000	45.216.000	31.651.200	9.495.360	105.504.000

Simulasi Omset Tahun Ke-1					
Bulan ke	laba bersih	Investor	Setor	Kas	Pengelola
		30%	70%	30%	70%
1	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
2	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
3	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
4	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
5	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
6	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
7	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
8	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
9	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
10	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
11	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
12	17.026.667	5.108.000	3.575.600	1.072.680	11.918.667
Jumlah	204.320.000	61.296.000	42.907.200	12.872.160	143.024.000

Simulasi Omset Tahun Ke-2					
1	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
2	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
3	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
4	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
5	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
6	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
7	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
8	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
9	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
10	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
11	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
12	21.195.556	6.358.667	4.451.067	1.335.320	14.836.889
Jumlah	254.346.667	76.304.000	53.412.800	16.023.840	178.042.667

Simulasi Omset Tahun Ke-4					
1	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
2	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
3	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
4	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
5	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
6	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
7	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
8	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
9	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
10	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
11	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
12	21.760.000	6.528.000	4.569.600	1.370.880	15.232.000
Jumlah	261.120.000	78.336.000	54.835.200	16.450.560	182.784.000

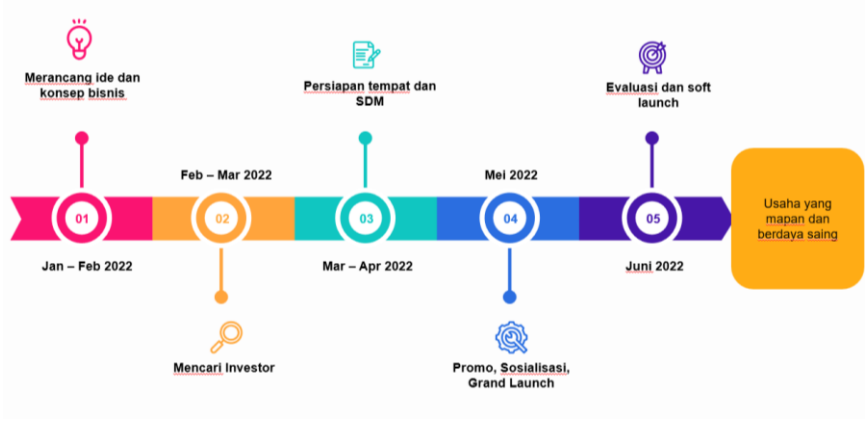
Gambar 7.2 *Simulasi Keuangan*

7.8 Rencana Resiko

Rencana resiko ini menyangkut rencana kedua untuk menyelamatkan keuangan/bisnis jika terjadi kegagalan usaha. Harus ada simulasi diawal tentang pembagian hasil, asset dan modal jika terjadi failed usaha. Dalam perjanjian ikatan kerja harus ada kejelasan jika sesama pemilik modal jika terjadi kegagalan usaha.

7.9 Schedule Setup

Pada bagian ini, perlu untuk menentukan *timeline* bagi pelaku usaha untuk nelakukan *setup* usaha hingga usaha berjalan normal. Kedisplinan dalam pengaturan waktu menjadi penentu terhadap capaian baik jangka pendek maupun jangka panjang. Berikut contoh gambaran proses membangun bisnis.



Gambar 7.3 *Gambaran Proses Membangun Bisnis*

7.10 Penutup

Idealnya, dalam pendirian usaha di bidang IT perlu mengikuti beberapa tahapan yang ada, mulai dari perencanaan hingga pelaksanaan usaha, namun adakalanya dalam memulai usaha dimulai dari modal nekat dan kesungguhan, tidak sedikit usaha/bisnis dibidang IT yang bertahan dan bahkan menjadi *Unicorn*. Dari sekian banyak usaha dibidang IT yang

berkembang, tidak sedikit juga yang bahkan harus gulung tikar. Dalam hal ini, manajemen risiko juga harus dipertimbangkan.

Bab 8

Sertifikasi Profesi IT dan Lembaga Yang Mengadakannya

8.1 Sertifikasi Profesi

Sertifikasi merupakan penetapan yang diberikan suatu organisasi setelah melalui proses pengujian terhadap kemampuan atau suatu keahlian. Sedangkan sertifikasi profesi merupakan pemberian pengakuan atas keterampilan, kemampuan maupun keahlian untuk profesi tertentu.

Sertifikasi memiliki bebagai jenis antara lain :

1. Sertifikasi akademik yang memberikan gelar Diploma, Sarjana, Master dan lain-lain.
2. Sertifikat Kompetensi Kerja, yaitu proses pemberian sertifikat kompetensi yang dilakukan secara sistematis dan objektif melalui uji kompetensi yang mengacu kepada Standar Kompetensi Kerja Nasional Indonesia (SKKNI), standar internasional atau standar khusus. (BPPTIK Kominfo, 2021)
3. Sertifikasi profesi, yaitu suatu sertifikasi yang diberikan berdasarkan keahlian tertentu untuk profesi tertentu.

Tujuan dari sertifikasi antara lain :

1. Membentuk tenaga praktisi TI yang berkualitas tinggi
2. Membentuk standar kerja TI yang tinggi
3. Pengembangan profesional yang berkesinambungan.

8.2 Profesi Di Bidang IT

Berbagai profesi di bidang IT (Fitriawati, 2019) antara lain :

1. Sistem analist.

   System analist Bertanggung jawab atas penelitian, perencanaan, pengkoordinasian, dan merekomendasikan pemilihan perangkat lunak dan sistem. Ruang lingkup pekerjaan system analist :

   a. Menganalisa sistem yang sudah ada dan membuat feasibility pengembangan sistem.
   b. Mengembangkan solusi yang paling efisien dan efektif.
   c. Menentukan teknologi yang akan digunakan dalam solusi pembangunan atau perancangan sistem.
   d. Menentukan framework dan standar implementasi pekerjaan yang akan digunakan dalam pembangunan dan pengembangan sistem.
   e. Mengarahkan tim dalam pengembangan agar dapat bekerja secara sinkron dan terarah.

2. Programmer

   Profesi yang bertugas untuk membuat sebuah program melalui bantuan bahasa pemograman yang dapat digunakan menyelesaikan permasalahan melalui otomatisasi dengan bantuan software. Berikut kualifikasi kompetensi yang harus dimiliki oleh seorang programmer :

- Mengenal teknologi dengan baik
- Memiliki logika yang baik dan algoritma yang efektif untuk memecahkan suatu masalah. Memahami bahasa pemograman(min. satu bahasa)
- Mengenal beragam sistem operasi.

3. Website programmer

   Profesi ini memiliki pekerjaan yang spesifik yaitu membuat aplikasi dengan hanya berbasiskan web saja. Pembuatan aplikasi ini berbasiskan web dan disimpan dalam sebuah server dimana memiliki service yaitu web server. Berikut ini merupakan kualifikasi kompetensi menjadi seorang web programmer.

