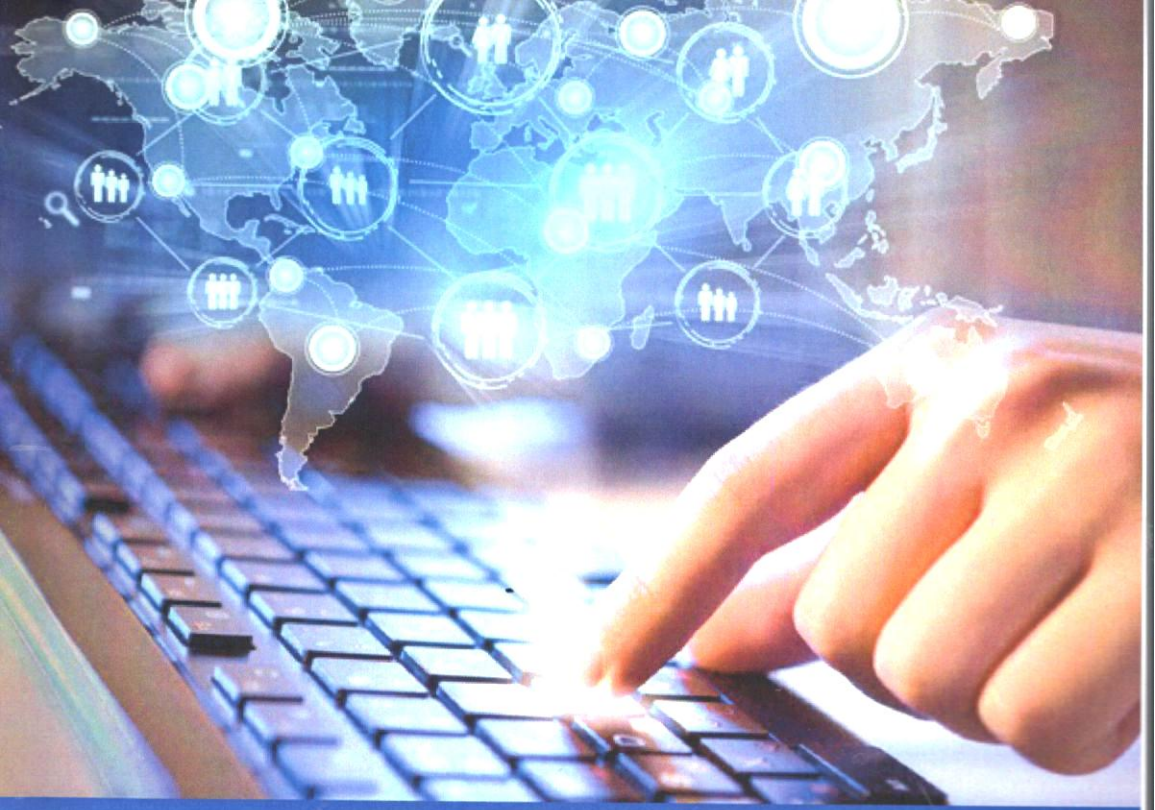


EKSPLOITASI TEKNOLOGI, CYBER PROTECTION DAN GENERASI ALPHA

Prof. Dr. I Gede A.B. Wiranata, S.H., M.H.
Dr. Rudi Natamihardja, S.H., D.E.A.
Bayu Sudjadmiko, S.H., M.H., Ph.D.

EKSPLOITASI TEKNOLOGI, CYBER PROTECTION DAN GENERASI ALPHA

EKSPLOITASI TEKNOLOGI, CYBER PROTECTION DAN GENERASI ALPHA

Prof. Dr. I Gede A.B. Wiranata, S.H., M.H.
Dr. Rudi Natamihardja, S.H., D.E.A.
Bayu Sudjadmiko, S.H., M.H., Ph.D.

AURA
ANUGRAH UTAMA RAHARJA

Perpustakaan Nasional RI:
Katalog Dalam Terbitan (KDT)

**EKSPLOITASI TEKNOLOGI,
CYBER PROTECTION DAN GENERASI ALPHA**

Penulis:
Prof. Dr. I Gede A.B. Wiranata, S.H., M.H.
Dr. Rudi Natamihardja, S.H., D.E.A.
Bayu Sudjadmiko, S.H., M.H., Ph.D.

Editor:
Prof. Dr. Sunarto, S.H., M.H.

Desain Cover & Layout
Team Aura Creative

Penerbit
AURA
CV. Anugrah Utama Raharja
Anggota IKAPI
No.003/LPU/2013

viii + 107 hal : 15,5 x 23 cm
Cetakan, Oktober 2019

ISBN: 978-623-211-116-5

Alamat
Jl. Prof. Dr. Soemantri Brojonegoro, No 19 D
Gedongmeneng Bandar Lampung
HP. 081281430268
082282148711
E-mail : redaksiaura@gmail.com
Website : www.aura-publishing.com

PRAKATA

Teknologi *borderless* memberikan dampak seperti dua mata pisau yang mempunyai sisi positif dan negatif. Eksploitasi teknologi yang dimotori oleh negara-negara maju terkadang memberikan ketergantungan kepada negara-negara berkembang sebagai konsumen. Dinamika sosial terhadap pemanfaatan teknologi baik di negara maju dan negara berkembang sangat mempengaruhi perkembangan dan pembangunan secara menyeluruh di suatu negara.

Indonesia sebagai negara keempat terbesar dalam jumlah penduduknya adalah salah satu negara yang paling banyak dalam memanfaatkan teknologi internet pada khususnya. Setiap lini pembangunan, Indonesia mulai menerapkan teknologi dalam prosesnya; *e-money*, *e-government*, *e-banking*, *e-management*, *e-library*, dll. Kondisi ini secara tidak langsung menciptakan budaya konsumerisme terhadap negara-negara berkembang. Buku Teks dengan judul "Eksploitasi Teknologi, Cyber Protection dan Generasi Alpha", ini memberikan deskripsi dan analisis hukum dan dinamika sosial mengenai praktek teknologi pada generasi alpha dan pembangunan di Indonesia.

Buku ini semula berasal dari Hibah Penelitian Guru Besar/Profesor yang bersumberkan bantuan dana Dipa Lembaga Penelitian dan Pengabdian Masyarakat Unila TA 2019. Hasil penelitian itu kemudian dikembangkan dan diperdalam dan akhirnya dituliskan dalam bentuk buku referensi ini.

Buku ini menitikberatkan pada kebijakan nasional dan internasional dalam usaha untuk melindungi data, pengguna dan teknologi internet dari efek-efek negatif teknologi itu sendiri.

Penulis mencoba menyajikan beberapa pemahaman dan panduan yang dapat dijadikan landasan dalam menyusun kebijakan teknologi bagi para pengguna, developer dan pemerintah dalam memaksimalkan pemanfaatan teknologi internet. Strategi dan tinjauan yuridis secara nasional juga penulis coba sajikan untuk menemukan analisa mendalam tentang kebijakan Indonesia mengenai praktek teknologi dan distribusi informasi sesuai dengan Undang-Undang No 36 tahun 1999 tentang Telekomunikasi dan Undang-Undang No 19 tahun 2016 tentang Perubahan Undang-Undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Semoga dengan hadirnya buku ini dapat memberikan informasi dan pemahaman khusus bagi mahasiswa Fakultas Hukum Universitas Lampung khususnya, dan bagi para pemerhati permasalahan teknologi pada umumnya.

Terima kasih dihaturkan kepada Ketua LP2M Universitas Lampung beserta jajarannya atas persetujuannya mendanai riset ini. Kepada Penerbit Aura Publisher layak pula dihaturkan terima kasih yang telah bersedia menerbitkan naskah buku ini.

Bandar Lampung, Oktober 2019

Prof. Dr. I Gede AB Wiranata, S.H., M.H, dkk.

DAFTAR ISI

I. TECHNOLOGY COLONIALISM ASSAULT DALAM PERKEMBANGANNYA 1

II. CYBER PROTECTION DALAM HUBUNGAN HUKUM DAN SOSIAL 7

2.1 Bank 8
2.2 Sosial Media 17
2.3 HAKI 22
2.4 E-Commerce 25
2.5 Government 28

III. INTERNATIONAL TELECOMMUNICATION UNION ONLINE PROTECTION GUIDELINES 39

3.1 International Telecommunication Union Guidelines For Children On Online Protection 2016 39
3.2 International Telecommunication Union Guidelines For Parents 46
3.3 International Telecommunication Union Guidelines For Industry On Child Online Protection. 53
3.4 International Telecommunication Union Guidelines For Policy Makers On Child Online Protection 61

IV. KERANGKA HUKUM NASIONAL TERHADAP DATA ONLINE DAN PENGGUNA 68

4.1 Perbankan 69
4.2 Sosial Media, dan Perlindungan data pribadi. 72
4.3 E-Commerce. 74
4.4 Hak Kekayaan Intelektual 77
4.5 Merek Dagang dan Jasa 77
4.6 Hak Cipta 80
4.7 Paten 84
4.8 Desain Tata Letak Sirkuit Terpadu 87
4.9 Desain Industri. 89

4.10 Rahasia Dagang 90

V. CYBER CRIME DAN UNDANG-UNDANG ITE 93

DAFTAR PUSTAKA 102

BAB I
TECHNOLOGY COLONIALISM ASSAULT DALAM PERKEMBANGAANNYA

Istilah kolonialisme bukan merupakan suatu istilah baru di tengah masyarakat dunia. Eksistensi dari kolonialisme sudah lama menjadi perhatian para filsuf politik dan moral dalam tradisi barat sejak perang salib dan penaklukan benua Amerika. Pada abad ke-19, ketika dominasi Eropa atas seluruh dunia mencapai puncaknya, ketegangan antara pemikiran liberal dan praktik kolonial menjadi sangat akut.[1] Kolonialisme diartikan sebagai suatu tindakan menguasai atau menduduki suatu wilayah atau negara dengan cara mendominasi secara keseluruhan suatu negara atas negara lain dimana kekuasaan atas negara tersebut berada di bawah kendali negara lain.[2] Pengertian kolonialisme memang hampir serupa dengan imperialisme, namun hal yang menjadi ciri dari praktik kolonialisme biasanya melibatkan pemindahan penduduknya ke wilayah baru, dimana para pendatang tinggal sebagai pemukim permanen sambil mempertahankan kesetiaan politik ke negara asal mereka.[3] Negara-negara yang melakukan kolonialisme membenarkan penaklukan mereka dengan beranggapan bahwa

[1] Margaret Khon dan Kavita Reddy. *Colonialism,* Stanford Encyclopedia of Philosophy, 2017. Diakses pada https://plato.stanford.edu/entries/colonialism/ tanggal 31 Juli 2019

[2] Stephen Ocheni dan Basil Nwankwo. Analysis of Colonialism and Its Impact in Africa, Cross Culture Communication, Vol. 8 No.3, 2012. 14 Juni 2012, hlm. 46

[3] *Loc.Cit.*

[4] Lauren Benton, The Legal Logic Of Wars Of Conquest: Truces And Betrayal In

mereka memiliki kewajiban secara hukum dan agama untuk mengambil alih tanah dan budaya masyarakat adat di wilayah tersebut. Hal ini mereka lakukan dengan alasan ingin memimpin para masyarakat adat atau primitif tersebut ke arah peradaban yang lebih maju dan manusiawi.[4]

Keberadaan kolonialisme sebenarnya sudah ada sejak zaman kekaisaran Yunani, Roma, Mesir, dan Phoenicia. Peradaban-peradaban ini memperluas kekuasaan mereka ke daerah-daerah sekitarnya sejak tahun 1550 sebelum masehi dan mendirikan koloni yang memanfaatkan sumber daya fisik dan populasi dari orang-orang yang mereka taklukkan untuk meningkatkan kekuatan dan sumber daya milik mereka.[5] Setelah runtuhnya zaman kekekasiaran, mucullah kolonialisme modern yang dimulai pada abad ke-15, dimana Portugal mulai mencari rute perdagangan baru dan mencari peradaban di luar Eropa. Setelah Portugis menaklukkan dan mengisi pulau-pulau seperti Madeira dan Cape Verde. Spanyol yang merupakan saingan mereka, memutuskan untuk ikut melakukan eksplorasi ke benua-benua baru yang diisi oleh orang-orang primitif. Peristiwa tersebut berlanjut hingga tahun 1914, dimana hampir sebagian besar negara-negara di dunia sudah dikolonisasi oleh bangsa Eropa seperti Inggris, Prancis, Belanda, Spanyol dan Portugis.[6] Akan tetapi setelah masuk ke abad 20, praktik kolonialisme secara konvensional yang memakan korban jiwa serta kerugian materiil yang besar sudah mulai ditinggalkan. Berdasarkan perspektif di abad ke-20, abad ini adalah abad yang sangat terpecah. Hal ini erat hubungannya dengan perang dunia dan mulai berkembangnya teknologi yang berkaitan langsung dengan perang, teknologi mobilisasi tenaga kerja, kontrol pertanian, ekstraksi sumber daya, dan pemberantasan penyakit yang dilakukan oleh

---

[4] Lauren Benton, The Legal Logic Of Wars Of Conquest: Truces And Betrayal In The Early Modern World, Duke Journal Of Comparative & International Law, Vol. 28, 2018. hlm 425-426.

[5] Ryan Schleeter. (2013). "First Rulers of the Mediterranean" diakses dalam https://www.national geographic. org/ news/first-rulers-mediterranean/ pada tanggal 31 Juli 2019

[6] Joan Ferrante. *Sociology: A Global Prespective.* (Belmont: Thomson Learning. Inc, 2008). hlm 216.

rezim kolonial dan penerusnya dengan upaya yang luar biasa dan kekuatan intervensionis di bawah tekanan perang global dan akibat yang disebabkan[7].

Sejak abad ke-20 bentuk kolonialisme berubah kearah kolonialisme berbasis teknologi digital atau yang sekarang disebut sebagai *digital-colonialism. Digital colonialism* adalah penyebaran baru kekuasaan *quasi imperial* atas orang banyak tanpa adanya persetujuan secara eksplisit, yang dimanifestasikan dalam aturan, desain, bahasa, budaya, dan sistem kepercayaan oleh kekuatan yang sangat dominan. Dahulu, kerajaan memperluas kekuatan mereka melalui kontrol aset-aset utama, dari rute perdagangan ke laut, jalur kereta api hingga logam mulia. Sekarang, perusahaan-perusahaan berbasis teknologi membangun kerajaan teknologi yang mengontrol data dan kekuatan komputasi untuk mendominasi dunia.[8] Kolonialisme digital atau *digital colonialism* diartikan sebagai bentuk dominasi struktural yang dilakukan melalui kepemilikan dan kendali terpusat dari tiga pilar inti ekosistem digital berupa perangkat lunak, perangkat keras, dan konektivitas jaringan.[9]

Pada zaman kolonialisme klasik[10], orang-orang Eropa mengambil alih tanah dari penduduk asli, mengeksploitasi tenaga mereka, menjalankan tata pemerintahan ekstrateritorial, dan menciptakan suatu ketergantungan dan menjarah warga asli wilayah tersebut melalui rencana yang terstrukur. Seperti perusahaan *East India Company* yang melakukan kolianisme ke wilayah-wilayah lain demi mengejar keuntungan dan kekuasaan dengan cara mengambil kepemilikan dan kendali atas infrastruktur yang strategis, termasuk pelabuhan, saluran air, dan jalur kereta api. Serupa dengan kolonialisme zaman klasik, kolonialisme digital berakar pada pembentukan teknologi sebagai tujuan mendapatkan keuntungan dan penjarahan. Saat ini, infrastruktur digital mengambil peran yang

---

[7] David Arnold, *Europe, Technology, and Colonialism in the 20th Century*. History and Technology Vol.21 No 1, 2005. hlm. 95

[8] Internet Health Report, *Resisting Digital Colonialism,* 2018 di download pada 1 Agustus 2019.

[9] Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South,* Race & Classroom Vol 60 No 4 2018. hlm. 2

[10] Zaman Kolinialisme klasik berawal pada abad ke 16 dan berakhir di abad ke 18.

sama seperti halnya jalur kereta api dan rute perdagangan maritim yang menjadi hal yang esensial pada zaman klasik. Perusahaan raksasa di bdiang teknologi telah menggunakan perangkat lunak, *cloud company*, dan layanan Internet terpusat untuk memata-matai pengguna, dan memroses data yang mereka kumpulkan.[11]

Beberapa teori mengungkapkan bahwa teknologi merupakan penggerak utama perubahan sosial di masyarakat dan menjadikan perubahan tersebut tidak dapat terhindarkan.[12] Hal ini sejalan dengan perkembangan teknologi yang telah membawa manusia ke suatu fase dimana setiap informasi telah diubah kedalam bentuk digital dan sebagian besar kegiatan masyarakat dapat dipermudah oleh teknologi. Sebagaimana yang kita tahu, bahwa saat ini manusia sulit sekali untuk tidak bergantung dengan teknologi sehingga menjadikan teknologi sebagai kebutuhan contohnya seperti kebutuhan hiburan (Tv, gawai, komputer dan lainnya), kebutuhan ilmu pengetahuan (*e-book*, *e-learning* dan lainnya)[13], bahkan saat ini, pemerintah sedang gencar menerapkan sistem *e-government* demi memudahkan administrasi di lingkup pemerintahan.

Dampak dari perkembangan teknologi yang tengah terjadi mengarah pada ketergantungan manusia terhadap teknologi sehingga perusahan teknologi yang berskala besar seperti *Google*, *Facebook*, *Uber*, *Microsoft*, *Apple*, *Samsung*, *Oppo*, dan lainnya dapat mempengaruhi cara kampanye, pemerintahan, dan mempengaruhi politik serta kebijakan pemerintah untuk membentuk standar global dalam melayani model bisnis mereka dibidang pengumpulan data atau pemantauan yang mengikis privasi banyak orang.[14] Kendali atas pilar-pilar ini memberi GAFAM (*Google* / *Alphabet*, *Amazon*,

---

[11] Michael Kwet, *Digital Colonialism is Threatening the Global South*, Al Jazeera 2019, didownload dalam https://www.aljazeera.com/topics/categories/science-and-technology.html pada 2 Agustus 2019

[12] Edmore Etekwe, *The Impact of Technology on Social Change: A Sociological Prespective,* Journal Research in Peace, Gender and Development Vol. 2 (11), 2012, hlm. 229.

[13] Richard Davis dan Ken Pease, *Crime, Technology, and the Future,* Security Journal, Perpetuity Press Ltd. 2000, hlm. 62.

[14] Renata Avila Pinto, *Digital Soverignity or Digital Colonialism,* Internet and Democracy Sur 27-v.15 n. 27, 2018. hlm. 17

Facebook, *Apple*, dan *Microsoft*) dan perusahaan raksasa lainnya, serta badan intelijen negara seperti *National Security Agency* (NSA) menjadi imperialis baru di komunitas internasional. Asimilasi ke dalam produk teknologi, model, dan ideologi kekuatan asing yang ada saat ini merupakan bentuk kolonisasi abad ke-21 yang dipimpin oleh negara-negara yang memiliki kendali atas perusahaan-perusahaan raksasa di bidang teknologi terhadap negara-negara berkembang.[15]

Berdasarkan penjabaran sebelumnya, sejatinya telah terjadi suatu kolonialisasi yang dilakukan korporasi di bidang teknologi digital yang didominasi oleh perusahaan dari negara-negara maju seperti Amerika Serikat dibidang mesin pencari/ *search engine* (*Google*), aplikasi penjelajah internet/*web browser* (*Google chrome*), sistem operasi gawai (*Google Android*, *Apple iOS*), sistem operasi *desktop* dan laptop (*Microsoft Windows*), perangkat lunak *office* (*Microsoft Office*, *Google Docs*), infrastruktur dan jasa penyimpanan *cloud* (*Amazon*, *Microsoft*, *Google*, *IBM*), *platform* sosial media (*Facebook*, *Twitter*), transportasi (*Uber*, *Lyft*), bisnis (*Microsoft LinkedIn*), *streaming video* (*Google YouTube*, *Netflix*, *Hulu*), dan iklan *online*.[16]

Penulis berpandangan, dominasi teknologi digital yang terjadi saat ini telah mengakibatkan monopoli dibidang jual/beli teknologi sehingga mengakibatkan sulitnya perusahaan teknologi domestik untuk berkembang dan bersaing dengan perusahaan teknologi multinasional sehingga timbul ketergantungan individu bahkan pemerintah terhadap teknologi tersebut. Seperti contoh teknologi transportasi (*Toyota*, *BMW*, *Ford*, *Suzuki*, *Yamaha*, *Ducati* dan lainnya), komunikasi (*Apple*, *Samsung*, *Oppo*, *Xiaomi* dan lainnya), bahkan persenjataan/militer (*Smith & Wesson*, *Sturm Ruger*, *Remington Arms* dan lainnya) yang secara rutin mendistribusikan produk-produknya ke setiap negara di dunia.

---

[15] Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South. Loc. Cit.*

[16] *Ibid.* hlm. 4.

Terjadi pergeseran makna pada nilai suatu teknologi yang saat ini lebih dari sekedar alat. Beberapa jenis dari teknologi memiliki sistem tersendiri terkait material non-budaya. Bahkan saat ini teknologi dapat menentukan pola pikir serta bagaimana manusia berhubungan satu sama lain dengan menganalisa perilaku si pengguna dan memanipulasi atau menggiring opini para pengguna.[17] Beberapa negara juga mengandalkan infrastruktur komunikasi yang sepenuhnya berada di sistem *cloud* yang misalnya digunakan pada pusat data asing di bawah undang-undang yang berlaku di luar negeri. Layanan-layanan tersebut diberikan berdasarkan ketentuan penggunaan yang terus berubah dan penangguhan layanan secara sewenang-wenang seakan Perusahaan teknologi memiliki kendali atas arah kebijakan suatu negara.[18] Permasalahan yang timbul tidak hanya tentang ketergantungan suatu bangsa pada penyedia asing atau hukum yang berlaku untuk data digital; tapi juga tentang tidak adanya kebijakan publik yang mampu mengendalikan pihak-pihak yang telah memegang kendali atas kemajuan teknologi untuk mengatasi masalah ini di semua tingkatan.[19]

Oleh karena itu, penulis berpendapat, diperlukannya kerangka hukum nasional yang setidaknya dapat memberikan batasan kepada perusahaan asing dalam menjalankan bisnisnya di Indonesia dan memberikan kewenangan pada Pemerintah untuk mengawasi, memonitor dan menjaga kestabilan pertumbuhan industri dalam negri serta perubahan perilaku warga negaranya agar terhindar dari efek koloniasasi di bidang teknologi digital.

---

[17] Edmore Etekwe, *The Impact of Technology on Social Change: A Sociological Prespective. Op.Cit.* hlm. 231.
[18] Renata Avila Pinto, *Digital Soverignity or Digital Colonialism, Op.Cit.* hlm 19.
[19] *Ibid.*

BAB II
CYBER PROTECTION DALAM HUBUNGAN HUKUM DAN SOSIAL

Teknologi informasi dan komunikasi telah menjadi komponen integral masyarakat dan ekonomi, juga berkontribusi signifikan terhadap pembangunan. Penggunaan sistem informasi dan komunikasi di negara kita telah menjadi meluas di sektor publik dan swasta, serta di kalangan warga dan terutama di sektor infrastruktur kritis seperti energi, sumber daya air, kesehatan, komunikasi transportasi dan jasa keuangan.

Informasi dan teknologi komunikasi, dan penggunaan Internet pada khususnya, menghubungkan semua komponen dalam ruang cyber yang membawa serta risiko keamanan cyber dan ketidakpastian.

Kelemahan keamanan dalam informasi dan sistem komunikasi dapat menyebabkan sistem seperti itu tidak berfungsi, bisa untuk dieksploitasi, atau kerugian ekonomi dalam skala besar, gangguan ketertiban umum dan / atau kompromi terhadap keamanan nasional.

Kerugian yang timbul dari serangan dunia maya telah mencapai tingkat yang luar biasa. Ini adalah fakta bahwa ruang cyber memberikan keuntungan seperti anonimitas dan penyangkalan atas serangan yang dilakukan terhadap sistem informasi atau data. Situasi ini mengungkapkan karakter asimetris risiko dan ancaman di ruang cyber dan membuatnya sulit untuk bertarung dengan ancaman ini.

Memastikan keamanan cyber absolut tidak lagi dapat dicapai dalam lingkungan Hidup. Jadi alih-alih, tujuannya adalah untuk menjaga risiko keamanan cyber tetap terkendali dan dalam tingkat yang dapat diterima.

Diakui bahwa berada di tempat terbuka dan terhubung lingkungan seperti Internet menghadirkan risiko tertentu dengan peningkatan aksesibilitas. Pengguna harus dipersiapkan untuk insiden dunia maya dalam mengelola risiko dengan pendekatan holistik yang mencakup semua pemangku kepentingan dan memastikan kesinambungan dengan mengurangi insiden-insiden ini dengan kerugian minimum, seperti misalnya tahu pemahaman mengenai hal-hal yang berhubungan dengan penggunaan teknologi dibawah ini.

2.1 Bank

Bank adalah bank sebagaimana dimaksud dalam undang-undang yang mengatur mengenai perbankan dan bank syariah sebagaimana dimaksud dalam undang- undang yang mengatur mengenai perbankan syariah. Lembaga Selain Bank adalah badan usaha bukan Bank yang berbadan hukum dan didirikan berdasarkan hukum Indonesia.[20] Perbankan di dunia telah lahir dan tercatat setua sejarah otentik yang dicatatkan manusia, hal ini dikarenakan sistem perbankan dalam bentuk yang sederhana telah ada paling tidak sejak tahun 2000 Sebelum Masehi di Babilonia. Pada waktu itu lembaga perbankan yang lebih dikenal dengan sebutan *Temples Of Babylon* mempunyai aktivitas berupa peminjaman emas dan perak dengan tingkat suku bunga 20% (dua puluh persen) setiap bulannya.[21] Hal tersebut diperkuat dengan bukti-bukti adanya juga instrumen yang digunakan dalam bentuk "janji" untuk membayar atau "perintah" untuk membayar dimana alat pembayaran yang digunakan masih berupa emas dan perak. Bank sebagai bagian dari sistem keuangan dan sistem pembayaran dalam suatu negara,

[20] Peraturan Bank Indonesia Nomor 18/40/Pbi/2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran

[21] Muhamad Djumhana. *Hukum Perbankan Di Indonesia*. Bandung: PT. Citra Aditya Bakti, 1993. hlm. 38.

memiliki peran yang sangat penting. Peran penting bank tersebut tidak terlepas dari fungsinya sebagai lembaga perantara keuangan (*financial intermediary*), yakni yang bergerak dalam kegiatan usaha penghimpunan dana (*fund raising*) dari masyarakat maupun penyaluran dana (*fund lending*) kepada masyarakat.[22] Menurut Sutan Remy Sjahdeini, hubungan kontraktual antara bank dan nasabah yang didasarkan pada prinsip kepercayaan (*fiduciary principle*), membawa konsekuensi agar bank tidak hanya memperhatikan kepentingan sendiri semata-mata, tetapi juga harus memperhatikan kepen- tingan nasabah penyimpan dana.[23] Kewajiban bank untuk memperhatikan kepentingan nasabahnya juga dilandasi dengan prinsip kerahasiaan (*confidential principle*). Prinsip ini mengharuskan atau mewajibkan bank untuk merahasiakan segala sesuatu yang berhubungan dengan data dan informasi mengenai nasabah, baik keadaan keuangannya maupun informasi yang bersifat pribadi.[24]

Prinsip menjaga kerahasiaan keadaan keuangan nasabah merupakan suatu hal yang sangat penting dalam menjalankan kegiatan usaha di bidang perbankan, karena dengan adanya jaminan keraha- siaan itu, akan menumbuhkan rasa "*confidence*" bagi nasabah yang membutuhkan suasana "*non-disclo- sure*" bagi keadaan keuangannya. Dari rasa "*confidence*" itu akan timbul suatu hubungan keper- cayaan (*fiduciary relationship*) antara bank dengan nasabahnya yang akan berdampak pula pada perkem- bangan bisnis perbankan bagi pihak bank yang dipercaya.[25] Konsep rahasia bank ini secara nyata muncul dan menjadi hukum ketika kasus *Court of Appeal* Inggris secara bulat memutuskan pendiriannya dalam kasus *Tournier v. National Provincial and Union Bank Of England*, tahun

---

[22] Marnia Rani. *Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank*. Vol. 2 No. 1. Jurnal Selat. 2014. Kepulauan Riau: Universitas Maritim Raja Ali Haji. hlm. 168

[23] Djoni S. Gazali dan rachmadi Usman. *Hukum Perbankan*. Sinar Grafika. Jakarta. 2010. hlm. 27-30.

