# LIABILITY KORPORASI PENGELOLA SISTEM ELEKTRONIK & DELIK TERKAIT PENYELENGGARAAN SISTEM ELEKTRONIK DI ERA INDUSTRI 4.0

Oleh: **Anton Hendrik Samudra**[1]

## PENDAHULUAN

Rezim konvergensi teknologi informasi komunikasi telah mengubah budaya dan perilaku masyarakat. Istilah konvergensi telematika digunakan oleh Makarim,[2] sedangkan Budhijanto menggunakan istilah teknologi informasi komunikasi. Keduanya sama-sama menggambarkan penggabungan fungsi jaringan telekomunikasi, media (audio-visual, baik sendiri-sendiri maupun gabungannya), dan perangkat (lunak atau keras, maupun gabungannya).

Dunia maya yang sekarang diketahui dan dikenal adalah hasil konvergensi teknologi informasi komunikasi atau telematika dan bagaikan realitas paralel kehidupan manusia. Setiap kemudahan didapat karenanya, dan dampaknya revolusioner terhadap kehidupan manusia, mulai dari perilaku interaksi individu, kelompok maupun industri. Sekarang ini hidup manusia sedang berada di tengah-tengah transformasi yang signifikan dalam dunia industri. Saking kuatnya warna transformasi tersebut, nama Industri 4.0 diberikan untuk merujuk fenomena ini.

Tingkatan konvergensi pada korporasi, dalam hal ini perusahaan, memunculkan adanya penggabungan perusahaan terkait industri komputer, telekomunikasi dan media. Misalnya: Microsoft Corporation yang juga berinvestasi dalam bidang penyiaran, televisi kabel, satelit, penerbitan dan industri internet. Contoh lainnya adalah Media Nusantara Citra (MNC) memiliki RCTI, Global TV, TPI, Mobile-8 Telecom, Infokom Elektrindo, Koran Sindo, dan Elektrindo Nusantara.[3]

Fenomena Industri 4.0 juga dikaitkan dengan *Industrial Internet of Things*, yang merupakan hal yang paling dibicarakan dalam konsep bisnis industrial di tahun-tahun terakhir. General Electric (GE) menggunakan istilah *"Industrial Internet"* untuk merujuk Industrial Internet of Things, Cisco menggunakan istilah *"internet of everything"*, sedangkan yang lainnya menyebutnya sebagai Internet 4.0 dan lain sebagainya.[4] Perkembangan industri berbasis internet bukannya tanpa preseden, di 15 tahun terakhir dapat dilihat dalam sektor B2C *(business-to-consumer)* di bidang retail, media dan jasa keuangan. Contohnya korporasi raksasa seperti Amazon, Netflix, eBay, Paypal, dsb.[5] Neama et al mencatat penjualan melalui *e-commerce* mencapai 1,2 Triliun USD pada tahun 2013 dan mencapai 1,92 Triliun USD ditahun 2016.[6]

---

[1]Dosen tetap Fakultas Hukum, Universitas Surabaya. Surel: antonhendrik@staff.ubaya.ac.id

[2]Edmon Makarim and et al., *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, Raja Grafindo Persada, Jakarta, 2005., h. 79

[3]Danrivanto Budhijanto, *Teori Hukum Konvergensi*, Refika Aditama, Bandung, 2014., h. 123.

[4]Alasdair Gilchrist, *Industry 4.0: The Industrial Internet of Things* (Apress, 2016), https://doi.org/10.1017/978-1-4842-2047-4., h. 1.

[5]*Ibid.*, h. 2.

[6]Ghadeer Neama, Rana Alaskar, and Mohammad Alkandari, "Privacy, Security, Risk, and Trust Concerns in e-Commerce," *Proceedings of the 17th International Conference on Distributed Computing and Networking - ICDCN '16, 2016*, 16, https://doi.org/10.1145/2833312.2850445., h. 1