   - Client – side scripwriting: Javascript
   - Server-side scripting: PHP, ASP, .NET, PERL, Python, Ruby
   - Database: MySQL, Oracle, PostgreSQL

4. Web Desainer

   Profesi ini mendesain halaman-halaman dari sebuah situs web yang mempunyai jiwa seni tinggi. Ruang Lingkup Kegunaan, standar W3C untuk HTML dan CSS dan kompabilitas tampilan pada browser yang berbeda. Menggarap, mengeskplorasi, dan mengimplementasikan tata letak dan artistik halaman web serta aspek komunikasi dari keduanya. Berikut ini merupakan kualifikasi kompetensi menjadi seorang web desainer:

   - Client – side scripwriting
   - Cascading Style sheets
   - HTML
   - Manipulasi gambar

- Animasi

5. Technical Engineering

   Atau teknisi, memelihara maupun memperbaiki perangkat yang berhubungan dengan perangkat sistem komputer. Ruang Lingkup Menguasai berbagai macam teknik troubleshooting dan penanganannya, seorang teknisi komputer juga harus mempunyai sikap yang baik sebagai seorang teknisi. Berikut ini adalah kualifikasi kompetensi yang harus dimilikidan dipahamimenjadi seorang teknisi :

   - Harus mengetahui dan menguasai berbagai macam dan tipe perangkat komputer yang ada didalamnya.
   - Harus mengetahui berbagai permasalahan kerusakan pada komputer (troubleshooting) dan menaganinya.
   - Mempunyai kemampuan untuk mengembangkan pengetahuan dan pengalaman sebgai panduan saat melakukan troubleshooting.
   - Memiliki kemampuan yang cukup dalam berbahasa inggris agar lebih mudah mempelajari manual perangkat hardware maupun software Komputer.

6. Network Engineering

   Atau arsitek jaringan desain dan pengimplementasian jaringan komputer, fokus dalam desain dan merencanakan. Adapun ruang lingkup pekerjaan seorang network engineer adalah :

   - Dapat bekerja pada sistem jaringan komputer.
   - Memasang, mendukung dan memelihara server hardware dan infrastruktur software baru.
   - Memonitor penggunaan jaringan.

- Memastikan cost-effective dan efisiensi penggunaan server.

7. System Administrator

   Atau admin, sysadmin, site admin, dll. Mampu memelihara dan menyelesaikan permasalahan pada bidang IT. Adapun ruang lingkup pekerjaan seorang system administrator adalah :

   - melakukan administrasi terhadap system,
   - melakukan pemeliharaan sistem
   - memiliki kewenangan menggunakan hak akses terhadap sistem , serta hal-hal lain yang berhubungan dengan pengaturan operasional sebuah sistem.

   Adapun kualifikasi kompetensi dari system administrator adalah :

   - Mengenali semua hardware yang ada di lingkungan kerja.
   - Menguasai lebih dari satu sistem operasi.
   - Memahami aplikasi yang sering digunakan, sesuai dengan aplikasi yang dipakai oleh perusahaan.
   - Memiliki ilmu pengetahuan dan pengalaman dalam bidang teknologi informasi, khususnya dalam hal supporting sistem, mulai dari pelacakan masalah (troubleshooting) hardware dan software

8. Game Developer

   Profesi game developer terbagi ke dalam beberapa bidang: Team leader, game designer, produser, programmer, artist, composer (music editor), script and text editor, cinematic.

9. Graphic Desainer

   Ahli dalam menggunakan grafis/gambar/apa saja yang berkaitan dengan penciptaan tanda, skema, logo, grafis, gambar, simbol, desain geometric dan lainnya, desainer grafis terlatih menggunakan program desain seperti Photoshop, Illustrator, Flash dan lainnya.

10. Animator

    Menciptakan berbagai ragam gambar yang akan membentuk ilusi seolah-olah bergerak pada saat ditayangkan dengan cepat yang disebut dengan frame.

8.3 Jenis Sertifikasi Kompetensi Di Bidang IT

Sertifikasi kompetensi dibidang IT dikategorikan menjadi :

1. Sertifikasi di bidang database. Contoh : Oracle.
2. Sertifififikasi di bidang bahasa pemrograman. Contoh : Unity, Java, Javascript, PHP, dan lain-lain.
3. Sertifikasi di bidang jaringan. Contoh : CISCO.
4. Sertifikasi di bidang Office. Contoh : Microsoft Office, Microsoft Excel.
5. Sertifkasi di bidang Computer Graphics dan Multimedi.

Beberapa contoh sertifikasi kompetensi yang telah diselenggarakan oleh BPPTIK Kominfo antara lain Pelatihan dan Sertifikasi bidang TIK berbasis SKKNI di bidang :

1. Pelatihan Teknisi Utama Jaringan Komputer
2. Pelatihan Junior Graphic Designer
3. Pelatihan Junior Network Administrator
4. Pelatihan Junior Web Developer

5. Pelatihan Junior Office Operator
6. Pelatihan Junior Web Developer
7. Pelatihan Junior Office Operator
8. Pelatihan Junior Network Administrator
9. Pelatihan Teknisi Utama Jaringan Komputer
10. Pelatihan Intermediate Animator
11. Pelatihan Introduction to Cybersecurity - Cybersecurity Essentials
12. Pelatihan Junior Office Operator
13. Pelatihan Junior Web Programming
14. Programming Essentials in Python

8.4 Jenis Sertifikasi Profesi Di Bidang IT

Berbagai profesi di bidang IT yang membutuhkan sertifikasi antara lain :

1. CCNA (*Cisco Certified Network Associate*) Sertifikasi Cisco ini adalah sertifikasi yang paling populer, program CCNA meliputi keterampilan administrasi dasar untuk *entry level* jaringan profesional yang bekerja dengan *mid-sized routed* dan *switched networks*. Keterampilan ini mencakup WAN, *IP address* dan protokol lainnya, jaringan nirkabel, dan keamanannya. Robert Half memperkirakan bahwa pemegang sertifikasi CCNA dapat meningkatkan gaji sebesar 9 persen. Daftar gaji tahunan *Global Knowledge*, rata-rata untuk mereka yang memegang CCNA adalah $ 79,536.
2. CCIE (*Cisco Certified Internetwork Expert*) CCIE, adalah sertifikasi Cisco dengan tingkat level tertinggi, dirancang untuk insinyur ahli jaringan. Menurut Cisco, Kurang dari 1 persen pekerja bidang jaringan profesional di seluruh dunia memiliki sertifikasi CCIE. Cisco tidak lagi melaporkan jumlah

sertifikasi yang telah diberikan, tetapi pada tahun 2011 perkiraan tidak resmi menyebutkan angka 5.496 di Amerika Serikat, CCIE dipandang sebagai salah satu sertifikasi yang paling menguntungkan. Sebagai contoh, Foote Partners memberi peringkat CCIE kedua setelah ahli desain *Cisco Certified* sebagai sertifikasi jaringan pembayar tertinggi pada tahun 2011. Mereka yang memegang CCIE *Routing* dan *Switching credential* dilaporkan mendapat gaji rata-rata $ 120,008, menurut *Global Knowledge*.