[24] *Ibid.* hlm.30.

[25] Marnia Rani. *Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank*. Vol. 2 No. 1. Jurnal Selat. 2014. Kepulauan Riau: Universitas Maritim Raja Ali Haji. hlm. 169.

1924. Suatu putusan pengadilan yang kemudian menjadi *leading case law* yang menyangkut ketentuan rahasia bank di Inggris dan kemudian dijadikan acuan oleh pengadilan-pengadilan negara lain yang menganut *common law system*. Bahkan 60 (enam puluh) tahun sebelum putusan *Tounier* tersebut, yaitu dalam perkara *Foster v. The Bank of London*, Tahun 1862, juri telah berpendapat bahwa terdapat kewajiban bagi bank untuk tidak boleh mengungkapkan keadaan keuangan nasabah bank yang bersangkutan kepada pihak lain.[26]

Kasus *Tournier v. National Provincial and Union Bank Of England*, tahun 1924 diawali oleh gugatan penggugat (*Tournier*) yaitu nasabah dari tergugat (*National Provincial and Union Bank Of England*) pada salah satu kantor cabangnya di *Moorgate Street Branch*. Hal ini dikarenakan, rekening nasabah di bank mengalami saldo negatif sebesar £9,- (sembilan Poundsterling). Bank mendesak nasabahnya untuk membayar dan nasabah menyepakati akan membayar secara mengangsur sebesar £1,- (satu Poundsterling) per minggu. Setelah tiga kali angsuran, nasabah menghentikan pembayaran angsurannya. Akan tetapi pimpinan cabang bank tersebut kemudian mengetahui bahwa nasabah tersebut menerima pembayaran dari nasabah lain berupa cek sebesar £45,- (empat puluh lima Poundsterling), tetapi tidak dimasukkan ke dalam rekeningnya. Cek tersebut ditagihkan melalui *London City and Midland Bank* untuk rekening sebuah rumah judi (*bookmaker* atau *gambler*). Kemudian Mr. Fennel sebagai pimpinan bank menelepon majikan dari nasabahnya untuk meminta alamat rumah dari nasabah tersebut. Di dalam pembicaraan melalui telepon tersebut diceritakan oleh Mr. Fennel bahwa nasabah mempunyai utang di bank dan ketika menerima cek tidak disetorkan ke rekening nasabah yang ada di bank, akan tetapi dialihkan ke rekening nasabah tersebut pada bank lain. Akibat informasi tersebut, kontrak antara nasabah dengan majikannya tidak diperpanjang dan nasabah diberhentikan dari pekerjaannya. Oleh karena hal tersebut, kemudian nasabah

---

[26] Sutan Remy Sjahdeini. *Rahasia Bank: Berbagai Masalah Disekitarnya dalam Hukum Perbankan*. Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia. hlm.27-28.

menggugat bank dengan alasan fitnah dan pencemaran nama baik. Bank dianggap tidak memenuhi kewajibannya dalam menjaga kerahasiaan (*slander and breach of duty confidentiality*). Dalam putusan akhir dari perkara ini dinyatakan bahwa hak dari nasabah untuk dijaga kerahasiaan informasinya oleh bank adalah suatu hak yang sah. Seluruh hakim yang memeriksa kasus tersebut berpendapat bahwa kewajiban untuk merahasiakan tidak saja terdapat pada moral, tetapi juga terdapat dalam hukum yang didasarkan pada hubungan kontraktual antara bank dan nasabah.[27]

Kasus tersebut bagi negara-negara penganut sistem *common law* seperti Amerika Serikat merupakan suatu rujukan dalam mengatur kewajiban didalam merahasiakan data nasabah (*duty of secrecy*) yang merupakan tanggung jawab bank untuk keperluan dan kepentingan nasabannya. *Duty of secrecy* terhadap nasabahnya merupakan suatu kewajiban yang ditetapkan didalam hubungan kontraktual yang terjadi antara bank dan nasabahnya, akan tetapi kewajiban tersebut tidak bersifat absolut tetapi mengandung kualifikasi atau pengecualian dengan alasan tertentu. Hakim didalam kasus tersebut yakni Bankes L.J. menguraikan bahwa pengecualian tersebut adalah[28]:

a. Apabila diatur dalam suatu undang-undang;
b. Apabila terdapat kepentingan umum;
c. Apabila kepentingan bank memang memerlukan;
d. Apabila terdapat persetujuan dari nasabah.

Kerahasiaan bank merupakan jiwa dari sistem perbankan yang didasarkan pada kelaziman dalam praktek perbankan, perjanjian kontrak antara bank dengan nasabah, serta peraturan tertulis yang ditetapkan oleh negara.[29] Sehingga sampai saat ini, maka rahasia bank tetap diterapkan oleh perbankan didalam menjalankan

---

[27] Pho Chu Chai dan Dennis Campbell. dalam Yunus Husein. *Rahasia Bank Privasi Versus Kepentingan Umum*. Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia. 2003. hlm.137.
[28] Yunus Husein. *Rahasia Bank Privasi Versus Kepentingan Umum*. Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia. 2003. hlm.137-138.
[29] Yunus Husein, *Op.Cit*, hlm.134.

usahanya. Suatu kelaziman atau disamakan dengan kebiasaan adalah suatu peristiwa sama ataupun terjadi secara bersamaan yang berulang terus menerus didalam kegiatan tertentu, sehingga perlu dipahami bahwa kebiasaan bukanlah merupakan hukum, tetapi suatu kebiasaan dapat menjadi sebuah hukum memerlukan dua untur yaitu pola tindak yang berulang dan masyarakat menerima pola tindakan tersebut sebagai sesuatu yang harus mereka patuhi dan diterima sebagai aturan yang mengikat (*opinion iurus necessitates*).[30]

Hal ini terus berkembang, sehingga pada akhirnya memunculkan 2 (dua) teori terkait dengan kerahasiaan bank, yaitu teori rahasia bank yang bersifat mutlak (*absolute theory*) dan teori rahasia bank yang bersifat relatif atau nisbi.[31] Berdasarkan teori rahasia bank yang bersifat multak (*absolut theory*) maka bank mempunyai kewajiban untuk menyimpan rahasia atau keterangan-keterangan mengenai nasabahnya yang diketahui bank karena kegiatan usahanya dalam keadaan apapun juga, dalam keadaan biasa atau dalam keadaan luar biasa. Teori ini sangat menonjolkan kepentingan individu, sehingga kepentingan negara dan masyarakat sering terabaikan. Penganut teori ini berpendirian, bahwa semua hal yang bersangkutan dengan orang, mutlak harus dirahasiakan tanpa pengecualian. Teori ini sangat bersifat individualistis dimana sangat bertentangan dan tidak menghargai akan kepentingan umum. Oleh karena itu, berkembanglah teori rahasia bank yang bersifat relatif atau nisbi dimana menurut teori ini bank diperbolehkan membuka rahasia atau memberi keterangan mengenai nasabahnya, apabila untuk kepentingan yang mendesak, misalnya untuk kepentingan negara atau kepentingan hukum. Teori ini banyak dianut oleh bank-bank dibanyak negara didunia sehingga dengan adanya pengecualian didalam ketentuan rahasia bank memungkinkan untuk kepentingan tertentu suatu badan atau instansi diperbolehkan

---

[30] Mochtar Kusumaatmadja dan B. Arief Sidharta, *Pengantar Ilmu Hukum Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum Buku I*. Bandung: Penerbit Erlangga, 2000. hlm. 65- 66.

[31] Hermansyah, *Hukum Perbankan Nasional Indonesia Edisi Revisi*, (Jakarta: Kencana Prenada Media Group. 2008. hlm. 120-121.

meminta keterangan atau data tentang keadaan keuangan nasabah yang bersangkutan sesuai dengan ketentuan perundang-undangan yang berlaku.

Di Indonesia, ketentuan terkait rahasia bank menjadi suatu problematika didalam penegakan hukum khususnya terkait dengan tindak pidana yang menggunakan bank sebagai suatu lembaga untuk menyimpan dana dari hasil tindak pidana tersebut. Hal tersebut terbukti di Indonesia, masalah *money laundering* kini menjadi perhatian utama dalam hubungannya dengan lembaga perbankan. Mantan Direktur *International Monetary Fund* (IMF) Michel Camdessus pernah mengungkapkan bahwa diperkirakan volume dari *money laundering* adalah antara 2% (dua persen) sampai dengan 5% (lima persen) dari *Gross Domestic Product* dunia.[32]Batas terbawah dari perkiraan tersebut dihasilkan dari kegiatan *narcotics trafficking, arms trafficking, bank fraud, securities fraud, counterfeiting* dan kejahatan sejenis. Yang dicuci di seluruh dunia setiap tahun mencapai jumlah hampir US$600.000.000.000,- (enam ratus milyar Dollar Amerika Serikat).[33] Hal ini sangat mengkhawatirkan bagi penegakan hukum di Indonesia dan keadaan tersebut menjadi lebih buruk dikarenakan hasil kejahatan *money laundering* yang dilakukan di Indonesia ternyata ditransfer oleh pelaku tindak pidana ke rekeningnya diluar negeri dengan tujuan untuk mendirikan atau melakukan investasi kedalam berbagai bisnis yang sah. Akan tetapi, apabila perbankan di Indonesia tidak menerapkan rahasia bank maka bisa dipastikan bahwa usaha perbankan di Indonesia tidak akan dapat berjalan dikarenakan nasabah tidak akan mempercayai bank tersebut karena nasabah tidak mendapat perlindungan terkait dengan data-datanya termasuk simpanannya yang ada pada bank tersebut. Oleh karena itu, hal yang harus dipahami adalah bahwa rahasia bank sangat erat hubungannya dengan perlindungan data dari nasabah, baik perlindungan data tersebut dari pihak eksternal maupun dari pihak internal bank itu

---

[32] N.H.T. Siahaan. *Money Laundering Pencucian Uang Dan Kejahatan Perbankan*. Jakarta: Pustaka Sinar Harapan. 2002. hlm.1.

[33] Sutan Remy Sjahdeini. *Money Laundering*. Jurnal Hukum Bisnis Vol.11 Jakarta: Yayasan Pengembangan Hukum Bisnis. 2000. hlm. 31.

sendiri akan tetapi perlindungan data tersebut juga harus berimbang dengan kebutuhan dari masyarakat atau negara guna penegakan hukum di Indonesia.

Di Indonesia, rahasia bank diatur didalam Pasal 40 Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 7 Tahun 1992 tentang Perbankan yang menyatakan

"Bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41 A, Pasal 42, Pasal 43, Pasal 44 dan Pasal 44 A.[34]"

Berdasarkan hal tersebut maka dapat dilihat bahwa bank di Indonesia wajib menerapkan rahasia bank, dimana rahasia bank yang diterapkan sebatas dan terbatas pada keterangan mengenai nasabah penyimpan dan simpanannya, sehingga keterangan selain terkait dengan nasabah penyimpan dan simpanannya bukan merupakan rahasia bank, misalnya keterangan mengenai debitur dan pinjamannya. Akan tetapi rahasia bank tersebut tidak diterapkan secara mutlak karena ada beberapa pengecualian yakni untuk kepentingan pajak, kepentingan peradilan pidana, kepentingan peradilan perdata antara bank dengan nasabah penyimpannya, tukar menukar informasi antar bank, badan urusan piutang dan lelang negara atau panitia urusan piutang negara dan pihak yang ditunjuk oleh nasabah penyimpan panitia urusan piutang.

Kewajiban untuk merahasiakan mengenai nasabah dan simpanannya dapat bersifat eksplisit atau implisit pada umumnya perjanjian bank dan nasabah tidak mencantumkan secara eksplisit kewajiban merahasiakan tersebut seperti terlihat pada perjanjian pembukaan rekening koran, tabungan dan deposito antara bank dan nasabah. Kewajiban merahasiakan selain dapat diatur dalam perjanjian antara bank dan nasabah, Undang-Undang juga diatur dalam peraturan intern bank yang bersangkutan. Dengan demikian, walaupun dalam perjanjian tidak diatur secara eksplisit, tetapi

[34] Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan Atas Undang- Undang Republik Indonesia Nomor 7 Tahun 1992 tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182.

berdasarkan itikad baik di dalam melaksanakan perjanjian, maka perjanjian antara bank dan nasabahnya dianggap mencantumkan secara diam- diam kewajiban merahasiakan tentang nasabah dan simpanannya. Hal ini sejalan dengan Pasal 7 huruf a Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang menyebutkan bahwa salah satu kewajiban pelaku usaha adalah bertikad baik dalam melakukan kegiatan usaha. Menurut Francis Neate dan Roger Mc Cormick terdapat beberapa alasan yang mengakibatkan perbedaan sifat pengaturan rahasia bank antara satu negara dengan negara lainnya[35] yaitu:

a. Latar belakang sejarah dan budaya suatu negara, misalnya Swiss menganggap masalah rahasia bank itu sangat serius, karena dalam sejarah rahasia bank di Swiss sangat diperlukan karena hal itu dilakukan dalam rangka melindungi harta pengungsi Yahudi yang dikejar oleh tentara Nazi pada Perang Dunia Ke II dimana pada saat itu juga diberlakukan rekening bank dengan menggunakan nomor saja (*numbered account*) untuk menyembunyikan dana yang dilarikan dari pengawasan Nazi. Menurut Werner De Capitani bahwa ketentuan pidana di Swiss untuk pelanggaran rahasia bank diterapkan dengan tujuan untuk mencegah tindakan memata- matai seluruh rekening yang ada di bank-bank di Swiss yang dilakukan oleh Nazi. Krisis ekonomi dunia pada waktu itu telah menyebabkan pelarian modal yang cukup besar dari Jerman ke Swiss. Sebagai tindakan balasan, pemerintah Jerman memperkenalkan peraturan terkait kontrol devisa pada tanggal 1 Agustus 1931 dengan tujuan untuk mencegah dana keluar dari Jerman ke Swiss. Akibat dari penerapan pidana atas rahasia bank yang diberlakukan di Swiss yaitu beberapa agen Jerman ditangkap karena telah mencoba mendapatkan informasi dari pegawai-pegawai bank Swiss. Akan tetapi situasi semakin memburuk setelah Adolf Hitler berkuasa pada tahun 1933 dan sebuah Undang-Undang Jerman diberlakukan

[35] Francis Neate and Robert Mc Cormick (ed), *Bank Confidentially*, (London, 1990), hlm. xviii- xix.

dengan tujuan untuk merampas hak milik orang-orang Yahudi. Warga Jerman dipaksa untuk menandatangani pernyataan yang memberikan kewenangan kepada para pegawai pemerintah Jerman untuk memperoleh informasi dari bank-bank Swiss. Akan tetapi *Swiss National Bank* segera mengeluarkan kebijakan dengan melarang pemberian informasi yang dilakukan dengan cara yang disahkan pemerintah Jerman. Walaupun ada kebijakan tersebut ternyata pada prakteknya kebijakan tersebut tidak mempengaruhi para pegawai pemerintah Jerman yang merupakan agen-agen Jerman tersebut, karena tidak ada ketentuan yang mengatur bahwa kegiatan-kegiatan tersebut dapat dipidana. Oleh karena itu, mengingat masalah rahasia bank dianggap sangat penting dan serius, maka penegakannya dilakukan juga dengan menggunakan hukum pidana yakni memberikan ancaman pidana bagi pelanggarnya. Dengan demikian berdasarkan hal tersebut jelas bahwa rahasia bank di Swiss tidak pernah dimaksudkan untuk melindungi kegiatan illegal, akan tetapi ditujukan untuk melindungi kebebasan pribadi (*personal liberties*).[36]

b. Masalah persaingan dalam penghimpunan dana, sebagaimana diketahui didalam dunia internasional khususnya sektor ekonomi dibidang perbankan, banyak juga dana bebas yang tidak mempunyai loyalitas pada satu negara manapun juga. Hal ini berakibat bahwa pemilik dana akan lebih senang untuk menyimpan uangnya di negara yang ketentuan rahasia banknya ketat. Hal sederhana yang menjadi parameter adalah kebijakan mengenai pengenaan sanksi pidana dimana jika diatur pengenaan sanski pidana maka merupakan salah satu indikasi utama bahwa pengaturan rahasia bank bersifat ketat.

---

[36] Olivier Dunant and Michele Wassmer, *Swiss Bank Secrecy: Its Limits Under Swiss and International Laws, Case W. Res.J.Int'l.l*, (Vol;.20:509, 1988), hlm.541

Di negara-negara dengan sistem *Common Law* pada umumnya diatur, bahwa kewajiban bank untuk merahasiakan berasal dari hubungan kontraktual antara bank dan nasabah sehingga apabila dilanggar dianggap sebagai suatu *civil wrong* atau pelanggaran perdata bukan pelanggaran pidana. Selanjutnya pula negara yang tidak menganut sistem *Common Law*, namun menganggap pengaturan masalah rahasia bank bersifat perdata. Apabila pelanggaran rahasia bank dianggap sebagai pelanggaran perdata, maka upaya yang dapat dilakukan oleh nasabah adalah menggugat bank dengan alasan cidera janji atau melakukan perbuatan melawan hukum.

2.2 Sosial Media

Perkembangan sosial media kian hari kian meningkat, pada tahun1997 awalnya sosial media ini lahir berbasiskan kepercayaan, namun mulai dari tahun 2000-an hingga tahun-tahun berikutnya sosial media mulai diminati semua orang hingga mencapai masa kejayaannya. Pada akhirnya dalam melaksanakan kinerja dan memungkinkan berbagai kegiatan untuk dilaksanakan dengan cepat, tepat dan akurat, sehingga meningkatkan produktivitas, dalam perkembangan sosial media ini akhirnya banyak bermunculan kegiatan- kegiatan pembelajaran yang berbasis elektronik.[37] Dampak pada manusia dengan peningkatan dunia media sosial adalah pada data pribadi seseorang yang seharusnya menjadi privasi. Privasi seseorang merupakan sesuatu yang harus dijaga kerahasiaanya. Ketika tidak ada privasi, maka hidup seseorang akan terasa seperti neraka dunia, karena rentan terhadap kebebasan seseorang untuk bebas berekspresi serta rentan terhadap penyalahgunaan data pribadinya oleh orang lain . Kekhawatiran lainnya yaitu terhadap informasi terkait hal-hal pribadi akan diketahui secara luas, khawatir bahwa setiap kegiatan yang dilakukan akan diketahui dan diawasi pihak tertentu.

[37] Hamzah B.Uno. *Teknologi Komunikasi dan Inofasi Pembelajaran*. Jakarta: Bumi Aksara. 2010. hlm. 57.

Di beberapa negara maju, masalah perlindungan data pribadi sudah dianggap sebagai bagian dari hak asasi manusia yang harus dilindungi dan oleh karenanya telah dituangkan dalam peraturan perundangan tersendiri. Eropa misalnya, sudah memiliki peraturan tentang perlindungan data pribadi selama lebih dari satu dekade.[38] Inggris mengatur tentang perlindungan data pribadi dalam *Data Protection Act* 1998 yang mulai berlaku sejak tahun 2000. Act ini merupakan pengganti dari peraturan sebelumnya (*Data Protection Act* 1984). Di Inggris terdapat suatu badan pelaksana yaitu *The Data Protection Commisioner* yang bertugas mengawasi semua pengguna data yang menguasai data pribadi. Perlindungan terhadap hak privasi individual dibuktikan dalam ketentuan *Data Protection* Act 1998 yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.[39] Data juga hanya boleh digunakan sepanjang diperlukan dan tidak boleh disimpan lebih lama dari seharusnya. Begitu kuatnya perlindungan terhadap data pribadi, Act ini bahkan melarang data pribadi ditransfer ke negara di luar Eropa kecuali apabila negara yang bersangkutan dapat menjamin perlindungan data yang serupa.

Negara tetangga kita juga telah mengatur mengenai perlindungan data pribadi dalam perundangan tersendiri. Malaysia mengaturnya dalam *Personal Data Protection* Act (PDPA) 2010, sementara Singapura mengaturnya dalam *Personal Data Protection* Act (PDPA) 2012.[40] PDPA 2010 milik Malaysia baru akan berlaku secara penuh per Agustus 2013, sedangkan PDPA 2012 milik Singapura baru berlaku secara penuh pada bulan Juli 2014. Kedua aturan milik Malaysia dan Singapura ini mempunyai banyak

---

[38] Gupinder Assi. *South East Asia: Data Protection Update*. Terdapat dalam https://www.bclplaw.com/images/content/2/0/v2/2020/Bryan-Cave-Client-Bulletin-South-East-Asia-Data-Protection-Updat.pdf. Yang diakses pada 22 Agustus 2019 pukul 11.41. hlm.1.

[39] Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*. Jakarta: RajaGrafindo Persada, 2005. hlm.170.

[40] Gupinder Assi, *Op.Cit*, h.1-3.

kemiripan karena tampaknya mempunyai sumber yang sama, yaitu mengacu pada aturan tentang perlindungan data pribadi yang dianut di Eropa (*European Data Protective Directive*). Perbedaan yang menarik dari PDPA 2012 yang dimiliki Singapura adalah bahwa PDPA 2012 ini memfasilitasi berdirinya sebuah badan bernama Do Not Call (DNC) *Registry*. Masyarakat dapat mendaftarkan nomor teleponnya pada DNC *Registry* dan secara resmi menolak untuk menerima telepon maupun pesan-pesan seperti SMS dan MMS dari marketing atau organisasi yang tidak dikehendakinya.

Namun perlindungan privasi tidak berarti tanpa batasan. Dalam hal tertentu terdapat informasi yang secara luas disepakati sebagai informasi pribadi yang tidak dilindungi bahkan atas nama hukum berhak disimpangi, misalnya informasi mengeni jumlah rekening yang dimiliki, nama ibu, maupun tanda lahir yang melekat pada tubuh. Pada umunya masyarakat menganggap informasi tersebut merupakan hal yang sifatnya pribadi. Namun ketika terjadi kondisi khusus yang mengharuskan terjadi pengungkapan data-data tersebut maka pemilik informasi tidak dapat menolak untuk memberitahukan atau mengemukakan informasi tersebut dengan dalih menyangkut privasi. Selama privasi tersebut terkait dengan kepentingan publik dan digunakan dengan terbatas dilindungi undang-undang, maka perlindungan privasi dapat terabaikan.

Dalam perkembangan teknologi, media sosial muncul sebagai saran berkomunikasi gaya baru. Hal ini tentu berpotensi terjadi penyalahgunaan data pada saat kegiatan interaksi antara pengguna media sosial. Perkembangan teknologi digital salah satunya termanifestasi dalam bentuk situs jejaring sosial, seperti Instagram, Facebook, Linked in, Path, dan lain sebagainya. Facebook selaku salah satu media sosial dengan jumlah pengguna terbanyak di dunia mempunyai tanggung jawab yang besar dalam melindungi pengguna terkait penyalahgunaan data. Melalui *Privacy Policy* dan *Statement of Rights and Responsibilities* Facebook melindungi hak – hak dari pengguna, serta mengatur kewajiban dari Facebook selaku penyedia sistem elektronik untuk mewujudkan kondisi yang aman dari penyalahgunaan data pribadi yang mungkin saja akan terjadi. Pengguna yang terdaftar dan sudah memiliki akun di media sosial

Facebook menyetujui perjanjian yang disebut *Statement of Rights and Responsibilities* dengan Facebook selaku penyedia sistem elektronik terkait dengan data pribadi. Terkait hal yang berkaitan dan terkandung hak intelektual, pengguna setuju untuk memberikan kewenangan sesuai dengan "*Privacy dan Apliciation Settings*", pengguna juga setuju untuk memberikan kewenangan *Non Exclusive, Privacy Policy, Transferable, Sub-Licensable, Royalty-Free, Worldwide License* untuk menggunakan segala hal terkait yang di post oleh pengguna (*IP License*). *IP License* ini berakhir ketika pengguna menghapus *IP Content* atau akun miliknya, kecuali apabila konten tersebut tidak di sebar pada akun lain dan mereka belum menghapusnya. Hal ini berarti bahwa Facebook tidak perlu meminta izin menampilkan hal yang terkait hak intelektual, bebas dari royalti ketika Facebook menggunakannya, sepanjang konten tersebut termasuk dalam post yang bersifat untuk konsumsi publik.[41]

Dalam *Privacy Policy* Facebook menerangkan bahwa jenis data yang diterima oleh Facebook dibagi menjadi dua, data publik dan privat. Data privat merupakan data yang dapat diakses oleh publik atau pengguna lain, sedangkan data privat hanya dapat dilihat oleh pihak yang dikehendaki oleh pengguna dalam hal ini Facebook selaku penyelenggara sistem elektronik. *Privacy Policy* Facebook juga menjelaskan jenis data atau informasi yang diterima Facebook, data yang diterima untuk pendataan mengenai akun, maupun aktivitas pengguna di media sosial tersebut. Ketika pengguna memperkenankan Facebook untuk menggunakan informasi mereka, pengguna selalu memiliki akses penuh informasinya.

Berkenaan dengan data pribadi, di negara maju, terminologi lain yang kerap kali digunakan adalah privacy/privasi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya. Menurut Yuwinanto, privasi merupakan konsep abstrak yang mengandung banyak makna. Penggambaran populer mengenai privasi antara lain adalah hak individu untuk

---

[41] Achmad Paku Braja Arga Amanda. *Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)*. Fakultas Hukum Brawijaya: Malang. 2012. hlm.4.

menentukan apakah dan sejauh mana seseorang bersedia membuka dirinya kepada orang lain atau privasi adalah hak untuk tidak diganggu. Privasi merujuk padanan dari Bahasa Inggris *privacy* adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka.[42]

Sampai saat ini kurang lebih 25 negara di dunia mempunyai undang-undang mengenai perlindungan data pribadi.[43]Edmon Makarim menjelaskan bahwa Inggris bukanlah negara pertama yang mempunyai aturan berkenaan dengan perlindungan data pribadi. Berdasarkan penelusuran diketahui bahwa sejarah mencatat negara yang pertama kali mengatur mengenai perlindungan data pribadi adalah negara bagian Hesse di Jerman pada tahun 1970 kemudian diikuti oleh Swedia pada tahun 1973 dan Amerika Serikat pada tahun 1974 dan Inggris pada tahun 1984.[44] Di Inggris aturan berkaitan dengan perlindungan data pribadi terdapat di dalam undang-undang perlindungan data 1998 (*The Data Protection* Act 1998). Dalam undang-undang tersebut disebutkan adanya suatu badan pelaksana yaitu The Data Protection Commisioner yang berwenang untuk mengawasi semua pengguna data yang menguasai data pribadi. Selain itu, perlindungan terhadap hak privasi individual juga disebutkan dalam ketentuan *Data Protection* Act 1998 yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.[45] Perlindungan terhadap data pribadi di Inggris bersifat kuat dan tegas, Act ini bahkan melarang

---

[42] Lia Sautunnida. *Urgensi Undang-undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia*. Vol. 20. No. 2. Anun Jurnal Ilmu Hukum. 2018. Universitas Syiah Kuala. hlm.374.

