PAJOUL (Pakuan Justice Journal Of Law) Volume 01, Nomor 01, Januari-Juni 2020, Halaman 1-32
https://journal.unpak.ac.id/index.php/pajoul/index **e-ISSN :**
p-ISSN :

ERA DISRUPSI TEKNOLOGI 4.0 DAN ASPEK HUKUM PERLINDUNGAN DATA HAK PRIBADI

Sri Ayu Astuti*
Program Studi Ilmu Hukum Pascasarjana Universitas Pakuan,
Jalan Pakuan No. 1 Bogor 16143
E-mail: saar_1126@yahoo.co.id
Naskah diterima : 13/05/2020, revisi : 14/05/2020, disetujui 16/05/2020

ABSTRACT

The stopping of the Covid Pandemic -19 gives the effect of changes in social interaction in life in the community especially when it is disrupted which has controlled human life sociologically and psychologically in every movement in life, especially since the existence of a pandemic there has been a change in work culture that was originally in the conventional form of switching to online space because of the policy of doing work by way of WFH work from home. Technological advances in the era of the utilization of technology 4.0 have become evident in their use, not even in their total mastery of internet applications, the interaction of everyone in Indonesia, including ethical behavior in communication in the technology space, eventually leading to legal problems that intersect with law enforcement of ITE Law Number 19 of 2016 against function of its use. every person who is in the vortex of using technological advances must be confronted with no maximum legal efforts to do legal protection of personal rights including personal data that is so easily accessed by implementing an internet-based technology system. This is the responsibility of the state, namely the organizer of the Government of the Republic of Indonesia in the jurisdiction of Indonesia, which grants permission to operate as an owner and manager of a technological system that carries out its operations in the sovereignty of a State, which can impose strict sanctions on the legal remedies for protecting every citizen from criminal acts of moving virtual.

Keywords: Disruption Era, Technological Uses, Personal data protection

ABSTRAK

Hentakan adanya Pandemi Covid -19 memberikan pengaruh terjadinya perubahan interaksi sosial dalam kehidupan dalam masyarakat terlebih diera disrupsi yang telah menguasai hidup manusia secara sosiologis dan psykologis disetiap gerak dalam kehidupan, apalagi sejak adanya pandemi terjadi perubahan budaya kerja yang semula dalam bentuk konvensional beralih ke ruang online karena adanya kebijakan melakukan pekerjaan dengan cara WFH work from home. Kemajuan teknologi dalam era kemanfaatan teknologi 4.0 menjadi nyata penggunaannya, bahkan belum secara total penguasaannya pada aplikasi internet, interaksi setiap orang di Indonesia termasuk perilaku etika dalam komunikasi di ruang teknologi hingga akhirnya menimbulkan permasalahan hukum yang bersinggungan dengan penegakkan hukum UU ITE Nomor 19 Tahun 2016 terhadap fungsi penggunaannya. setiap orang yang berada dalam pusaran penggunaan kemajuan teknologi harus dihadapkan tidak maksimalnya upaya hukum dilakukannya perlindungan hukum hak pribadi termasuk data-data pribadi yang begitu mudah diakses dengan penerapan sistem teknologi berbasis

internet. Hal ini menjadi tanggungjawab negara yakni penyelenggara Pemerintah Republik Indonesia di wilayah hukum Indonesia yang memberikan ijin beroperasinya pemilik sekaligus pengelola sistem teknologi yang melakukan operasionalnya dalam kedaulatan suatu Negara, yang dapat memberikan sanksi tegas terhadap upaya hukum perlindungan setiap warga negara atas tindak pidana kejahatan yang bergerak secara virtual.

Kata Kunci : Era Disrupsi, Kemanfaatan Teknologi, Perlindungan data pribadi

A. PENDAHULUAN

Pandemi *Corona Virus Diseases COVID-19* seperti menghentak situasi saat ini dan mau tidak mau setiap orang dipaksa harus memahami kondisi yang tidak memberikan kenyamanan bagi setiap orang. Tentu berhubungan dengan perilaku budaya sosial masyarakat Indonesia yang biasa berkomunikasi secara berkelompok. Kondisi ini juga terkait dengan budaya kerja yang sebelumnya bekerja dengan sistem konvensional dipaksa mengambil bagian dalam pesatnya perkembangan teknologi era disrupsi 4.0 dengan melakukan kerja menggunakan teknologi yaitu secara *online* atau dikenal istilah WFH (*Work from Home*) . teknologi menjadi jembatan komunikasi aktif dengan berbagai sendi-sendi kehidupan manusia, baik secara ekonomi, keagamaan bahkan dalam proses bidang pengajaran dan pendidikan dan berbagai institusi di Pemerintahan. Era Disrupsi (*disruption era*) menyajikan kekuatan teknologi, informasi dan komunikasi berbasis dengan kemanfaatan media internet menjadi kekuatan baru dalam memberikan pemenuhan kemudahan bagi setiap orang guna membantu setiap pergerakan tanpa mengenal batas ruang dan waktu, dengan segala bentuk resiko dan pertanggungjawaban hukum yang ditimbulkan akibat perilaku setiap orang yang memanfaatkan teknologi dengan niat dan tujuan yang berbeda, disinilah tantangan kejahatan terkait dalam perlindungan data pribadi yang menjadi hak mutlak setiap orang yang menjadi subjek hukum di negara hukum kedaulatan Negara Republik Indonesia.

Dalam proses percepatan perubahan teknologi dengan keberadaan sumber daya manusia diperlukan penguatan akan literasi media. Ini penting mengingat banyaknya kejahatan berbasis media internet dalam kontekstual percepatan teknologi disebabkan oleh perbuatan melanggar hukum yang dilakukan manusia sebagai sumber melakukan kegiatan di ruang media berbasis internet, atau dikenal dengan sebutan *cybercrime.*

Perilaku menyimpang dari sumber daya manusia bila tidak memiliki penguatan terhadap literasi media akan berimplikasi terhadap perbuatan melanggar hukum hingga menimbulkan tindak kejahatan yang dilakukan dengan menggunakan ruang siber (*cyber space*) .

Dalam perubahan percepatan teknologi telah merubah pola kehidupan setiap manusia di ruang peradaban era teknologi. Situasi itu terkait dengan tindak kejahatan manusia yang telah berubah dari sistem konvensi ke ruang siber, sudah pasti akan menimbulkan kerugian bagi setiap orang dalam setiap kegiatannya menggunakan media internet.

Teknologi informasi memegang peranan yang sangat penting dalam arus informasi, komunikasi dalam ruang siber (*cyberspace*) dari yang memberikan dampak positif hingga negatif. Perubahan tatanan kehidupan masyarakat di bidang sosial dan ekonomi berubah sangat cepat dalam beberapa tahun terakhir, khususnya dalam komunikasi aktif di bidang pengguna media sosial yang secara konvensional terjadi percepatan yang melesat tajam dalam penggunaan komunikasi sosial aktif lewat media elektronik.

Saat sebagian masyarakat menunjuk pada fungsi sumber daya manusia yang telah siap dengan konsekuensi logis terhadap perubahan dan memiliki penguatan terhadap literasi media, maka dapat memberikan hasil yang positif secara berarti (*significan*), namun yang baru melek terhadap fungsi media itu sendiri dengan percepatan transaksi secara keseluruhan sendi-sendi kehidupan tentu akan menimbulkan persoalan hukum yang sangat tidak menarikakibat kejahatan dari penggunaan fungsi media atau dikenal dengan kejahatan siber (*cybercrime*), seperti terjadinya *hacking*, *cracking*, *cyber terrorism*, dan perilaku transaksi ekonomi yang didasari niat dengan sengaja menipu sebagaimana investasi bodong memiles, belum lagi Bank tidak dapat menjamin dan menjaga kerahasiaan pemilik data terkait kepemilikan dana yang tersimpan di bank tersebut dan ini semua merupakan karakter sifat kejahatan yang berbasis media internet (*internet fraud*).

Pada kondisi di atas pentingnya kesadaran untuk menguasai prinsip-prinsip perrlindungan terhadap sumber daya manusia sebagai pengguna utamadalam arus lalu lintas di kehidupan dunia siber. ini terkait dengan kebijakan hukum yang harus memiliki penguatan penegakkan hukum untuk memberikan kepastian hukum pada hak dan kewajiban hukum bagi setiap orangsebagai subjek hukum yang melakukan seluruh transaksi kegiatan dalam ruang kehidupan pranata sosial dengan media internet.

Perkembangan masyarakat modern akan mengalami juga bentuk kejahatan yang berbeda dari sifat dan bentuknya, dapat dikatakn semakin rumit dengan pola perilaku kejahatan yang sengaja dibuat semakin beragam dengan menggunakan media berbasis internet, ini terkait dengan pembuktian atas kejahatan yang dilakukan di ruang siber tersebut.

Kendati demikian hukum tidak boleh berhenti dan statis namun sebagaimana perkembangan kejahatan dari perkembangan teknologi itu hukum pun harus mengikuti pergerakannya secara dinamis pula, ini merupakan kesepakatan para ahli hukum dan semua ini dimaksudkan untuk satu tujuan terciptanya ketertiban dan keadilan, ketentraman bagi masyarakat.

Hukum yang bergerak dinamis akan memberikan perhatian serius dalam mengikuti perkembangan masyarakat dengan berbagai bentuk kejahatan dan sifat kejahatan yang berubah mengikuti perkembangan jaman itu. Tentunya ini memiliki maksud hukum positif tidak terjadi kekosongan hukum (*rechtsvacuum*), guna memberikan perlindungan dan kepastian hukum pada subjek hukum sebagai korban (*victim*) atas kejahatan karena dampak kejahatan berbasis media internet. Menunjuk fungsi perlindungan pada fungsi sifat hukum itu maka hukum yang dinamis sangat dipengaruhi oleh aspek hukum dalam pembaharuan hukum.