3. RHCE (*Red Hat Certified Engineer*) RHCE ditargetkan untuk *senior system administrators* yang bekerja dengan sistem Linux enterprise. Dibangun pada sertifikasi RHCSA dasar, sertifikasi RHCE meliputi IP *traffic routing*, *virtual host* dan konfigurasi *Private Directory* dan untuk Keterampilan sistem Red Hat tingkat menengah. Red Hat adalah satu-satunya Linux *credential* yang dimasukkan pada tahun 2012 dalam daftar sertifikasi Robert Half Technology. RHCE juga merupakan penghasil gaji tertinggi dalam sertifikasi Linux, dengan gaji rata-rata $ 92,322 pada tahun 2011 survei *Global Knowledge*.
4. MCTS (*Microsoft Certified Technology Specialist*) MCTS dan MCITP menawarkan pelatihan teknologi terbaru seperti Microsoft Exchange Server 2010, Windows Server 2008 dan SQL Server 2008. Tingginya permintaan pada bidang yang meliputi MCTS: Windows Server 2008 R2, Server atau Desktop Virtualisasi. MCTS sangat cocok untuk profesional IT atau pengembang dengan setidaknya satu tahun pengalaman.
5. Para Profesional dengan MCTS berpendapatan rata-rata $ 73,474 dalam laporan *Global Knowledge* tahun 2011. Catatan Robert Half bahwa dukungan staf IT dapat mengklaim dorongan laba 6 persen untuk Windows Server 2008 expertise. Keterampilan SharePoint bisa menambahkan premi

gaji 12 persen untuk pengembang di Amerika Serikat, sementara keterampilan database SQL Server dilaporkan bisa meningkatkan gaji sebesar 10 persen untuk profesional database.

6. MCITP (*Microsoft Certified IT Professional*) *Microsoft's intermediate-level credential* dibangun di atas sertifikasi MCTS. Bidang sertifikasi utama meliputi Enterprise Desktop Administrator, Server Administrator dan Enterprise Messaging Administrator. *Global Knowledge* menunjukkan bahwa MCITP Enterprise Administrator bersertifikat profesional mendapatkan penghasilan rata-rata $ 79,824.

7. PMP (*Project Management Professional*) PMP, dianggap sebagai standar yang paling menguntungkan untuk manajer proyek, tersedia untuk calon dengan setidaknya tiga tahun pengalaman industri, gelar sarjana dan 35 jam pendidikan manajemen proyek. PMP memvalidasi keterampilan yang diperlukan untuk memimpin sebuah proyek teknologi, termasuk perencanaan, penganggaran dan pelaksanaan proyek. Menurut *Project Management Institute*, profesional PMP meningkatkan daya penghasilan mereka sebesar 10 persen. Robert Half memperkirakan bahwa manajer proyek menerima $ 76,250 hingga $ 113,000 di Amerika Serikat pada 2011. Dengan PMP, gaji rata-rata bisa mencapai $ 103,570, kata Global Knowledge.

8. CISSP (*Certified Information Systems Security Professional*) Sertifikasi CISSP dari (ISC)^2 adalah salah satu top-produktif sertifikasi dalam bidang keamanan, dengan gaji rata-rata $ 100,735 per *Global Knowledge*. Para profesional bidang Keamanan dengan setidaknya lima tahun pengalaman dapat mengikuti sertifikasi ini. Dikenal diantara *PCWorld's IT* sertifikasi di tahun 2010, CISSP memvalidasi kompetensi dalam berbagai bidang seperti keamanan arsitektur,

kriptografi, keamanan telekomunikasi, keamanan pengembangan aplikasi dan masih banyak lagi.

9. CCSA (*Check Point Certified Security Administrator*) *Check Point's* sertifikasi CCSA dan CCSE tergabung di CISSP terdaftar pada Robert Half Technology dari *security credentials* dengan permintaan terbesar pada tahun 2012. kualifikasi CCSA tingkat awal, membutuhkan pengetahuan dasar tentang jaringan. Para profesional CCSA menunjukkan kemampuan administrasi untuk sistem Check Point 3D *Security*, dari implementasi dan konfigurasi untuk manajemen sehari-hari. *Global Knowledge* melihat upah rata-rata $ 93,512 untuk CCSA bersertifikat profesional, sementara Robert Half menghitung bahwa keterampilan administrasi *Check Point Firewall* dapat menambahkan premi gaji 7 persen.
10. Vmware *Certified Professional* Keterampilan bidang virtualisasi berada di bagian atas daftar keinginan pengusaha IT pada tahun 2012. Robert Half menyebut VCP sertifikasi virtualisasi merupakan permintaan terbesar untuk 2012 dan memprediksi premi gaji dari 9 persen untuk para profesional internet serta system engineers dengan kualifikasi ini. VCP menunjukkan keterampilan dalam penyebaran dan administrasi perusahaan teknologi virtualisasi VMware vSphere 4. Trek yang berbeda mengakomodasi tingkat keterampilan baik dasar dan lanjutan. Tidak ada penghitungan resmi untuk VCPs di seluruh dunia, tetapi masyarakat VCP memperkirakan ada lebih dari 20.000 profesional bersertifikat. *Global Knowledge* menunjukkan pendapatan sebesar $ 87,151 untuk IT pro dengan sertifikasi ini.
11. Comp IAA+ untuk entry level dukungan IT profesional, sertifikasi A+ tetap merupakan vendor- neutral credential penting. Teknologi perusahaan seperti Dell dan Intel, dan

pemerintah federal, mendukung dan memerlukan sertifikasi A+ untuk pekerjaan teknisi servis IT. Sertifikasi ini mencakup pemeliharaan, pencegahan, jaringan, instalasi, keamanan dan troubleshooting. Seorang profesional A+ mendapatkan gaji tahunan rata-rata $ 67,608 pada tahun 2011 survei Global Knowledge, dibandingkan dengan $ 49,930, tahun 2010 rata-rata upah tahunan untuk semua computer support specialist dilaporkan oleh Biro Statistik Tenaga Kerja. CompTIA A+ Teknisi PC adalah salah satu sertifikasi untuk mengirim beberapa keuntungan nilai pasar tahun terakhir ini, menurut laporan 2011 Agustus *Foote Partners*.