[43] Radian Adi Nugraha. *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*. Universitas Indonesia. 2012. hlm.31.

[44] Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian), dalam Radian Adi Nugraha, Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia. 2012. hlm 50.

[45] *Ibid*. hlm. 50.

data pribadi ditransfer ke negara di luar Eropa kecuali apabila negara yang bersangkutan dapat menjamin perlindungan data yang sama. Berkaitan dengan hal ini pemerintah Indonesia juga belum menjadikan poin transfer data ke negara lain menjadi salah satu hal yang penting untuk dibicarakan, padahal hal tersebut sangat penting dalam menjawab tantangan dan kesempatan dalam era ekonomi digital saat ini yang cakupannya bahkan luas sampai pada level transaksi internasional. Berdasarkan Pasal 14 dari *Data Protection* Act 1998 menjelaskan bahwa apabila pengadilan menemukan bahwa data pribadi diproses oleh pengontrol data tidak akurat, pengadilan dapat memerintahkan perbaikan, menghalangi, penghapusan atau kerusakan dari data tersebut. Bagi mereka sedang terkena dampak langsung dari pengolahan data pribadi dapat meminta Badan Komisaris untuk mengevaluasi proses untuk menentukan jika memenuhi ketentuan *Data Protection* Act 1998. Data subyek berhak untuk mengklaim kompensasi untuk setiap kerugian yang diderita sebagai akibat dari pelanggaran *Data Protection* Act oleh pengontrol data dan mungkin juga mengklaim kompensasi untuk bahaya yang ditimbulkan.

2.3 HAKI

Hak Cipta merupakan hak eksklusif bagi Pencipta atau Pemegang Hak Cipta untuk mengumumkan atau memperbanyak ciptaannya, yang timbul secara otomatis setelah suatu ciptaan dilahirkan tanpa mengurangi pembatasan menurut peraturan perundang-undangan yang berlaku.[46] Ditinjau dari substansinya, HKI ada- lah "*product of mind*". Oleh karena itu, setiap karya intelektual patut diakui, dihormati, dilin- dungi dan dihargai baik secara moral maupun secara hukum.[47] Perlindungan hak kekayaan intelektual (HKI) sangat diperlukan oleh Indonesia, karena HKI merupakan salah satu alat pemicu untuk mendorong pertumbuhan ekonomi nasional melalui penciptaan iklim usaha yang sehat,

[46] Undang-Undang Hak Cipta No. 19 tahun 2002 Pasal 2

[47] Lista Widyastuti, "Ide Dan Kekayaan Intelektual", *Me- dia HKI-Buletin Informasi Dan Keragaman Hak Kekayaan Intelektual*. Vol. VII. No.03, Juni 2010.

sehingga dapat bersaing dengan HKI milik asing. Hal tersebut dikemukakan Sekretaris Jenderal Kementerian Perindustrian Ansari Bukhari ketika menyampaikan sambutannya pada acara Forum Koordinasi HKI di Palembang, pekan lalu. Sebagaimana diketahui, sejak Indonesia menjadi anggota Organisasi Perdagangan Dunia (WTO) yang diratifikasi melalui Convention Establishing the WTO dan telah disahkan dalam UU No. 7/1994 tentang *Agreement Establishing the World Trade Organization*, Indonesia perlu membuka diri tentang aspek lalu lintas perdagangan secara Internasional. Dalam ratifikasi atau persetujuan tersebut, di samping mengatur tentang lingkungan dan mutu produk industri melalui penerapan standard ISO yang telah diadopsi oleh Indonesia menjadi Standard Nasional Indonesia (SNI), maka diatur pula tentang norma standar Internasional untuk perlindungan Hak Kekayaan Intelektual (HKI) dan aspek-aspek dagang yang terkait dengan HKI yang disebut dengan *Trade Related Aspect of Intellectual Property Right Agreement* (TRIPs).[48]

Lahirnya persetujuan TRIPs/WTO sesungguhnya dimaksudkan untuk melindungi dan menegakkan hak kekayaan intelektual melalui promosi inovasi teknologi serta pengalihan dan penyebaran teknologi yang nantinya dapat memberikan keuntungan bagi pencipta atau juga bagi pengguna pengetahuan teknologi. Oleh karena itu, pengaturan dan penerapan sistem perlindungan HKI di Indonesia harus disesuaikan dengan kondisi sosial-budaya nasional agar tetap berdasarkan prinsip-prinsip dasar Pancasila sebagaimana pembangunan hukum yang baik adalah hukum yang sesuai dengan kehidupan masyarakat.[49] Pada dasarnya konsep HKI meliputi hak milik hasil pemikiran (intelektual) yang melekat pada pemiliknya dan bersifat tetap maupun eksklusif, dan hak yang diperoleh pihak lain atas izin dari pemilik sehingga bersifat sementara. Hasil kemampuan berpikir ini adalah ide yang kemudian dijelmakan dalam wujud

---

[48] Terdapat dalam https://kemenperin.go.id/artikel/3736/Kemenperin-Dorong-Perlindungan-Hak-Kekayaan-Intelektual yang diakses pada 24 Agustus 2019 pukul 20.07 WIB.

[49] Mochtar Kusumaatmadja. *Konsep-Konsep Hukum dalam Pembangunan* Bandung: PT. Alumni. 2002. hlm.10.

ciptaan atau invensi. Sedangkan hak yang diperoleh pihak lain atas izin dari pemilik, sebagaimana hak untuk memperbanyak, hak untuk menggunakan produk tertentu atau hak untuk menghasilkan suatu produk tertentu.[50] Salah satu isu yang menarik dan saat ini tengah berkembang dalam lingkup kajian HKI adalah perlindungan hukum terhadap kekayaan intelektual yang dihasilkan oleh masyarakat asli atau masyarakat tradisional. Kekayaan intelek- tual yang dihasilkan oleh masyarakat asli tradi- sional ini mencakup banyak hal mulai dari sis- tem pengetahuan tradisional (*traditional know- ledge*), karya-karya seni, hingga apa yang dike- nal sebagai *indigenous science and technology*. Dalam hal ini, masyarakat telah berpikir secara kreatif tentang cara menghasilkan sesuatu secara inovatif dan tetap mengangkat serta menon- jolkan warisan budaya bangsa.[51]

Dalam upaya membangun sistem perlindungan HKI, hukum harus menyesuaikan proses perkembangan di masyarakat. Hukum merupakan keseluruhan kaidah dan asas yang mengatur kehidupan manusia dalam masyarakat termasuk adanya lembaga untuk pelaksanaan hukum tersebut.[52] Hukum juga pencerminan nilai-nilai yang berlaku dalam masyarakat, sehingga hukum yang baik adalah hukum yang sesuai dengan hukum yang hidup (*the living law*) dalam masyarakat. Pada dasarnya pembangunan sistem hukum HKI mengandung makna ganda.Pertama, dimaknai sebagai suatu usaha untuk memperbaharui hukum positif agar sesuai dengan kebutuhan hukum masyarakat dan kepentingan nasional. Kedua, dimaknai sebagai usaha untuk memfungsionalisasikan hukum HKI agar dapat mendukung proses pembangunan dengan adanya keikutsertaan hukum dalam mendorong terjadinya perubahan sosial ke arah yang dikehendaki undang-undang tentang HKI. Oleh karenanya, pembangunan sistem hukum perlindungan HKI sangat berkaitan

---

[50] Abdulkadir Muhammad. *Kajian Hukum Ekonomi Hak Kekayaan Intelektual* Bandung: PT Citra Aditya Bakti. 2007. hlm. 160.

[51] Devi Rahayu, "Perlindungan Hukum Terhadap Hak Cipta Motif Batik Tanjungbumi Madura", *Mimbar Hukum,* Vol. 23 No. 1, februari 2011, Yogyakarta: FH UGM, hlm. 117.

dengan pembaharuan hukum positif untuk mendorong perubahan sosial agar tidak menimbulkan kerugian pada masyarakat.

2.4 E-Commerce

Kemajuan teknologi telah membawa perubahan dan pergeseran yang cepat dalam suatu kehidupan tanpa batas. Pada era globalisasi ini, perekonomian dunia mengalami perubahan yang pesat disebabkan oleh kegiatan financial, produksi, investasi dan perdagangan yang saling tergantung antar negara. Globalisai telah menyatukan ekonomi dunia, sehingga batas-batas antar negara dalam berbagai praktik bisnis seakan-akan dianggap tidak berlaku lagi.[53] Begitu pula perdagangan internasional yang mengalami perkembangan akibat pengaruh perkembangan teknologi. Perkembangan perdagangan yang dipengaruhi dengan teknologi disebut dengan *electronic commerce (e-Commerce)*. E-Commerce merupakan salah satu mekanisme transaksi yang menggunakan jaringan komunikasi elektronik seperti internet yang digunakan baik oleh negara maju maupun negara berkembang sehingga aktivitasnya tidak dapat lagi dibatasi dengan batasan geografis karena mempunyai karakteristik lintas batas *(borderless world* baik di tingkat nasional maupun global) sehingga dapat meningkatkan efisiensi dan kecepatan penyelenggaraan bisnis serta pemerintahan.[54]

Perkembangan *e-commerce* terjadi ketika internet mulai diperkenalkan. Seiring dengan perkembangan tersebut, timbulnya permasalahan dalam transaksi *e-commerce* internasional sudah tentu tidak dapat dihindari. untuk memecahkan dan mengantisipasi masalah tersebut, maka para pihak yang melakukan trnasaksi *e-commerce* internasional akan berhadapan dengan dua sistem hukum negara yang berbeda. Melihat hal tersebut maka perlu adanya upaya untuk mengharmonisasi hukum tiap negara yang berkaitan mengenai perdagangan elektronik (*e-commerce*) internasional.

---

[53] Shinta Dewi. 2009. *Cyber Law Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional.* Cetakan ke-1. Bandung: Widya Padjajaran. Hlm. 1.

[54] *Ibid.* hlm. 2.

Upaya harmonisasi dapat dilakukan melalui lembaga atau organisasi internasional, baik yang sifatnya publik seperti PBB dengan badan kelengkapannya seperti UNCTAD atau UNCITRAL, atau lembaga yang bersifat privat seperti kamar dagang internasional (ICC) atau melalui lembaga-lembaga regional.[55] Lembaga yang sampai saat ini telah mengatur mengenai transaksi atau perdagangan internasional melalui perkembangan teknologi informasi berupa internet atau media elektronik lainnya ialah *United Nations Commission on International Trade Law* (UNCITRAL), sehingga penulis tertarik untuk membahas peran UNCITRAL pada harmonisasi hukum transaksi perdagangan elektronik (*e-commerce*) internasional. Menghadapi perkembangan transaksi *e-commerce*, negara-negara membentuk hukumnya untuk memecahkan dan mengantisipasi permasalahan dalam bidang transaksi *e-commerce*. Namun, hukum tiap-tiap negara cenderung berbeda sehingga hal tersebut dapat menjadi halangan dalam transaksi *e-commerce* internasional. Oleh karena itu, diperlukan suatu upaya untuk mengharmonisasi hukum tiap negara yang berbeda. Yang dimaksud dengan harmonisasi disini, menurut Hannu Honka adalah menyeragamkan aturan-aturan atau prinsip-prinsip substantif.[56]

Sebagaimana yang telah dijelaskan diatas, adapun lembaga yang sampai saat ini telah berperan dalam mengharmonisasi hukum transaksi *e-commerce* ialah *United Nations Commission on International Trade Law* (UNCITRAL) yang merupakan *subsidiary organs* Perserikatan Bangsa-Bangsa (PBB). UNCITRAL berperan dalam mengharmonisasi hukum transaksi *e-commerce* internasional. Berdasarkan Resolusi No.2205 (XXI) tanggal 17 Desember 1966 mengenai Pendirian *United Nations Commissions on International Trade Law* oleh Majelis Umum PBB, pada BAB I menyatakan bahwa Majelis Umum PBB memutuskan untuk membentuk UNCITRAL yang berperan khusus dalam meningkatkan perkembangan harmonisasi dan unifikasi hukum perdagangan internasional. Pada tahun 1996,

---

[55] Huala Adolf. 2010. *Dasar-Dasar Hukum Kontrak Internasional.* Edisi Revisi Cetakan Ketiga. Bandung: PT Refika Aditama. hlm. 34.

[56] Hannu Honka. *Harmonization of Contract Law hrough International Trade: A Nordic Perspective.* 1996 Tulane European and Civil Law Forum. hlm. 113.

UNCITRAL berhasil merumuskan suatu aturan hukum cukup penting yakni UNCITRAL *Model Law on Electronic Commerce*.[57] *Model Law* tersebut dibuat sebagai wujud peran UNCITRAL untuk mengharmonisasi hukum dalam transaksi *e-commerce*. Sebagaimana telah ditentukan pada Resolusi No.2205 (XXI), yang tercantum dalam BAB II mengenai Organisasi dan Fungsi-fungsi *United Nations Commission on International Trade Law*, poin ke-8 huruf (c) yaitu: "*The Commission shall further the progressive harmonization and unification of the law of international trade by:...(c) Preparing or promoting the adoption of new international conventions, model laws and uniform laws and promoting the codification and wider acceptance of international trade terms, provisions, customs and practices, in collaboration, where appropriate, with the organizations operating in this field;..*"[58] *Model Law* berarti dibuatnya aturan-aturan itu tetapi tidak mengikat negaranegara, jadi negara-negara tersebut bebas untuk mengikuti seluruh isi aturan, sebagian, atau bahkan menolak *Model Law* tersebut. Aturan tersebut dapat dikatakan hanya menjadi pedoman untuk membantu negara-negara di dalam membuat perundangan nasionalnya. Begitu pula halnya pada *Model Law on Electronic Commerce* 1996 ini tidak mengikat negara-negara dalam pembuatan hukumnya mengenai perdagangan elektronik. Sebagaimana halnya merupakan salah satu daripada tujuan utama pembentukan *Model Law* ini, yaitu menggalakkan aturan-aturan hukum yang seragam dalam penggunaan jaringan komputer guna transaksi-transaksi komersial.[59]

Pada Pasal 4 mengenai Variasi dari Kesepakatan dalam *Model Law* tersebut, menunjukkan bahwa negara-negara dapat melakukan suatu perjanjian terlebih dahulu sebelum melakukan transaksi *e-commerce* sebagai bentuk daripada harmonisasi tersebut. Namun,

---

[57] Huala Adolf. *Op.cit.* hlm. 42.

[58] http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/005/08/IMG/NR0000508.pdf?OpenElement

[59] UNCITRAL. *Model Law on Electronic Commerce with Guide to Enactment.* 1996. *With additional article 5 bis as adopted in 1998.* Yang disahkan oleh Majelis Umum PBB dengan Resolusi No. 51/162 tanggal 16 Desember 1998.

hingga sampai saat ini Indonesia belum membuat secara khusus mengenai undang-undang transaksi perdagangan elektronik (*e-commerce*) untuk menghadapi permasalahan dalam proses perdagangan elektronik dan sebagai wujud harmonisasi terhadap aturan-aturan secara internasional. Selama ini Indonesia hanya memberikan wujud pengaturan yang terkait mengenai *e-commerce* dengan diundangkannya Undang-undang Nomor 11 Tahun 2008 jo. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2.5 Government

Dalam perkembangan teknologi informasi saat ini, berbagai macam kegiatan baik dalam konteks pemerintahan, transaksi bisnis, komersil ataupun komunikasi berlangsung melalui media elektronik (*online*). Data atau informasi yang disampaikan melaui media elektronik itu sesungguhnya merupakan hal yang berharga. Selain itu, kegiatan yang berlangsung *online* tersebut juga memiliki risiko karena dapat menimbulkan masalah apabila data atau informasi tersebut bocor sehingga bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Data pribadi menjadi objek yang sangat vital di dunia internasional terkait dengan perlindungannya saat ini. Data pribadi adalah data yang berkenaan dengan cirri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.[60] Pengertian lain dari "data pribadi" adalah data yang berupa identitas, kode, symbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia.[61]

---

60 http://kamusbahasaindonesia.org/data%20pribadi/miripKamusBahasaIndoneisa.ord Diakses pada 25 Agustus 2019.

61 Rosalinda Elsina Latumahina. *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya.* Jurnal GEMA AKTUALITA. Vol. 3 No. 2. Desember 2014. Hlm. 16. Berdasarkan Pasal 1 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016, data pribadi adalah data persoalan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Istilah perlindungan data pertama kali digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur tentang perlindungan data pribadi dengan diberlakukannya aturan berkenaan dengan perlindungan data pribadi tersebut ke dalam sebuah aturan perundang-undangan yang bersifat sistematis.[62] Pemberlakuan aturan berkaitan dengan data pribadi tersebut karena pada masa itu alat yang digunakan untuk menyimpan data penduduk adalah komputer untuk keperluan pendataan sensus penduduk. Akan tetapi pada praktiknya sering terjadi banyak penyalahgunaan yang dilakukan oleh pihak pemerintah maupun pihak swasta. Oleh sebab itu diperlukan adanya aturan perundang-undangan yang akomodatif dan yang bisa memberikan jaminan dan keamanan terhadap data pribadi sehingga penggunaan data pribadi tersebut tidak dapat disalahgunakan. Masing-masing negara menggunakan terminologi yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantif kedua istilah tersebut mempunyai definisi yang hampir sama sehingga kedua istilah tersebut sering digunakan secara bergantian. Seperti misalnya Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi sedangkan negara-negara Uni Eropa, Malaysia dan Indonesia sendiri dalam UU ITE menggunakan istilah data pribadi.[63]

Di dalam data pribadi mencakup fakta-fakta, komunikasi atau pendapat yang berkaitan dengan individu yang merupakan informasi yang sifatnya rahasia, pribadi atau sensitif sehingga pribadi yang bersangkutan ingin menyimpan atau membatasi orang lain untuk mengoleksi, menggunakan atau menyebarkannya kepada pihak lain. Menurut Jerry Kang, data pribadi mendeskripsikan suatu informasi yang erat kaitannya dengan seseorang yang dapat membedakan karateristik masing-masing pribadi.[64] Pada prinsipnya bentuk

---

[62] Shinta Dewi, sebagaimana dikutip Rosalinda Elsina Latumahina. Lihat juga. Wafiya. *Perlindungan Hukum Bagi Nasabah yang Mengalami Kerugian dalam Transaksi Perbankan melalui Internet.* Kanun Jurnal Ilmu Hukum. Vol. 14 No. 1. 2012.

[63] *Ibid.* hlm. 17.

[64] Radian Adi Nugraha. *Analisis Yuridis mengenai Perlindungan Data Pribadi dalam Cloud Computing System ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik.* Universitas Indonesia. 2012. hlm. 31.

perlindungan terhadap data pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri.[65] Berkenaan dengan data pribadi, di negara maju, terminologi lain yang kerap kali digunakan adalah *privacy*/privasi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya.[66] Menurut Yuwinanto, privasi merupakan konsep abstrak yang mengandung banyak makna. Penggambaran populer mengenai privasi antara lain adalah hak individu untuk menentukan apakah dan sejauh mana seseorang bersedia membuka dirinya kepada orang lain atau privasi adalah hak untuk tidak diganggu. Privasi merujuk padanan dari Bahasa Inggris *privacy* adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka.[67] Menurut Kamus Besar Bahasa Indonesia, definisi dari privasi adalah bebas, kebebasan atau keleluasaan. Hak atas privasi ini juga dimuat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM)/*Universal Declaration of Human Rights* (UDHR) Pasal 12, yang menyatakan: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"

Berdasarkan beberapa definisi dan istilah berkenaan dengan data dan informasi juga privasi tersebut diatas dapat dipahami bahwa data dan informasi itu berkenaan dengan kehidupan individu dan juga dekat kaitannya dengan konsep kerahasian atau hak privasi seseorang yang harus dijaga dan dilindungi oleh aturan perundang-undangan. Sampai saat ini kurang lebih 25 negara di dunia

---

[65] *Ibid.* hlm. 32.
[66] Rosalinda Elsina Latuhamina, *Op. Cit.* hlm. 17.
[67] Helmy Prasetyo Yuwinanto. *Privasi Online dan Keamanan Data.*

mempunyai undang-undang mengenai perlindungan data pribadi.[68] Edmon Makarim menjelaskan bahwa Inggris bukanlah negara pertama yang mempunyai aturan berkenaan dengan perlindungan data pribadi. Berdasarkan penelusuran diketahui bahwa sejarah mencatat negara yang pertama kali mengatur mengenai perlindungan data pribadi adalah negara bagian Hesse di Jerman pada tahun 1970 kemudian diikuti oleh Swedia pada tahun 1973 dan Amerika Serikat pada tahun 1974 dan Inggris pada tahun 1984.[69] Di Inggris aturan berkaitan dengan perlindungan data pribadi terdapat di dalam undang- undang perlindungan data 1998 (*The Data Prot ection Act 1998*). Dalam undang-undang tersebut disebutkan adanya suatu badan pelaksana yaitu *The Data Protection Commisioner* yang berwenang untuk mengawasi semua pengguna data yang menguasai data pribadi. Sementara di Indonesia badan komisioner ini tidak disebutkan dalam aturan manapun. Badan komisiner ini dianggap penting sebagai pihak yang melakukan pengawasan terhadap data atau informasi yang digunakan dalam berbagai transaksi yang berlangsung di media *online*. Selain itu, perlindungan terhadap hak privasi individual juga disebutkan dalam ketentuan *Data Protection Act* 1998 yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.[70] Perlindungan terhadap data pribadi di Inggris bersifat kuat dan tegas, Act ini bahkan melarang data pribadi ditransfer ke negara di luar Eropa kecuali apabila negara yang bersangkutan dapat menjamin perlindungan data yang sama. Berkaitan dengan hal ini pemerintah Indonesia juga belum menjadikan poin transfer data ke negara lain menjadi salah satu hal yang penting untuk dibicarakan, padahal hal tersebut sangat penting dalam menjawab tantangan dan kesempatan dalam era ekonomi

---

[68] Radian Adi Nugraha. *Op. Cit.* hlm. 45.

[69] Edmon Makarim. *Pengantar Hukum Telematika (suatu kompilasi kajian).* Dalam Radia Adi Nugraha, *Analisis Yuridis mengenai Perlindungan Data Pribadi dalam Cloud Computting System ditinjau dari Undang-undang Informasi dan Transaksi Elektronik.* Universitas Indonesia. 2012. Hlm. 50.

[70] *Ibid.* hlm. 50.

digital saat ini yang cakupannya bahkan luas sampai pada level transaksi internasional. Para pihak yang diatur dalam ketentuan *Data Protection* Act 1998, adalah meliputi:

a. *The Data Protection Commisioner*
   Semua pengguna data yang menguasai data pribadi harus mendaftar pada badan ini.
b. *Data Subject*/Subjek Data
   Artinya setiap individu yang menjadi subjek dari data pribadi tersebut.
c. *Data Controller* (Pengguna Data)
   Artinya setiap orang yang menentukan tujuan dan cara mengolah data pribadi.
d. *Data Processor*
   Artinya yang dipersamakan dengan *computer bureau* (biro komputer), yaitu orang (di luar ppegawai *data controller*) yang memproses data atas nama *data controller*.

Beberapa prinsip penting dari *Data Protection* Act adalah sebagai berikut:

a. *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.* (Data pribadi harus diperoleh hanya untuk satu atau lebih tujuan yang spesifik dan sah dan tidak boleh diproses lebih lanjut dengan cara apapun yang tidak sesuai dengan tujuan-tujuan tersebut);
b. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.* (Data pribadi yang diproses untuk tujuan apapun tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan-tujuan tersebut);
c. *Personal data shall be processed in accordance with the rights of data subjects under this* Act. (Data pribadi harus diproses sesuai dengan hak dari subjek data berdasarkan aturan undang-undang);
d. *Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal*

data and against accidental loss or destruction of, or damage to personal data. (Tindakan teknis dan organisasi yang sesuai harus diambil terhadap pihak yang tidak berwenang dan tidak sah untuk memproses data pribadi dan terhadap kerugaian dan kerusakan yang tidak terduga atau kerusakan tterhadap data pribadi);

e. *Personal data shall not be transferred to a country or territory outside the Euuropian Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.* (data pribadi tidak boleh ditransfer ke negara atau ke wilayah luar area ekonomi Eropa kecuali negara atau wilayah itu menjamin adanya perlindungan yang sama terhadap hak dan kebebasan dari subjek data berkaitan dengan proses data pribadi).

Berdasarkan Pasal 14 dari *Data Protection Act* 1998 menjelaskan bahwa apabila pengadilan menemukan bahwa data pribadi diproses oleh pengontrol data tidak akurat, pengadilan dapat memerintahkan perbaikan, menghalangi, penghapusan atau kerusakan dari data tersebut. Bagi mereka sedang terkena dampak langsung dari pengolahan data pribadi dapat meminta Badan Komisaris untuk mengevaluasi proses untuk menentukan jika memenuhi ketentuan *Data Protection Act* 1998. Data subyek berhak untuk mengklaim kompensasi untuk setiap kerugian yang diderita sebagai akibat dari pelanggaran *Data Protection Act* oleh pengontrol data dan mungkin juga mengklaim kompensasi untuk bahaya yang ditimbulkan. Negara tetangga Malaysia sudah terlebih dahulu daripada Indonesia mengatur mengenai perlindungan data pribadi dalam bentuk undang-undang tersendiri.[71]

[71] Zuryati Mohamed Yusoff. *The Malaysian Personal Data Protection Act 2010: A Legislation Note, New Zealand Journal of Public and International Law.* Vol. 9. No. 1. 2011. hlm. 6.