Maka perkembangan teknologi 4.0 terhadap peradaban manusia yang berkembang di ruang siber, tetap berjalan dalam prinsip kehidupan yang sesuai akan adab dan etika manusia sebagai makhluk sosial dengan kemanfaatan media (*convergance of media*) untuk mampu berjalan harmoni dan meminimalisir kejahatan akibat dari dampak revolusi teknologi 4.0 itu sendiri.

Indonesia telah memiliki regulasi Nasional dalam menyelesaikan permasalahan hukum terkait kejahatan dunia siber (*cybercrime*) atas perbuatan melawan hukum tersebut, seperti memanipulasi data, *hacking* dan tindak penipuan dengan menggunakan fasilitas media internet. Undang-Undang nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ini diharapkan mampu mengurai persoalan hukum akibat perbuatan melawan hukum dengan berbagai bentuk kejahatan yang ada. Tentu saja diharapkan melakukan penegasan penguatan terhadap penggunaan alat bukti elektronik yang telah diakui sebagai satu diantara ketetapan alat bukti berdasarkan ketentuan alat Bukti elektronik yang termuat Pasal 5 Ayat (1) Undang-Undang ITE yang mengatur bahwa Informasi Elektronik dan/atau Dokumen elektronikdan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Alat bukti elektronik ini memenuhi persyaratan materiil dan dan formil, sejalan juga dengan ketentuan Pasal 184 Ayat (1) Kitab Undang-Undang Hukum Acara Pidana KUHAP dikarenakan adanya perluasan penguatan terhadap keberadaan dokumen elektronik yang mengikat dan diakui sebagai alat bukti yang sah guna memberikan kepastian hukum terhadap penyelenggaraan sistem elektronik, khususnya dalam hal pembuktian yang berkaitan dengan perbuatan hukum yang dilakukan melalui sistem elektronik.

Apa yang tersampaikan di atas, terlihat begitu penting aspek perlindungan terhadap sumber daya manusia dalam percepatan revolusi teknologi 4.0 guna menempatkan fungsi kebenaran dan menegakkan kebenaran atas keberhakannya sebagai pemilik kebenaran, dan memberikan hukuman (*punishment*) yang pasti pada seseorang yang dengan sengaja melakukan perbuatan melawan hukum dengan pembuktian yang seharusnya dan menjadikan efek jera (*deterrend effect*) sebagaimana tujuan hukum memberikan keadilan dan ketertiban masyarakat.

B. METODE PENELITIAN

Jenis Penelitian ini adalah penelitian hukum normatif yang menggunakan kombinasi pendekatan sosiologi (sociological approach), dan pendekatan perundang-undangan (statute approach), serta pendekatan hukum media (media of law), juga perubahan budaya teknologi 4.0 dalam media digital (*the change of culture technology 4.0 in digitalization media*) . Hal itu diterapkan untuk dilakukan pendalaman dan menelisik perkembangan norma-norma hukum dan lembaga-lembaga hukum yang mengambil kebijakan terhadap perubahan penggunaan teknologi media dengan sistem digital berabasis internet, yang terkait dengan dampak timbulnya persoalan hukum ditengah masyarakat era digital atau lebih popular dengan istilah masyarakat era disrupsi. Dampak persoalan hukum yang terjadi adanya upaya melanggar perbuatan hukum dengan cara meretas akun hak privasi dan data pribadi setiap orang yang aktif dalam menggunakan media digital. Pendekatan perundang-undangan (*statute approach*) dengan cara menelaah semua undang-undang dan regulasi yang terkait dengan substansi masalah penelitian ini.[1]

Pendekatan ini dilakukan terkait dengan hak Privasi dan data hak pribadi dalam penggunaan media digital di era disrupsi. Sedangkan bahan hukum terdiri dari bahan hukum primer yaitu berbagai peraturan perundang-undangan yang ada dan digunakan serta adanya Resolusi dari Majelis PBB, bahan

[11] Peter Mahmud Marzuki , *Penelitian Hukum*, Kencana Jakarta , 2005, hlm. 126

sekundernya berupa buku teks yang terkait dengan permasalahan, sedangkan bahan hukum tersier merupakan petunjuk atau penjelasan terhadap bahan hukum primer dan bahan hukum sekunder seperti literasi teknologi informasi dan komunikasi, kamus hukum, dan ensiklopedia. Pengumpulan ketiga bahan tersebut dilakukan melalui studi kepustakaan dengan mengumpulkan dan menganalisis bahan – bahan kepustakaan sperti terjadi perbuatan melawan hukum dengan memasuki dan meretas akun pribadi orang lain, sekaligus menghacker akun orang lain. Juga banyaknya fenomena penggunaan media digitalisasi secara serentak dan memaksa setiap orang melakukan perubahan budaya berinteraksi secara sosial dalam penggunaan media digitalisasi yang memungkinkan banyaknya terjadi kasus hukum di ruang media siber (*cyber media*) khususnya dimasa terjadinya wabah *pandemic covid* – 19, maka penulis melakukan penelusuran juga di ruang siber , dengan demikian penulis juga melakukan analisa bahan hukum penelitian dengan metode analisis induktif.

C. PEMBAHASAN

Era disrupsi memberikan ruang kemudahan bagi interaksi sosial dalam kehidupan manusia, dengan kemanfaatan teknologi, sekaligus juga memberikan persoalan dalam penyimpangan penggunaan untuk tujuan utama yaitu memberikan kemanfaatan dalam pergerakan manusia. Kondisi itu yang merasakan kenyamanan dengan kemudahan teknologi berubah menjadi permasalahan hukum atas tindakan perbuatan melawan hukum dengan melakukan kejahatan penggunaan teknologi dengan berbagai modus operandi hingga merugikan orang lain atas perbuatannya yang dilakukan dengan sengaja, ataupun yang sifatnya lalai, dan tidak sengaja karena ketidakmampuan dalam penguasaan teknologi atau lebih dekat dengan istilah literasi media teknologi (*the literation of technology*).

Apalagi disaat kondisi pandemic Covid 19 ini masyarakat sosial Indonesia mengalami *culture shock* perubahan yang membuat suatu daya paksa bagi masyarakat nya melakukan semua transaksional komunikasinya dengan menggunakan aplikasi media sosial yang berbasis internet, dampak dari kebijakan Penyelenggara Pemerintah melakukan perintah bekerja dari rumah yang dikenal dengan istilah WFH Work From Home.

Dari kebijakan tersebut menimbulkan permasalahan hukum baru yaitu terbukanya hak hukum data pribadi yang seharusnya mendapatkan perlindungan. Tetapi Pemerintah dalam hal ini yang memiliki tanggungjawab akan penggunaan dan beroperasinya pengelolaan sistem internet di

wilayah hukum, belum maksimal melakukan penerapan melindungan penggunaan data pribadi. Maka perang dagang dalam pengelolaan internet pun juga terjadi saling menunjuk dan menclaim bahwa sistem internet yang dikelolanya yang terbaik. Contoh antara sistem zoom dan sistem dikelola oleh google sepetei meet me, menjadi sistem internet yang banyak digunakan, bahwa tidak banyak yang memahami bahwa sejatinya model penerapan aplikasi model penggunaan internet apapun penamaannya, sebenarnya awal pintu masuknya adalah penggunaan akun dasar yang dimiliki setiap orang dalam proses yang dengan sengaja mengikatkan diri dengan sistem pengelolaan internet itu.

Perlindungan hukum pengguna yang masuk dalam pusaran sistem berbasis internet itu tidak mugkin lepas dari ruang pantauan pergerakan slot demi slot pada frekuensi yang menggunakan kekuatan satelit, tinggal pagar pelindung [ada] pada sistem pengelolaan yang dilkaukan oleh sistem operasional yang tentunya masih menggunakan fungsi manusia sebagai operator diruang virtual tersebut.

Disinilah sikap tegas Pemerintah khususnya Kementrian yang mengelola Komunikasi dan Informasi mampu memberikan hak perlindungan hukum bagi setiap orang warga negara Indonesia di dalam wilayah kedaulatan Negara Republik Indonesia yang dapat membahayakan dan bahkan menimbulkan kerugian materiil dan immateriil atas dampak dari penggunaan teknologi 4.0 dengan segala konsekuensi logis. Ada banyak dampak buruk terjadi dari ancaman, peretasan hingga sistem hack, yang banyak dialami para *entrepreneur* yang berada di ruang start up sebagai jembatan dalam perubahan sistem ekonomi yang berjalan dengan menggunakan internet bahkan saat ini dalam ruang kerja bagi setiap institusi.