12. Sebuah infrastruktur data yang banyak bagi IT profesionals dalam teknologi cutting-edge seperti arsitektur perusahaan sosial, peran mendasar seperti dukungan Microsoft Windows, dan spesialiasi seperti analisis bisnis. Sertifikasi Teknologi Informasi menawarkan cara untuk menghadapi berbagai tantangan dari lingkungan komputasi yang selalu berubah, dengan kesempatan untuk mengembangkan keahlian dalam teknologi terkini.

8.5 Lembaga Yang Mengadakan Sertifikasi Profesi Di Bidang IT

Teknologi yang terus berkembang dan juga kebutuhan tenaga kerja dengan keterampilan tertentu yang terus meningkat berakibat meningkat pula kebutuhan atas sertifikasi profesi dan sertifikasi keterampilan di bidang IT. Lembaga yang mengadakan dan mengeluarkan sertifikasi di bidang IT antara lain :

1. Badan Nasional Sertifikasi Profesi (BNSP)

   Badan Nasional Sertifikasi Profesi (BNSP) Badan Nasional Sertifikasi Profesi (BNSP) dibentuk berdasarkan Peraturan Pemerintah Nomor 23 tahun 2004 atas perintah UU Nomor 13 tahun 2003, tentang Badan Nasional Sertifikasi Profesi,

utamanya pasal 4 Ayat 1) : Guna terlaksananya tugas sertifikasi kompetensi kerja sebagaimana dimaksud dalam Pasal 3, BNSP dapat memberikan lisensi kepada lembaga sertifikasi profesi yang memenuhi persyaratan yang ditetapkan untuk melaksanakan sertifikasi kompetensi kerja. Ayat 2): Ketentuan mengenai persyaratan dan tata cara pemberian lisensi lembaga sertifikasi profesi sebagaimana dimaksud dalam ayat 1) ditetapkan lebih lanjut oleh BNSP. BNSP merupakan badan independen yang bertanggung jawab kepada Presiden yang memiliki 30 kewenangan sebagai otoritas sertifikasi personil dan bertugas melaksanakan sertifikasi kompetensi profesi bagi tenaga kerja. Pembentukan BNSP merupakan bagian integral dari pengembangan paradigma baru dalam sistem penyiapan tenaga kerja yang berkualitas.

2. Lembaga Sertifikasi Profesi (LSP)

   Pengertian Lembaga Sertifikasi Profesi Apa dan Siapa LSP Lembaga Sertifikasi Profesi (LSP) adalah lembaga pelaksanaan kegiatan sertifikasi profesi yang memperoleh lisensi dari Badan Nasional Sertifikasi Profesi (BNSP). Lisensi diberikan melalui proses akreditasi oleh BNSP yang menyatakan bahwa LSP bersangkutan telah memenuhi syarat untuk melakukan kegiatan sertifikasi profesi. Sebagai organisasi tingkat nasional yang berkedudukan di wilayah Republik Indonesia, LSP dapat membuka cabang yang berkedudukan di kota lain.

   Fungsi dan tugas LSP antara lain :

   1. Sebagai sertifikator yang menyelenggarakan sertifikasi kompetensi. Tugas sebagai berikut :
   2. Membuat materi uji kompetensi.
   3. Menyediakan tenaga penguji (asesor).

4. Melakukan asesmen.
5. Menyusun kualifikasi dengan mengacu kepada KKNI.
6. Menjaga kinerja asesor dan TUK.
7. Membuat materi uji kompetensi.
8. Pengembangan skema sertifikasi.

LSP dipersiapkan pembentukannya oleh suatu panitia kerja yang dibentuk oleh atau dengan dukungan asosiasi industri terkait. Susunan panitia kerja terdiri dari ketua bersama sekretaris, dibantu beberapa anggota. Personal panitia mencakup unsur industri, asosiasi profesi, instansi teknis terkait dan pakar.

Tugas panitia kerja antara lain:

1. Menyiapkan badan hukum
2. Menyusun organisasi maupun personel
3. Mencari dukungan industri maupun instansi terkait.
4. Surat permohonan untuk memperoleh lisensi ditujukan kepada BNSP

Kinerja LSP dipantau secara periodik melalui laporan kegiatan Surveilen dan monitoring LSP yang melakukan pelanggaran terhadap ketentuan BNSP dikenakan sanksi sampai pada pencabutan lisensi Kinerja pemegang sertifikat dipantau melalui laporan pengguna jasa (industri).

3. Lembaga Kursus dan Pelatihan (LKP)

Lembaga Kursus dan Pelatihan (LKP) adalah salah satu bentuk satuan Pendidikan Nonformal yang diselenggarakan bagi masyarakat yang memerlukan bekal pengetahuan, keterampilan, kecakapan hidup, dan sikap untuk mengembangkan diri, mengembangkan profesi, bekerja,

usaha mandiri, dan/atau melanjutkan pendidikan ke jenjang yang lebih tinggi.

Setiap Lembaga Kursus dan Pelatihan (LKP) wajib mengadakan Uji Kompetensi di lembaganya masing-masing tergantung dari kompetensi yang dimiliki oleh lembaga. Tujuan dari Uji Kompetensi ini adalah untuk meningkatkan profesionalisme pendidik/instruktur untuk melaksanakan kegiatan pembelajaran melalui LKP sehingga dapat menciptakan lulusan yang kompeten dan siap kerja atau berusaha secara mandiri.

DAFTAR PUSTAKA

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. Processor: Jurnal Ilmiah Sistem Informasi, Teknologi Informasi Dan Sistem Komputer, 10(2), 509–516. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107

Afriani & Azmi. (2020). "Penerapan Etika Komunikasi di Media Sosial: Analisis pada Grup Whatapps Mahasiswa PPKn Tahun Masuk 2016 Fakultas Ilmu Sosial Universitas Negeri Padang." *Journal of Civic Education.* Volume 2 No 3.

Agus, A. A., & Riskawati. (2016). Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar). Jurnal Supremasi, 11(1), 20–29. https://doi.org/https://doi.org/10.26858/supremasi.v11i1.3023

Anggara, Y. (2019). Jenis Cybercrime Berdasarkan Aktivitasnya. Academia.Edu. https://www.academia.edu/13503623/Jenis_Cybercrime

Ardiyanti, H., Hadyanto, D. T., Krislamawaty, D., & Irwansyah. (2018). Swafoto: Sebuah Pendekatan Teori Manajemen Privasi Komunikasi. Aspirasi: Jurnal Masalah-Masalah Sosial, 9(1), 101–117. https://doi.org/https://doi.org/10.46807/aspirasi.v9i1.995

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. Jurnal Bisnis Dan Ekonomi (JBE), 18(2), 185–195.