Malaysia mengaturnya dalam *Personal Data Protection* Act (PDPA) 2010. Malaysia *Personal Data Protection* Act (PDPA) 2010 akhirnya disahkan oleh parlemen Malaysia pada awal Mei 2010. Dengan berlakunya Undang-undang ini, maka Malaysia untuk pertama kalinya memiliki Undang-undang yang mengatur secara spesifik mengenai privasi dan memberikan perlindungan terkait data pribadi.[72] Aturan dari PDPA ini bertujuan untuk mengatur pengolahan data pribadi oleh pengguna data dalam konteks transaksi komersial, dengan maksud menjaga kepentingan subjek data itu. Hal ini dicapai dengan memastikan bahwa persetujuan dari subjek data diperoleh sebelum pengolahan data pribadi serta memberikan data dengan subjek hak untuk mengakses, benar dan juga kontrol pengolahan data pribadi mereka. Hal tersebut sama halnya dengan apa yang disebutkan di dalam Pasal 26 UU ITE Indonesia. Selain PDPA, aturan lain berkaitan dengan perlindungan data pribadi yang berlaku di Malaysia yaitu: *a. Communication and Multimedia* Act 1998, *b. Computer Crimes* Act 1997, *c. Copyright* Act 1987, *d. Digital Signature* Act 1997, *e. Electronic Commerce* Act 2006, *f. Electronic Government Activities* Act 2007, *g. Payment System* Act 2003, *h. Credit Reporting Agencies* Act 2010, *i. Telemedicine* Act 1997, *j. Penal Code dan k. Communication and Multimedia Content Code.* PDPA 2010 ini dirancang sebagai undang-undang untuk melindungi data pribadi dengan mematuhi beberapa prinsip perlindungan data pribadi dengan beberapa modifikasi dan perubahan yang kemudian disesuaikan dengan kebutuhan dan keaadan lokal di Malaysia.[73]

Dengan berlakunya PDPA 2010 tersebut, setiap individu akan mendapat hak-hak baru seperti hak untuk diinformasikan mengenai data pribadinya serta hak untuk mengakses, mengkoreksi dan juga mengontrol pengolahan atau penggunaan data pribadi mereka oleh pihak lain. Transfer data pribadi lintas batas (*cross-border transfer*) juga diatur dalam PDPA. Sama halnya dengan Inggris yang juga mengatur tentang transfer data antar negara. PDPA menetapkan

---

[72] New Data Privacy Lawin Malaysia. http://www.bakermckenzie.com/RRSingaporeNewDataPrivacyLawAug10/ diakses pada 25 Agustus 2019.

[73] *Op. Cit.* hlm. 6.

bahwa tidak ada transfer data pribadi di luar Malaysia dapat terjadi kecuali pada tempat yang telah ditetapkan oleh Menteri Informasi, Kebudayaan dan Komunikasi. Kemudian negara tujuan tempat data pribadi ditransfer wajib memiliki tingkat perlindungan yang memadai yang setidaknya setara dengan tingkat perlindungan yang diberikan oleh PDPA Malaysia.[74] Berkaitan dengan hal tersebut, Indonesia belum mengatur tentang transfer data antar negara. Sebenarnya hal tersebut sangat penting untuk segera diatur sehingga Indonesia bisa bersaing di level internasional dalam kegiatan ekonomi dan bisnis digital dengan memiliki aturan yang akomodatif berkaitan dengan data pribadi.

PDPA 2010 memuat tujuh prinsip hukum setiap pengguna data dan mengharuskan bagi pengguna data untuk menyesuaikan dengan beberapa prinsip antara lain; prinsip umum, justifikasi untuk pemrosesan data seperti persetujuan, prinsip pemberitahuan dan pilihan. Hak untuk mendapatkan informasi tentang tujuan pemrosesan data; prinsip keterbukaan. Tidak bersifat tertutup kecuali berkaitan dengan tujuan; prinsip keamanan. Menjamin data tersebut akurat dan update; prinsip akses, hak individu untuk mengakses ke data pribadinya). Kewajiban untuk mengambil langkah yang praktis untuk perlindungan data; prinsip retensi. Tidak menyimpan data lebih lama dari yang diperlukan; prinsip integritas data.[75] Ketujuh prinsip ini mengatur secara komprehensif mengenai perlindungan data pribadi. Contohnya dalam *Retention Principle*, data pribadi yang diproses untuk tujuan apapun harus tidak disimpan lebih lama dari yang diperlukan untuk pemenuhan tujuan perlindungan data pribadi. Dalam hal ini akan menjadi tugas dari pengguna data untuk mengambil semua langkah-langkah yang wajar untuk memastikan bahwa semua data pribadi dihancurkan atau dihapus secara permanen. Dengan adanya PDPA 2010 ini, jaminan keamanan bagi data pribadi pengguna media elektronik di Malaysia pun meningkat.

---

[74] Gupinder Assi. *Op. Cit.* hlm. 6.

[75] Abu Bakar Munir. *The Malaysian Persona IdataProtection Bill.* http://profabm.blogspot.com/20-09/12/malaysian-personal-data-protection-bill.html. diakses pada 25 Agustus 2019.

Aturan berkaitan dengan Perlindungan data pribadi di Indonesia masih lemah dan bersifat umum karena aturannya termaktub dalam beberapa peraturan perundang-undangan yang terpisah dan hanya menggambarkan konsep perlindungan data pribadi secara general dan aturan yang hanya dituangkan dalam bentuk Peraturan Menteri Komunikasi dan Informatika Republik Indonesia. Beberapa aturan Undang-undang yang terpisah tersebut antara lain terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008, Undang-Undang Nomor 43 Tahun 2009, tentang Kearsipan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), dan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk).

Selain beberapa aturan tersebut diatas secara implisit, Konstitusi Indonesia (UUD NKRI 1945) memuat norma tentang Perlindungan data pribadi. Pasal 28 G ayat (1) memuat "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya,...".[76] Pengaturan mengenai perlindungan data pribadi diatur dalam beberapa Pasal di UU ITE. UU ini memang belum memuat aturan perlindungan data pribadi secara tegas dan komprehensif. Meskipun demikian, secara tidak langsung UU ini melahirkan pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Penjelasan tentang data elektronik pribadi diamanatkan lebih lanjut oleh UU ITE dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Perlindungan data pribadi dalam sebuah sistem elektronik di UU ITE meliputi perlindungan dari penggunaan tanpa

[76] Daniar Supriadi. *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya.* September 2017. http://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh-daniar-supriyadi.

izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses dan interferensi ilegal. Terkait dengan perlindungan data pribadi dari penggunaan tanpa izin, Pasal 26 UU ITE menyebutkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.[77] Dalam penjelasannya, Pasal 26 UU ITE juga menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang. UU ITE (11/2008 *jo.* 19/2016) sebagai UU generik memuat norma perlindungan data pribadi pada Pasal 26, yang pada intinya, penggunaan setiap data dan informasi di media elektronik yang terkait dengan data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan atau berdasarkan hukum positif (peraturan perundang-undangan). Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) *consent*/ persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar *lawful data processing*. Akan tetapi menurut Sonny Zulhuda, dari International Islamic University Malaysia mengatakan bahwasanya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik masih sangat tidak signifikan dalam mengatur penggunaan data pribadi karena Pasal yang ada dalam UU ITE tersebut hanya merupakan ketentuan umum dan tidak menjelaskan berbagai isu masalah yang banyak di bicarakan di level internasional saat ini.[78] Jadi dapat dipahami berdasarkan deskripsi diatas bahwa aturan berkenaan dengan Perlindungan Data Pribadi Indonesia masih bersifat umum dan terletak terpisah-pisah dalam beberapa aturan undang-undang. Selain itu juga diharapkan pemerintah dan parlemen Indonesia untuk segera membahas RUU Perlindungan Data Pribadi sehingga Indonesia akan lebih siap

[77] Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 26 ayat (1).

[78] Syarpani. *Tinjauan Yuridis terhadap Perlindungan Data Pribadi di Media Elektronik (*berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*)*. Jurnal Beraja Niti. Vol. 3 Nomor 6 2014. hlm. 7.

menghadapi tantangan ekonomi digital juga dapat memberikan jaminan keamanan terhadap data pribadi pengguna serta dapat memberikan sanksi yang tegas terhadap pihak yang menyalahgunakan data pribadi pihak lain.

BAB III
INTERNATIONAL TELECOMMUNICATION UNION ONLINE PROTECTION GUIDELINES

3.1 International Telecommunication Union Guidelines For Children On Online Protection 2016

Pada tahun 2016, ITU telah merevisi dan menerbitkan *Guidelines for Children on Child Online Protection* edisi ke 2. *Guidelines* ini diharapkan dapat menjadi pedoman bagi anak-anak dalam melindungi dirinya sendiri dari efek negatif dari internet seperti *cyberbullying*, pencurian identitas dan pelecehan saat daringsaat menjelajahi internet. Oleh karena itu selain peran pemerintah dan orang tua atau wali yang sangat penting dalam melindungi anak, kesadaran dan pengetahuan anak yang berbeda berdasarkan usianya dalam menyikapi internet tidak kalah pentingnya. Berikut tiga kelompok usia dari pengguna muda internet yaitu: [79]

a. Kelompok usia 5-7 tahun

   Banyak anak pada usia ini yang masih belum mampu untuk membaca dan mengerti tentang ketentuan yang sering kali muncul dalam situs atau aplikasi sehingga orang tua atau wali harus berperan aktif dalam menjaga dan memastikan keamanaan anak. Selain itu orang tua atau wali harus mulai memberikan batasan pada anak dalam menggunakan gawai untuk mencegah efek ketagihan pada anak.

[79] *Internatonal Telecommunication Union,* 2016, *Guidelines for Children on Child Online Protection 2016,* hlm. 29-31.

b. Kelompok usia 8-12 tahun

Anak di rentang usia ini sudah mulai mengenal aplikasi *chatting* dan sosial media. Oleh karena itu anak harus berhati-hati memberikan kepercayaannya kepada teman yang ia kenal saat daring, tetap menjaga kerahasiaan data pribadi, mengatur akun menjadi privat sehinga akun tersebut tidak dapat diakses oleh orang lain tanpa seizin anak dan tetap menjaga kerahasiaan dari *password* komputer, akun sosial media, atau lainnya sehingga tidak memungkinkan adanya pencurian atau penjebolan data. Saat bermain *game* anak harus menjaga sikap jangan sampai mencaci orang lain atau membagi informasi pribadinya kepada pemain lain. ITU juga menyarankan kepada anak usia ini agar terus menjalin komunikasi dengan orang tua atau saudara yang leboh tua. Apabila ingin menemui teman virtual mereka secara nyata, disarankan untuk mengajak orang tua atau saudaranya lebih tua. Anak usia ini sering kali terpengaruh dengan teman *online* mereka. Oleh karena itu tidak disarankan kepada anak untuk ikut berkata kasar atau melakukan perbuatan tidak menyenangkan di dunia digital. Selain itu, perlu diingat bahwa saat anak membagikan foto atau video diri mereka di internet maka konten milik mereka tidak hanya dapat dilihat oleh orang terdekat mereka namun juga orang lain yang tidak dikenal. Apabila konten tersebut sudah tersebar di dunia digital maka selamanya konten itu akan ada di dunia digital.

c. Kelompok usia 13 tahun ke atas.

Anak-anak usia 13 tahun keatas memang sedang mengalami fase pubertas dimana secara psikologis dan mental anak sedang mengalami perubahan dari anak-anak menuju dewasa. Oleh karena itu anak harus mampu menyaring informasi serta situs dan aplikasi yang tidak membahayakan diri mereka sendiri. Keingintahuan anak mengenai masalah sex dan asmara merupakan salah satu efek yang ditimbulkan dari perubahan

hormon yang terjadi pada diri anak sehingga anak di usia ini sangat rentan terjerumus dalam *grooming*[80] predator anak.

Anak harus sadar bahwa tidak semua orang yang mereka kenal di internet adalah orang yang sama di dunia nyata. Apabila ditemukannya hal demikian penting bagi anak untuk menyimpan pesan atau ajakan dari pelaku untuk dijadikan bukti kepada polisi untuk menangkap pelaku. Anak usia ini juga tidak luput dari *online bullying*. Oleh karena itu sangat disarankan pada mereka untuk tidak membagikan data pribadi mereka ke internet agar tidak disalahgunakan oleh pihak lain. Selain itu anak harus mengerti tentang hak cipta milik orang lain. Mereka tidak bisa membagikan foto atau video atau *software* ciptaan orang lain tanpa izin pemilik hak. Apabila melanggar hak cipta milik orang lain, anak harus mengerti konsekuensi hukum yang akan mereka terima.

Dalam *guidelines* ini, anak diperkenalkan dengan pedoman yang bisa mereka gunakan untuk menjaga diri mereka saat daring yaitu SMART *rules*. ITU tidak hanya memberikan perhatiannya kepada orang dewasa, namun juga anak-anak. *Guidelines* ini berfokus pada anak dimana *guideline* ini memberikan panduan dalam melindungi diri mereka di dunia digital dengan menerapkan metode SMART yang merupakan singkatan dari:[81]

a. *Set your limits*

   Anak harus menjaga privasi mereka saat menggunakan sosial media atau layanan daring lainnya bahkan dari keluarga dan sahabat. Berfikir duakali sebelum menyebarkan atau berbagi apapun saat daring, karena

[80] *Grooming* adalah suatu cara untuk mendapatkan kepercayaan anak atau remaja untuk berbagi informasi tentang ketertarikan akan sesuatu yang nantinya akan mengarah pada topik yang -memiliki unsur sexual yang bertujuan untuk mempengaruhi atau memancing anak ketempat dimana orang tersebut dapat mengeksploitasi anak secara sexual

[81] *Ibid,* hlm. 29-43

setelah hal tersebut tersebar di internet maka akan sangat sulit untuk menghapus atau mencegah orang lain menggunakannya. Menghargai hak orang lain layaknya menghargai hak sendiri adalah salah satu hal yang penting untuk di lakukan saat daring.

b. *Meeting online friends offline.*
Terkadang orang yang kita kenal saat daring ternyata sangat berbeda dengan kepribadiannya di dunia nyata. Anak harus sadar bahwa tidak semua orang yang mereka kenal di internet adalah orang yang baik. Oleh karena itu saat hendak menemui teman daring secara langsung, anak dapat mengajak seseorang yang ia percaya untuk menemaninya saat bertemu dengan orang tersebut.

c. *Accepting invitation/friendship,*
Anak harus lebih bijak dan selektif dalam menerima undangan pertemanan yang diajukan oleh orang lain di sosial media atau aplikasi lain.

d. *React*
Dalam penggunaan internet, anak harus dapat melindungi diri mereka dengan cara mengabaikan dan meninggalkan situs atau konten yang memiliki unsur-unsur yang tidak pantas, memblokir setiap orang yang mengirimkan *e-mail* atau komentar yang kasar, mengancam dan mengganggu, hindari orang asing yang berbicara mengenai sex, apabila anak sudah terjerumus dalam perangkap predator maka orang tua atau wali harus bijak dalam menasehati dan menolong anak mereka.

e. *Tell Someone about your concern*
Saat anak memiliki masalah dan tidak memiliki tempat untuk mencurahkannya maka ia akan mencoba untuk mencari orang untuk di ajak bicara di internet. Sangat berbahaya apabila anak menceritakan kehidupannya di sosial media atau dengan orang yang tak dikenal. Karena secara tidak sadar anak sudah membuka privasinya kepada orang lain. Oleh karena itu jika anak anda terlihat

memiliki masalah, maka segeralah berbicara dengannya dan berikan nasihat yang membangun.

Hasil yang diharapkan dalam *guideline* ini adalah anak dapat memiliki kendali penuh atas data pribadinya di dunia digital dan dunia nyata. ITU menyadari bahwa masih banyak orang tua yang sibuk bekerja untuk memenuhi kebutuhan keluarga tanpa memiliki waktu untuk dihabiskan dengan anak. Oleh karena itu, dalam *guideline* ini, ITU menitikberatkan tanggung jawab atas perlindungan data pribadi serta privasi anak kepada diri sang anak karena sudah waktunya bagi anak untuk sadar akan hak dan kewajiban yang melekat pada dirinya dalam dunia digital maupun dunia nyata sejak dini. Secara garis besar, *guideline* ini menekankan bahwa anak memiliki tanggung jawab atas dirinya sendiri. Anak harus sadar tentang resiko yang ada saat mereka daring maupun tidak.

ITU juga menerangkan bahwa terdapat bahaya yang mengancam anak saat mereka *online* seperti:[82]

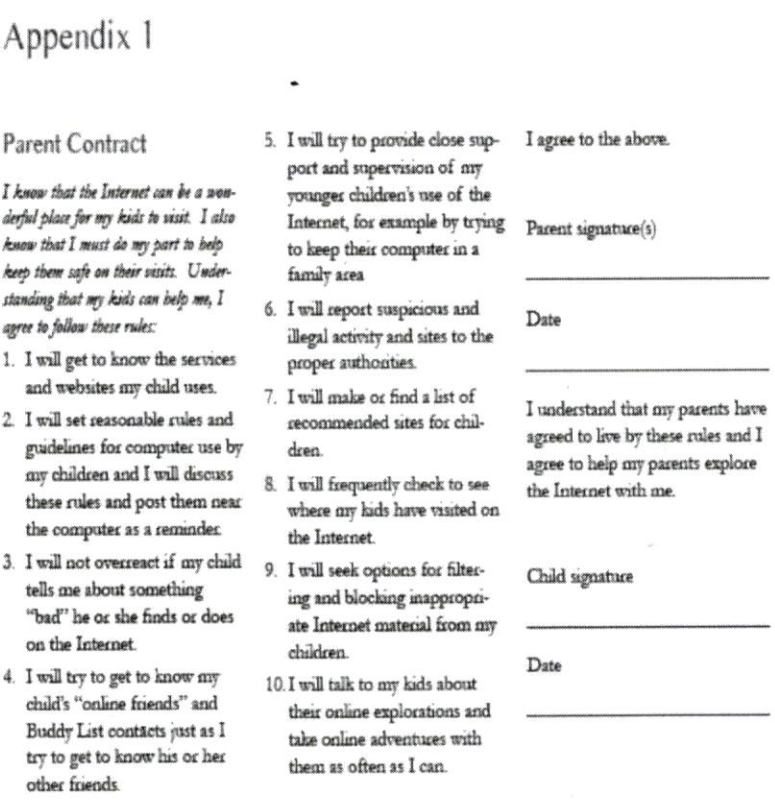
a. *Online bullying*;
b. Eksploitasi anak;
c. Penculikan;
d. Konten ilegal;
e. Pencurian data privasi;
f. Pelanggaran hak cipta
g. *Cyber grooming*; dan
h. Penipuan

Pada halaman terakhir *guideline* ini, ITU melampirkan *Appendix* 1 yang menyediakan contoh kontrak tentang *parent's control* kepada seluruh orang tua sebagai bentuk komitmen orang tua dalam melindungi keamanan anak saat daring khususnya data pribadi sang anak. Substansi yang teremuat dalam *appendix* 1 adalah berupa persetujuan serta pernyataan oleh seluruh orang tua dan wali anak untuk berkomitmen dalam melindungi anak mereka saat

[82] *Ibid.* hlm. 44-57.

daring dengan cara belajar memahami internet dan aplikasi yang paling sering digunakan oleh anak, mendukung anak serta mengawasi anak dalam penggunaan internet. Kontrak ini dibuat dalam rangka menegaskan komitmen dan fokus orang tua dalam merawat anak sebagiamana yang bisa dilihat pada gambar 1.

Gambar.1. *Appendix* 1: *Parent Contract*



Appendix 1

Parent Contract

I know that the Internet can be a wonderful place for my kids to visit. I also know that I must do my part to help keep them safe on their visits. Understanding that my kids can help me, I agree to follow these rules:

1. I will get to know the services and websites my child uses.
2. I will set reasonable rules and guidelines for computer use by my children and I will discuss these rules and post them near the computer as a reminder.
3. I will not overreact if my child tells me about something "bad" he or she finds or does on the Internet.
4. I will try to get to know my child's "online friends" and Buddy List contacts just as I try to get to know his or her other friends.
5. I will try to provide close support and supervision of my younger children's use of the Internet, for example by trying to keep their computer in a family area.
6. I will report suspicious and illegal activity and sites to the proper authorities.
7. I will make or find a list of recommended sites for children.
8. I will frequently check to see where my kids have visited on the Internet.
9. I will seek options for filtering and blocking inappropriate Internet material from my children.
10. I will talk to my kids about their online explorations and take online adventures with them as often as I can.

I agree to the above.

Parent signature(s)

Date

I understand that my parents have agreed to live by these rules and I agree to help my parents explore the Internet with me.

Child signature

Date

Sumber: *Guidelines for Children on Child Online Protection* 2016

Pada bagian kontrak orang tua dalam *Appendix* 1, menysaratkan sang anak untuk membaca dan memahami hak serta kewenangan yang dimiliki oleh orang tua, apakah melanggar hak asasi manusia mereka atau tidak. Dalam hal ini orang tua harus

memberikan penjelasan kepada sang anak sejelas-jelasnya tanpa ada unsur tipu muslihat. Apabila sang anak sudah paham dan setuju, maka anak tersebut harus menandatangani perjanjian yang sudah dibuat dan disepakati bersama. Selanjutnya ITU juga memberikan suatu perjanjian kepada anak untuk kooperatif dalam hal penggunaan teknologi. Contohnya seperti memberitahukan orang tua tentang aplikasi yang sedang digunakan, teman baru di internet dan melaporkan segala keluhannya kepada orang tua. *Guideline* ini tidak dapat berjalan efisien tanpa adanya kerjasama antara negara, orang tua dan pendidik.

Gambar.2. *Appendix 1: Child's Contract*

Child's Contract

I know that the Internet can be a wonderful place to visit. I also know that it is important for me to follow rules that will keep me safe on my visits. I agree to the following rules:

1. Wherever possible I will choose a safe and sensible screen name for myself that will not broadcast any personal information about my family or me.
2. I will keep all of my passwords private.
3. I will discuss with my parents all of the different programmes and applications I use on my computer and on the internet, and talk to them about the sites I visit. Before I download or load a new programme or join a new site I will check with my parents first to make sure they approve.
4. When considering signing up to a new online service I will avoid those which demand too much personal information and try to opt for those which ask for less.
5. I will always take steps to find out what personal information about me will be published by the service by default in my profile and will always opt for the maximum degree of privacy.
6. I will not share my personal information, or that of my parents or any other family member, in any way, shape or form, online or with someone I meet online. This includes, but is not limited to name, address, telephone number, age or school name.
7. I will treat others the way I want to be treated.
8. I will use good manners when I'm online, including good language and respect. I will not pick fights or use threatening or mean words.
9. I will make my own personal safety my priority, since I know there are some people who might be online and pretend to be someone they're not.
10. I will be honest with my parents about people I meet online and will tell them, without always being asked, about these people. I won't answer any e-mails or instant messages from anyone my parents have not approved.
11. If I see or read things that are bad, icky or mean, I will log off and tell my parents so they can try to make sure it never happens again.
12. I will tell my parents if I receive pictures, links to bad sites, e-mail or instant messages with bad language or if I'm in a chat room where people are using swear words or mean and hateful language.
13. I will not send anything in the post to anyone I've met online, without my parents' okay. If I get something in the post from someone I've met online, I'll tell my parents immediately (because that means they have my private information).
14. I will not do anything online that someone asks me to if it makes me feel uncomfortable, especially if I know it's something my parents would not be happy about or approve of.

15. I will not call, write a snail mail or meet in person anyone who I've met online without my parents' approval or without a trusted adult coming with me.
16. I understand my parents will supervise my time online and may use software to monitor or limit where I go online. They're doing this because they love me and want to protect me.

I will teach my parents more about the Internet so we can have fun together and learn cool new things.

I agree to the above.

Child signature

_____

Date

_____

I promise to protect my child's safety online by making sure these rules are followed. If my child encounters unsafe situations and tells me, I will handle each situation with maturity and good sense, without blaming anyone, and will calmly work through it with my child to ensure their safer Internet experiences in the future.

Parent signature(s)

_____

Date

_____

Sumber: *Guidelines for Children on Child Online Protection* 2016

Perjanjian yang ada dalam *Appendix* ini diharapkan dapat menanamkan rasa tanggung jawab dan menumbuhkan kesadaran pada diri anak untuk bertanggung jawab dalam berperilaku di dunia digital dan memberikan keleluasaan kepada orang tua untuk mengawasi dan melindungi anak dari bahaya yang mengintai saat anak sedang daring.