Akun dan konten yang dicermati oleh Pemerintah dari Kementerian Kominfo masih terkonsentrasi atas putusan kebijakan pada perilaku tindak criminal yang dianggap membahayakan negara saja belum lebih demikian juga aparat hukum yang memiliki tanggungjawab hukum melindungi hak setiap orang yang jelas dilindungi hak dasar pribadinya dalam ketentuan Undang-Undang Dasar Negara Repbulik Indonesia tidak diberikan secara maksimal. Ada banyak contoh bagaimana para enterpreuner yang bergerak sebagai pedagang online masih belum memiliki jaminan perindungan hukum maksimal terhadap data pribadinya yang bisa saja mendapat perlakuan yang tidak nyaman dari pesaingnya hingga akun sesorang bisa saja dibajak atau di hack, dan mengambil serta menguasai Akun dan bisa menembus data pribadi seseorang yang dianggap menjadi pesaing

dagangnya secara individu yang ada kemungkinan juga dikenakan pajak, padahal kita bisa secara kasat mata mana pedagang besar dan kecil dalam sistem start up itu melakukan transaksi dagangnya. Demikian juga hal yang sama akan bisa terjadi dalam hubungan komunikasi melaksanakan pekerjaan dari rumah atau WFH yang tidak memiliki sistem pengamanan yang baik, karena sistem canggih belum bisa kita sampaikan karena adanya keterbatasan kemampuan. Bandingkan dengan WTC di Negara Adi Daya dengan sistem teknologi yang canggih saja bisa ditembus sistem datanya dan selanjutnya dapat diketahui posisi mana yang bisa ditembus secara phisycally untuk dihancurkan terjadilah peristiwa 11 September peledakan WTC di negara Adi Kuasa tersebut.

Illustrasi tersebut tidak banyak yang menyadari bahwa sistem satelit bisa dikendalikan atas kepentingan politik, demikian juga perlindungan data pribadi dapat menjadi alat yang digunakan dan diperjual belikan. Bila lalai dengan prinsip kehati-hatian maka masyarakat dan aparat hukum hanya focus pada kepentingan pribadi terkait pada kepentingan kelompok dan elit politik maka akan timbul kesenjangan sikap adil pada rakyat yang membutuhkan, karena aparat hukum masi belum melakukan *framing* cara pikirnya pada fungsi perlindungan hukum yang diberikan seharusnya pada setiap subjek hukum yang mengalami kerugian atas perilaku perbuatan melawan hukum yang dilakukan atas kepentingan tertentu dengan merugikan orang lain, bahkan aparat hukum hanya terjebak pada ketentuan Pasal 27 yang tercantum dalam UU ITE Nomor 19 Tahun 2019, yang hanya menunjuk pada kelompok yang kuat tapi tidak melindungi subjek hukum yang merupakan rakyat kecil di Negara hukum Repbulik Indonesia yang banyak menggunakan sistem media sosial, dalam penguatan Literasi Media.

Pihak aparat hukum dan masyarakat pengguna sistem online berbasis internet masih berada dalam pusaran euphoria penggunaan saja, belum jauh pada bentuk pemahaman yang kuat literasi media dan fungsi-fungsinya dan ujung akhirnya atas dampak perkembangan perilaku dari percepatan teknologi 4.0 itu adalah dengan memberikan hukuman penjara yang diharapkan memberikan efek jera, alih-alih memberikan sanksi dan efek jera justru yang terjadi tidak memberikan dampak positif. Semua itu disebabkan oleh kurang gencarnya pemerintah dan institusi terkait memberikan sosialisasi atas dampak hukum atas perubahan perilaku dan budaya sosial dalam kehidupan masyarakat teknologi yang dikenal dengan sebutan masyarakat milenial, yang menjadikan adanya minus dari kondisi itu adalah tidak adanya penguatan proses memahami kesadaran hukum akan bahaya dari ketidakmampuan meletakkan diri pada fungsi literasi media

dengan segala fungsinya, ini pun terjadi di ruang pendidikan, yang seharusnya menjadi dasar lompatan dalam pemberian pemahaman pentingnya kesadaran hukum atas dampak dari percepatan perkembangan teknologi 4.0 dengan perilaku *loose control* terhadap budaya sosial pada masyarakat sosial yang harus melek teknologi sebagai kebutuhan dasar masyarakat teknologi saat ini.

A. Era Disrupsi Teknologi 4.0 dan Aspek Hukum Perlindungan Sumber Daya Manusia

Sumber daya manusia di era teknologi, informasi dan komunikasi saat ini menghadapi tuntutan untuk lebih cermat dalam mengelola kekuatan penguasaan ruang teknologi dan perangkatnya. Perkembangan teknologi informasi dan komunikasi yang menjadi satu dalam satu wadah media berbasis internet telah mampu mengubah pola perilaku dan berpikir masyarakat yang memberikan perubahan dalam peradaban kehidupan manusia. Semua dunia menjadi tanpa batas (*borderless*) yang menyebabkan juga terjadi perubahan dalam ruang perilaku terhadap kehidupan sosial dan ketentuan hukum, disebabkan kemajuan peradaban menggunakan kemanfaatan media teknologi.

Kondisi tersebut tentu saja menuai konsekuensi logis yaitu terjadinya perubahan dalam perilaku perbuatan kejahatan sekaligus cara penanganan kejahatan yang ditimbulkan di ruang virtual. Kejadian perilaku kejahatan dalam dunia virtual, daring lebih pada upaya penggunaan kemudahan tekhik dalam berinteraksi melalui dunia siber. Upaya kejahatan dengan berbagai cara menipu, meretas dengan kecanggihan penggunaan teknologi itu membuat aparat hukum memerlukan penyesuaian dibidang knowledge dan keilmuan dalam penanganan dan penegakkan dibidang hukum terhadap tindakan kejahatan dengan sistem kejahatan yang telah memasuki sistem teknologi baik yang masih dilakukan dengan sistem penggunaan teknologi sederhana hanya dengan menggunakan nomor kontak personal pelaku kejahatan melalui pesan singkat atau berupaya mengajak komunikasi dengan membawa pada berita bohong atau mencoba hipnotis lewat komunikasi. Tekhnik tindakan kejahatan lain yang lebih canggih dengan menggunakan teknik teknologi dengan sistem meretas dan memasuki pekarangan situs hak rumah orang lain didalam ruang siber tanpa ijin. Hal ini menunjuk terjadi perilaku penyimpangan seseorang dengan melakukan perbuatan melawan hukum, maka terkait perilaku tersebut diperlukan tindakan upaya memberikan perlindungan bagi setiap orang dalam penggunaan kemanfaatan teknologi di setiap aktivitasnya yang telah banyak berpindah dari ruang gerak konvensional ke dunia virtual.

Pesatnya perkembangan ruang media baru (*new of media*), melahirkan istilah kejahatan siber (*cybercrime*) di dalam rezim baru, kondisi ini menunjuk pada hukum baru atau disebut dengan hukum siber (*cyber of law*). Di dalam peradaban kemajuan teknologi dengan kemanfaatannya yang begitu luas hadir berbagai macam bentuk *cybercrime* yang mengikuti percepatan teknologi yang diserap dan digunakan dalam keseharian hidup masyarakat, misalnya kejahatan manipulasi data, *spionase, sabotase, money laudring, penipuan secara online, hacking* dan berbagai macam kejahatan lain dengan menggunakan kekuatan teknologi.

Kecepatan dan keterpaduan perkembangan teknologi computer dengan pola sistem komunikasi dengan berbasis sistem telekomunikasi, menjadi sangat populer bagi setiap sumber daya manusia dalam menggunakan kemanfaatannya dan telah menjadi bagian hidup menjadi nyata diruang siber hingga kejahatan konvensional pun berpindah ke ruang siber (*cyber space*).

Terkait pendefinisian pengertian *cybercrime* ada beberapa pendapat didalam istilah yang berkembang sesuai kebutuhan penggunaannya. Dari beberapa kepustakaan *cybercrime* sering diindentikkan sebagai *computer crime* (*Gamble, Teri and Michael, communication* Work Wikipedia 2015). Namun beberapa ahli juga menyampaikan pendapatnya yang berbeda antara perbedaan penggunaan *cybercrime* dengan *computer crime*, dikatakan merupakan dua istilah yang berbeda sebagaimana yang dikatakan oleh Nazyra abdul manaf sebagai berikut:2

"*Defined broadl, computer crime could reasonably include a wide variety of criminal offences, activities, or issues. It also known as a crime commited using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, adishonest bank clerk who unauthorisendly transfersa customer's money to a dormant account for his own interest or a person without permission has obtained access to other persons computer confidential. These situations require direct accsess by a hacker to the victim's computer. There is no internet lie involved, or only limited networking used such as the Local Area Network (LAN) whereas, cyber – crimes are crimes commited virtually through internet online. This means that the crimes could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as cybercrimes or vice versa, since they have same impact in law".*

[2] Agus Raharjo, *Cyber crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002, hlm.1

Pendapat di atas memberikan penjelasan dan menunjuk bahwa computer crime merupakan tindak kejahatan yang tidak melibatkan peran jaringan terkoneksi dengan internet, melainkan hubungan langsung antara tindak kejahatan dengan computer sebagai sarana kejahatannya. Sekalipun melibatkan jaringan koneksi internet hanya sebatas pada jaringan LAN sedangkan *cybercrime* merupakan tindakan kejahatan yang menggunakan koneksi internet untuk melakukannya, yang berarti dapat dilakukan hingga menembus negara lain, kendati demikian tidak ada salahnya untuk menyebut *computer crime* sebagai *cybercrime* begitu pula sebaliknya, karena keduanya menimbulkan akibat hukum yang sama yaitu memberikan dampak kerugian bagi orang lain.

Secara penggunaan menunjuk alat teknologi, memang terdapat perbedaan mendasar dari *cybercrime* dengan *computer crime* sebagaimana yang dikemukakan di atas yaitu adanya unsur computer yang terkoneksi melalui perangkat telekomunikasi dalam bentuk internet *online* yang menjadi media bagi seseorang atau kelompok untuk melakukan pelanggaran dan/atau kejahatan.[3]

Pada pelanggaran kontekstual dengan kekuatan literasi media menjadi penting bahwa Literasi disini tidak hanya sampai dan mampu membaca dan menggunakan perangkat computer atau smartphone dengan basis internet, guna memenuhi kebutuhan dalam berkomunikasi tetapi lebih dari itu menekan pada sumber daya manusia yang harus mampu menguasai dan mengendalikan kemampuan dirinya secara emosional masuk dalam pusaran teknologi terkait dengan penggunaan media computer dengan koneksitasnya, agar terhindar dari perbuatan melanggar dan melawan hukum.