Ashleigh, M. J., & Nandhakumar, J. (2002). Trust and technologies: implications for information technology supported work practices. ECIS 2002 Proceedings, 64.

Bachtiar, A., Reno, A., Prajuhana, A., & Atmadja, A. D. (2018). Daftar Unit Kompetensi Okupasi dalam Kerangka Kualifikasi Nasional Indonesia bidang Teknologi

Informasi dan Komunikasi (TIK). In E. Indrajit & Surono (Eds.), *Pusat Pengembangan Literasi dan Profesi SDM Informatika. Kementerian Komunikasi dan Informatika RI* (1st ed., Vol. 1).

Bapenda Jabar. (2017). Jenis Cybercrime Berdasarkan Motif dan Aktivitasnya. Bapenda.Jabarprov.Go.Id. https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime-berdasarkan-motif-dan-aktivitasnya/

Buamona, S. (2019). White Collar Crime (Kejahatan Kerah Putih) dalam Penegakan Hukum Pidana. Madani Legal Review, 3(1), 28–38. https://doi.org/10.31850/malrev.v3i1.343

Certiport. (2021). *Databases 1.* Information Technology Specialist. https://shop.audentestechnologies.com/product/information-technology-specialist-database/

CNN Indonesia (2020) Pemerintah Blokir 1759 akun medsos sebar hoaks corona. CNN Indonesia. Diakses dari https://www.cnnindonesia.com/teknologi/20201018192938- 185-559832/pemerintah-blokir-1759-akun-medsos-sebar-hoaks-corona

Cornelius, S., & Leidner, D. (2021). Acceptance of anthropomorphic technology: a literature review.

D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.

Enggarani, N. S. (2012). Penanggulangan Kejahatan Internet di Indonesia. Jurnal Ilmu Hukum, 15(2), 149–168. http://hdl.handle.net/11617/4010

Fahrimal, Yuhdi. (2018). "Netiquette: Etika Jejaring Sosial Generasi Milenial dalam Media Sosial." *Jurnal Penelitian Pers dan Komunikasi Pembangunan.* Vol 22 No 1.

Fazio, L. De, & Sgarbi, C. (2012). New research perspectives about stalking: the phenomenon of cyberstalking. Pensa MultiMedia Editore, 6(3). https://core.ac.uk/download/pdf/322533319.pdf

Fitriawati, Mia. 2019. Sertifikasi Profesi di Bidang IT. Repository Unikom: Bandung, Jawa Barat.

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. Mediator: Jurnal Komunikasi, 6(2), 255–264. https://doi.org/10.29313/mediator.v6i2.1194

Galih, Y. S. (2015). Kejahatan Tingkat Tinggi. Jurnal Ilmiah Galuh Justisi, 3(2), 257. https://doi.org/10.25157/jigj.v3i2.423

Handayani, P. (2013). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). Jurnal Dimensi, 2(2), 1–8. https://doi.org/https://doi.org/10.33373/dms.v2i2.119

Hasjim, A. L., & Erniwati. (2020). Kebijakan Hukum Pidana dalam Merehabilitasi Narapidana Anak. Justici, 12(1), 1–14. http://ejournal.iba.ac.id/index.php/justici/article/view/177

https://bpptik.kominfo.go.id/2012/05/09/260/10-sertifikasi-teknologi-informasi-untuk-meningkatkan-karir-di-2012/

https://lsp.smkn2tegal.sch.id/berita/detail/fungsi-dan-tugas-lembaga-sertifikasi-profesi-lsp

https://www.kompasiana.com/yunus85439/61b779aa62a7047782217532/pentingnya-etika-berkomunikasi-di-era-digital

Illiyyin, D. Z. (n.d.). Jenis-Jenis Cyber Crime Berdasarkan Motif. Retrieved July 6, 2022, from https://dienazhafirablog.wordpress.com/cyber-crime/jenis-jenis-cyber-crime-berdasarkan-motif/

Isnanto, R. (2009). Buku Ajar Etika Profesi. In *Buku Ajar Etika Profesi*. Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro. https://www.academia.edu/7242425/BUKU_AJAR_ETIKA_PROFESI_oleh_R_Rizal_Isnanto_ST_MM_MT_Program_Studi_Sistem_Komputer

Kamasa, F. (2014). Kejahatan Kerah Putih, Kontraterorisme dan Perlindungan Hak Konstitusi Warga Negara dalam Bidang Ekonomi. Jurnal Konstitusi, 11(4), 782–804. https://doi.org/10.31078/jk1149

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. Jurnal TIMES, 5(2), 35–42. https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556

Kominfo, Japelidi, Siberkreasi, 2021, Modul Etis Bermedia Digital

Kominfo, Katadata. (2020) Status Literasi Digital Indonesia 2020, Hasil Survei di 34 Provinsi

Kompas, 2021, Pentingnya Etika Komunikasi Digital https://adv.kompas.id/baca/pentingnya-etika-komunikasi-digital/

Kompasiana.com, 2021, "Pentingnya Etika Berkomunikasi di Era Digital":

Kumalasari, Vivi. 2021. Etika Profesi di Bidang Teknologi Informasi. Penerbit Yayasan Prima Agus Teknik, Semarang.

Kusmastuti, Frida, Dkk. (2021). "Modul Etis Bermedia Digital." Jakarta: Kementrian Komunikasi dan Informatika.

Kusmastuti, Frida, Dkk. (2021). "Modul Etis Bermedia Digital." Jakarta: Kementrian Komunikasi dan Informatika.

Legalku. (n.d.). Jenis-Jenis Cyber Crime dan Perlindungan Hukumnya. Legalku.Com. Retrieved July 7, 2022, from https://www.legalku.com/jenis-jenis-cyber-crime-dan-perlindungan-hukumnya/#!

M. E. Fuady, "'Cybercrime': Fenomena Kejahatan melalui Internet di Indonesia," *Mediat. J. Komun.*, vol. 6, no. 2, pp. 255–264, 2005, doi: 10.29313/mediator.v6i2.1194.

Marwin. (2013). Penanggulan Cyber Crime Melalui Penal Policy. Asas: Jurnal Hukum Ekonomi Syari'ah, 5(1). https://doi.org/https://doi.org/10.24042/asas.v5i1.1693

Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media Grup.

Mathilda, F. (2012). Cyber Crime dalam Sistem Hukum Indonesia. SIGMA-Mu - Jurnal Publikasi Hasil Penelitian Dan Gagasan Ilmiah Multidisiplin, 4(2), 34–45. https://doi.org/https://doi.org/10.35313/sigmamu.v4i2.870

Maulana, D., Zulfahrein, R., Surini, Ningsih, P. S., & Hariyati, C. (2017). Hijacking. https://www.academia.edu/35697225/Makalah_HIJACKING

Merdeka, R. M. (2022). Mengenal Blue Collar Crime dan Jenis Kejahatan Lainnya. Greatdayhr.Com. https://greatdayhr.com/id-id/blog/blue-collar-crime-adalah/

Munir, N. (2017). *Pengantar Hukum Siber Indonesia* (Edisi Keti). PT RajaGrafindo Persada.