3.2 International Telecommunication Union Guidelines For Parents

Orang tua sering kali berasumsi bahwa anak-anak lebih aman apabila berada di rumah menggunakan sebuah komputer, atau di sekolah daripada berada di tempat lain seperti taman bermain atau lainnya. Asumsi semacam ini tidak sepenuhnya benar, karena pada saat anak berada dirumah bersama gawai atau komputer miliknya yang terhubung dengan internet, maka anak tersebut dapat

berpetualang di dunia digital yang sama bahayanya dengan dunia nyata.[83]

Substansi dari *guidelines* ini dibentuk berdasarkan *Child Online Protection Agenda* sebagai bagian dari *Global Cybersecurity Agenda*, dengan tujuan membentuk fondasi dunia digital yang aman untuk generasi saat ini dan yang akan datang.[84] Selain menjelaskan tentang bahaya yang ada, *guidelines* ini memberikan masukan bagi tenaga pendidik, orang tua dan wali dalam mengkontrol kegiatan anak saat daring. Dalam rangka menjamin keamanan anak dalam menggunakan internet, orang tua dan wali dapat mengambil tindakan sebagai berikut:[85]

a. Membuka sesi dialog antara orang tua atau wali dengan anak mereka tentang aktivitas mereka saat menjelajahi internet seperti dengan siapa saja ia berkomunikasi, apa saja yang dilakukan anak ketika menggunakan telepon genggam, komputer dan tablet mereka;
b. Membaca syarat ketentuan yang diberikan oleh pengelola situs internet, pengelola aplikasi serta membuat aturan bersama-sama dengan anak mereka. Orang tua dan wali juga harus mengawasi dan menjamin penggunaan media elektronik oleh anak;
c. Mengedukasi anak berkaitan dengan tanggung jawab dan penggunaan teknologi secara umum serta memberikan nasihat kepada anak untuk menggunakan akal sehat saat menjelajahi internet;
d. Mengecek apakah situs tersebut memiliki:
    a. Fitur pengawasan orang tua;
    b. Menjaga *history*[86] pada aplikasi *browser*[87] pengguna;
    c. Situs tersebut mengizinkan foto atau video disebar;

---

[83] *International Telecommunication Union,* 2016, *Guidelines for Parents, Guardians and Educators on Child Online Protection, ITU,* hlm.2.
[84] *Ibid.* hlm. 1.
[85] *Ibid.* hlm. 60-67
[86] *History* adalah fasilitas untuk mencatat dan menyimpan data sejarah penelusuran dan penggunaan internet.
[87] *Browser* adalah program yang digunakan untuk menjelajahi dunia Internet atau untuk mencari informasi tentang suatu halaman web yang tersimpan di komputer.

d. Sistem pelaporan dan pemblokiran seperti alat untuk melaporkan adanya konten yang tidak pantas;
e. Sistem *rating*, orang tua serta wali harus sadar dan mengerti tentang fungsi simbol *rating* dan penggunaannya sebagai alat penting untuk mencegah anak dari konten-konten yang tidak pantas; dan
f. Sistem verifikasi usia.

e. Ikut terlibat dengan aktivitas anak saat terhubung internet agar orang tua dapat mengetahui apakah situs atau aplikasi itu pantas bagi anak atau tidak;
f. Bijaksana dalam menyikapi perilaku anak di media sosial;
g. Berwaspada karena terkadang anak memiliki sifat yang berbeda saat mereka daring dan tidak, oleh karena itu orang tua harus sering berkomunikasi secara langsung dengan anak-anaknya sehingga orang tua dapat mengerti dan memahami situasi dan kondisi anaknya;
h. Memahami budaya daring sehingga orang tua dan wali dapat mengakses dan mengerti tentang fungsi dan kegunaan dari aplikasi atau situs;
i. Mengajarkan anak-anak untuk tidak membagi akses informasi mereka seperti *password*[88] dengan saudara atau teman-temannya;
j. Secara umum situs anak-anak harus aman dan menyediakan konten yang indah, kreatif dan mengedukasi anak;
k. Menempatkan komputer ditempat yang mudah untuk diawasi, seperti di ruang keluarga atau di tempat-tempat yang sering di lewati oleh anggota keluarga lainnya. Dengan menempatkan komputer di tempat terbuka dapat memudahkan orang tua atau anggota keluarga lainnya untuk melihat dan ikut terlibat dalam aktivitas anak saat menggunakan komputer;

[88] *Password* adalah adalah kumpulan karakter atau string yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (multiuser) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut.

l. Menginstal *firewall*[89] dan *antivirus* untuk memastikan komputer yang digunakan oleh anak tidak mudah terjangkit virus yang dapat merusak data hingga mencuri data dari komputer yang digunakan anak;

m. Membuat aturan mengenai penggunaan internet dan perangkat pribadi seperti telepon genggam, tablet dan lainnya. Orang tua dan wali juga harus mengajarkan kepada anak tentang resiko serta bahaya yang ada di internet sehingga anak dapat menempatkan dirinya dengan baik saat daring;

n. Orang tua harus terbiasa dengan situs internet yang sering dikunjungi oleh anak dan mengetahui bagaimana anak menghabiskan waktunya saat daring. Sebelum mengizinkan anak untuk mengunjungi situs tersebut orang tua harus memahami syarat dan ketentuan privasi yang disyaratkan oleh pengelola situs bersama dengan anaknya dengan hati-hati dan teliti sehingga orang tua tidak merasa kecolongan atau dirugikan;

o. Mencari informasi mengenai bagaimana seharusnya mengakses internet dengan aman serta memeriksa kemanan dari situs internet. Hal ini dapat dilakukan dengan melihat katalog atau website resmi dari badan atau organisasi yang bergerak di bidang perlindungan anak seperti UNICEF, COPPA, KPAI dan lainnya;

p. Menggunakan *software* yang memiliki fungsi memblokir dan menyaring situs yang ada di internet. Dalam menggunakan *software* ini, orang tua harus menjelaskan alasan serta tujuannya kepada sang anak. Orang tua dan wali juga harus berhati-hati dalam menggunakannya jangan sampai berlebihan sehingga melanggar privasi anak;

---

[89] *Firewall* adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Saat ini, pengertian *firewall* difahami sebagai sebuah istilah generik yang merujuk pada fungsi firewall sebagai sistem pengatur komunikasi antar dua jaringan yang berlainan.

q. Pengelola situs atau perusahaan aplikasi harus menyertakan persetujuan dari orang tua atau wali sebelum memintakan atau mengelola data pribadi sang anak. Orang tua dan wali harus mengerti tujuan dan metode pengumpulan dan pengelolaan dari data pribadi anak tersebut sehingga apabila terjadi ketidaksesuaian dengan tujuan awal, orang tua atau wali dapat meminta ganti kerugian atau memberhentikan pengumpulan dan pengelolaan data oleh perusahaan atau pengelola situs internet;

r. Orang tua dan wali harus memastikan bahwa situs tersebut sesuai dengan usia sang anak. Sehingga saat anak melakukan pembelian barang atau jasa dari situs tersebut, barang dan jasa yang dipesan sesuai dengan usia sang anak;

s. Memblokir akses konten dan jasa yang tidak pantas. Hal ini dapat dilakukan dengan mengubah pengaturan pada *browser* yang akan digunakan anak;

t. Membuat perjanjian dengan sang anak terkait penggunaan gawai. Perjanjian tersebut haruslah bersifat fleksibel. Sehingga apabila kedepannya terdapat konten yang tidak pantas maka orang tua dan anak dapat menghapus akun anak dari situs atau aplikasi tersebut;

u. Mengawasi dan melaporkan iklan yang mengandung unsur-unsur yang tidak pantas dilihat anak;

v. Membekali anak dengan literasi media internet sehingga anak dapat menjaga dirinya saat daring;

w. Melarang anak untuk berbagi data pribadi mereka dengan orang lain. Anak harus diajarkan mengenai seberapa pentingnya data pribadi dan akibat yang dapat ditimbulkan apabila data pribadi anak tersebar di internet;

x. Memberikan pengertian pada anak tentang akibat dari penyebaran foto atau penggunaan webcam saat mereka daring dengan menyertakan alamat rumah, nomor plat mobil, nama sekolah, nomor telepon dan informasi lain yang menunjukkan identitas sang anak;

y. Memperingatkan anak untuk tidak mudah mengekspresikan emosinya kepada orang asing. Memberikan pengertian

kepada anak bahwa apa yang mereka tulis di internet dapat dilihat oleh semua orang termasuk predator anak dan pelaku *bully*[90] di internet;

z. Mengecek halaman profil anak di sosial media dengan melihat *history* dari akun anak dan jika perlu untuk memantau aktivitas mereka dan dengan siapa mereka berkomunikasi;

aa. Pastikan bahwa anak mengikuti aturan tentang batas usia yang diberikan oleh situs atau aplikasi internet; dan

bb. Memastikan anak tidak menggunakan nama lengkap mereka yang dapat mengidentifikasi diri mereka seperti nama jalan tempat tinggal, sekolah, Nomor telepon, klub olahraga dan lainnya.

Kontrol orang tua memegang peran penting dalam perlindungan anak. Oleh karena itu perusahaan teknologi seperti *Microsoft* dan *Apple* sudah menyediakan sistem pengawasan dalam sistem *windows* atau *ios* milik mereka..[91] Oleh karena itu ITU menghimbau orang tua untuk belajar memahami penggunaan fitur pengawasan ini agar di waktu yang bersamaan anak dapat memaksimalkan fungsi dari internet serta aman dalam menggunakannya. Orang tua, wali dan tenaga pendidik juga harus mengajarkan tanggung jawab dan perilaku positif dalam menggunakan internet seperti:

a. Mengajarkan anak cara menginstal dan menggunakan anti-virus saat anak daring agar tehindar dari *hacking* atau virus *ransomware*;

b. Dalam rangka melindungi anak saat daring, orang tua haruslah mengerti terlebih dahulu mengenai cara mengoperasikan internet dengan baik. Contohnya seperti mengetahui cara mengoperasikan dan memaksimalkan fitur *blocking* yang ada dalam *browser* di komputer anak.

---

[90] *Bully* adalah tindakan kekerasan, ancaman, atau paksaan untuk menyalahgunakan atau mengintimidasi orang lain. Perilaku ini dapat menjadi suatu kebiasaan dan melibatkan ketidakseimbangan kekuasaan sosial atau fisik.

[91] *Ibid.* hlm.75

c. Melarang anak untuk membagikan data pribadinya di internet, seperti di sosial media, aplikasi permainan atau saat berhubungan dengan orang asing.

ITU juga merekomendasikan tenaga pendidik untuk melakukan beberapa tindakan sebagai berikut:

a. Menggunakan pendekatan menyeluruh terkait tanggung jawab dalam keselamatan elektronik;
b. Mengembangkan ketentuan *acceptable use policy* (AUP) yang mensyaratkan tenaga pendidik mengerti mengenai bahaya yang mengintai anak di internet. Ketentuan ini berisikan hal-hal yang boleh dan tidak boleh dilakukan oleh anak saat daring. Apabila ditemukan sang anak tidak menaati ketentuan tersebut, pihak sekolah dapat memanggil orang tua sang anak untuk selanjutnya mendiskusikan tindakan yang dapat diambil atau pihak sekolah bisa langsung menjatuhkan sanksi yang wajar kepada sang anak atas perbuatannya saat daring;
c. Meningkatkan kesadaran anak dan remaja terkait dengan bahaya penyebaran data pribadi kepada orang asing di internet;
d. Membantu anak-anak untuk mengembangkan strategi perlindungan pada diri anak ketika pengawasan orang dewasa dan perlindungan teknologi tidak tersedia;
e. Membantu anak-anak memahami bahwa mereka tidak bertanggung jawab atas tindakan dipaksakan orang lain. Para pendidik juga harus memberikan sanksi yang akan diterapkan sekolah jika anak-anak bertindak tidak semestinya saat daring;

Orang tua yang merupakan pelindung utama anak-anak juga dapat mengatur perlindungan data pribadi anak dengan memanfaatkan fasilitas yang telah disediakan dalam sistem komputer. Langkah pertama yang harus orang tua lakukan adalah memperbarui sistem *windows* komputer dengan versi yang terbaru. Selanjutnya orang tua harus membuatkan akun untuk anaknya dalam sistem komputer anak dengan cara melihat panduan pada

komputer yang telah tersedia dalam menu *control panel*. Saat ini, aplikasi *browser* seperti *safari*, *chrome*, *firefox* dan lainnya memiliki catatan akses yang secara otomatis menunjukkan situs apa saja yang telah diakses oleh anak sehingga orang tua dapat memantau aktivitas anak saat daring melalui fitur ini.

3.3 International Telecommunication Union Guidelines For Industry On Child Online Online Protection.

Ledakan teknologi informasi dan komunikasi telah menciptakan peluang yang belum pernah terjadi sebelumnya bagi anak-anak dan orang muda untuk berkomunikasi, terhubung, berbagi, belajar, mengakses informasi dan mengungkapkan pendapat mereka tentang hal-hal yang mempengaruhi kehidupan mereka dan komunitas mereka. Tetapi akses yang lebih luas dan lebih mudah tersedia di internet dan teknologi seluler juga memiliki tantangan signifikan terhadap keselamatan anak-anak - baik online maupun offline.

Untuk mengurangi risiko revolusi digital sambil memungkinkan lebih banyak anak dan remaja memetik manfaatnya, pemerintah, masyarakat sipil, komunitas lokal, organisasi internasional dan sektor swasta harus bersatu untuk tujuan yang sama. Industri teknologi memiliki peran penting dalam membangun fondasi untuk penggunaan yang lebih aman dan lebih aman dari layanan berbasis Internet dan teknologi lainnya - untuk anak-anak saat ini dan generasi mendatang.

Bisnis harus melindungi anak-anak, memberikan perhatian khusus dan melindungi privasi data pribadi bagi para pengguna muda, menjaga hak mereka atas kebebasan berekspresi, dan menerapkan sistem untuk menangani pelanggaran hak-hak anak ketika itu terjadi. Jika undang-undang tentang lingkungan belum memenuhi hukum internasional, bisnis memiliki peluang dan tanggung jawab untuk menyelaraskan praktik bisnis mereka dengan standar-standar tersebut.

Pedoman baru untuk Industri tentang Perlindungan Daring Anak ini menyediakan kerangka kerja untuk semakin banyak perusahaan yang mengembangkan , menyediakan atau

memanfaatkan teknologi informasi dan komunikasi dalam penyampaian produk dan layanan mereka. Perusahaan-perusahaan semacam itu berada dalam posisi yang baik untuk mendorong solusi inovatif, menciptakan platform digital yang dapat memperluas peluang pendidikan dan memungkinkan anak-anak dan remaja untuk terlibat dalam kehidupan sipil komunitas mereka untuk menjadi warga dunia yang benar-benar global.

Inisiatif lokal dan nasional sangat penting untuk berkolaborasi dalam pedoman pelengkap bagi pemerintah yang membahas perumusan, implementasi, pengelolaan, dan pemantauan Rencana Aksi Negara untuk memperkuat perlindungan anak di internet. Internet tidak mengenal batas, dan upaya kita untuk melindungi anak-anak harus ambisius dan berjangkauan luas.

Inisiatif Perlindungan Daring Anak (COP) adalah jaringan multi-pemangku kepentingan yang diluncurkan oleh International Telecommunication Union (ITU) untuk mempromosikan kesadaran akan keselamatan anak di dunia online dan untuk mengembangkan alat praktis untuk membantu pemerintah, industri, dan pendidik.[92]

Sebagai bagian dari inisiatif , pada tahun 2009, ITU menerbitkan satu set COPGuidelines untuk empat kelompok: anak-anak; orang tua, wali, dan pendidik; industri, dan pembuat kebijakan. Pedoman untuk Industri tentang Perlindungan Anak Online bertujuan membangun fondasi untuk penggunaan layanan berbasis Internet yang lebih aman dan teknologi terkait untuk anak-anak saat ini juga generasi mendatang.

Menanggapi kemajuan substansial dalam teknologi dan konvergensi, ITU, UNICEF dan mitra COP telah mengembangkan dan memperbarui Pedoman untuk berbagai perusahaan yang mengembangkan, menyediakan atau menggunakan telekomunikasi atau kegiatan terkait dalam pengiriman produk dan layanan mereka. Pedoman baru untuk Industri

Perlindungan Anak Online adalah hasil konsultasi dengan anggota COP Initiative, serta konsultasi terbuka yang lebih luas yang mengundang anggota masyarakat sipil, bisnis, akademisi,

[92] For more information, see, ITU 'Child Online Protection', www.itu.int/cop

pemerintah, media, organisasi internasional, dan kaum muda untuk memberikan umpan balik mengenai Pedoman. Pedoman berlaku untuk keselamatan anak-anak saat menggunakan teknologi informasi dan komunikasi (TIK).

Terdapat lima bidang utama untuk melindungi dan mempromosikan hak anak:

a. Mengintegrasikan pertimbangan hak-hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang tepat.

   Mengintegrasikan pertimbangan hak anak mengharuskan perusahaan mengambil langkah-langkah memadai untuk mengidentifikasi, mencegah, memitigasi dan, jika sesuai, memulihkan potensi dan dampak buruk aktual pada hak-hak anak. Prinsip-prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia menyerukan kepada semua bisnis untuk menerapkan kebijakan dan proses yang sesuai untuk memenuhi tanggung jawab mereka untuk menghormati hak asasi manusia.

   Bisnis harus memberikan perhatian khusus kepada anak-anak dan remaja sebagai kelompok yang rentan dalam hal perlindungan data dan kebebasan berekspresi. Resolusi Umum PBB, "Hak atas privasi di era digital" menegaskan kembali hak cipta dan kebebasan berekspresi tanpa mengalami gangguan yang melanggar hukum.[93]

   Selain itu, Resolusi Dewan Hak Asasi Manusia tentang "Promosi, perlindungan, dan kenikmatan hak asasi manusia" di Internet ", mengakui sifat global dan terbuka dari Internet sebagai kekuatan pendorong dalam mempercepat kemajuan menuju pembangunan dan menegaskan hak-hak yang sama yang dimiliki orang secara offline juga harus dilindungi secara

[93] United Nations General Assembly Resolution, "The right to privacy in the digital age",
A/RES/68/167, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

online.[94] Negara yang tidak memiliki kerangka hukum yang memadai untuk melindungi hak anak-anak untuk privasi dan kebebasan berekspresi, perusahaan harus mengikuti ketekunan yang ditingkatkan untuk memastikan kebijakan dan praktik sejalan dengan hukum internasional.

b. mengembangkan standar untuk menangani masalah pelecehan seksual anak

Protokol Opsional untuk Konvensi Hak-Hak Anak tentang penjualan anak-anak, pelacuran anak, dan pornografi anak mendefinisikan 'pornografi anak' sebagai representasi apa pun, dengan cara apa pun, dari seorang anak yang terlibat dalam kegiatan-kegiatan explicitsexual yang nyata atau disimulasikan atau representasi seksual apa pun. bagian dari seorang anak untuk tujuan primarileksual.[95]

Dari semua materi pelecehan seksual anak yang dianalisis oleh Internet WatchFoundation pada 2013, 81 persen korban anak-anak tampaknya berusia 10 tahun atau lebih muda, dan 51 persen gambar menggambarkan aktivitas seksual antara orang dewasa dan anak-anak, termasuk pemerkosaan dan penyiksaan.[96]

Fakta-fakta yang mengganggu ini menggarisbawahi pentingnya tindakan kolaboratif antara industri, pemerintah, penegak hukum, dan masyarakat sipil untuk memerangi materi pelecehan seksual anak. Sementara banyak pemerintah menangani penyebaran dan distribusi materi pelecehan seksual anak dengan memberlakukan undang-undang,

---

[94] United Nations Human Rights Council Resolution, "The promotion, protection and enjoyment of human rights on the Internet",

[95] United Nations, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2, New York, 25 May
2000, www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.asp

[96] Internet Watch Foundation, 'Annual & Charity Report 2013', LINX, UK, https://www.iwf.org.uk/accountability/annual- reports/2013-annual-report

mengejar dan menuntut para pelaku kekerasan, meningkatkan kesadaran, dan mendukung anak-anak untuk pulih lebih dari penyalahgunaan atau eksploitasi, banyak negara belum memiliki sistem yang memadai.

Diperlukan mekanisme di setiap negara untuk memungkinkan masyarakat umum melaporkan konten yang kasar dan eksploitatif dari sifat ini. Industri, penegakan hukum, pemerintah, dan masyarakat sipil harus bekerja sama dengan satu sama lain untuk memastikan bahwa kerangka hukum yang memadai sesuai dengan standar internasional tersedia. Kerangka kerja tersebut harus mengkriminalkan semua bentuk pelecehan dan eksploitasi seksual anak, termasuk melalui bahan pelecehan anak, dan melindungi anak-anak yang menjadi korban pelecehan atau eksploitasi tersebut, dan memastikan bahwa pelaporan, proses investigasi, dan penghapusan konten bekerja seefisien mungkin.

c. Menciptakan lingkungan online yang lebih aman bagi semua usia.

Sangat sedikit hal dalam hidup yang dapat dianggap benar-benar aman dan bebas risiko sepanjang waktu. Bahkan di kota-kota di mana pergerakan lalu lintas sangat diatur dan dikendalikan dengan ketat, kecelakaan masih terjadi. Dengan cara yang sama, ruang maya bukan tanpa risiko, terutama untuk anak-anak. Anak-anak dapat dianggap sebagai penerima, peserta, dan aktor di lingkungan online mereka.

Risiko yang mereka hadapi dapat dikategorikan ke dalam tiga bidang[97]:

a. Konten yang tidak pantas

Anak-anak dapat menemukan konten yang dipertanyakan saat mencari sesuatu yang lain dengan mengklik tautan

[97] Livingstone, S., and L. Haddon, 'EU Kids Online: Final report', EU Kids Online, London School of Economics and Political Science, London (EC Safer Internet Plus Programme Deliverable D6.5), June 2009, p. 10

yang mungkin tidak berbahaya dalam pesan instan, di blog atau saat berbagi file. Anak-anak juga dapat mencari dan membagikan materi yang dapat dipertanyakan. Apa yang dianggap konten berbahaya bervariasi dari satu negara ke negara lain, namun contohnya termasuk konten yang mempromosikan penyalahgunaan zat, ras, perilaku mengambil risiko atau bunuh diri, anoreksia atau kekerasan.

b. Perilaku yang tidak pantas
Anak-anak dan orang dewasa dapat menggunakan Internet untuk melecehkan atau bahkan mengeksploitasi orang lain. Anak-anak kadang-kadang dapat menyiarkan komentar menyakitkan atau gambar yang memalukan atau mencuri konten atau melanggar hak cipta.

c. Kontak yang tidak pantas
Baik orang dewasa maupun orang muda dapat menggunakan Internet untuk mencari anak-anak atau orang muda lain yang rentan. Seringkali, tujuan mereka adalah meyakinkan target bahwa mereka telah mengembangkan hubungan yang bermakna, tetapi tujuan yang mendasarinya adalah manipulatif. Mereka mungkin berusaha membujuk anak untuk melakukan tindakan seksual atau tindakan pelecehan lainnya secara online, menggunakan kamera web atau alat perekam lain, atau mereka akan mencoba mengatur pertemuan langsung dan kontak fisik. Proses ini sering disebut sebagai 'perawatan'. Keselamatan daring adalah tantangan komunitas dan peluang bagi industri, pemerintah, dan masyarakat sipil untuk bekerja sama untuk menetapkan prinsip dan praktik keselamatan. Industri dapat menawarkan beragam pendekatan teknis, alat, dan layanan untuk orang tua dan anak-anak. Ini dapat mencakup alat-alat penawaran untuk mengembangkan sistem verifikasi usia baru atau untuk menempatkan pembatasan pada konsumsi anak-anak atas konten dan layanan, atau untuk membatasi orang-orang

yang memiliki kontak dengan anak-anak atau waktu di mana mereka dapat pergi online.

d. Mendidik anak-anak, orang tua, dan guru tentang keselamatan anak-anak dan tanggung jawab mereka dalam ICT

Langkah-langkah teknis dapat menjadi bagian penting untuk memastikan bahwa anak-anak dilindungi dari risiko potensial yang mereka hadapi online, tetapi ini hanya satu elemen dari persamaan. Alat kontrol orang tua dan peningkatan kesadaran dan pendidikan juga merupakan komponen kunci yang akan membantu memberdayakan dan menginformasikan anak-anak dari berbagai kelompok umur, serta orang tua, pengasuh dan pendidik.

Meskipun perusahaan memiliki peran penting dalam memastikan bahwa anak-anak menggunakan TIK di possibleway yang paling bertanggung jawab dan paling aman, tanggung jawab ini dibagi dengan orang tua, sekolah, dan anak-anak. Banyak perusahaan berinvestasi dalam program pendidikan yang dirancang untuk memungkinkan pengguna membuat keputusan tentang konten dan layanan. Perusahaan membantu orang tua, pengasuh dan guru dalam membimbing anak-anak dan remaja menuju pengalaman online dan ponsel yang lebih bertanggung jawab dan sesuai. Ini termasuk *signposting* konten yang sensitif terhadap usia dan memastikan bahwa informasi tentang barang-barang seperti harga konten, syarat berlangganan, dan cara membatalkan langganan, dikomunikasikan dengan jelas.

Penting juga untuk memberikan informasi langsung kepada anak-anak tentang penggunaan TIK yang lebih aman dan perilaku positif dan bertanggung jawab. Selain meningkatkan kesadaran tentang keselamatan, perusahaan dapat memfasilitasi pengalaman positif dengan mengembangkan konten untuk anak-anak tentang rasa

hormat, ramah, dan berpikiran terbuka ketika menggunakan TIK dan tidak mau mencari teman. Mereka dapat memberikan informasi tentang tindakan yang harus diambil jika mereka memiliki pengalaman negatif seperti intimidasi atau perawatan daring, membuatnya lebih mudah untuk melaporkan kejadian semacam itu dan menyediakan fungsi untuk tidak menerima pesan anonim.

e. Mempromosikan teknologi digital sebagai mode untuk meningkatkan keterlibatan sipil
Konvensi Hak-hak Anak, dalam pasal 13, menyatakan bahwa "anak harus memiliki hak atas kebebasan berekspresi; hak ini harus mencakup kebebasan untuk mencari, menerima, dan memberikan informasi dan gagasan dalam segala jenis, terlepas dari batas, baik secara tertulis, dalam bentuk cetak, dalam bentuk seni, atau melalui media lain dari pilihan anak.

"Perusahaan dapat memenuhi rasa hormat mereka terhadap hak-hak sipil dan politik anak-anak dengan memastikan bahwa teknologi, undang-undang dan kebijakan yang dikembangkan untuk melindungi anak-anak dari bahaya online tidak memiliki konsekuensi yang tidak diinginkan dengan menekan partisipasi dan ekspresi atas hak mereka atau mencegah mereka mengakses informasi yang penting bagi kesejahteraan mereka.

Pada saat yang sama, bisnis juga dapat mendukung hak-hak anak dengan menawarkan mekanisme dan alat untuk memfasilitasi partisipasi kaum muda. Mereka dapat menekankan kapasitas Internet untuk memfasilitasi keterlibatan positif dalam kehidupan sipil yang lebih luas, mendorong kemajuan sosial, dan mempengaruhi keberlanjutan dan ketahanan masyarakat, misalnya, dengan berpartisipasi dalam kampanye sosial dan lingkungan dan menahan mereka yang bertanggung jawab.

Dengan alat dan informasi yang tepat, anak-anak dan remaja ditempatkan untuk mengakses peluang perawatan kesehatan, pendidikan dan pekerjaan, dan untuk menyuarakan pendapat dan kebutuhan mereka di sekolah, masyarakat dan negara. Mereka dapat

mengakses informasi tentang hak-hak mereka dan menuntut informasi, baik dalam hal hak atas informasi mengenai hal-hal yang mempengaruhi mereka, seperti kesehatan seksual mereka, atau akuntabilitas politik dan pemerintah. Perusahaan juga dapat berinvestasi dalam penciptaan pengalaman online yang sesuai. anak-anak dan keluarga. Mereka dapat mendukung pengembangan teknologi dan konten yang mendorong dan memungkinkan anak-anak dan remaja untuk belajar, berinovasi dan menciptakan solusi

Perusahaan-perusahaan dapat secara proaktif mendukung hak-hak anak dengan bekerja untuk menyimpan kesenjangan digital. Partisipasi anak-anak membutuhkan literasi digital kemampuan untuk memahami dan berpartisipasi dalam dunia digital. Tanpa kemampuan ini, warga negara tidak akan dapat berpartisipasi dalam banyak fungsi sosial yang telah menjadi 'digital', termasuk tetapi tidak terbatas pada pengarsipan pajak, mendukung kandidat politik, menandatangani *onlinepetitions*, mendaftarkan kelahiran, atau hanya mengakses komersial, kesehatan, pendidikan informasi budaya. Kesenjangan antara warga negara yang dapat mengakses forum-forum ini dan mereka yang tidak dapat karena kurangnya akses Internet atau literasi digital akan terus melebar - menempatkan kelompok-kelompok yang disebutkan terakhir pada kerugian yang signifikan. Perusahaan dapat mendukung prakarsa multimedia untuk memberikan keterampilan digital yang dibutuhkan anak-anak untuk menjadi warga negara yang percaya diri, terhubung, dan terlibat aktif.

3.4 International Telecommunication Union Guidelines For Policy Makers On Child Online Protection

Teknologi yang saat ini disebut sebagai "Internet" memicu pertumbuhan eksponensial dari Internet yang menyebabkannya menjadi pilihan yang sangat berharga dalam kehidupan kita, baik secara ekonomi maupun sosial, dan telah membawanya untuk menciptakan fitur yang tampaknya permanen dari kehidupan modern.

Pada awal revolusi Internet, pengguna kagum pada kemungkinan menghubungi orang dan mengakses informasi dan zona waktu melalui beberapa klik mouse mereka. Namun, untuk melakukannya, mereka harus berada di lokasi tetap di depan perangkat komputer yang sering besar atau massal, biasanya PC. Saat ini orang dapat terhubung ke jaringan global menggunakan mobil, komputer laptop atau perangkat portabel, sering dengan kemampuan video dan akses berkecepatan sangat tinggi. Banyak konsol game juga memungkinkan Internet dan ini telah mendorong pertumbuhan besar dalam permainan on-line di kalangan anak-anak dan remaja.

Butuh waktu sekitar 20 tahun untuk mencapai miliar pengguna ponsel pertama, namun miliar kedua mendaftar hanya dalam beberapa tahun terakhir. Sebaliknya, butuh 125 tahun untuk mencapai miliar pengguna telepon tetap pertama. Evolusi dari telepon seluler generasi kedua tothird ini sama pentingnya dengan lompatan awal dari analog ke digital. Itu dimulai lebih dari satu dekade lalu dan berkembang dengan cepat.

Teknologi generasi keempat yang baru muncul mempertahankan em-phasis pada akses seluler tetapi memakan kecepatan yang lebih tinggi. Jaringan pita lebar dan konvergensi media menghasilkan jalan baru untuk mendistribusikan hiburan digital. Perangkat pengguna kini multi-fungsi dan semakin personal. Dalam waktu dekat, kemajuan dalam komputasi terkoneksi akan memungkinkan ratusan juta objek memiliki kemampuan untuk berkomunikasi satu sama lain melalui Internet, membuka aplikasi rumah tangga dan bisnis yang tak terhitung jumlahnya. Di pasar telepon tetap dan seluler, transisi ke kapasitas tinggi jaringan disertai dengan pergeseran ke jaringan berbasis IP.