Ini dikarenakan computer digunakan sebagai media perbuatan pelaku melakukan akses secara *illegal*, dan melakukan penyerangan terhadap jaringan yang bukan merupakan haknya yaitu terkait dengan sistem pengamanan jaringan (*networking*). Itu menunjuk pada perbuatan seseorang yang telah memiliki niat dengan maksud dan tujuan melakukan kejahatan seperti halnya kejahatan konvensional misal pencurian data dan pemalsuan data.

Untuk itu diperlukan perangkat hukum untuk mengatasi kejahatan yang bersifat global ini. Kejahatan dalam dunia virtual ini seringkali dilakukan dengan menembus batas wilayah hukum suatu negara (*transnational*) dengan pola terorganisir, kejahatannya dikenal dengan istilah *transnational organice crime* dikarenakan kejahatan yang terorganisir itu melampaui batas negara seperti misalnya kejahatan terorisme, *trafficking*, kejahatan di ruang perbankan dan berbagai modus

[3] Maskun, *Kejahatan siber (cyber crime)*, Kencana Pranada Media Group, Jakarta 2013, hlm.44

operandi beragam dengan pola terorganisir. Tentu ini akan bersinggungan dengan yurisdiksi hukum negara mana yang berlaku terhadap penanganan pelaku dalam lingkup kejahatannya yang sangat luas dengan beragam bentuknya.

Dari berbagai cakupan *cyber crime* yang merambah berbagai kegiatan kehidupan masyarakat ada beberapa kategori yang perlu menjadi titik perhatian yaitu :[4]

a. Penyiaran di ruang Publik melalui Media Sosial

   Bentuk- bentuk tindak pidana yang dapat dilakukan meliputi memperolok, (*mockering*), merendahkan (*humiliating*), fitnah (*slandering*), pencemaran nama baik (*defamation*), penyesatan (*mislead),* kebohongan (*lie*), menghasut (*incite*), melecehkan (*insulting*), kekerasan (*violence*), Pornografi, perjudian (*gambling*), Penyalahgunaan Narkoba, pengabaian nilai-nilai agama (*neglecting religious value*), martabat manusia (*human dignity*) serta membahayakan hubungan Internasional (*jeopardizing International relations*);

b. Kesusilaan

   Variasi tindak pidana kesusilaan mencakup pedopili *(paedophilia*), eksploitasi seksual terhadap anak (*sexual exploitation of children*), pertunjukan sex cecara live (*live sex shows*), *obscene and indecend transmission, obscene and indecent telephone calls.*

c. Telematika

   akses *illegal (hacking), cracking, intersepsi illegal, gangguan data (data interference),* gangguan sistem *(system interference),* penyalahgunaan peralatan, pemalsuan yang berkaitan dengan computer, penipuan yang menggunakan internet.

d. .Hak Kekayaan Intelektual

   Pelanggaran atas Hak Kekayaan Intelektual dapat berupa pelanggaran hak cipta (*copy rights infringement) , cybersquatting, cyberparasites, typosquatting, domain hijacking.*

e. Privasi

   menyangkut privasi terutama atas data dan informasi pribadi, bentuk tindak pidana yang sering dilakukan misalnya, pencurian identitas (*identity thief),* akses *illegal* serta diseminasi terhadap

[4] Akbar Kurnia Putra, *Jurnal Ilmu Hukum –Harmonisasi Konvensi cyber Crime dalam Hukum Nasional*, 2014 hlm.99

privasi dan data pribadi yang bersifat *sensitive (illegal access and dissemination of privacy and sensitive personal data).*

f. .Terorisme

Terorisme dalam *cyber crime* merupakan bentuk kejahatan yang baru dan disebut dengan *cyberterrorism*. *Cyber terrorism* berupa perbuatan dengan motif politik terhadap situs resmi suatu negara, informasi, sistem computer dan data yang mengakibatkan kekerasan terhadap rakyat sipil dan dilakukan oleh sub-nasional grup atau kelompok rahasia.

g. .Perdagangan dan keuangan

kegiatan perdagangan dan keungan dengan bentuk tindak pidana yang dilakukan meliputi: *spamming, internetscam, carding, page jacking, phising, security fraud, cyberlaundring, illegal trafficking of alcohol and drug*.

h. Perpajakan

Dalam bidang perpajakan bentuk tindak pidana yang dilakukan biasanya berupa penghindaran pajak (*tax evasion*) atau penggelapan pajak (*tax emblezzlement*) terhadap objek pajak yang dilakukan melalui transaksi internet.

Cakupan yang begitu luas, tersebut dengan menggunakan sarana computer berbasis internet ini dikendalikan oleh manusia, itu berarti menunjuk kejahatan yang terjadi potensinya adalah adanya subjek hukum dalam hal ini seseorang. Bila terjadi sifat dan bentuk kejahatan di ruang siber sudah pasti ada fungsi manusia yang melakukan pergerakan kegiatan unsur kejahatan yang dilakukan dengan memberikan kerugian pada manusia lainnya. Maka perilaku kejahatan itu dilakukan oleh seseorang yang memiliki niat dengan sengaja melakukan perbuatan melawan hukum dalam penggunaan sarana media teknologi, informatika dan komunikasi yang lebih populer disebut kejahatan di ruang maya atau *cybercrime*.

Dalam pandangan ahli hukum Barda Nawari Arief, bahwa delik-delik yang dikategorikan sebagai kejahatan dunia maya (*cyber crime*), dengan merujuk *Convention on cyber crime dari Dewan Eropa (council of Europe*) Nomor 25 Tahun 2000, dapat diuraikan bahwa kejahatan itu mencakup computer crime, dan delik yang dimaksud itu adalah sebagai berikut:[5]

1. Delik-delik terhadap kerahasiaan , Integrtas, dan ketersediaan data dan sistem computer ,yaitu :

[5] Abdul Wahid, Mohammad Labib, *Kejahatan Mayantara (cybercrime),* Refika Aditama, Bandung, 2005, hlm. 24

a. Mengakses sistem computer tanpa hak (*illegal access*);
b. Tanpa hak menangkap /mendengar pengiriman dan pemancaran (*illegal /interception*);
c. Tanpa hak merusak data (*data interference*);
d. Tanpa hak mengganggu sistem (*system interference*);
e. Menyalahgunakan perlengkapan (*misuse of device*)

2. Delik yang berhubungan dengan computer : pemalsuan, dan penipuan (*computer related offence, forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child phornography*).
4. Delik-delik yang berhubungan dengan hak cipta (*offence – related of infringiments of copyright*).

Dari delik yang dipaparkan di atas, maka terlihat jelas karakteristik *cyber crime* dibandingkan kejahatan secara konvensional sebagaimana berikut ini :[6]

a. Perbuatan yang dilakukan secara *illegal*, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyber space*) sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
c. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, dan kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
e. Perbuatan tersebut sering dilakukan secara transnational/melintasi batas negara.

Penekanan dari kejahatan siber yang dilakukan di ruang siber adalah dilakukan oleh seseorang yang memiliki kemampuan menguasai media internet, menggunakan ruang *virtual* dan mampu juga menembus batas ruang dan waktu serta wilayah hukum negara, yang dikenal dengan kejahatan melampaui batas negara (*transnational crime*). Dalam kontekstual ini dimaksudkan setiap sumber daya manusia yang berada di zona era digital harus mampu mengelola sifat dan bentuk

[6] *ibid*

telekomunikasi, informasi, dan kemampuan komunikasi yang cerdas agar tidak terjebak dalam pusaran bentuk kejahatan siber.

Keterdidikan dan keterlatihan dalam mengelola mentalitas diperlukan bagi setiap orang karena ini akan mempengaruhi seseorang dalam pengambilan keputusan saat melakukan interaksi di ruang siber. Tingginya penggunaan media komunikasi berbasis internet yang mempengaruhi perubahan pola interaksi komunikasi sosial dalam masyarakat memberikan dampak hukum pada fungsi sebab dan akibat timbulnya permasalahan hukum, bagi masyarakat sosial yang belum siap terhadap pengelolaan fungsi sistem digitalisasi atas kebutuhan penting mengkonsumsi informasi dan mengelola informasi itu sendiri.

Untuk itu diperlukan penguasaan literasi media yang serius agar tidak masuk di dalam pusaran arus permasalahan hukum yang sering terjadi dalam masyarakat sosial yang akhir-akhir ini dipadati oleh kasus penipuan dan pencemaran nama baik, kelemahan pada fungsi kurangnya literasi media bagi sumber daya manusia memang perlu ditingkatkan dalam pemahaman tentang akibat hukum dan perlindungan hukumnya atas ketentuan dari berlakunya Undang-Undang Nomor 19 Tahun 2016 tentang Informatika dan Transaksi Elektronik atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang ITE, bagi setiap orang.

Ketentuan yang diatur di dalam Undang-Undang tentang Informasi dan Transaksi Elektronik berlaku untuk setiap orang, itu berarti secara *outomatically* terdapat juga upaya pemberian perlindungan hukum bagi setiap orang akibat dari dampak perbuatan melawan hukum yang dilakukan oleh seseorang baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia dan yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

B. Kemanfaatan Teknologi 4.0 Terkait Perlindungan Hukum Data Privasi Terhadap Hak Asasi Manusia

Percepatan teknologi dalam era digitalisasi, membawa konsekuensi logis atas penggunaannya. Konsekuensi itu adalah tersebarnya data privasi setiap orang dalam penggunaan kemanfaatan teknologi saat melakukan aktivitas secara virtual dengan sistem digitalisasi, dengan banyak meminta data- data pribadi sebagai syarat penggunaan lanjut dari teknologi untuk mengakses internet.