Mustika, P. (2017). Profesionalisme Pustakawan. *Buletin Perpuatakaan UII*, *1*(57), 27–35. https://journal.uii.ac.id/Buletin-Perpustakaan/article/view/9097

Mustika, Rieka. (2018). "Etika Berkomunikasi di Media Online dalam Mengakal *Hoax*." *Jurnal Diakom.* Vol 1 No 2.

Mutiah, Albar, Fitrianto, & Rafiq. (2019). "Etika Komunikasi dalam Menggunakan Media Sosial." *Global Komunika.* Vol 1 No 1.

Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia. Jurnal Ilmiah Hukum Dirgantara, 11(2), 44–56. https://doi.org/https://doi.org/10.35968/jihd.v11i2.767

Pemerintah Republik Indonesia, Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Puspita, N. (2022). Perbedaan antara white collar crime dengan blue collar crime dalam hal pelaku kriminalitasnya. Roboguru.Ruangguru.Com. https://roboguru.ruangguru.com/question/perbedaan-antara-white-collar-crime-dengan-blue-collar-crime-dalam-hal-pelaku_QU-IYA9LGFV

Putra, B. K. B. (2019). Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) di Indonesia. Pamulang Law Review, 1(1), 1. https://doi.org/10.32493/palrev.v1i1.2842

R. A. Aco Agus, "Penanganan Kasus Cyber Crime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *J. Supremasi*, vol. 11, no. 1, pp. 20–29, 2016.

Rofadhilah, Taufik, & Hakim. (2018). "Dampak Penggunaan Teknologi Internet terhadap Etika dan Akhlaq Anak dalam Keluarga di Jakarta Utara." *Jisamar: Journal of Information System, Applied, Management, Accounting and Research.* Vol 2 No 1.

Safira, A. P. (2020). Cybercrime: Pengertian, Tipe, dan Langkah Mencegahnya. Goldenfast.Net. https://www.goldenfast.net/blog/cybercrime-adalah

Santi, D. K. (2017). Kejahatan Kerah Putih (White Collar Crime) di Asia. Medium.Com. https://medium.com/@dwitaks/kejahatan-kerah-putih-white-collar-crime-di-asia-5199c723601e#:~:text=Kejahatan kerah putih atau white,mempengaruhi suatu kebijakan dan keputusan.

Schilling, M., A. (2017). Strategic Management of Technological Innovation Fifth Edition. Mc Graw Hill Education

Schneider, X. (2019). The Responsible Research and Innovation (RRI) Roadmap.

Schultz, J. (2021). *IC3 GS5 Computer Fundamental.pdf*. Applied Educational System (AES). https://www.aeseducation.com/blog/ic3-gs5-certification#:~:text= The IC3 GS5 Computing Fundamentals Exam ,Computer Software Architecture domain includes 13... More

Siahaan, A. P. U. (2018). Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia. Jurnal Teknik Dan Informatika, 5(1), 6–9. https://jurnal.pancabudi.ac.id/index.php/Juti/article/view/82

Singal, E. P. (2021). Primum Remedium Dalam Hukum Pidana sebagai Penanggulangan Kejahatan Kerah Putih (Money Laundering). Lex Crimen, 10(6), 197–205. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/34419

Singh, H. P. (2018). Domain Name Disputes and Their Resolution under UDRP Route: A Review. Archives of Business Research, 6(12), 147–156. https://doi.org/10.14738/abr.612.5786

Stahl, B. C. (2011). IT for a better future: how to integrate ethics, politics and innovation. Journal of Information, Communication and Ethics in Society.

Stahl, B. C., Eden, G., Jirotka, M., & Coeckelbergh, M. (2014). From computer ethics to responsible research and innovation in ICT: The transition of reference discourses informing ethics-related research in information systems. Information & Management, 51(6), 810-818.

Suharto, B., & Kurniawan, A. B. (2020). Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising). JHP 17 (Jurnal Hasil Penelitian), 5(2), 57–61. https://doi.org/https://doi.org/10.30996/jhp17.v5i2.6109

Surniandari, A. (2016). UUITE dalam Melindungi Hak Cipta sebagai Hak Atas Kekayaan Intelektual (HKI) dari Cybercrime. Cakrawala - Jurnal Humaniora, 16(1). https://doi.org/https://doi.org/10.31294/jc.v16i1.1276

Suwinardi. (2017). Profesionalisme Dalam Bekerja. *Orbith*, *13*(2), 81–85. https://jurnal.polines.ac.id/index.php/orbith/article/view/965/782

Syifaudin, E. (2021). Apa itu Cyber Crime? Kenali 8 Jenis dan Cara Pencegahannya. Exabytes.Co.Id. https://www.exabytes.co.id/blog/apa-itu-cyber-crime/

Søraker, J. H. (2008). The moral status of information and information technologies: a relational theory of moral status. In Information Security and Ethics: Concepts,

Methodologies, Tools, and Applications (pp. 3829-3847). IGI Global.

Umam, M. Sulkhanul. (2019). "Orientasi Etika dan Cyber Security Awarness (Studi Kasus pada UMKM di Bantul)." *Jurnal Akuntansi & Manajemen Akmenika.* Vol 16 No.2.

Wahyono, T. (2009). Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi (D. Hardjono (ed.); 2nd ed.). ANDI. https://perpustakaan.kominfo.go.id/index.php?p=show_detail&id=2308

Wellyana, ddk. (2022). "Etika Penggunaan Media Sosial di Kalangan Remaja." *Batara Wisnu Journal: Indonesian Journal of Community Services.* Vol 2 No 2.