Akibatnya, penggunaan voice overInternet Protocol (VoIP) sedang naik daun (misalnya melalui layanan seperti Skype atau Vonage) tetapi demikian juga kemungkinan menonton gambar bergerak melalui jaringan IP. Teknologi baru seperti penyiaran video digital dan penyiaran multimedia digital akan memungkinkan pemirsa untuk menonton konten yang dialirkan pada layanan seluler kapan saja, di mana saja. Dunia hiburan tampaknya memasuki

seluruh newera. Pada saat yang sama, teknologi digital memiliki dampak signifikan pada sifat interaksi sosial. Telepon seluler telah mengubah cara orang berkomunikasi, mengatur rapat, dan melakukan banyak tugas.

Anak-anak dan remaja, juga orang dewasa, semakin menjalani bagian-bagian penting dari kehidupan mereka dengan bantuan teknologi-teknologi baru ini, dan sebagai akibatnya, mereka mengambil risiko yang mereka miliki karena terjerat dengan berbagai aspek perilaku mereka yang lebih luas. Sekarang tidak lagi memungkinkan untuk menarik garis yang rapi antara masalah "Internet" yang disebut, dan masalah "dunia nyata".

Situs Jejaring Sosial Dimensi yang sangat baru dan sangat kreatif yang menjadi ciri khas situs jejaring sosial adalah cara mereka menyatukan beberapa teknologi Internet yang sudah ada bersama-sama ke satu tempat, menambahkan fitur baru, dan menciptakan antarmuka yang ramah pengguna. Antarmuka baru ini berarti itu telah menjadi sangat mudah untuk menggunakan berbagai fitur. Ini telah memicu pertumbuhan yang cepat dalam popularitas situs jejaring sosial yang telah mengejutkan banyak orang, terutama orangtua.

Di banyak yurisdiksi foto-grafik atau video anak-anak yang dieksploitasi dan dilecehkan secara seksual disebut "pornografi anak" atau "gambar tidak senonoh anak-anak". Hari ini banyak praktisi lebih suka menggunakan istilah "materi pelecehan anak" atau CAM karena dirasakan bahwa ini lebih banyak akurat menyampaikan sifat konten yang sebenarnya.

Ini adalah istilah yang biasanya digunakan dalam dokumen ini. Internet telah sepenuhnya mengubah skala dan sifat produksi dan distribusi CAM. Revolusi seksual pertengahan 1960-an, yang ditandai oleh keterbukaan terhadap ekspresi dan variasi seksual, memunculkan permintaan yang berkembang akan pornografi, dengan toko buku dewasa bermunculan di banyak Eropa dan Amerika. Toko-toko ini dan tentu saja bisnis gaya pesanan lengkap dan menyediakan banyak sekali pornografi dari segala penjuru spektrum keparahan. Permintaan akan pornografi disambut dengan semangat oleh sejumlah pemain kunci di seluruh dunia.

Beberapa pornografi yang dibeli, dijual, dan diperdagangkan termasuk gambar anak-anak yang dilecehkan secara seksual. Undang-undang anti-CAM yang disahkan pada tahun 1977 di Amerika Serikat segera menyebar ke Eropa dan produksi CAM segera berkurang dan didorong ke bawah tanah.

Sementara orang dewasa dan anak-anak sama-sama terpapar pada serangkaian risiko dan bahaya online, anak-anak dan remaja sering kali sangat rentan. Anak-anak masih dalam proses pengembangan dan pembelajaran. Ini memiliki konsekuensi karena kapasitas mereka untuk mengidentifikasi, menilai dan mengelola risiko potensial. Gagasan bahwa anak-anak sangat rentan dan harus dilindungi dari semua bentuk eksploitasi diuraikan dalam Konvensi PBB tentang Hak-Hak Anak.

Ada sejumlah masalah yang berkaitan dengan penggunaan Internet oleh anak-anak dan remaja yang menjadi perhatian utama para pemimpin dan anak-anak, serta pemerintah, politisi dan komunitas pembuat kebijakan. Kekhawatiran ini dapat diringkas sebagai berikut:

a. Konten Internet kemampuan mengekspos anak-anak dan remaja terhadap konten ilegal, misal: CAM.
b. Kemampuan Internet untuk mengekspos anak-anak dan remaja terhadap materi yang legal tetapi usia tidak dimiliki, misal: citra yang sangat keras.
c. Kemampuan Internet untuk mengekspos anak-anak dan remaja ke pemangsa seksual, baik mereka orang dewasa atau orang legal lainnya.
d. Cara di mana Internet dapat mengekspos anak-anak ke komunitas online yang berbahaya seperti situs yang mendorong anoreksia, melukai diri sendiri atau bunuh diri serta sumber pengaruh politik yang mendukung kekerasan, kebencian, dan ekstremisme politik.

Cara Internet telah membuka pembagian digital baru di antara anak-anak dan orang muda, baik dalam hal mereka yang memiliki akses siap dan nyaman untuk itu, sekolah, dan di tempat lain, dan mereka yang tidak; antara mereka yang percaya diri dan mahir

menggunakannya dan mereka yang tidak. Perpecahan ini mengancam untuk memperkuat atau memperluas pola yang ada, baik yang menguntungkan maupun yang tidak menguntungkan, atau mungkin menciptakan perbedaan baru. Potensi Internet untuk menggabungkan dan bahkan memtermagnikasi kerentanan yang ada pada anak-anak dan remaja tertentu dan menambah kesulitan yang mungkin mereka hadapi di dunia offline.

Pada umumnya akan diperlukan untuk berada di tempat badan hukum yang menjelaskan bahwa setiap dan setiap kejahatan yang dapat dilakukan terhadap anak di dunia nyata dapat, secara mutatis mutandis, juga dilakukan di Internet atau di jaringan elektronik lainnya. Mungkin juga perlu untuk mengembangkan undang-undang baru atau menyesuaikan yang sudah ada untuk melarang jenis perilaku tertentu yang hanya dapat terjadi di Internet, misalnya godaan jarak jauh anak-anak untuk melakukan atau menonton tindakan seksual, atau "merawat" anak-anak untuk bertemu di dunia nyata. dunia untuk tujuan seksual.

Tambahan untuk tujuan ini pada umumnya akan diperlukan untuk berada di tempat kerangka hukum yang melarang penyalahgunaan komputer untuk penjahat, peretasan penjahat atau penggunaan kode komputer lain yang berbahaya atau tidak berdasarkan kesepakatan dan menetapkan bahwa Internet adalah tempat di mana kejahatan dapat terjadi.

Beberapa pemerintah nasional merasa bermanfaat untuk menyatukan semua pemangku kepentingan dan pemain utama untuk fokus pada pengembangan dan penerapan inisiatif nasional untuk menjadikan Internet tempat yang lebih aman bagi anak-anak dan orang muda, dan meningkatkan kesadaran akan masalah dan cara menangani mereka dengan sangat baik. cara praktis. Ini akan menjadi penting dalam strategi ini untuk menyadari bahwa Internet sekarang dapat diakses melalui beberapa jenis perangkat yang berbeda. Komputer hanyalah salah satu dari banyak cara untuk online. Ponsel, konsol game, dan PDA juga semakin penting. Penyedia akses nirkabel dan telepon tetap harus dilibatkan. Selain itu di banyak negara jaringan perpustakaan umum, Telecenter dan

kafe internet dapat menjadi sumber penting dari akses Internet terutama untuk anak-anak dan remaja.

Beberapa negara merasa menguntungkan untuk membangun model pengaturan sendiri atau bersama dalam kaitannya dengan pengembangan kebijakan dalam hal ini. daerah dan melalui model seperti itu mereka memiliki, misalnya, menerbitkan kode praktik yang baik untuk membimbing industri Internet dalam hal langkah-langkah yang dapat bekerja paling baik ketika menghasilkan anak-anak dan remaja agar lebih aman secara online. Ini juga berhasil di tingkat regional, misalnya di Uni Eropa di mana kode-Uni Eropa telah dipublikasikan, baik untuk situs jejaring sosial dan jaringan telepon seluler sehubungan dengan penyediaan konten dan layanan untuk anak-anak dan remaja melalui jaringan mereka.

Self dan co-regulation dapat menjadi cara yang sangat efektif untuk membantu melibatkan dan mempertahankan keterlibatan semua pemangku kepentingan yang relevan dan juga dapat sangat efektif dalam hal meningkatkan kecepatan dengan mana tanggapan yang tepat terhadap perubahan teknologi dapat dirumuskan dan diterapkan. Sekolah dan pendidikan sistem umumnya akan memainkan bagian yang sangat penting dalam mengusir strategi nasional seperti itu, tetapi strategi tersebut juga perlu melangkah lebih luas dari itu.

Pertimbangan juga harus diberikan untuk meminta bantuan media massa dalam mempromosikan pesan dan kampanye penyadaran. Perlu Mengembangkan Sumber Daya Lokal yang Merefleksikan Hukum Nasional dan Norma Budaya Lokal. Banyak perusahaan Internet besar menghasilkan situs web yang berisi banyak sekali informasi tentang masalah online untuk anak-anak dan remaja.

Namun, sangat sering materi ini hanya akan tersedia dalam bahasa Inggris atau dalam kelompok bahasa yang sangat sempit. Oleh karena itu, sangat penting bahwa bahan diproduksi secara lokal yang mencerminkan undang-undang setempat dan norma budaya setempat. Ini akan sangat penting untuk kampanye keamanan Internet atau materi pelatihan apa pun yang dikembangkan. Kebutuhan akan Pendidikan Publik dan Aktivitas.

Orangtua,wali dan profesional, seperti guru, memiliki peran penting untuk dimainkan dalam membantu menjaga anak-anak dan remaja agar lebih aman secara online. Program pendidikan dan penjangkauan harus dikembangkan yang membantu membangun kesadaran akan masalah tersebut dan juga menyediakan strategi untuk menghadapinya.

Ketika memproduksi materi pendidikan, penting untuk diingat bahwa banyak orang yang baru mengenal teknologi tidak akan merasa nyaman menggunakannya. Oleh karena itu, penting untuk memastikan bahwa bahan-bahan keselamatan tersedia baik dalam bentuk tertulis atau diproduksi menggunakan media lain yang membuat pendatang baru akan merasa lebih akrab, misalnya dengan video.

Dalam setiap kampanye pendidikan dan kesadaran, penting untuk menentukan nada yang tepat. Olahpesan berbasis rasa takut harus dihindari dan karena keunggulan harus diberikan kepada banyak fitur positif dan menyenangkan teknologi baru. Internet memiliki potensi besar sebagai sarana untuk memberdayakan anak-anak dan orang muda menemukan dunia baru. Mengajar bentuk perilaku online yang bertanggung jawab adalah tujuan utama dari program pendidikan dan kesadaran.

BAB IV
KERANGKA HUKUM NASIONAL TERHADAP DATA ONLINE DAN PENGGUNA

Dunia maya adalah suatu tempat bagi masyarakat dunia untuk melakukan segala interaksi dan transaksi yang berhubungan dengan internet. Baik kegiatan jual-beli, salam-sapa dan memperolah segala informasi dan berita dari seluruh pelosok dunia. Dunia maya kini sangat mempermudah setiap kegiatan di kehidupan bermasyarakat, kita dapat membeli barang yang tidak dijual dilokasi kita, kita dapat memperoleh informasi yang bukan di negara kita dan kita dapat mendengar kabar dari keluarga maupun teman yang tidak tinggal didekat kita. Semua kegiatan yang kita lakukan di dunia maya melewati jaringan internet yang luas hingga pelosok dunia. Kita memerlukan akun yang akan membawa kita kepada tempat kegiatan yang akan kita lakukan, seperti kita harus mengisi data untuk membuat email agar dapat melakukan kegiatan bersurat kabar digital atau kita harus membuat sebuah akun untuk melakukan transaksi perbankan maupun jual-beli.

Semua kegiatan kita di dunia internet memiliki kekuatan hokum sendiri, seperti semua peraturan yang telah diatur dalam Undang-undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik . Secara garis besar, kegiatan yang kita lakukan di dunia maya terdiri dari, transaksi perbankan, *social media*, *e-commerce*, *government*, *technology transfer* dan sebagainya. Semua kegiatan tersebut memiliki aspek HAKI, merk, perlindungan data dan sebagainya. Pada umumnya, setiap kegiatan perjanjian yang kita

lakukan bersumber pada satu peraturan, yaitu Pasal 1313 KUHPerdata yang mengatur bahwa : "suatu persetujuan adalah suatu perbuatan dengan mana 1 (satu) orang atau lebih mengikatkan dirinya terhadap 1 (satu) orang lain atau lebih".

Selain itu, Undang-undang Nomor 19 tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Adapun dalam pasal 1 ayat (2) menyatakan transaksi elektronik adalah "perbuatan hukum yang dilakukan dengan menggunakan jaringan komputer dan atau media elektronik lainnya". Selanjutnya mengenai perlindungan hukum dari transaksi elektronik diatur dalam pasal 26 Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yang berbunyi:

a. "kecuali ditentukan lain oleh peraturan perundang-undangan penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan"
b. "setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat 1, dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini"

Ketika kegiatan di dunia nyata saja banyak penjahat yang memiliki peluang untuk melakukan tindakan kejahatan padahal peraturan dan hukuman sudah diatur jelas dalam peraturan nasional, lantas, bagaimana pelindungan nasional terhadap pengguna internet yang memiliki jaringan hingga ke pelosok dunia?

4.1 Perbankan

Perkembangan teknologi informasi sangatlah pesat, termasuk pada bidang perbankan. Kegiatan perbankan kini dapat dilakukan melalui media elektronik, atau melalui internet, yang biasa kita sebut dengan *internet banking*, dimana saluran jaringannya digunakan untuk memberikan layanan perbankan seperti membuka rekening, transfer dan segala pembayaran yang bersifat online yang dalam pelaksanaannya wajib menerapkan manajemen risiko pada tiap aktifitas layanannya secara efektif, yang meliputi pengawasan aktif

Dewan Komisaris dan Direksi, sistem pengamanan, dan manajemen risiko.[98] Perlindungan hokum terhadap masyarakat pengguna layanan *internet banking* diberikan langsung oleh pihak bank dari segi keamanan teknologi yang sudah maksimal dan memenuhi aspek-aspek *confidentially, integrity, authentication, availability, access control* dan *non-repudiation.*[99]

Pada akhir tahun 1988, telah dibuat Undang-undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-undang Nomor 7 Tahun 1992 tentang Perbankan. Undang-undang Nomor 10 Tahun 1998 mengubah/menggantikan/menambah beberapa pasal dari Undang-undang Nomor 7 Tahun 1992. Salah satu pelaksanaan kegiatan perbankan dalam memberikan pelayanan kepada nasabah, baik secara konvensional maupun melalui media alternatif lainnya seperti *internet banking. Internet Banking* merupakan suatu bentuk pemanfaatan media internet oleh bank dalam mempromosikan dan melakukan transaksi perbankan secara online, baik dari produk yang bersifat konvensional maupun baru. Terdapat beberapa hal yang harus kita cermati berkaitan dengan konsep internet banking, yaitu mengenai privasi atau keamaan data nasabah bank, karena karakteristik layanan internet banking sangat rawan akan aspek perlindungan data pribadi nasabah bank tersebut.[100]

Terdapat beberapa ketentuan yang dapat digunakan sebagai dasar hokum dalam memberikan perlindungan hokum atas data pribadi nasabah dalam penyelenggaraan layanan *internet banking*, seperti Pasal 29 Ayat (4) Undang-undang Nomor 10 Tahun 1998 tentang Perbankan yang mengatur bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan

---

[98] Bank Indonesia. 2004. *Surat Edaran No.6/18/DPNP: Penerapan Manajemen resiko pada aktivitas pelayanan jasa bank melalui Internet (Internet Banking).* Dikutip dari http://www.bi.go.id/id/peraturan/arsip-peraturan/ Perbankan2004/se-6-18-04-dpnp.pdf. Diakses pada 20 Agustus 2019, 14.54 WIB.

[99] Eko Aribowo. (n.d). *Aspek Keamanan Komputer.* https://www.academia.edu/8236936/Aspek_Keamanan_Komputer_eko_aribowo_S.T._M.Kom. (n.d): UAD. Diakses pada 20 Agustus 2019, 14.57 WIB.

[100] Dwi Ayu Astrini. (2015). *Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking dari Ancaman Cybercrime Lex Privatum*, Vol.III/No. 1/Jan-Mar/2015. (n.d): (n.d). hlm 150-151.

timbul resiko kerugian sehubungan dengan transaksi nasabah yang dilakukan oleh bank. Hal itu diatur dengan mengingat bahwa bank berdiri berdasarkan dana dari masyarakat yang disimpan pada bank atas dasar kepercayaan.[101]

Selanjutnya, terdapat ketentuan dalam Undang-undang Perbankan yaitu Pasal 40 Ayat (1) dan (2) yang mengatur bahwa bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal sebagai mana diatur dalam Pasal 41, Pasal 41A, Pasal 43, Pasal 44 dan Pasal 44A. Nasabah pengguna layanan *internet banking* disebut juga sebagai konsumen, sehingga nasabah pengguna *internet banking* juga mendapat perlindungan dari Pasal 2 Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang mengatur bahwa, perlindungan konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan dan keselamatan serta kepastian hokum. Dengan berlakunya undang-undang tentang perlindungan konsumen, memberikan konsekuensi logis terhadap pelayanan jasa perbankan, baik itu kegiatan bank yang memanfaatkan internet maupun tidak.

Pasal 26 UU ITE juga mengatur bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan, maka dengan adanya peraturan ini, ketika terdapat penggunaan informasi melalui media elektronik yang dilakukan tanpa persetujuan orang yang bersangkutan adalah termasuk kedalam pelanggaran. Pasal 22 Undang-undang Nomor. 36 Tahun 1999 tentang Telekomunikasi mengatur bahwa, setiap orang dilarang melakukan perbuatan tanpa hak dan tidak sah, atau memanipulasi. Ketentuan ini dapat kita analogikan dalam perlindungan data pribadi nasabah dalam penyelenggaraan layanan *internet banking*, namun terdapat sedikit perbedaan dari objek data atau informasi yang dilindungi, dimana ketentuan Pasal 22 UU Telekomunikasi menitikberatkan pada data yang ada dalam jaringan dan data yang sedang di transfer.

---

[101] Pasal 29 Ayat (3) Undang-undang Nomor 10 Tahun 1998 tentang Perbankan.

Beberapa ketentuan perundang-undangan diatas dapat diberlakukan pada berbagai macam kasus mengenai data pribadi nasabah dan hak nasabah apabila mengalami kerugian dalam layanan *Internet Banking* namun hal tersebut tergantung kepada jenis kasusnya. Ketentuan perundang-undangan perbankan tidak dapat diberlakukan pada kasus (*Typosquatting*) yang merugikan nasabah, karena dalam hal ini keterangan atau data nasabah yang bocor tidak melibatkan pihak-pihak yang terkait dalam lembaga perbankan tersebut. Data nasabah yang sampai kepada pihak lain tersebut disebabkan kekurang hati-hatian nasabah yang dimanfaatkan si pelaku tindak kejahatan dengan membuat situs plesetan yang hampir sama. Berdasarkan uraian keseluruhan perlindungan hukum atas data pribadi nasabah dalam penyelenggara *Internet Banking* tersebut diatas yang dilakukan melalui cara *self regulation* dan *government regulation*[102], maka dapat ditarik kesimpulan bahwa upaya perlindungan hukum telah dilakukan namun belum mencerminkan asas keseimbangan. Sampai saat ini belum ada ketentuan khusus atau aturan yang mencerminkan suatu hak dan kewajiban yang seimbang antara penyelenggara *Internet Banking* dan nasabah sendiri.

4.2 Sosial Media, dan Perlindungan Data Pribadi

Dalam merespon perkembangan teknologi dibidang komunikasi, pertukaran data dan perdagangan, Pemerintah telah mengesahkan Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Berdasarkan Pasal 1 ayat (2) menyatakan transaksi elektronik adalah "perbuatan hukum yang dilakukan dengan menggunakan jaringan computer dan atau media elektronik lainnya".

Banyak hal yang bisa dilakukan di dunia virtual seperti halnya dalam media sosial seperti *Facebook*, *twitter*, *Instragram*, dan lainnya sehingga terjadinya kejahatan di dunia digital. Larangan terhadap

[102] Budi Agus Riswandi. (2005). *Aspek Hukum Internet Banking*. Jakarta: Rajagrafindo Persada. hlm. 200.

segala kejahatan yang menyangkut data pribadi seseorang sebenarnya sudah diatur dalam Pasal 26 yang menyatakan bahwa setiap orang yang hendak menggunakan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan pemilik. Apabila terjadinya pelanggaran atau pemilik merasa dirugikan oleh pihak penyelenggara sistem elektronik, pemilik data dapat mengajukan gugatan kepada pihak penyelenggara sesuai dengan peraturan yang berlaku.

Pengguna sosial media harus berhati-hati dalam menyimpan atau mengambil foto milik pengguna lain, karena apabila seorang pengguna melakukan hal tersebut tanpa izin pemilik konten, maka pengguna tersebut dapat dijerat dengan Pasal 26 undang-undang *a quo*. Selanjutnya, setiap orang berhak untuk dilindungi data pribadinya dari intersepsi atau penyadapan[103] atas informasi yang bersifat privat seperti catatan hutang, riwayat sakit dan data pribadi lainnya baik yang tidak menyebabkan perubahan maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau pengehentian proses transmisi atau pertukaran data tersebut kecuali yang dilakukan oleh aparat penegak hukum dalam rangka penegakan hukum berdasarkan undang-undang yang telah ditegaskan dalam Pasal 31 undang-undang *a quo*.

Lebih lanjut, dalam Pasal 32 disebutkan bahwa setiap pengguna dilarang secara melawan hukum mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan serta mengakibatkan dapat diaksesnya suatu dokumen atau informasi elektronik milik pengguna lain tanpa izin pemilik data ke publik. Konsekuensi bagi pengguna yang melanggar ketentuan dalam Pasal 31 *jo* Pasal 32 dapat dikenakan sanksi berdasarkan Pasal 47 yaitu pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah). *jo* Pasal 48 ayat 1,

[103]Yang dimaksud sebagai intersepsi atau penyadapan dalam UU ITE adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

seseorang yang melanggar ketentuan Pasal 32 ayat (1) akan dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah), dilanjutkan dengan ayat 2 yang menyebutkan akan dipidana seseorang yang melanggar ketentuan Pasal 32 ayat (2) dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp.3000.000.000,00 (tiga miliar rupiah) dan ayat 3 dengan ancaman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.5000.000.000,00 (lima miliar rupiah) bagi setiap orang yang melangar ketentuan Pasal 32 ayat (3).

Kejahatan data pribadi tidak hanya selesai sampai pada penyadapan atau intervensi terhadap foto, video, music atau dokumen elektronik lain. Banyak ditemukannya pencurian identitas akibat diketahuinya data pribadi seseorang yang berujung pada banyak kejahatan. Apabila seorang pengguna menyalahgunakan data pribadi milik pengguna lain dengan memanipulasi, menciptakan, merubah, menghilangkan, merusak dokumen elektronik dengan tujuan agar dianggap sebagai data otentik, dapat dipidana berdasarkan Pasal 51 dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah). Akan tetapi kerangka hukum yang ada saat ini masih belum mendefinisikan atau mengklasifikasikan data yang boleh atau tidak boleh dikumpulkan oleh para pengguna. Oleh karena itu para pengguna sosial media harus berhati-hati dalam menyimpan atau mengambil dokumen elektronik milik orang lain atau mengupload dokumen milik mereka sendiri.

4.3 E-Commerce

Banyaknya kemudahan dalam mengakses internet membuat konsumen *e-commerce* meningkat, beberapa alasannya antara lain, adalah praktis, kemudahan sistem pembayaran, efisiensi waktu dan banyaknya harga promo yang menarik dari pelaku usaha online.[104]

---

[104] Deky Pariadi. (2018). *Pengawasan E-commerce Dalam Undang-undang Perdagangan dan Undang-undang Perlindungan Konsumen*. Jurnal Hukum & Pembangunan 48 Nomor 3 tahun 2018. hlm. 652.

Demi menjaga keamanan dan kenyamanan bertansaksi para pengguna *e-commerce*, Pemerintah telah mengesahkan Undang-Undang No 7 Tahun 2014 Tentang Perdagangan (UU Perdagangan) dan Undang- undang No 8 tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen) dan Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Mengingat bahwa produsen berada dalam kedudukannya yang lebih kuat, baik secara ekonomis maupun dari segi kekuasaan (*bargaining power, bargaining pasition*) dibanding dengan konsumen, maka konsumen perlu mendapat advokasi, perlindungan, serta upaya penyelesaian sengketa secara patut atas hak haknya.[105] Perlindungan itu dibuat dalam suatu peraturan perundang undangan serta dilaksanakan dengan baik. Berdasarkan Pasal 4 UU Perlindungan Konsumen, hak konsumen meliputi:

a. Hak Atas Kenyamanan, Keamanan, Dan Keselamatan Dalam Mengkonsumsi Barang Dan/Atau Jasa;
b. Hak Untuk Memilih Barang Dan/Atau Jasa Serta Mendapatkan Barang Dan/Atau Jasa Tersebut Sesuai Dengan Nilai Tukar Dan Kondisi Serta Jaminan Yang Dijanjikan;
c. Hak Atas Informasi Yang Benar, Jelas, Dan Jujur Mengenai Kondisi Dan Jaminan Barang Dan/Atau Jasa;
d. Hak Untuk Didengan Pendapat Dan Keluhannya Atas Barang Dan/Atau Jasa Yang Digunakan;
e. Hak Untuk Mendapatkan Advokasi, Perlindungan, Dan Upaya Penyelesaian Sengketa Perlindungan Konsumen Secara Patut;
f. Hak Untuk Mendapat Pembinaan Dan Pendidikan Konsumen;
g. Hak Untuk Diperlakukan Atau Dilayani Secara Benar Dan Jujur Serta Tidak Diskriminatif;
h. Hak Untuk Mendapatkan Kompensasi, Ganti Rugi Dan/Atau Penggantian, Apabila Barang Dan/Atau Jasa Yang Diterima Tidak Sesuai Dengan Perjanjian Atau Tidak Sebagaimana Mestinya;

[105] *Ibid.*

i. Hak-Hak Yang Diatur Dalam Ketentuan Peraturan Perundang-Undangan Lainnya.