Selanjutnya data privasi tersebut tidak didukung oleh perlindungan hukum bagi setiap orang yang merupakan subjek hukum sebagai penggunanya.

Banyaknya pelanggaran hukum yang terjadi karena mengakses data secara *illegal* ini menimbulkan keprihatinan sendiri, akibat dari kebijakan *e-government* oleh pemerintah dan tidak dapat dihindari disebabkan kebutuhan pada era disrupsi (*disruption era*). Karena dalam era disrupsi ini segala sesuatu terjadi secara random, baik hal positif maupun negatif, seseorang dapat melakukan kemudahan di ruang siber tetapi juga akan menimbulkan kejadian yang berbahaya, dan ini semua terkait dengan dampak hukum dari perilaku atas perbuatan melawan hukum di ruang siber dalam potensi pusaran era digitalisasi, hingga menakibatkan kerugian bagi subyek hukum lainnya.

Maka beberapa instrument hukum Internasional telah mengupayakan mengatur prinsip-prinsip data privasi yang diakui secara Internasional dan menjadikan fondasi bagi hukum perlindungan data nasional dan modern. Ada banyak instrument hukum berupaya melakukan perlindungan hukum privasi diantara perjanjian Internasional yang melindungi data privasi adalah :[7]

1. Deklarasi Universal tentang Hak Asasi Manusia 1948 (UDHR)

   Deklarasi Universal tentang Hak Asasi Manusia 1948 UDHR merupakan Instrumen Internasional pertama yang melindungi hak Privasi seseorang secara khusus diatur pada Pasal 12 yakni :

   " *No one shall be subjected to arbitrary interference with his Privacy, family, home or correspondence, not to attacs upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks*."

   Artinya semua orang harus mendapat perlindungan hukum karena mereka memiliki hak untuk tidak diganggu privasinya, keluarganya, tempat tinggal, dan korespodensi ataupun kehormatan serta reputasinya. Di dalam Pasal 12 tersebut bahwa Istilah Privasi dianggap sebagai *Umbrella terms* karena dikaitkan dengan perlindungan hak lain yaitu keluarga, tempat tinggal, korespondensi juga termasuk kehormatan dan nama baiknya.

[7] *Asbjorn eide, Alfredsson Gudmundur, (et al), 1992, The Universal Declaration of Human Rights: a Commentary, Oslo, hlm. 188-214*

Secara substantif pengaturan privasi di dalam Pasal 12 UDHR memberikan perlindungan yang sangat luas karena meliputi hak tentang :

1. *Phisical Privacy*

   Perlndungan priasi yang berkaitan dengan tempat tinggalnya , contoh sesseorang tidak boleh memasuki rumah orang lain tanpa izin pemilik, Negara tidak boleh menggeledah rumah seseorang tanpa adanya surat penahanan, negara tidak boleh melakukan penyadapan terhadap tempat tinggal seseorang.
2. *Decisional Privacy*

   Perlindungan privasi terhadap hak untuk menentukan kehidupannya sendiri termasuk kehidupan keluarganya. Contoh dia mempunyai hak untui menentukan kehidupan rumah tangganya sendiri, cara mendidik anak.
3. *Dignity*

   Melindungi harga diri seseorang termasuk nama baik dan reputasi seseorang.
4. *Informational Privacy*

   Privasi terhadap informasi artinya hak untuk menentukan cara seseorang melakukan dan menyimpan data privasinya.

UDHR menjadi intrumen Internasional yang paling penting karena telah disepakati hampir di seluruh Negara dalam upaya memberikan perlindungan hukum pada setiap orang. Isi dari UDHR juga mengatur secara komprehensif tentang hak-hak dasar umat manusia disebut dengan *common standard of achievement for all peoples and all nations* yang tercantum dalam pembukaan UDHR dan privasi merupakan salah satu hak dasar yang dilindungi UDHR.

Terkait dengan perlindungan hak asasi manusia, Indonesia juga meratifikasi dan memasukkannya dalam ketentuan Undang-Undang Dasar Negara Republik Indonesia dalam ketentuan Bab XA Hak Asasi Manusia, ini bisa memberikan hak bagi setiap orang dalam negara hukum Negara Kesatuan Republik Indonesia bisa menegakkan hak nya yang tidak boleh dilanggar oleh siapapun, atas kepentingan perlindungan hak Pribadi atau hak Privasi. Ini sejalan dengan

Konvensi Eropa tentang Hak Asasi (ECHR, 1950) adopsi dari *dari Convention for the Protection of Human Rights* (ECHR) Tahun 1950 dalam ketentuan Pasal 8 dari ECHR menyatakan bahwa :[8]

"*everyone has the right to respect for his private and familylife, his home and his correspondence*"

Ini diartikan secara luas terkait istilah dalam teknologi yang netral sehingga berlaku agi pasar elektronik dan lingkungan online. Khususnya kasus dalam *European Court of Human Rights* (ECHR) menegaskan bahwa Pasal 8 mengatur mengenai perlindungan penting bagi data privasi. Dalam Pasal 8 ayat (2) ECHR juga mengatur tentang kewajiban Pemerintah dalam menjalankan tugasnya tidak melanggar Privasi warga negara. Hal ini terkait dengan penangkapan, penyidikan, yang harus selalu berdasarkan hukum.

C. Peraturan Perundang-Undangan di Indonesia Dalam Memberikan Perlindungan Hukum Privasi

Menelisik ketentuan perlindungan hak privasi di era digital, Majelis Umum Perserikatan Bangsa-Bangsa pada Tahun 2014 mengeluarkan upaya mengambil Resolusi-nya, dengan tegas Komite ketiga Majelis Umum PBB (*The Third Committee of the United Nations General Assembly*) tanggal 25 November 2014 melakukan resolusi dengan menyerukan negara-negara untuk menghormati dan melindungi hak privasi di era digital. Resolusi itu merupakan respon gerakan yang dimotori oleh Jerman dan Brasil yang didukung oleh 35 negara, termasuk Indonesia. Sebelum Resolusi diadopsi, pada November 2013 Jerman dan Brasil mengajukan upaya rancangan resolusi dengan ketentuan berikut yang menjadi perhatian bersama , yakni :[9]

1. Tujuan dan prinsip Piagam Perserikatan Bangsa-Bangsa;
2. Hak asasi Manusia dan Kebebasan dasar yang diabadikan dalam Delarasi Universal Hak asasi manusia dan perejanjian hak asasi manusia Internasional yang relevan, termasuk Kovenan Internasional tentang Hak-hak Sipil dan Politik dan Kovenan Interenasional tentang Hak ekonomi, sosial dan Budaya;
3. Bahwa laju perkembangan teknologi memungkinkan individu di seluruh dunia untuk menggunakan teknologi informasi dan komunikasi baru dan pada saat yang bersamaan juga

[8] *European Convention for the protection of Human rights*
[9] *Brazil and Germany :draft resolution, United Nations General Assembly, November 2013*

meningkatkan kapasitas pemerintah, perusahaan, dan individu untuk melakukan pengawasan, intersepsi dan pengumpulan data yang mungkin melanggar atau melanggar hak manusia, khususnya ha katas privasi, sebagaimana diatur dalam Pasal 12 Deklarasi universal Hak asasi Manusia dan Pasal 17 dari Kovenan Internasional tentang Hak Sipil dan Politik, dank arena itu merupakan isu peningkatan kepedulian;

4. Bahwa terdapat hak manusia dalam hal tidak ada intervensi sewenang-wenang atau secara tidak sah terhadap privasi, keluarga, rumah atau Korespodens, serta terdapat ha katas perlindungan hukum terhadap gangguan-gangguan tersebut, dan mengakui bahwa perlindungan ha katas privasi penting bagi realisasi ha katas kebebasan berekspresi dan untuk menyatakan pendapat tanpa gangguan, dan salah satu dasar dari masyarakat demokratis;
5. Bahwa penghormatan sepenuhnya terhadap kebebasan untuk mencari, menerima dan menyampaikan informasi, termasuk pentingnya akses informasi dan partisipasi demokratis adalah hal yang penting;
6. Bahwa pengawasan yang melanggar hukum atau sewenang-wenang dan/ atau intersepsi komunikasi, serta pengumpulan tidak sah atau sewenang-wenang data privasi, sebagai tindakan yang sangat intrusive, melanggar hak rivasi dan kebebasan bereskpresi dan mungkin bertentangan dengan prinsip-prinsip masyarakat demokratis;
7. Bahwa meskipun kekhawatiran tentang keamanan publik dapat membenarkan pengumpulan dan perlindungan informasi sensitif tertentu, negara harus memastikan kepatuhan penuh dengan kewajiban mereka dibawah hukum hak asasi manusia Internasional;
8. Terdapat keprihatinan terhadap dampak negatif yang dihasilkan dari kegiatan pengawasan dan/ atau intersepsi komunikasi, termasuk pengawasan ekstra teritorial dan/ atau intersepsi komunikasi ekstra teritorial, serta pengumpulan data privasi, khususnya ketika dilakukan dalam skala massal, mungkin dapat berpengaruh terhadap hak asasi manusia;
9. Bahwa negara harus memastikan bahwa setiap tindakan yang diambil untuk memerangi terorisme sesuai dengan kewajiban mereka di bawah hukum Internasional, hak asasi manusia Internasional khususnya, pengungsi, dan hukum humaniter.