Whatsapp (n.d). (2020) Pemberitahuan cara menggunakan Whataspp dengan bertanggungjawab. Diakses melalui https://faq.whatsapp.com/general/security-andprivacy/how-to-use-whatasapp-responsibily/?lang=id

Yulianty, F. (2021). Contoh Kasus Cyber Crime dan Penyelesaiannya. https://kuliahonline.unikom.ac.id/?listmateri/&detail=45650

Biografi Penulis

Dr. Maniah, S.Kom., M.T lahir di Kota Palembang pada tanggal 27 Juli 1967, memperoleh gelar Doktor pada tahun 2021 dari Program Doctor of Computer Science, Binus University dan gelar Magister Komputer pada tahun 2005 dari Institut Teknologi Bandung konsentrasi Sistem Informasi dan gelar Sarjana Komputer di bidang Sistem Informasi pada tahun 1992 dari ST. INTENS Bandung. Beliau memulai karir sebagai praktisi di bidang teknologi informasi dan pernah menduduki jabatan sebagai Senior Analyst Programming pada tahun 1995 s/d 2003 di PT. Dirgantara Indonesia. Tahun 2008 beliau memulai karirnya sebagai dosen, dan sejak tahun 2012 s/d saat ini beliau aktif sebagai dosen tetap Program Studi D3 Manajemen Informatika Politeknik Pos Indonesia, serta aktif juga sebagai tim asesor uji kompetensi LSP-1 Politeknik Pos Indonesia. Dalam bidang akademis, beliau aktif dalam menulis artikel ilmiah sampai saat ini sudah memiliki 15 Publikasi, diantaranya terindeks Scopus sebanyak 5 Publikasi, berjudul: "A Systematic Literature Review: Risk Analysis in Cloud Migration", "Risk Analysis of Cloud Computing in the Logistics Process", "Risk Assessment on Cloud Computing for The Learning System in The Education Environmentthe International Conference on Engineering, Technalogy and Education {TALE 2019)", "Survey on Threats and Risks in the Cloud Computing Environment", "The Trigger". Factors and Constraints on e-Supply Chain Processes : A Systematic Literature Review". Konsentrasi mata kuliah yang diampu beliau diantaranya Database Fundamental, Analisis dan Perancangan Sistem Informasi, Sistem Informasi Enterprise, Pengujian Perangkat Lunak. Sebagai bentuk pengabdian kepada masyarakat, ia pun pernah terlibat aktif sebagai trainer pada Pelatihan Advance

Freight Management di PT. Pos Logistik Indonesia, Penataan Desa Wisata di Desa Cihanjuang Kec. Parongpong Kab. Bandung Barat, serta Pendampingan dalam Implementasi Penggunaan Aplikasi Dropbox dan Google Drive di Desa Cihanjuang Kec. Parongpong Kab. Bandung Barat. Adapun karya buku yang telah ditulisnya berjudul "Analisa dan Perancangan Sistem Informasi : Pendekatan Secara Praktis dengan Contoh Kasus": Saat ini beliau menjabat sebagai Kepala Satuan Penjaminan Mutu Internal (SPMI) di Politeknik Pos Indonesia.

Irfan Sophan Himawan, SE, MM dilahirkan di Cianjur, 16 April 1979. Latarbelakang pendidikan bidang akuntansi, dan saat ini sedang menempuh Pendidikan S3 di University Teknologi Mara (UiTM) Malaysia mengambil jurusan Akuntansi Forensik ~ Financial Criminology. Selain sebagai Dosen, sebelumnya aktif sebagai Asisten Peneliti di Pusat Pengembangan Akuntansi (PPA) FE UGM dan Peneliti di Pusat Studi Akuntansi Sektor Publik Yogyakarta. Dalam melaksanakan Aktivitas Tri Dharma Perguruan Tinggi, selain aktif mengajar, penulis juga aktif dalam kepengurusan Perkumpulan Dosen Peneliti Indonesia (PDPI) dan sebagai Narasumber Kominfo RI dalam Kegiatan Literasi Digital untuk Tahun 2021. Kemudian, penulis juga aktif melakukan berbagai kajian regulasi akuntansi dan keuangan daerah serta memberikan pendampingan dalam Penyusunan Laporan Keuangan Entitas Swasta (perusahaan jasa, dagang dan manufaktur) maupun Entitas Sektor Publik, di beberapa pemerintahan daerah di Indonesia. Sinta ID : 6686947, Google Scholar ID : B847gs8AAAAJ&hl, ORCID ID : 0000-0002-8460-2185, WoS ID ACK-8782-2022

Erlangga, S.Kom., M.Kom. lahir di Menggala, pada 10 Maret 1987. Menyelesaikan pendidikan Stata 1 Sarjana Komputer (S.Kom.) tahun 2010 di Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bandar Lampung (UBL), dan menyelesaikan pendidikan Strata 2 Magister Komputer (M.Kom.) tahun 2013 di Program Studi Teknik Informatika, STMIK Eresha Jakarta. Saat ini pria yang biasa disapa pak Ega dan menggunakan nama Erlangga Zildjian di Instagram dan Facebooknya, beraktifitas sebagai dosen tetap, sebagai pengelola jurnal penelitian dan jurnal pengabdian di Fakultas Ilmu Komputer UBL. Beberapa posisi di kampus UBL yang pernah diamanatkan kepada penulis, yaitu sebagai Operator EPSBED (Evaluasi Program Studi Berbasis Evaluasi Diri), Operator Feeder PDDIKTI (Pangkalan Data Pendidikan Tinggi), Social Media Specialist, Internal Auditor, Sekretaris LSPM (Lembaga Sistem Penjaminan Mutu).
ORCiD: https://orcid.org/0000-0001-7146-058X
Selengkapnya: https://bit.ly/erlanggazil

Sri Wahyuni, S.H., M.H. Lahir di Jakarta pada tanggal 22 Juli 1983. Telah menyelesaikan studi S1 Ilmu Hukum di Fakultas Hukum Universitas Trisakti pada tahun 2005 dan melanjutkan studi Ilmu Hukum di Fakultas Hukum Universitas Indonesia dan meraih gelar Magister Hukum pada tahun 2007. Saat ini aktif sebagai dosen di Fakultas Hukum Universitas Bhayangkara Jakarta Raya. Publikasi yang telah dihasilkan antara lain yaitu buku Hukum Perikatan, terbitan PT. RajaGrafindo Persada, ISBN: 978-623-231-781-9 tahun 2021, buku

Bantuan Hukum, terbitan PT. Raja Grafindo Persada, ISBN: 978-623-372-340-4 tahun 2022.

Dini Hamidin, S.Si., MBA., MT. lahir di Kota Bandung pada tanggal 02 Desember 1975. Ia Lulus pada tahun 1994 hingga mendapat 2 gelar Magister Manajemen Teknologi dan Sistem Informasi di institut Teknologi Bandung. Saat ini ia tercatat sebagai dosen tetap untuk mata kuliah Analisis dan Perancangan Sistem Informasi, Model Bisnis Digital/Ecommerce dan Supply Chain Manajemen dan Rekayasa Perangkat Lunak di Politeknik Pos Indonesia Bandung. Selain mengajar ia aktif dalam kegiatan tridarma lainnya diantaranya ialah penelitian dan pengabdian. Kegiatan penelitian internal dan eksternal pernah dilakukannya. Beberapa penelitian yang berhasil didanai oleh Ristekdikti dari tahun 2015 hingga sekarang berkaitan dengan perencanaan, perancangan dan penggunaan teknologi informasi di bidang logistik dan supply chain management dan telah memiliki beberapa hak cipta atas perangkat lunak dan berbagai konsep strategi dan perencanaan teknologi informasi yang dilaksanakan bersama tim peneliti dan mahasiswa. Sebagai bentuk pengabdian kepada masyarakat, ia pun pernah tergabung dalam associate trainer di Lembaga Pelatihan Prima Yasa Eduka (PYE) dan pernah terlibat aktif sebagai trainer di bimbingan teknis bantuan TIK SMP pada tahun 2021 dan beberapa kali sebagai narasumber di berbagai pelatihan dan pada kegiatan webminar. Adapun karya buku yang telah ditulisnya sejak tahun 2017, diantaranya berjudul :