Konsumen juga berhak mendapatkan pembinaan dan pendidikan mengenai bagaimana berkonsumsi yang baik. Produsen pelaku usaha wajib memberi informasi yang benar dan mendidik sehingga konsumen makin dewasa bertindak dalam kebutuhannya, bukan sebaliknya mengekspolitasi kelemahan konsumen terutama wanita dan anak anak.[106] Selanjutnya, dalam UU Perdagangan juga telah mengatur mengenai perdagangan melalui sistem elektronik atau *e-commerce*, yang diatur dalam Pasal 65 UU Perdagangan yang mewajibkan pelaku usaha *e- commerce* untuk menyediakan data dan /atau informasi secara lengkap dan benar sehingga akan memudahkan untuk menelusuri legalitasnya. Hal ini sangat baik dalam segi perlindungan konsumen namun, implementasi dari ketentuan ini akan sulit terwujud jika aturan pelaksananya tidak segera diterbitkan oleh pemerintah, karena *e-commerce* itu sendiri sangat kompleks dan terjadi di lintas negara.[107]

Berdasarkan Pasal 9 UU ITE, jual beli secara elektronik penjual maupun pembeli memiliki hak dan kewajiban, oleh karena itu penjual bertanggung jawab memberikan informasi secara benar dan jujur atas produk yang ditawarkan kepada pembeli atau konsumen. Apabila seorang konsumen mengalami kerugian akibat penipuan atau barang yang dikirimkan tidak sesuai dengan deskripsi barang di situs penjualan, maka konsumen dapat melaporkan hal tersebut ke aparat penegak hukum dalam hal ini Polisi atau meminta ganti kerugian kepada penjual. Akan tetapi, keterbatasan sumber daya yang dimiliki aparat penegak hukum selama ini menjadi kendala dalam penegakan hukum dibidang *e-commerce* apabila sang pembeli dan penjual berada di wilayah hukum yang berbeda. Oleh karena itu perlu adanya suatu prosedur hukum yang dapat mengakomodir para konsumen dalam membela haknya. Pemerintah juga dapat meminta

---

[106] Asep Rohandi. (2015). *Perlindungan Konsumen Dalam Transaksi E-Commerce Perspektif Hukum Nasional dan Internasional.* Ecodemica Vol III. No 2 Tahun 2015. hlm 476.

[107] *Ibid.* hlm. 656.

kepada para penyedia layanan *e-commerce* untuk mensosialisasikan prosedur ganti rugi dan juga meningkatkan pengawasan terhadap penjual yang menggunakan lapak digital miliknya

4.4 Hak Kekayaan Intelektual

Secara umum pengertian Hak Kekayaan Intelektual (HKI) adalah hak-hak yang secara hukum diberikan untuk melindungi nilai ekonomi bagi usaha-usaha kreatif. Jenis-jenis perlindungan terhadap HKI meliputi:

a. Merek (Trademarks),
b. Hak Cipta (Copy Rights),
c. Patent (Patents),
d. Disain Industri (Industrial Designs),
e. Rahasia Dagang (Trade Secrets),
f. Indikasi Geografis (Geographical Indications),
g. Disain Tataletak Sirkuit Terpadu (Layout Design of Integrated Circuits) dan
h. Perlindungan Varietas Tanaman (Plant Variety Protection).

4.5 Merek Dagang dan Jasa

Pengaturan tentang Merek memiliki sejarah yang Panjang dalam system hukum di Indonesia. Pada awalnya pengaturan tentang merek diatur dalam Undang-undang Nomor 21 Tahun 1961 tentang Merek Perusahaan dan Perniagaan. ABerdasarkan pertimbangan tersebut, pada tanggal 1 April 1992 telah diundangkannya Undang-undang Nomor 19 Tahun 1992 tentang Merek.[108] Akan tetapi dalam perjalannya, Undang-undang Undang-undang Nomor 19 Tahun 1992 tentang Merek tidak dapat mengikuti perkembangan yang terjadi sehingga diubah dengan Undang-undang nomor 14 tahun 1997 tentang Merek dan Undang-undang *a quo* kembali diubah dengan Undang-undang Nomor 15 tahun 2001 tentang Merek. Akan tetapi, pada tahun 2016 Pemerintah kembali

[108] Abdulkadir Muhammad. (2010). *Hukum Perusahaan Indonesia* cetakan Keempat. Bandung: PT Citra Aditya Bakti. hlm. 399.

mengesahkan pengaturan terkait merek melalui Undang-undang Nomor 20 Tahun 2016 tentang Merek dan Indeks Geografi.

Dalam Undang-undang Merek tahun 2016, merek yang dilindungi meliputi merek dagang dan jasa. Berdasarkan pasal 2 ayat (3) UU Merek tahun 2016, merek yang dilindungi terdiri atas tanda berupa gambar, logo, nama, kata, huruf, angka, susunan warna, dalam bentuk 2 (dua) dimensi dan/atau 3 (tiga) dimensi, suara, hologram, atau kombinasi dari 2 (dua) atau lebih unsur tersebut untuk membedakan barang dan/atau jasa yang diproduksi oleh orang atau badan hukum dalam kegiatan perdagangan barang dan/atau jasa. Setiap orang yang hendak memiliki hak atas sebuah merek diwajibkan untuk mendaftarkan mereknya terlebih dahulu ke http://www.dgip.go.id/#. Setelah disetujui maka hak atas merek yang didaftrakan sebelumnya sudah melekat pada diri sang pendaftar. Selanjutnya, dalam hal jangka waktu perlindungan terhadap merek tersebut dijelaskan dalam Pasal 35 Undang-undang *a quo*, yang menentukan:

a. Merek terdaftar mendapat pelindungan hukum untuk jangka waktu 10 (sepuluh) tahun sejak Tanggal Penerimaan.
b. Jangka waktu pelindungan sebagaimana dimaksud pada ayat (1) dapat diperpanjang untuk jangka waktu yang sama.
c. Permohonan perpanjangan sebagaimana dimaksud pada ayat (2) diajukan secara elektronik atau non- elektronik dalam bahasa Indonesia oleh pemilik Merek atau Kuasanya dalam jangka waktu 6 (enam) bulan sebelum berakhirnya jangka waktu pelindungan bagi Merek terdaftar tersebut dengan dikenai biaya.
d. Permohonan perpanjangan sebagaimana dimaksud pada ayat (2) masih dapat diajukan dalam jangka waktu paling lama 6 (enam) bulan setelah berakhirnya jangka waktu pelindungan Merek terdaftar tersebut dengan dikenai biaya dan denda sebesar biaya perpanjangan.

Selanjutnya, hak atas merek juga dapat dialihkan karena:[109]

a. Pewarisan;
b. Wasiat;
c. Wakaf;
d. Hibah;
e. Perjanjian; atau
f. Sebab lain yang dibenarkan oleh peraturan perundang-undangan.

Apabila sang pemilik hak atas merek menemukan ada pihak yang menggunakan atau menyalahgunakan merek dagang atau jasa miliknya, maka pemilik hak dapat melakukan gugatan yang ditujukkan ke Pengadilan Niaga. Gugatan dapat diajukan ke Pengadilan Niaga.[110] Adapun sanksi pidana bagi para pelaku penyalahgunaan atau penggunaan merek tanpa izin diatur dalam Pasal 101 dan 102 yaitu:

Pasal 101 menentukan:

Setiap Orang yang dengan tanpa hak menggunakan tanda yang mempunyai persamaan pada keseluruhan dengan Indikasi Geografis milik pihak lain untuk barang dan/atau produk yang sama atau sejenis dengan barang dan/atau produk yang terdaftar, dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Setiap Orang yang dengan tanpa hak menggunakan tanda yang mempunyai persamaan pada pokoknya dengan Indikasi Geografis milik pihak lain untuk barang dan/atau produk yang sama atau sejenis dengan barang dan/atau produk yang terdaftar, dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

---

[109] Pasal 41 Undang-undang Nomor 20 Tahun 2016 tentang Merek dan Indeks Geografis.
[110] *Ibid.* Pasal 83.

Pasal 102 menentukan:

Setiap Orang yang memperdagangkan barang dan/atau jasa dan/atau produk yang diketahui atau patut diduga mengetahui bahwa barang dan/atau jasa dan/atau produk tersebut merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 100 dan Pasal 101 dipidana dengan pidana kurungan paling lama 1 (satu) tahun atau denda paling banyak Rp200.000.000,00 (dua ratus juta rupiah). Selanjutnya berdasarkan Pasal 103 Undang-undang Merek menentukan bahwa penyalahgunaan atau penggunaan merek tanpa izin termasuk kedalam delik aduan.

4.6 Hak Cipta

Pengaturan hak cipta diatur dalam Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta yang sebelumnya diatur dalam Undang-undang Nomor 19 tahun 2002 tentang hak cipta yang sudah tidak sesuai dengan perkembangan hukum dan kebutuhan masyarakat sehingga perlu diganti dengan Undang-Undang yang baru. Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan.[111] Undang-Undang ini berlaku terhadap:

a. Semua ciptaan dan produk hak terkait warga negara, penduduk, dan badan hukum Indonesia;
b. Semua ciptaan dan produk hak terkait bukan warga negara indonesia, bukan penduduk indonesia, dan bukan badan hukum indonesia yang untuk pertama kali dilakukan pengumuman di indonesia;
c. Semua ciptaan dan/atau produk hak terkait dan pengguna ciptaan dan/atau produk hak terkait bukan warga negara indonesia, bukan penduduk indonesia, dan bukan badan hukum indonesia dengan ketentuan:

[111] Pasal 1 Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta

d. Negaranya mempunyai perjanjian bilateral dengan negara republik indonesia mengenai pelindungan hak cipta dan hak terkait; atau
e. Negaranya dan negara republik indonesia merupakan pihak atau peserta dalam perjanjian multilateral yang sama mengenai pelindungan hak cipta dan hak terkait.[112]

Pencipta atau pemegang Hak cipta memiliki hak ekonomi sebagaimana yang diatur dalam Pasal 9 yaitu berupa:

a. Penerbitan ciptaan;
b. Penggandaan ciptaan dalam segala bentuknya;
c. Penerjemahan ciptaan;
d. Pengadaptasian, pengaransemenan, atau pentransformasian ciptaan;
e. Pendistribusian ciptaan atau salinannya;
f. Pertunjukan ciptaan;
g. Pengumuman ciptaan;
h. Komunikasi ciptaan; dan
i. Penyewaan ciptaan.

Berdasarkan Undang-undang ini Hak Cipta, hak cipta merupakan benda bergerak yang tidak berwujud yang bisa dialihkan. Berdasarkan pasal 16, hak cipta dapat beralih dan dialihkan dengan cara:

a. Pewarisan;
b. Hibah;
c. Wakaf;
d. Wasiat;
e. Perjanjian tertulis; atau
f. Sebab lain yang dibenarkan sesuai dengan ketentuan peraturan perundang-undangan.

Sering kali orang terpeleset kedalam kasus pelanggaran hak cipta dikarenakan kurang memahami tentang hal apa saja yang

[112] *Ibid.* Pasal 2.

merupakan pelanggaran hak cipta atau bukan. Berdasarkan pasal 44 UU Hak Cipta, Penggunaan, pengambilan, Penggandaan, dan/atau pengubahan suatu Ciptaan dan/atau produk Hak Terkait secara seluruh atau sebagian yang substansial tidak dianggap sebagai pelanggaran Hak Cipta jika sumbernya disebutkan atau dicantumkan secara lengkap untuk keperluan:

a. Pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah dengan tidak merugikan kepentingan yang wajar dari Pencipta atau Pemegang Hak Cipta;
b. Keamanan serta penyelenggaraan pemerintahan, legislatif, dan peradilan;
c. Ceramah yang hanya untuk tujuan pendidikan dan ilmu pengetahuan; atau
d. Pertunjukan atau pementasan yang tidak dipungut bayaran dengan ketentuan tidak merugikan kepentingan yang wajar dari Pencipta.

Hak cipta memiliki masa berlaku yang beragam, dalam Pasal 58 UU Hak Cipta disebutkan bahwa masa berlaku ciptaan berupa:

a. Buku, pamflet, dan semua hasil karya tulis lainnya;
b. Ceramah, kuliah, pidato, dan Ciptaan sejenis lainnya;
c. Alat peraga yang dibuat untuk kepentingan pendidikan dan ilmu pengetahuan;
d. Lagu atau musik dengan atau tanpa teks;
e. Drama, drama musikal, tari, koreografi, pewayangan, dan pantomim;
f. Karya seni rupa dalam segala bentuk seperti lukisan, gambar, ukiran, kaligrafi, seni pahat, patung, atau kolase;
g. Karya arsitektur;
h. Peta; dan
i. Karya seni batik atau seni motif lain,

Akan berlaku selama hidup Pencipta dan terus berlangsung selama 70 (tujuh puluh) tahun setelah Pencipta meninggal dunia, terhitung mulai tanggal 1 Januari tahun berikutnya. Apabila hak cipta

tersebut dimiliki oleh badan hukum, maka maka akan berlaku selama 50 tahun sejak pertama kali dilakukan pengumuman. Selanjutnya, bagi ciptaan berupa:

a. Karya fotografi;
b. Potret;
c. Karya sinematografi;
d. Permainan video;
e. Program komputer;
f. Perwajahan karya tulis;
g. Terjemahan, tafsir, saduran, bunga rampai, basis data, adaptasi, aransemen, modifikasi dan karya lain dari hasil transformasi;
h. Terjemahan, adaptasi, aransemen, transformasi atau modifikasi ekspresi budaya tradisional;
i. Kompilasi ciptaan atau data, baik dalam format yang dapat dibaca dengan program komputer atau media lainnya; dan
j. Kompilasi ekspresi budaya tradisional selama kompilasi tersebut merupakan karya yang asli,
k. Berlaku selama 50 (lima puluh) tahun sejak pertama kali dilakukannya pengumuman.[113]

Penyelesaian sengketa Hak Cipta dapat dilakukan melalui alternatif penyelesaian sengketa, arbitrase, atau pengadilan. Pengadilan yang berwenang adalah Pengadilan Niaga.[114] Apabila di kemudian hari si pemilik hak cipta mengalami kerugian akibat perbuatan pihak lain yang menyalahgunakan ciptaannya, maka pemilik hak cipta dapat melakukan gugatan berupa ganti kerugian.[115] Seseorang yang melakukan penyalahgunaan hak cipta juga tidak dapat terlepas dari sanksi pidana berupa penjara dan/atau denda sebagaimana yang diatur dalam Pasal 112-119. Akan tetapi perlu diingat kembali bahwa aturan ini merupakan delik aduan.

---

[113] *Ibid.* Pasal 59.
[114] *Ibid.* Pasal 95.
[115] *Ibid.* Pasal 96.

4.7 Paten

Pengaturan tentang paten yang terbaru diatur dalam Undang-undang Nomor 13 Tahun 2016 tentang Paten. Paten adalah hak eksklusif yang diberikan oleh negara kepada inventor atas hasil invensinya di bidang teknologi untuk jangka waktu tertentu melaksanakan sendiri invensi tersebut atau memberikan persetujuan kepada pihak lain untuk melaksanakannya.[116] Invensi dianggap baru apabila tanggal penerimaan invensi tersebut tidak sama dengan teknologi yang sudah diumumkan atau sudah ada sebelumnya. [117]

Inventor berhak mendapatkan imbalan berdasarkan perjanjian yang dibuat oleh pihak pemberi kerja dan Inventor, dengan memperhatikan manfaat ekonomi yang diperoleh dari invensi dimaksud. Adapun imbalan yang dimaksud dapat dibayarkan berdasarkan:

a. Jumlah tertentu dan sekaligus;
b. Persentase;
c. Gabungan antara jumlah tertentu dan sekaligus dengan hadiah atau bonus; atau
d. Bentuk lain yang disepakati para pihak.
e. Hak atas Paten dapat beralih atau dialihkan baik seluruhnya maupun sebagian karena:
f. Pewarisan;
g. Hibah;
h. Wasiat;
i. Wakaf;
j. Perjanjian tertulis; atau
k. Sebab lain yang dibenarkan berdasarkan ketentuan peraturan perundang-undangan[118]

---

[116] Pasal 1 ayat (1) Undang-undang Nomor 13 Tahun 2016 tentang Paten.
[117] *Ibid.* Pasal 5.
[118] *Ibid.* Pasal 74.

Dalam hal tidak terdapat kesesuaian mengenai cara perhitungan dan penetapan besarnya Imbalan, para pihak dapat mengajukan gugatan ke Pengadilan Niaga.[119] Berdasarkan Pasal 19 *UU Paten, pemegang paten memiliki hak eksklusif untuk melaksanakan paten yang dimilikinya dan untuk melarang pihak lain* yang tanpa persetujuannya dalam hal paten-produk:

a. Membuat,
b. Menggunakan,
c. Menjual,
d. Mengimpor,
e. Menyewakan,
f. Menyerahkan, atau
g. Menyediakan untuk dijual atau disewakan atau diserahkan produk yang diberi paten;[120]

Apabila Pemegang Paten atau penerima Lisensi mengalami kerugian akibat ada pihak yang dengan sengaja melakukan perbuatan sebagaimana yang dimaksud dalam Pasal 19 UU Paten, maka pemegang paten dapat mengajukan gugatan ganti rugi kepada Pengadilan Niaga.[121] Pemegang Paten memiliki kewajiban untuk membuat produk atau menggunakan proses di Indonesia[122] dan membayar biaya tahunan.[123] Perlindungan terhadap Paten diberikan untuk jangka waktu 20 (dua puluh) tahun terhitung sejak Tanggal Penerimaan dan tidak dapat diperpanjang. Pemberitahuan terkait tanggal mulai dan berakhirnya jangka waktu Paten dicatat dan diumumkan melalui media elektronik dan/atau media non-elektronik.[124] Sedangkan bagi paten sederhana, diberikan untuk jangka waktu 10 (sepuluh) tahun terhitung sejak Tanggal Penerimaan dan tidak dapat diperpanjang.[125] Pemerintah juga telah menyediakan

[119] *Ibid.* Pasal 12.
[120] *Ibid.* Pasal 19.
[121] *Ibid.* Pasal 143.
[122] *Ibid.* Pasal 20.
[123] *Ibid.* Pasal 21.
[124] *Ibid.* Pasal 22.
[125] *Ibid.* Pasal 23.

sanksi pidana bagi setiap orang yang melanggar ketentuan dalam Pasal 160 UU Paten yang menentukan:
Setiap orang tanpa persetujuan Pemegang Paten dilarang:

a. dalam hal Paten-produk: membuat, menggunakan, menjual, mengimpor, menyewakan, menyerahkan, dan/ atau menyediakan untuk dijual, disewakan, atau diserahkan produk yang diberi Paten; dan/atau
b. dalam hal Paten-proses: menggunakan proses produksi yang diberi Paten untuk membuat barang atau tindakan lainnya sebagaimana dimaksud dalam huruf a.

Adapun Sanksi pidana bagi orang yang melanggar ketentuan dalam Pasal 160 Undang-undang *a quo* adalah:
Pasal 161 menentukan:

Setiap Orang yang dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 160 untuk Paten, dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

Pasal 162 menentukan:

Setiap Orang yang dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 160 untuk Paten sederhana, dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

Pasal 163 menentukan:

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 161 dan/atau Pasal 162, yang mengakibatkan gangguan kesehatan dan/atau lingkungan hidup, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 161 dan/atau Pasal 162, yang mengakibatkan kematian manusia, dipidana dengan pidana penjara paling lama 10

(sepuluh) tahun dan/atau denda paling banyak Rp3.500.000.000,00 (tiga miliar lima ratus juta rupiah).

Selanjutnya, tindak pidana sebagaimana dimaksud dalam Pasal 161, Pasal 162, dan Pasal 164 merupakan delik aduan.[126]

4.8 Desain Tata Letak Sirkuit Terpadu

Berdasarkan Undang-undang Nomor 32 Tahun 2000 tentang Desain Tata Letak Sirkuit Terpadu, yang dimaksud dengan desain tata letak adalah kreasi berupa rancangan peletakan tiga dimensi dari berbagai elemen, sekurang-kurangnya satu dari elemen tersebut adalah elemen aktif, serta sebagian atau semua interkoneksi dalam suatu Sirkuit Terpadu dan peletakan tiga dimensi tersebut dimaksudkan untuk persiapan pembuatan Sirkuit Terpadu. Sedangkan definisi sirkuit terpadu adalah suatu produk dalam bentuk jadi atau setengah jadi, yang di dalamnya terdapat berbagai elemen dan sekurang-kurangnya satu dari elemen tersebut adalah elemen aktif, yang sebagian atau seluruhnya saling berkaitan serta dibentuk secara terpadu di dalam sebuah bahan semikonduktor yang dimaksudkan untuk menghasilkan fungsi elektronik.[127]

Desain tata letak sirkuit terpadu dinyatakan orisinal apabila desain tersebut merupakan hasil karya mandiri pendesain, dan pada saat desain tata letak sirkuit terpadu tersebut dibuat tidak merupakan sesuatu yang umum bagi para pendesain.[128] Perlindungan terhadap Hak Desain Tata Letak Sirkuit Terpadu diberikan kepada Pemegang Hak sejak pertama kali desain tersebut dieksploitasi secara komersial di mana pun, atau sejak Tanggal Penerimaan hingga jangka waktu selama 10 (sepuluh) tahun.[129] Hak Desain Tata Letak Sirkuit Terpadu dapat beralih atau dialihkan dengan:

---

[126] *Ibid.* Pasal 165.
[127] Pasal 1 ayat (1 dan 2) Undang-undang Nomor 32 Tahun 2000 tentang Desain Tata Letak Sirkuit Terpadu.
[128] *Ibid.* Pasal 2.
[129] *Ibid.* Pasal 4.

a. Pewarisan;
b. Hibah;
c. Wasiat;
d. Perjanjian tertulis; atau
e. Sebab-sebab lain yang dibenarkan oleh peraturan perundang-undangan;[130]

Sebagaimana yang dimaksud dalam Pasal 8, pemegang hak memiliki hak eksklusif untuk melaksanakan hak desain tata letak sirkuit terpadu yang dimilikinya dan melarang orang lain yang tanpa persetujuannya:

a. Membuat,
b. Memakai,
c. Menjual,
d. Mengimpor,
e. Mengekspor dan/atau mengedarkan barang yang di dalamnya terdapat seluruh atau sebagian desain yang telah diberi hak desain tata letak sirkuit terpadu.

Akan tetapi apabila digunakan demi kepentingan penelitian dan pendidikan sepanjang tidak merugikan kepentingan yang wajar dari pemegang desain tata letak sirkuit terpadu maka hal ini diperbolehkan oleh Undang-undang *a quo*. Pemegang Hak atau penerima Lisensi Desain Tata Letak Sirkuit Terpadu dapat menggugat siapa pun yang dengan sengaja dan tanpa hak melakukan penggunaan desain tata lekat sirkuit tanpa izin sang pemegang hak.

Apabila pemegang hak menemukan timbulnya kerugian akibat hal tersebut maka dapat mengajukan gugatan ganti kerugian ke pengadilan niaga[131] atau dapat menempuh jalan alternatif berupa arbitrase atau penyelesaian sengketa alternatif lainnya.[132] Undang-undang *a quo* juga menyediakan hukuman pidana kepada setiap orang yang melakuka penyalahgunaan atau penggunaan desain tata letak sirkuit tanpa izin pemegang hak yaitu berupa pidana penjara

[130] *Ibid.* Pasal 23,
[131] *Ibid.* Pasal 38.
[132] *Ibid.* Pasal 39.

paling lama 3 (tiga) tahun dan/atau denda paling banyak Rp 300.000.000,00 (tiga ratus juta rupiah). Namun, perlu diketahui bahwa tindak pidana yang dimaksud ini merupakan delik aduan, artinya pihak yang merasa dirugikan harus melaporkan terlebih dahulu kejahatan ini baru kemudian dapat diproses secara hukum.[133]

4.9 Desain Industri

Pasal 1 ayat (1) Undang-undang Nomor 31 Tahun 2000 tentang Desain Industri menentukan bahwa yang dimaksud desain industri adalah suatu kreasi tentang bentuk, konfigurasi, atau komposisi garis atau warna, atau garis dan warna, atau gabungan daripadanya yang berbentuk tiga dimensi atau dua dimensi yang memberikan kesan estetis dan dapat diwujudkan dalam pola tiga dimensi atau dua dimensi serta dapat dipakai untuk menghasilkan suatu produk, barang, komoditas industri, atau kerajinan tangan. Desain industri dianggap baru apabila pada tanggal penerimaan, desain industri tersebut tidak sama dengan pengungkapan yang telah ada sebelumnya.[134] Perlindungan terhadap Hak Desain Industri diberikan untuk jangka waktu 10 (sepuluh) tahun terhitung sejak Tanggal Penerimaan.[135] Orang yang berhak memperoleh hak desain industri adalah orang yang menciptakan atau disebut juga pendesain.[136] Hak Desain Industri dapat beralih atau dialihkan dengan:

a. Pewarisan;
b. Hibah;
c. Wasiat;
d. Perjanjian tertulis; atau
e. Sebab-sebab lain yang dibenarkan oleh peraturan perundang-undangan.[137]

---

[133] *Ibid.* Pasal 42.
[134] Pasal 2 Undang-undang Nomor 31 Tahun 2000 tentang Desain Industri.
[135] *Ibid.* Pasal 5.
[136] *Ibid.* Pasal 6.
[137] *Ibid.* Pasal 31.

Berdasarkan Pasal 9 UU *a quo*, Pemegang Hak Desain Industri memiliki hak eksklusif untuk melaksanakan Hak Desain Industri yang dimilikinya dan untuk melarang orang lain yang tanpa persetujuannya:

a. Membuat,
b. Memakai,
c. Menjual,
d. Mengimpor,
e. Mengekspor, dan/atau
f. Mengedarkan barang yang diberi hak desain industri.

Akan tetapi dikecualikan apabila pemakaian Desain Industri tersebut digunakan untuk kepentingan penelitian dan pendidikan sepanjang tidak merugikan kepentingan yang wajar dari pemegang hak Desain Industri[138] Apabila timbul kerugian akibat penyalahgunaan dan/atau penggunaan desain industri tanpa izin pemegang hak, maka Pemegang Hak Desain Industri atau penerima Lisensi dapat mengajukan gugatan ke pengadilan niaga terhadap siapa pun yang dengan sengaja dan tanpa hak melakukan perbuatan tersebut berupa gugatan ganti rugi; dan/atau penghentian semua perbuatan yang dilarang. Pemerintah juga telah membuat aturan terkait sanksi pidana bagi setiap orang yang menyalahgunakan dan/atau menggunakan desain industri tanpa izin pemegang hak berupa pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 300.000.000,00 (tiga ratus juta rupiah) sebagai upaya perlindungan atas hak desain industri dari tindak penyalahgunaan

4.10 Rahasia Dagang

Perlindungan rahasia dagang sudah diatur dalam Undang-undang nomor 30 Tahun 2000 tentang rahasia dagang. Menurut Pasal 1 Undang-undang *a* quo, yang dimaksud dengan rahasia dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena

[138] *Ibid.* Pasal 9.

berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik rahasia dagang. Lingkup perlindungan rahasia dagang meliputi metode produksi, metode pengolahan, metode penjualan, atau informasi lain di bidang teknologi dan/atau bisnis yang memiliki nilai ekonomi dan tidak diketahui oleh masyarakat umum.[139] Pasal 3 undang-undang *a quo* menentukan:

a. Rahasia Dagang mendapat perlindungan apabila informasi tersebut bersifat rahasia, mempunyai nilai ekonomi, dan dijaga kerahasiaannya melalui upaya sebagaimana mestinya.
b. Informasi dianggap bersifat rahasia apabila informasi tersebut hanya diketahui oleh pihak tertentu atau tidak diketahui secara umum oleh masyarakat.
c. Informasi dianggap memiliki nilai ekonomi apabila sifat kerahasiaan informasi tersebut dapat digunakan untuk menjalankan kegiatan atau usaha yang bersifat komersial atau dapat meningkatkan keuntungan secaraekonomi.
d. Informasi dianggap dijaga kerahasiaannya apabila pemilik atau para pihak yang menguasainya telah melakukan langkah-langkah yang layak dan patut.