Ini menjadi tonggak penting adanya upaya perlindungan atas hak privasi dalam era disrupsi di masa teknologi digital. yang diadopsi adalah mengenai hak privasi di Era Digital (*The Rights of*

Privacy in digital Age).terlebih dalam pergerakan situasi dan kondisi masyarakat media yang banyak menggunakan kemanfaatan teknologi 4.0 perlindungan data pribadi menjadi sangat urgent untuk dilakukan upaya perlindungan hukum bagi setiap pengguna. Dalam hal ini khususnya menjadi tanggungjawab dari pengelola media berbasis internet dan Pemerintah yang memberikan ijin beroperasinya akses Media berbasis internet tersebut.

Privasidan perlindungan data privasi di masa musim pandemi covid 19 ini dan adanya kebijakan *Work From Home* saat ini menjadi jelas kemanfaatan teknologi 4.0 sangat membantu turut memperlancar segala bentuk kegiatan masyarakat terkait tanggungjawab pekerjaannya yang semula berada di perkantoran beralih ke rumah. Namun kondisi ini membutuhkan media berbasis internet yang memperlacar capaian tujuan dalam keterkaitan menyelesaikan pekerjaan, menjadi permasalahan yang timbul dan harus dihadapi adalah mengantisipasi bocornya data yang dipergunakan dalam ruang media teknologi saat transformasi komunikasi dan informasi ketika sedang berlangsung melalui media berbasis teknologi internet itu.

Perlindungan dasar hak dasar hidup bangsa Indonesia ada dan merujuk pada Pasal 28G dari Undang-Undang Dasar 1945 sebagai pedoman untuk membuat peraturan lebih khusus tentang perlindungan data privasi.

Pasal 28G Undang-Undang Dasar 1945 Negara republik Indonesia, menyatakan :

"*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlidungan dari ancaman ketakutan untuk berbuat atau tidak berbuat seseuatu yang merupakan hak asasi."*

Adanya ketentuan dasar dalam UUD 1945 itu makaharus kita lihat secara serius bahwa ini dapat membantu menegkkan hukum yang terkait dengan perlindungan hukum atas hak pribadi, sekalipun bunyi Pasal 28 G itu bunyinya tidak secara eksplisit. Kendati demikian ketentua Undang-Undang Dasar tersebut tidak secara eksplisit tapi cukup menjelaskan dan menunjuk adanya perlindungan hak asasi manusia.

Sesuai perkembangan teknologi di era disrupsi ini perlindungan hukum terhadap data pribadi adalah hak asasi manusia yang menjadi sangat penting untuk disampaikan dalam ruang hukum dan disosialisasikan kepada masyarrakat Indonesia yang tidak menyadari bahwa hak pribadi mereka adalah bentuk hak hukum secara personal, hal ini dikarenakan masyarakat Indonesia adalah masyarakat komunal yang kehidupannya sangat terbuka dan kebiasaan yang budaya yang mudah percaya pada orang lain.

Ada beberapa peraturan perundangan yang didalamnya telah mengatur tentang hak pribadi (privasi) dalam berbagai bidang diantaranya ada Undang-Undang Perbanka, Undang-Undang Telekomunikasi, Undang-Undang Perlindungan Konsumen, Undang-Undang Hak Asasi Manusia, Undang-Undang Administrasi Kependudukan, Undang-Undang Kesehatan dan Undang-Undang Informasi Transaksi Elektronik, serta Undang-Undang Keterbukaan Informasi Publik, meski semua tersebut tidak banyak diketahui masyarakat kita, akan fungsi dan kemanfaatan bagi hak asasi-nya, ini dikarenakan koordinasi antara aparat hukum dan pemerintah yang menyelenggarakan kebijakan tersebut tidak memiliki *goodwill* dalam penerapan pelaksanaan penyelenggaraan pelayanan birokrasi yang bersih. Itu dapat diketahui dalam berbagai kasus yang terjadi akhir-akhir ini hingga bila terdapat masalah hukum terkait kejahatan media eletronik berbasis internet, yang menjadi ruwet adalah *relationship* dari keterkaitan pembuat kebijakan dalam memberikan keputusan yang mendukung pihak yang dirugikan justru menjadi semakin tidak memiliki kepastian, dikarenakan petugasnya masih terlalu apatis dalam memberikan pelayanan yang seharusnya.

Penulis mengambil beberapa ketentuan peraturan perundanng –undangan sebagai penguatan hukum dari pemberlakuan upaya perlindungan hukum terhadap data privasi atau data pribadi terkait pelaksanaan dan penggunaan Teknologi 4.0 di ruang siber. hal itu terdapat dalam ketentuan yang bisa kita lihat narasi perlindungan hukum data pribadi ini menjadi penguatan pada fungsi penegakkan dan kepastian hukum yang harus menjadi perhatian aparat hukum untuk memberikan pemeliharaan atas hak data pribadi perseorangan yang dijamin oleh negara, dan pengguna kemanfaatan teknologi 4.0 di ruang disrupsi saat ini, diantaranya adalah :[10]

[10] Sinta Dewi Rosadi, *Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama, Bandung,, 2015, hlm.94-112

1. Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan ;

Undang-Undang Perbankan dalam pengaturannya meliputi masalah-masalah harus memelihara data-data privasi nasabah yang harus dilindungi, seperti Pasal 1 Ayat 28 Undang-Undang Perbankan 1998 menyebutkan definisi dari rahasia bank sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanannya.

Di dalam Pasal 40 Undang-Undang Perbankan Tahun 1998 juga disebutkan bahwa masalah rahasia bank, bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal tertentu yang dibolehkan. Pengaturan tersebut mengisyaratkan adanya perlindungan privasinasabah tidak hanya berkenaan dengan data keuangan baik itu merupakan simpanan atau produk bank lain miliknya tetapi juga data privasi nasabah yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data privasi lain di luar data keuangan. Pasal ini akan terkait dengan ketentuan Pasal 47 yang menunjuk siapa saja yang bertanggungjawab dan memiliki kewajiban harus memegang teguh rahasia bank tersebut.

Kendati demikian Undang-Undang Perrbankan memberikan pengecualian terhadap kepentingan perpajakan, penyelesaian piutang bank, kepentingan peradilan dalam perkara pidana yang dapat diberikan pada pihak aparat hukum seperti Polisi, Jaksa, atau Hakim atas ijin Pimpinan sebagaimana tercantum pada Pasal 42, dalam Perkara Perdata sebagaiman tercantum pada Pasal 43 dan Peraturan perlindungan dari data privasi nasabah juga diatur tentang pengaturan pidana dari pelanggaran rahasia bank yang diatur dalam ketentuan Pasal 47 Ayat (1) dan (2) yaitu :

Pasal 47 Ayat (1)

"*Barang siapa tanpa membawa perintah tertulis atau izin dari Pimpinan Bank Indonesia sebagaiman dimaksud dalam Pasal 41 dan 41A dan Pasal 42 dengan sengaja bank atau pihak terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekurang-kurangnya Rp.10.000.000.000 (sepuluh miliar rupiah) dan paling banyak Rp. 200.000.000.000 (dua ratus miliar rupiah)*"

Pasal 47Ayat 2

"Anggota Dewan Komisari, Direksi, Pegawai Bank atau pihak terafiliasi lainnya yang dengan sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40, diancam dengan pidana penjara sekurangkurangnya 2 (dua) tahun penjara dan paling lama 4 (empat) tahun serta denda sekurang-kurangnya Rp.4.000.000.000 (empat miliar rupiah) dan paling banyak Rp.8.000.000.000 (delapanmiliar rupiah)"

Satu lagi data privasi yang harus dilindungi terrkait perbankan yang masih relevan dalam sistem teknologi dengan berbasis internet, yang dapat digunakana untuk penguatan dalam perlindungan hukum bagi data pribadi hak asasi manusia atas kemudahan dan percepatan sistem perbankan dapat digunakan adalah prinsip kehati – hatian terkait dengan :

(a) permintaan Ahli Waris yang sah dari Nasabah atas penyimpanan dana yang telah meninggal dunia sebagaimana tercantum dalam Pasal 44 Ayat (2);

(b) Atas Persetujuan, permintaan atau Kuasa dari nasabah penyimpanan secara tertulis dapat diberikan pengecualiaan tanpa harus memperoleh izin pimpinan Bank Indonesia sebagaimana tercantum dalam Pasal 44 Ayat (1);

Dari aplikasi di lapangan ketentuan tersebut di atas dapat menjamin kerahasiaan dikarenakan ada persyaratan tertentu yang harus dibawa oleh Pihak yang berkepentingan dan sesuai prosedur yang berlaku secara hukum. Kendati demikian terdapat pengecualian yang sangat rawan terjadi kebocoran dalam menjaga kerahasiaan data pribadi setiap orang yaitu akan tetapi ada kelemahan yang tertera dalam ketentuan Pasal 44 memberikan penjelasan sebagai berikut :

" tukar menukar informasi antar bank diperbolehkan dengan tujuan untuk memperlancar dan mengamankan kegiatan usaha bank,antara lain guna mencegah kredit rangkap serta mengetahui keadaan dan statur dari suatu bank yang lain.''