1. Analisis dan Perancangan Sistem Informasi
2. Perspektif Pedagogik Manajemen Pendidikan

3. Strategi Pemasaran di Era Digital

Dr. Astri Dwi Andriani, M. Si lahir pada tanggal 21 April 1991 di Kabupaten Cianjur. Astri adalah lulusan Program Doktoral Ilmu Komunikasi di Universitas Padjadjaran. Pernah jadi penyiar radio, reporter, pimpinan redaksi majalah, dan *public relation officer manager*, hingga akhirnya pada tahun 2015 Astri menambatkan hati pada dunia pendidikan, dengan menjadi dosen bidang ekonomi dan komunikasi di beberapa universitas, diantara Universitas Putra Indonesia, Universitas Terbuka, dan Universitas Bisnis Indonesia. Selain aktivitas akademik, Astri aktif dalam kegiatan organisasi dan sosial, diantaranya mengemban tugas tambahan sebagai Dekan di Fakultas Ilmu Komunikasi Universitas Putra Indonesia, *partnership director* di Next Generation (NXG) Indonesia, Ketua Yayasan Digimom Indonesia, dan aktif menjadi pembicara pada Gerakan Nasional Literasi Media Digital Yayasan Siberkreasi di bawah naungan Kementrian Komunikasi dan Informatika Republik Indonesia. Astri juga aktif sebagai peneliti di Poldata Indonesia Consultant dan tenaga ahli pada beberapa institusi pemerintahan, kementrian, dengan bidang kajian kepemudaan, komunikasi, literasi media digital, dan *public speaking.*

Dwiny Meidelfi, S.Kom., M.Cs. lahir di Kota Padang pada tanggal 9 Mei 1986. Ia Lulus pada tahun 2012 hingga mendapat gelar Master of Computer Science dari Universitas Gadjah Mada Yogyakarta. Saat ini ia tercatat sebagai dosen tetap di Jurusan Teknologi Informasi, Politeknik Negeri Padang. Selain mengajar ia aktif dalam kegiatan tridarma lainnya diantaranya ialah penelitian dan pengabdian. Saat ini ia pun diamanahi sebagai Ketua Indonesian Computer Electronics and Instrumentation Support Society (IndoCEISS) PP Sumatera Barat dan menjadi editor serta reviewer di beberapa jurnal nasional dan internasional. Penelitian yang berhasil didanai oleh Ristekdikti dari tahun 2018 hingga sekarang berjudul: Open Data Pariwisata Indonesia Berbasis Android Sebagai Tujuan Wisata Dunia, Model Sistem Informasi Terpadu Untuk Optimalisasi Kinerja Pengelolaan Koperasi. Ia aktif Tim Kurikulum di Politeknik Negeri Padang dan sebagai Dosen Pembimbing Lapangan (DPL) Program Magang dan Studi Independen Bersetifikat (MSIB) Kemdikbudristek. Adapun artikel yang telah ditulis dan dipublikasikannya serta terindeks scopus, diantaranya berjudul :

1. Intelligence Eye for Blinds and Visually Impaired by Using Region-Based Convolutional Neural Network (R-CNN)
2. The Optimization of PCI Interference in the 4G LTE Network in Padang
3. The implementation of SAW and BORDA method to determine the eligibility of students' final project topic
4. Large dataset classification using parallel processing concept
5. Open Data of Indonesian Tourism Based on Android
6. Hybrid of AHP and TOPSIS for loan approval decision

Yuyun Khairunisa, M.Kom lahir di Kota Tanggamus pada tanggal 28 Desember 1986. Ia Lulus pada tahun 2015 hingga mendapat gelar Magister Ilmu Komputer di IPB University. Saat ini ia tercatat sebagai dosen tetap untuk mata kuliah Kecerdasan Buatan dan Media Digital Interaktif di Politeknik Negeri Media Kreatif.. Selain mengajar ia aktif dalam kegiatan tridarma lainnya diantaranya ialah penelitian dan pengabdian. Saat ini ia pun diamanahi sebagai Kepala Pusat Karir Polimedia dan menjadi editor Jurnal Multimedia dan IT.

ETIKA PROFESI TEKNOLOGI INFORMASI & KOMUNIKASI

Buku Etika Profesi Teknologi Informasi & Komunikasi membahas hal-hal yang erat kaitannya dengan profesionalisme praktisi di bidang IT dan komunikasi. Etika-etika yang berhubungan dengan komunikasi, interaksi, kolaborasi dalam ruang digital disampaikan dengan lugas dalam buku ini sebagai sumber rujukan yang memungkinkan individu maupun organisasi untuk belajar dan memanfaatkan peluang usaha di bidang IT dengan baik. Karakteristik Teknologi Informasi & Komunikasi pada organisasi sangat beragam sehingga memunculkan berbagai permasalahan di kehidupan bermasyarakat salah satunya yaitu *Cyber Crime* yang dibahas dalam bab tersendiri dalam buku ini. Selanjutnya, *Cyber Law* yang merupakan jawaban terhadap munculnya *Cyber Crime* juga dibahas dengan ringkas, terutama pada poin-poin hukum telematika dan UU ITE yang perlu diketahui oleh praktisi di bidang IT dan komunikasi.

Pembahasan dalam buku ini dilengkapi dengan panduan-panduan praktis dan yuridis dalam usaha di bidang IT, sehingga sangat bermanfaat bagi praktisi professional yang menjalankan usahanya di bidang IT dan komunikasi. Analisis kelayakan usaha, analisis pasar, sampai dengan perencanaan keuangan, dan analisis risiko menjadi pembahasan yang cukup penting untuk diketahui. Terakhir buku ini ditutup dengan penjelasan berbagai profesi dan sertifikasi di bidang IT dan komunikasi yang akhir-akhir ini banyak beredar di masyarakat.

TOHAR MEDIA
No Anggota IKAPI : 022/SSL/2019
Workshop : JL. Rappocini Raya Lr.II A No 13 Kota Makassar
Redaksi : JL. Muhktar dg Tompo Kabupaten Gowa
Perumahan Nayla Regency Blok D No 25
Telp. (0411) 8987659 Hp. 085299993635
https://toharmedia.co.id

ISBN 978-623-5603-75-9
9 786235 603759