Pemilik rahasia dagang memiliki hak untuk menggunakan sendiri rahasia dagang yang dimilikinya dan memberikan lisensi kepada atau melarang pihak lain untuk menggunakan rahasia dagang atau mengungkapkan Rahasia Dagang itu kepada pihak ketiga untuk kepentingan yang bersifat komersial.[140] Hak Rahasia Dagang dapat beralih atau dialihkan dengan:

a. Pewarisan;
b. Hibah;
c. Wasiat;
d. Perjanjian tertulis; atau
e. Sebab-sebab lain yang dibenarkan oleh peraturan perundang-undangan.

---

[139] Pasal 2 Undang-undang Nomor 30 Tahun 2000 tentang Rahasia Dagang.
[140] *Ibid.* Pasal 4.

Apabila timbul suatu sengketa yang menyebabkan kerugian pemegang hak rahasia dagang, maka pemegang hak rahasia dagang atau penerima lisensi dapat menggugat siapa pun yang dengan sengaja dan tanpa hak menggunakan rahasia dagang tanpa izin dari pemiliknya, yang diajukan ke pengadilan negri.[141] Para pihak juga dapat menyelesaikan perselisihan tersebut melalui arbitrase atau alternatif penyelesaian sengketa.[142]

Pemerintah juga telah menyediakan perlindungan kepada pemegang hak rahasia dagang atas hak ekslusifnya. Barang siapa yang dengan sengaja mengungkapkan Rahasia Dagang, mengingkari kesepakatan atau mengingkari kewajiban tertulis atau tidak tertulis untuk menjaga Rahasia Dagang yang bersangkutan dan/atau memperoleh atau menguasai Rahasia Dagang tersebut dengan cara yang bertentangan dengan peraturan perundang-undangan yang berlaku, maka akan dikenakan sanksi pidana berupa pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp.300.000.000,00 (tiga ratus juta rupiah). Perlu diketahui bahwa tindak pidana yang dimaksud disini merupakan delik aduan.[143]

[141] *Ibid.* Pasal 11.
[142] *Ibid.* Pasal 12.
[143] *Ibid.* Pasal 17.

BAB V
GUIDELINES ONLINE USERS DI INDONESIA

Peraturan perundang-undangan nasional yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum telah ada yaitu Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Teknologi Informasi adalah istilah umum untuk teknologi apapun yang dapat membantu manusia dalam membuat, mengubah, menyimpan, mengkomunikasikan dan/atau menyebar-kan informasi. Teknologi informasi sangat membantu manusia dalam melakukan kegiatan sehari-hari seperti bisnis, pendidikan, perbankan, kesehatan, dan komunikasi. Kegiatan yang dilakukan menggunakan sistem teknologi informasi tidak dapat diragukan lagi menjadi hal yang bergantung dalam kehidupan manusia. Ketergantungan manusia dalam dunia teknologi membuat UU ITE dan masyarakat indonesia terlepas dari sistem hukum yang ada, karena terdapat beberapa hal yang tidak kita temukan penyelesaian masalah di dalam UU ITE. Dalam hal ini maka harus terbuat sebuah Undang-undang terarah dalam semua yang terpaut di dalamnya dan melindungi masyarakat secara baik dan pasti yang melindungi dengan tenteram, transparan dan tidak mengganggu hak-hak asasi manusia yang ada.

Perlu dipahami bahwa globalisasi membuat manusia dapat saling berinteraksi antara satu dengan lainnya menggunakan teknologi informasi berbasis jaringan sosial yang dapat bersifat tertutup maupun terbuka dengan serangkaian perangkat hokum yang dapat mengumpulkan dan menyiapkan ataupun menyimpan

data secara online, berdasarkan identitas yang dimiliki oleh pribadi seseorang. Indonesia sebagai negara ke-empat perkembangan pengguna internet terbanyak di dunia[144] saat ini sedang menghadapi sebuah kesempatan dan juga tantangan dalam perkembangan dunia teknologi dan digital.

Bagaimanapun juga tanpa adanya keamanan dalam dunia cyber yang ketat, 150 juta pengguna internet di indonesia akan berada dalam risiko keamanan di dunia teknologi. Para pengguna internet di Indonesia seharusnya berperilaku lebih bijak dalam dunia internet. Dengan 56% dari populasi di indonesia, sekitar 150 juta orang merupakan pengguna internet, angka ini naik dari 13% pengguna internet di indonesia di tahun 2018 silam.

Lemahnya keamanan *cyber* di indonesia, indonesia sering menjadi subjek dari banyaknya penyerangan *cyber* yang terjadi.[145] Untuk mengisi celah ini, pemerintah perlu mendorong dikeluarkannya sebuah peraturan perundang-undangan untuk keamanan dunia maya. Peraturan perundang-undangan ini penting untuk membantu pemerintah membedakan antara menangani serangan terhadap pertahanan dunia maya dan kejahatan dunia maya. Serangan terhadap pertahanan siber menargetkan keamanan nasional kita. Penyerang ini sebagian besar teroris atau negara asing yang bermusuhan. Kejahatan dunia maya merujuk pada kejahatan apa pun di dunia maya. Saat ini, pemerintah tampaknya tidak dapat membedakan keduanya. Sementara itu polisi menangani kejahatan dunia maya dan telah membentuk direktorat kejahatan dunia maya. Selain kepolisian, Kementerian Luar Negeri telah mulai menggunakan diplomasi dunia maya, penggunaan instrumen diplomatik dan metode untuk menemukan solusi untuk masalah dunia maya. Misalnya, Indonesia memainkan peran aktif membahas norma-norma dunia maya dan masalah-masalah kejahatan dunia

---

[144]Digital 2019: *Global Digital Overview*. Terdapat dalam www.datareprtal.com/reports/digital-2019-global-digital-overview.com, diakses pada 25 Agustus 2019.

[145]*Web Attack Security Report* 2019. https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/web-attack-visualization.jsp, diakses pada 25 Agustus 2019.

maya di Kelompok Ahli Pemerintahan PBB (UNGGE) dan Kantor PBB untuk Narkoba dan Kejahatan (UNODC).[146]

Terakhir, untuk menanggapi serangan siber, Kementerian Komunikasi dan Informatika telah membentuk tim, yang dikenal dengan Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center), untuk memastikan keamanan internet di Indonesia. Karena BSSN baru didirikan dua tahun lalu, koordinasi antara lembaga-lembaga ini masih berada dalam tahap awal. Selain itu, BSSN belum membangun infrastruktur yang solid dan menunjuk lembaga yang bertanggung jawab untuk setiap sektor.

Menurut Simandjuntak, Kejahatan merupakan suatu tindakan anti sosial yang dapat merugikan, tidak pantas dan tidak dapat dibiarkan karena dapat menimbulkan kegocangan dalam masyarakat. Sedangkan *Cybercrime* adalah suatu tindakan yang menggunakan dan berkaitan dengan pemanfaatan sebuah teknologi informasi dengan tujuan kriminal berteknologi tinggi dan di akses oleh pelanggan internet dengan menyalahgunakan kemudahan teknologi digital.[147] Di indonesia sendiri *Cybercrime* dikategorikan ke dalam tindak pidana khusus meskipun masih dalam unsur utama KUHP. Pada tahun 2008 sendiri DPR RI telah mengesahkan Rancangan Undang-undang informasi dan Transaksi Elektronik (ITE) menjadi sebuah Undang-undang. Menurut Soepraptomom kejahatan siber atau *cybercrime* sendiri terbentuk sebagai berikut:

a. *Computer Fraud* atau Penipuan Komputer

   Adalah berupa pencucian uang atau harta benda dengan menggunakan sarana komputer/*cyber* dengan melawan hukum.

---

[146]*Mewujudkan keamanan siber bagi Indonesia: Apa yang harus dilakukan?*. Terdapat dalam http://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813, diakses pada 27 Agustus 2019.

[147]Rudi Hermawan. (n.d). *Kesiapan Aparatur Pemerintah Dalam Menghadapi Cybercrime di Indonesia*. ISSN: 1979-276x. Jakarta: Universitas Indraprasta PGRI Jakarta. hlm. 45.

b. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
c. *Hacking*, atau melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
d. Perbuatan pidana komunikasi, yaitu *hacking* yang dapat membobol sistem online komputer yang menggunakan sistem komunikasi.

Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Termasuk dalam perbuatan ini penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sarana komputer/telekomunikasi. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan. Sedangkan menurut Undang-undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU ITE tidak memberikan definisi yang lengkap mengenai *cybercrime*, tetapi mengelompokan yang mengacu pada *Convention on Cybercrimes*[148]. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu:

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari:
b. Kesusilaan (Pasal 27 Ayat (1) UU ITE)
c. Perjudian (Pasal 27 Ayat (2) UU ITE)
d. Penghinaan dan/atau Pencemaran nama baik (Pasal 27 Ayat (3) UU ITE)

[148]Josua Sitompul. (2012). *Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa. hlm. 136.

e. Berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE
f. Menimbulkan rasa kebencian berdasaran SARA (Pasal 28 Ayat (2) UU ITE)
g. Mengerimkan informasi yang berisi ancaman kekerasan atau menakuti-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE)
h. Dengan cara apapun melakukan akses ilegal (Pasal 29 UU ITE)
i. Intersepsi cara apapun melakukan akses ilegal (Pasal 31 UU 19/2016)
j. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:
k. Gangguan terhadap informasi atau Dokumen Elektronik (data interference – Pasal 32 UU ITE)
l. Gangguan terhadap sistem Elektronik (system interference – Pasal 33 UU ITE)
m. Tindak Pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE)
n. Tindak Pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE)
o. Tindak Pidana Tambahan (accessoir Pasal 36 UU ITE); dan
p. Pemberatan-Pemberatan terhadap ancaman (Pasal 52 UU ITE).
[149]

Kita sering menggunakan kata "kejahatan dunia maya" untuk memasukkan serangkaian kegiatan kriminal yang melibatkan komputer atau perangkat lain seperti ponsel dan kamera. Ini dapat termasuk *cyber-bullying*, panggilan telepon atau pesan ofensif, mengakses atau mendistribusikan pornografi anak, perawatan online anak-anak untuk kegiatan seksual, peretasan, berbagi file ilegal dan berbagai bentuk penipuan. Meskipun hukum menggunakan arti sempit "kejahatan dunia maya" (dalam Persemakmuran *Cybercrime* Act 2001, "*cybercrime*" hanya berlaku

[149]Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

untuk kasus-kasus terhadap data komputer dan sistem), dokumen ini menggunakan arti yang lebih luas dari "kejahatan dunia maya".

Delik *CyberBullying* minim digunakan karena definisi yang salah kaprah dalam penyusunan undang-undangnya. Hal ini diketahui karena lebih seringnya digunakan istilah pencemaran nama baik ketimbang delik *cyberbullying* padahal sifat kedua tindak kejahatan ini berbeda. *Cyberbullying* tidak selalu berupa hinaan namun dapat berbentuk sebuah ancaman atau intimidasi. Sedangkan, pencemaran nama baik menyerang kehormatan atau reputasi. Hal ini sama dengan *revenge porn* di dunia maya, *revenge porn* atau pornografi balas dendam adalah kasus pornografi dengan modus operandi baru di indonesia, sebenarnya *revenge porn* sudah banyak terjadi di beberapa negara lain dan sangat merugikan korbannya.

Menurut Carmen M. Cusack sendiri *revenge porn* adalah produksi pornografi atau distribusi oleh pasangan intim dengan maksud membuat malu atau melecehkan korban.[150] Para pelaku yang *melakukan revenge Porn ini tanpa persetujuan korban , menurut Nadya Karima Melati, revenge* Porn atau balas dendan porno adalah bentuk pemaksaan, ancaman terhadap seseorang, umumnya perempuan, untuk menyebarkan konten porno atau berupa foto atau video yang pernah dikirimkan kepada pelaku. Perilaku ini bertujuan untuk mempermalukan, mengucilkan dan menghancurkan hidup korban. Pelaku bisa merupakan pacar, mantan pacar yang ingin kembali, atau orang yang tidak bisa diidentifikasi.[151]

Menurut UNICEF pada tahun 2016 *revenge porn* merupakan tindakan *cyberbullying* yang bisa berakibat fatal, mulai dari penurunan performa akademis sampai tindakan bunuh diri. Dalam UU ITE sendiri *cyberbullying* memiliki definisi yang terbatas karena memakai bentuk "menakut-nakuti yang ditunjukan secara pribadi"

---

[150]Carmen M.Cusack. (2014). *Pornography and The Criminal Justice System.* CRC Press. hlm. 145.

[151]Nadya Karima Melati. (2018). *Bagaimana Mencari bantuan dalam Kasus Revenge Porn*. Terdapat dalam https://magdalene.co/story/bagaimana-mencari-bantuan-dalam-kasus-revenge-porn, diakses pada 27 Agustus 2019.

atau "ancaman kekerasan", padahal banyak bentuk lain dari *cyberbullying*. UU ITE di Indonesia diharapkan bersifat *lex spesialist*, yang merupakan penyempurna dalam undang-undang pendukungnya dan merukan analagi yang lebih luas terhadap KUHP. Dalam menangani kasus *cybercrime* diperlukan penyidik yang mempunyai cukup pengalaman, aparat hukum seperti polisi, jaksa dan hakim diperlukan untuk melakukan pendidikan mengenai *cybercrime* di negara-negara. Di indonesia sendiri Permen/Kepmen Kominfo merupakan turunan hukum dari UU ITE. Indonesia bersama dengan Kepolisian RI bekerja sama dengan Amerika Serikat melalui *International Criminal Investigative Training Assistance Program* (ICITAP) melatih lebih dari 100 orang polisi se-Jawa Timur mengenai cara mengatasi *cybercrime*.

Dalam menangani *cyberbullying* dan *revenge porn* Pasal 45 Jo. Pasal 27 ayat (1) UU No.19 Tahun 2016 tentang Perubahan ayas UU No, 11 Tahun 2008 tentang informasi dan Transaksi Elektronik Jo. Pasal 64 berbunyi: "*setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau menstransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan*". Pasal ini mengandung makna mengetahui dan menghendaki dilakukannya suatu perbuatan yang dilarang oleh UU ITE atau mengetahui dan menghendaki terjadinya suatu akibat dilarangan UU ITE. Terkait dengan oasal 27 Ayat (1) UU ITE, yang dengan sengaja dimaksud ditunjukan terhadap perbuatan mendistribusikan, mentsransmisikan atau membuat dapat diaksesnya informasi atau dokumen elektronik yang memiliki muatan yang melanggar norma kesusilaan. Dalam melakukan tuntutan terhadap kasus *cyber*, pembuktian dan alat bukti memegang peranan yang sangat penting dalam proses peradilan. Dengan dunia yang terus berkembang maka tidak dipungkiri adanya modus-modus tindak kejahatan yang baru, maka aturan yang dapat merespon suatu perkembangan dalam mengikuti perkembangan tindak pidana tersebut.

Menurut Lawrence M. Friedman, sistem hukum yang baik akan tercipta melalui beberapa unsur yaitu:[152]

a. Struktur

   Pengertian struktur adalah sistem pengadilan. Khusus di dalam membentuk sistem hukum teknologi informasi, perlu dipersiapkan sampai sejauh mana pengadilan di Indonesia dapat menyelesaikan kasus pelanggaran privasi, khususnya yang dilakukan dalam lalu lintas *e-commerce*. Pengadilan memerlukan suatu pemahaman yang mendalam mengenai pelanggaran privasi dalam *e-commerce*. Kemampuan dan kemauan para aparat penegak hukum (hakim, jaksa dan polisi) diperlukan agar memahami apa itu pelanggaran privasi khususnya dalam kaitan dengan *e-commerce*. Hakim dan penegak hukum lainnya harus mampu menyelesaikan kasus-kasus yang muncul sebagai akibat terjadinya perubahan kondisi sosial masyarakat tersebut. Pada akhirnya, dengan adanya struktur yang memadai, diharapkan dapat memberikan kontribusi terhadap pembentukan hukum yang responsif. Hukum responsif adalah hukum yang dapat mengakomodasi dan mengikuti perubahan zaman terutama dalam hal ini berkaitan dengan hukum teknologi informasi yang selalu cepat berubah.

   Lebih jauh, struktur dapat pula berarti bagaimana proses penyusunan undang-undang harus dilaksanakan, termasuk melakukan penelitian untuk menggali aspirasi dan kepentingan masyarakat, mengiventarisasi peraturan-peraturan terkait dengan melibatkan sebanyak mungkin *stake holder*.

b. Substansi

   Substansi berkaitan dengan isi peraturan perundang-undang, yang antara lain meliputi: (1) perbuatan hukum apa saja yang akan diatur; (2) asas-asas yang akan diterapkan baik asas

[152]Sinta Dewi. (2016). *Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia*. Yustisia Vol. 5 No. 1 Januari – April 2016. Bandung: Universitas Padjadjaran. hlm. 28-29.

filosofis, yuridis, dan sosiologis; (3) prinsip-prinsip apa saja yang akan menjadi landasan dalam suatu peraturan perundang-undangan (termasuk juga prinsip-prinsip yang telah diterapkan secara internasional, misalnya *fair information principles*; dan yang terakhir (4) lembaga mana yang akan mengimplementasikan dan menerapkan sanksi terhadap pelanggar peraturan, sehingga undang-undang yang akan disusun nantinya dapat diterapkan secara efektif.

c. Budaya Hukum

Suatu sistem hukum dapat tercipta dengan baik sangat ditentukan pula oleh sejauh mana perilaku masyarakat dalam mempersepsikan hukum melalui mekanisme tradisi hukum yang digunakan untuk mengatur kehidupan suatu masyarakat. Budaya hukum Indonesia memiliki karakteristik bahwa pembentukan hukum dilakukan oleh badan legislatif atas usul dari departemen terkait, melalui masukan dari masyarakat.

DAFTAR PUSTAKA

Buku

Adolf, Huala. 2010. *Dasar-Dasar Hukum Kontrak Internasional.* Edisi Revisi Cetakan Ketiga. Bandung: PT Refika Aditama

Amanda, Achmad P. 2012. *Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik).* Fakultas Hukum Brawijaya: Malang.

Dewi, Shinta. 2009. *Cyber Law Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional.* Cetakan ke-1. Bandung: Widya Padjajaran.

Djumhana, Muhammad. 1993. *Hukum Perbankan Di Indonesia.* Bandung: PT. Citra Aditya Bakti.

Ferrante, Joan. *Sociology: A Global Prespective.* (Belmont:Thomson Learning. Inc, 2008).

Gazali, Rachmadi. 2010. *Hukum Perbankan.* Jakarta : Sinar Grafika.

Hermansyah. 2008. *Hukum Perbankan Nasional Indonesia Edisi Revisi,* (Jakarta: Kencana Prenada Media Group.

Hermawan, Rudi. *Kesiapan Aparatur Pemerintah Dalam Menghadapi Cybercrime di Indonesia.* ISSN: 1979-276x. Jakarta: Universitas Indraprasta PGRI Jakarta.

Kusumaatmadja, Arief Sidharta. 2000. *Pengantar Ilmu Hukum Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum Buku I.* Bandung: Penerbit Erlangga.

Makarim, Edmon. 2005. *Pengantar Hukum Telematika (Suatu Kompilasi Kajian).* Jakarta: RajaGrafindo Persada.

Muhammad, Abdulkadir. 2007. *Kajian Hukum Ekonomi Hak Kekayaan Intelektual* Bandung: PT Citra Aditya Bakti.

Muhammad, Abdulkadir. 2010. *Hukum Perusahaan Indonesia.* Cetakan Keempat. Bandung: PT Citra Aditya Bakti.

Riswandi, Budi. 2005. *Aspek Hukum Internet Banking.* Jakarta: RajaGrafindo Persada.

Siahaan. 2002. *Money Laundering Pencucian Uang Dan Kejahatan Perbankan.* Jakarta: Pustaka Sinar Harapan.

Sitompul, Josua. 2012. *Cyberlaw: Tinjauan Aspek Hukum Pidana.* Jakarta: Tatanusa

Uno, Hamzah. 2010. *Teknologi Komunikasi dan Inofasi Pembelajaran.* Jakarta: Bumi Aksara.

Jurnal

Asep Rohandi. 2015. "Perlindungan Konsumen Dalam Transaksi E-Commerce Perspektif Hukum Nasional dan Internasional". Ecodemica Vol III. No 2 Tahun 2015.

David Arnold. 2005 "Europe, Technology, and Colonialism in the 20th Century". History and Technology Vol.21 No 1.

Deky Pariadi. 2018. "Pengawasan E-commerce Dalam Undang-undang Perdagangan dan Undang-undang Perlindungan Konsumen". Jurnal Hukum & Pembangunan 48 Nomor 3 tahun 2018.

Devi Rahayu. 2011. "Perlindungan Hukum Terhadap Hak Cipta Motif Batik Tanjungbumi Madura", *Mimbar Hukum*, Vol. 23 No. 1, Yogyakarta: FH UGM.

Dwi Ayu Astrini. 2015. "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking dari Ancaman Cybercrime Lex Privatum". Vol. III/No. 1/Jan-Mar/2015

Edmore Etekwe. 2012. "The Impact of Technology on Social Change: A Sociological Prespective". Journal Research in Peace, Gender and Development Vol. 2 (11).

Lauren Benton. 2018. "The Legal Logic Of Wars Of Conquest: Truces And Betrayal In The Early Modern World, Duke Journal Of Comparative & International Law". Vol. 28.

Lia Sautunnida.2018. "Urgensi Undang-undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia". Vol. 20. No. 2. Anun Jurnal Ilmu Hukum. Universitas Syiah Kuala

Marnia Rani. 2014. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank". Vol. 2 No. 1. Jurnal Selat. Kepulauan Riau: Universitas Maritim Raja Ali Haji

Marnia Rani. 2014. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank". Vol. 2 No. 1. Jurnal Selat. 2014. Kepulauan Riau: Universitas Maritim Raja Ali Haji

Michael Kwet. 2018. "Digital Colonialism: US Empire and the New Imperialism in the Global South". Race & Classroom Vol 60 No 4.

Olivier Dunant and Michele Wassmer. 2010. "Swiss Bank Secrecy: Its Limits Under Swiss and International Laws, Case W". Res.J.Int'l.l, (Vol;.20:509, 1988),

Renata Avila Pinto. 2018. "Digital Soverignity or Digital Colonialism, Internet and Democracy" Sur 27-v.15 n. 27.

Rosalinda Elsina Latumahina. 2014. "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya". Jurnal GEMA AKTUALITA. Vol. 3 No. 2.

Richard Davis dan Ken Pease. 2000. "Crime, Technology, and the Future, Security Journal, Perpetuity Press Ltd.

Sinta Dewi. 2016. "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia". Yustisia Vol. 5 N. 1 Januari – April 2016. Bandung: Universitas Padjadjaran.

Stephen Ocheni dan Basil Nwankwo. 2012. " Analysis of Colonialism and Its Impact in Africa, Cross Culture Communication". Vol. 8 No. 3, 2012.

Sutan Remy Sjahdeini. 2000. "Money Laundering". Jurnal Hukum Bisnis Vol.11 Jakarta: Yayasan Pengembangan Hukum Bisnis.

Internet

Abu Bakar Munir. *The Malaysian Persona IdataProtection Bill.* http://profabm.blogspot.com/20-09/12/malaysian-personal-data-protection-bill.html. diakses pada 25 Agustus 2019

Daniar Supriadi. *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya.* September 2017. http://www.hukumonline.com/berita/baca/It59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh-daniar-supriyadi.

Digital 2019: *Global Digital Overview.* Terdapat dalam www.data reprtal.com/reports/digital-2019-global-digital-overview.com, diakses pada 25 Agustus 2019

Eko Aribowo. (n.d). *Aspek Keamanan Komputer.* https://www.academia.edu/8236936/Aspek_Keamanan_ Komputer_eko_aribowo_S.T._M.Kom. (n.d): UAD. Diakses pada 20 Agustus 2019, 14.57 WIB

Gupinder Assi. *South East Asia: Data Protection Update.* Terdapat dalam https://www.bclplaw.com/images/content/2/0/v2/2020/Bryan-Cave-Client-Bulletin-South-East-Asia-Data-Protection-Updat.pdf. Diakses pada 22 Agustus 2019 pukul 11.41. hlm.1.

Internet Health Report, *Resisting Digital Colonialism*, 2018 di download pada 1 Agustus 2019.

Margaret Khon dan Kavita Reddy. *Colonialism*, Stanford Encyclopedia of Philosophy, 2017. Diakses pada https://plato.stanford.edu/entries/colonialism/ tanggal 31 Juli 2019.

Mewujudkan keamanan siber bagi Indonesia: Apa yang harus dilakukan?. Terdapat dalam http://theconversation.com/mewujudkan-keamanan-siber-bagi-indonesia-apa-yang-harus-dilakukan-116813, diakses pada 27 Agustus 2019.

Michael Kwet, *Digital Colonialism is Threatening the Global South*, Al Jazeera 2019, didownload dalam https://www.aljazeera.com/topics/categories/science-and-technology.html pada 2 Agustus 2019.

Nadya Karima Melati. (2018). *Bagaimana Mencari bantuan dalam Kasus Revenge Porn.* Terdapat dalam https://magdalene.co

/story/bagaimana-mencari-bantuan-dalam-kasus-revenge-porn, diakses pada 27 Agustus 2019.

Ryan Schleeter. (2013). "First Rulers of the editerranean" diakses dalam https://www.nationalgeographic.org/news/first-rulers-mediterranean/ pada tanggal 31 Juli 2019.

Web Attack Security Report 2019. https://www.akamai.com /us/en /resources/our-thinking/state-of-the-internet-report/web-attack-visualization.jsp, diakses pada 25 Agustus 2019.

Peraturan Perundang-Undangan

Bank Indonesia. 2004. *Surat Edaran No.6/18/DPNP: Penerapan Manajemen resiko pada aktivitas pelayanan jasa bank melalui Internet (Internet Banking).* Dikutip dari http://www.bi.go.id/id/peraturan/arsip-peraturan/ Perbankan2004/se-6-18-04-dpnp.pdf. Diakses pada 20 Agustus 2019, 14.54 WIB.

Undang-undang Nomor 20 Tahun 2016 tentang Merek dan Indeks Geografis.

Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Undang-undang Nomor 10 Tahun 1998 tentang Perbankan

Peraturan Bank Indonesia Nomor 18/40/Pbi/2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.

Peraturan Bank Indonesia Nomor 18/40/Pbi/2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.

Undang-Undang Hak Cipta No. 19 tahun 2002.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 26 ayat (1).

Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan Atas Undang- Undang Republik Indonesia Nomor 7

Tahun 1992 tentang Perbankan, Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182

Lain-Lain

Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian), dalam Radian Adi Nugraha, Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, Universitas Indonesia. 2012.

Hannu Honka. *Harmonization of Contract Law hrough International Trade: A Nordiç Perspective.* 1996 Tulane European and Civil Law Forum.

Pho Chu Chai dan Dennis Campbell. dalam Yunus Husein. *Rahasia Bank Privasi Versus Kepentingan Umum.* Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia. 2003.

Radian Adi Nugraha. *Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik.* Universitas Indonesia. 2012.

Sutan Remy Sjahdeini. *Rahasia Bank: Berbagai Masalah Disekitarnya dalam Hukum Perbankan.* Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia.

UNCITRAL. *Model Law on Electronic Commerce with Guide to Enactment.* 1996. *With additional article 5 bis as adopted in* 1998. Yang disahkan oleh Majelis Umum PBB dengan Resolusi No. 51/162 tanggal 16 Desember 1998.

Yunus Husein. *Rahasia Bank Privasi Versus Kepentingan Umum.* Jakarta: Program Pascasarjana Fakultas Hukum Universitas Indonesia. 2003.