Ini diharapkan dapat memberikan penilaian terhadap tingkat resiko tinggi sebelum melakukan transaksi dengan nasabah atau bank lain. Kerawanan yang dimaksud adalah tidak semua ada itikad baik dari setiap orang yang terkait dalam keterkaitan pada fungsi pekerjaaan seseorang di perbankan bukti yang ada dilapangan seringkali marketing dari bank lain bisa menyasar menelpn ke nomor telepon yang menjadi data pribadi hanya untuk urusan menawarkan produk perbankan, disini akan

terjadi hal yang tidak dinginkan untuk perilaku perbuatan melawan hukum lainnya sebagaimana kasus hukum pembobolan dana nasabah.

2. Undang- Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik ;

Bila kita lihat Pengertian sistem elektronik menurut Pasal 1 angka 5 UU ITE Nomor 19 tahun 2016 adalah serangkaian perangkat dan prosedur elketronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

Dari pengertian di atas tentang sistem elektronik dapat diketahui bahwa yang termasuk ke dalam sistem elektronik adalah *jaringan internet*, *layanan e-banking*, *e-government*, *jejaring sosial*, *media elektronik*, *websites*, dan yang terkait lainnya dengan sistem teknologi. Tentunya di dalam kemanfaatan Teknologi Informasi perlindungan data privasi menjadi hal penting untuk menjadi perhatian dikarenakan menjadi salah satu bagian dari hak privasi dan data pribadi merupakan konsentrasi dalam uapaya hukum memberikan hak hukum bagi penggunanya.

Guna memberikan rasa aman bagi pengguna sistem elektronik, Undang-Undang ITE mengatur megenai perlindungan atas data pribadi sebagai bentuk hak asasi manusia dan hak perlindungan terhadap hak data pribadi atau lebih menekankan pada hak privasi ini dituangkan dalam ketentuan Pasal 26 Ayat (1) Undang – Undang ITE .

Pasal 26 Ayat (1) Undang Undang ITE yang berbunyi :

"*Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data privasi seseorang harus dilakukan atas persetujuan orang yang bersangktuan*."

Makna dari perlindunganhak privasi dalam ketentuan Undang-Undang ITE dalam penjelasannya adanya perlindungan hak pribadi yang mengandung pengertian berikut ini :

1. Hak merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan ;

2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai;
3. Hak Pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Penggunaan setiap informasi dan data privasi dengan teknologi di masa era disrupsi ini bila dilakukan tanpa persetujuan pemilik data yang berhak maka ini menjadi pelanggaran hak pribadi atau hak privasi.

Diatur juga tentang adanya upaya mengakses sistem elektronik untuk memperoleh informasi atau dokumen elektronik, intersepsi atau melakukan penyadapan terhadap data atau informasi elektronik, dan memindahkan serta mentransfer informasi elektronik adalah perbuatan yang dilarang dan diancam dengan pidana. Meskipun telah terdapat penjelasan pada ketentuan Pasal 26 UU ITE itu, kewajiban perlindungan sebagai upaya hukum yang seharusnya dilakukan dengan seksama dan penguatan prosesnya yang harus dilakukan oleh aparat pihak terkait seperti penyelenggara pemerntah dalam hal ini sebagai tanggungjawab pemerintah di bidang pengelolaan komunikasi dan informasi belum sepenuhnya terdapat dalam nafas Undang-Undang ITE yang ada secara khusus.

3. Undang –Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Undang-Undang ini memberikan perlindungan akan data Informasi Publik yang dihimpun oleh badan public diatur dalam Pasal 6 Ayat (30 Undang-Undang Keterbukaan Informasi Publik, berdasarkan aturan terdapat informasi publik yang tidak dapat diberikan oleh badan public, yaitu :

1. Informasi yang dapat membahayakan negara;
2. Informasi yang berkaitan dengan kepentingan perlindungan usaha dari persaingan usaha yang tidak sehat;
3. Informasi yang berkaitan dengan hak-hak pribadi;
4. Informasi yang berkaitan dengan rahasia jabatan, dan/atau.
5. Informasi Publik yang diminta belum dikuasai atau didokumentasikan.

Jelas dan tegas dalam pengaturan tersebut di atas bahwa badan publik tidak dapat memberikan informasi publik yang salah satunya berkaitan dengan hak-hak pribadi. Ini dapat dilihat Pasal 52 Undang-Undang Keterbukaan Informasi publik mengatur bahwa badan publik yang dengan sengaja tidak menyediakan, memberikan dan/atau tidak menerbitkan informasi public berupa informasi publik secara berkala, informasi publik yang wajib diumumkan secara serta merta, informasi publik yang harus diberikan atas dasar permintaan sesuai dengan Undang-Undang ini, dan mengakibatkan kerugian bagi orang lain dikenakan pidana kurungan paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp.5.000.000,00 (lima juta rupiah).

Dengan demikian diketahui bahwa beberapa ketentuan peraturan perundang – undangan yang dimbali penulis beberapa untuk melihat pernyataan tegas akan upaya hukum terhadap perlidungan hak privasi yang terkait langsung dengan data pribadi sebagai hak asasi manusia itu telah ada dan mendapatkan jaminan perlindungan hukum terhadap hak privasi dari ketentuan Undang-Undang yang berlaku.

Praktik yang terjadi pada beberapa Negara – negara di dunia memang diwarnai pengaruh dari ketentuan hukum uni eropa yang lebih dulu melangkah mengambil penguatan terhapa perlindungan data privasi, dan Indonesia sebagai bagian pergaulan masyarakat hukum Internasional pun mengadopsi beberapa ketentuan hasil dari pertemuan Internasional.

Era disrupsi dengan kemanfaatan teknologi 4.0 akan terus bergulir untuk mencapai generasi lebih lanjut yaitu generasi 5.0 yang sudah diberlakukan oleh beberapa negara yang sudah melaksanakanya, tiu berarti tantangan baru sudah di depan mata untuk harus tegas Indonesia memiliki Komitmen memberikan pemahaman sadar kemanfaatan dan bahaya dari teknologi itu sendiri terhadap batasan dari adanya hak privasi akan data pribadi.

Ruang teknologi dan kecanggihannya tentu dapat disalahgunakan untuk kepentingan bagi pelanggaran hukum terhadap data privasi itu, contoh ramainya penyalahgunaan E-KTP saat pelaksanaan Pemilu 2019, disebabkan ruang disrupsi sudah melakukan aplikasi dari E-Government, meskipun kita fahami tujuannya baik tetapi niat jahat dating dari manapun, dan ini perlu adanya komitmen tegas dari aparat hukum khususnya pihaka terkait polisi, Jaksa, dan Pengadilan serta pemerintah daerah dan ujung tombak dari urusan masyarakat sipil, juga masyarakat lebih luas lagi,

harus dibekali pemahaman tentang adanya kerawanan dari penyalahgunaan dalam penerapan fungsi *E-Government* terhadap pelanggaran kepentingan Hak Privasi dan data pribadi itu.

Perkembangan teknologi di era disrupsi mengubah semua paradigm kehidupan dari batas wilayah, waktu, nilai-nilai dala]m sendi kehidupan, logika berpikir, perilaku sosial hingga pola kerja y]ang sekarang sudah mulai digunakan secara serentak seiring terjadinya wabah pandemic covid 19 dengan diterbitkan peraturan *Work From Home* maka seluruh tanggungjawab dilakukan dengan menggunakan kemajuan teknologi berbasis internet.

Kondisi tersebut menuntut setiap orang dipaksa menguasai berbagai bentuk sistem media teknologi berbasis internet, tetapi sekaligus menuai konsekuesni logis, terjadi timbul kejahatan berbasis teknologi dengan kenyataan sistem computerized atau digitalisasi berkejaran dengan ketentuan penegakkan dan kepastian hukum terhadap perlindungan hak privasi setiap orang selaku subjek hukum.

Dengan demikian dibutuhkan pendekatan secara sosiologis dan yuridis yang harus disampaikan pada yang berhak yaitu masyarakat pengguna media teknologi aktif. Kementerian Komunikasi dan Informatika mulai melakukan pelatihan terhadap bentuk perlindungan kepada pengguna internet di Indonesia dari kejahatan siber termasuk dalam kategori penipuan berbasis internet, dengan cara;[11]

1. Pembentukan Regulasi yang mengkhususkan pengaturan perlindungan Hukum Privasi data pribadi;
2. Pendekatan Infrastruktur;
3. Pendekatan masyarakat

Terkait hal tersebut di atas maka Kementerian Komunikasi dan Informatika telah melakukan upaya hukum dengan pihak aparat hukum pada lintas tanggungjawab terkait yaitu pihak kepolisiandengan melakukan kegiatan edukatif terkait pencegahan praktik *internet fraud* khusus yang bersinggungan dengan perlindungan hukum pivasi terhadap pengamanan data pribadi, diantaranya sebagai berikut :

1. Meningkatkan awareness keamanan informasi kepada masyarakat dan aparat penegak hukum;

[11] Maskun, Wiwik Meilarati, *Aspek Hukum Berbasis Internet*, Keni Media, Bandung, 2017, hlm.96-99

2. Meningkatkan pengetahuan dan kemampuan aparat penegak hukum (Polis, Jaksa dan Hakim) mengenai trend Kejahatan siber dan penegakkan hukum nya baik legal dan tekhnis digital forensik, agar tidak bertindak secara liar hukum yang ada di dalam masyarakat;
3. Mengembangkan Regulasi yang dibutuhkan dan diperlukan yaitu data pribadi, sertifikasi kelaikan, sertifikasi keandalan, dan tanda tangan elektronik;
4. mendorong penyelenggara *e-commerce* untuk mendaftarkan sistem elektroniknya dengan maksud dapat diketahui oleh masyarakat sebagai penyelenggara yang terpercaya;
5. Mengadakan *assessment* indeks keamanan informasi kepada instansi atau lembaga pemerintah agar instansi tersebut memahami kondisi keamanan informasi mereka dan dapat mengambil upaya yang diperlukan untuk meningkatkan keamanan informasi.

Maka dalam penyelesaian permasalahan hukum akibat kejahatan dengan sengaja menabrak ketentuan perlindungan hak privasi terrhadap data pribadi dengan menggunakan kecanggihan teknologi di masa percepatan era digitalisasi yang terus berkembang, ddapat dilakukan dengan pendekatan penafsiran atau interpretasi menjadi sangat penting dan strategis dilaksanakan.

D. Kesimpulan dan Saran

Kesimpulan Dari sampaian paparan di atas tadi maka dapat menjadi perhatian penting adalah menjadi penting bagi semua pengguna Tekologi 4.0 dengan kemanfaatannya. Benar beberapa produk Undang-Undang mencantukan adanya perlindungan data privasi akan bocornya data pribadi ke wilayah yang tidak berhak, namun belum maksimal dalam penerapannya di lapangan.

Ini banyak kita dapati bagaimana setiap orang seringkali mendapati orang tidak dikenal mampu menghacker akun pemilik data pribadi. Padahal diketahui telah ada UU ITE diterbitkan di Indonesia yaitu UU ITE Nomor 19 Tahun 2016 dan ada banyak berbagai negara telah menerbitkan kebijakan peraturan perundang-undangan khusus untuk melakukan personal *information protection act* , bahkan Perserikatan Bangsa-Bangsa melalui Majelis Umum telah mengeluarkan Resolusinya terkait Hak Privasi di Era digital, pada tahun 2014, yang diadopsi 35 Negara di dunia bahkan Indonesia juga turut mengadopsi Resolusi ini. Ini dilakukan terkait dengaan jaminan hak asasi manusia , dan penghormatan terhadap hak kebebasan pribadi, sekaligus perlindungan hukum atas

kesewenangan dari pihak yang memiliki niat jahat, adanya perlindungan dari dampak negatif akibat ekstrateritorial dari perkembangan teknologi era digital.

Maka dalam upaya perlindungan hukum terhadap pengguna komunikasi dan informatikan dengan media berbasis internet di era disrupsi ini diperlukan pendekatan yuridis dan sosiologi. Pendekatan yuridis harus mendorong harmonisasi hukumdengan memperkecil potensi konflik antar negara, pendekatan sosiologis adalah dengan memberikan sosialisasi dan pelatihan terus menerus dalam penggunaan teknologi dan juga pendekatan dengan sistem market online, dikarenakan telah banyak market yang dengan sadar menggunakan media daring untuk kepentingan interaksi pemasaran suatu produksi. Diharapkan dengan pendekatan dan terbitnya Undang-Undang perlindungan Hukum data Privasi dapat memberikan kepastian hukum dan harmonisasi terrcapainya instrument hukum Nasional dan Internsional agar dapat memiliki kekutan mengikat dan adanya pertanggungjawaban hukum yang jelas dan tegas akan kewajiban Negara dalam melindungi warganegaranya di wilayah territorial dan batas territorial yang berlaku secara global atau *global privacy rules*, tentunya akan berdampak terhadap semua negara yang memiliki komitment internasional atas dampak hukum dari kemajuan teknologi 4. 0 terhadap perlindungan bagi setiap pengguna media digital dan hak privasinya.

Sesuai dengan kesimpulan di atas, penulis dapat mengajukan 3 (tiga) macam saran. Ketiga macam saran tersebut adalah sebagai berikut:

1. Penguasaan teknologi atau dikenal dengan istilah literasi media teknologi, tidak hanya jeda pada fungsi menggunakan saja tetapi mampu mengendalikan diri dan emosi, dalam kemanfaatan penggunaan teknologi khususnya menjalankan prinsip kehati hatian terhadap data pribadi yang tidak harus dibuka secara terbuka dalam ruang siber media teknologi yang tanpa batas tersebut.
2. Memahami ketentuan Peraturan perundang-undangan terkait dampak dari keterbukaan dalam informasi yang diberikan ke ruang publik dan dampak hukum yang ditimbulkan atas perbuatan hukum.
3. Pemerintah penyelenggara kebijakan terkait komunikasi dan informatika harus melakukan pendekatan multiaspek dalam penanggulang kejahatan dengan pendekatan sistemik yaitu aspek sosial, budaya, teknologi , politik dan hukum masing- masing dengan sistem saling terkait dan mempengaruhi untuk bersama – sama menanggulangi kejahatan atas kebocoran data pribadi

maka Pemerintah sebagai penyelenggara terlaksanannya penggunaan media elektronik dalam sendi kehidupan masyarakat media berbasis internet, harus mampu semaksimal mungkin memberikan perlindungan hukum atas hak data pribadi setiap orang di negara berdaulat Negara Republik Indonesia

4. Maka keberpihakan pada pengguna yang tidak memahami teknologi dan sering menjadi objek penipuan berbasis internet dengan mencuri data pribadi, menjadi prioritas utama dilakukan oleh pihak aparat hukum terkati yaitu kepolisian, jaksa dan Hakim, bukan malah sebaliknya.

E. Ucapan Terimkasih

Penulis ingin mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan dan semangat, sehingga tulisan ini dapat diselesaikan.

F. Biodata Singkat Penulis

Penulis bernama lengkap Sri Ayu Astuti ini lahir di Balikpapan Kalimantan Timur, mengambil Pendidikan Doktor Ilmu Hukum di Universitas Islam Bandung dengan Konsentrasi Hukum Media dan S3 Ilmu Hukum tersebut diselesaikan pada Tahun 2012 dengan Predikat *Cumlaude*. Penulis yang saat ini adalah Dosen Tetap di Prodi Hukum Pasca Sarjana Universitas Pakuan Bogor sejak Tahun 2019 merupakan Pemerhati Media sekaligus pernah melewati tugas sebagai insane Media Mainstream yaitu pada Institusi media Pemeritah TVRI saat masih bernaung di bawah pengelolaan Departemen Penerangan Republik Indonesia. Penulis yang telah akrab dengan teknologi media sejak menjadi seorang Penyiar TVRI di Tahun 1986 ini pernah berkarir diberbagai Perusahaan Migas dan terus mencermati perkembangan Teknologi Media terlebih saat berada di Perusahaan Pengeboran Minyak milik Amerika dan Australia bernama Petrosea, setelah itu penulis memutuskan masuk dalam pusaran Media Mainstream secara total pada Tahun 1992 sebagai Reporter dan *News Presenter* hingga menjabat sebagai Kabid Hukum dan akhirnya Penulis melepas karirnya di TVRI Jawa Timur pada Tahun 2005 beralih dari PNS-nya dari Departemen Penerangan Republik Indonesia ke ruang Pendidikan Tinggi Dirjen Dikti 1 Mei 2005 untuk pertamakali ditempatkan mengajar di FISIP UPN sekaligus sebagai staf Biro Akademik, dan Tahun 2008 beralih tugas ke Universitas Muhammadiyah Sidoarjo yang dikenal dengan UMSIDA sebagai Dosen Fakultas Hukum sekaligus menjabat sebagai Dekan Fakultas Hukum. Penulis juga aktif di

berbagai Kegiatan Masyarakat satu diantaranya pernah menjadi Kabid Media di Forum Koordinasi Pencegahan Terorisme, FKPT Jawa Timur dari Tahun 2012/2017, Penulis aktif sebaggai Ketua Bidang I Organisasi dan Pembinaan Daerah Ikatan Alumni Lemhannas RI IKAL ToT Sulawesi Selatan angkatan I 2018/2023, Penulis merupakan Anggota Bidang Non Litigasi Majelis Hukum dan HAM PP Muhammadiyah Jakarta 2016/2020, Penulis juga merupakan Dewan Kehormatan dari Perikatan Advokad Nusantara PERKASA Dewan Pimpinan Pusat Surabaya 2020/2025, Penulis sebagai *Vice* Presiden Asosiasi Perhimpunan Doktor Hukum Indonesia APDHI 2018/2022, penulis juga merupakan Editor ahli di Majalah Kirana Surabaya sekaligus sebagai penulis aktif.

DAFTAR PUSTAKA

A. Buku- Buku

Agus Raharjo, *Cyber crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, , 2002

Akbar Kurnia Putra, *Jurnal Ilmu Hukum –Harmonisasi Konvensi cyber Crime dalam Hukum Nasional*, 2014

Abdul Wahid, Mohammad Labib, *Kejahatan Mayantara (cybercrime)*, Refika Aditama, Bandung, 2005

Asbjorn eide, Alfredsson Gudmundur, (et al), 1992, The Universal Declaration of Human Rights: a Commentary, Oslo

Danrivanto Budhijanto, Hukum, Telekomunikasi, Penyiaran dan Teknologi Informasi Regulasi dan Konvergensi, Refika Adhitama, Bandung, 2010

Peter Mahmud Marzuki , *Penelitian Hukum*, Kencana Jakarta , 2005

Maskun, *Kejahatan siber (cyber crime)*, Kencana Pranada Media Group, Jakarta , 2013

Maskun, Wiwik Meilarati, *Aspek Hukum Berbasis Internet*, Keni Media, Bandung, 2017

Niniek Suparni, *Cyberspace, Problematika dan antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009

Sinta Dewi Rosadi, *Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama, Bandung,, 2015

B. PERATURAN DAN PERUNDANG-UNDANGAN DAN KONENSI

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan

Undang-Undang Nomor 19 Tahun 2016 TentangInformasi dan Transaksi elektronika

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

Brazil and Germany :draft resolution, United Nations General Assembly, November 2013