Setiap perbuatan hukum dalam media konvergensi teknologi informasi komunikasi atau telematika dilaksanakan melalui sarana berupa sistem elektronik. Setiap otorisasi, verifikasi, dan autentikasi semua dilakukan melalui informasi elektronik dan/atau dokumen elektronik. Ada sisi lain dari "mata uang" atas semua proses yang memudahkan tersebut. Preferensi-preferensi pengguna layanan, data pribadi, tanda tangan digital, dan informasi elektronik pribadi lainnya masuk dalam sistem yang diselenggarakan oleh penyelenggara sistem elektronik. Belum lagi adanya akses yang juga memungkinkan memberikan kemudahan bagi orang yang memiliki niat jahat untuk mengakses akun-akun milik orang lain atau perangkat keras pintar milik orang lain yang tersambung ke jaringan dengan bermacam-macam motif jahat. Informasi elektronik, dokumen elektronik, dan sistem elektronik rentan terhadap serangan-serangan *hacking* maupun *cracking*, oleh karena itu dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara RI Tahun 2008 Nomor 58, Tambahan Lembaran Negara RI Nomor 4843) selanjutnya disebut UU ITE, yang diubah dengan Undang-undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara RI Tahun 2016 Nomor 251, Tambahan Lembaran Negara RI Nomor 5952) yang selanjutnya disebut Perubahan UU ITE mengatur larangan terhadap perbuatan-perbuatan tersebut dan mengancamnya dengan pidana.

Dalam Pasal 1 angka 6 UU ITE diatur bahwa penyelenggaraan sistem elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat. Hal itu berarti tentu saja penyelenggaraan, terdapat pihak yang menyelenggarakan. Lebih lanjut dalam Pasal 3 dikatakan pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Terdapat elemen kehati-hatian yang harus diperhatikan dan dilaksanakan oleh penyelenggara sistem elektronik. Dalam Pasal 1 angka 4 Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348), selanjutnya disebut sebagai PP Penyelenggaraan Sistem dan Transaksi Elektronik, dan ditegaskan dalam Pasal 1 angka 2 Peraturan Menteri Komunikasi dan Informatika No. 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik menyebutkan: "Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain." Korporasi memiliki peluang untuk menjadi penyelenggara sistem elektronik, dan tentu saja korporasi ada yang menjadi penyelenggara sistem elektronik. Sistem elektronik didefinisikan sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.[7]

Ruang lingkup penyelenggaraan sistem elektronik disebutkan dalam Pasal 4 PP Penyelenggaraan Sistem dan Transaksi Elektronik meliputi:

a. pendaftaran;
b. Perangkat Keras;
c. Perangkat Lunak;
d. tenaga ahli;

[7]Baca Pasal 1 angka 5 UU ITE, Pasal 1 angka 4 PP Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 1 angka 1 Permenkominfo Tata Cara Pendaftaran Penyelenggara Sistem Elektronik

e. tata kelola;
f. pengamanan;
g. Sertifikasi Kelaikan Sistem Elektronik; dan
h. pengawasan.

Terdapat kewajiban-kewajiban yang ditetapkan bagi penyelenggara sistem elektronik dalam Peraturan Pemerintah tersebut. Seperti dalam hal tata kelola, dalam Pasal 26 UU ITE jo. Perubahan UU ITE mengenai penggunaan informasi elektronik yang berkaitan dengan data pribadi mengharuskan adanya persetujuan dari pemilik data tersebut. Terkait data pribadi, saat ini juga Rancangan Undang-undang tentang Perlindungan Data Pribadi sedang dibahas di DPR. Mengenai pengamanan jaringan dan juga keandalan operasi sistem elektronik juga disebutkan dalam peraturan pemerintah tersebut.

Tata kelola dan pengamanan yang baik dalam penyelenggaraan sistem elektronik sangat diperlukan. Selain untuk memenuhi kepercayaan pengguna, transaksi elektronik menggunakan sistem elektronik berpotensi menjadi pilar penting perekonomian dengan keberadaan *e-commerce*.[8] Tanpa adanya kepercayaan pengguna sistem elektronik, *e-commerce* tidak berkembang, perekonomian negara tidak akan bisa bersaing dengan negara lain yang sedang serius mengembangkan *economy* 4.0. Penyelenggara sistem elektronik harus mampu melakukan tugasnya dengan mengamankan dari segala bentuk serangan siber. Paling tidak harus mempersulit pelaku kejahatan telematika dan mengeliminasi segala bentuk sarana yang dapat dieksploitasi untuk melakukan serangan terhadap sistem elektronik.

Penyelenggaraan pemerintahan juga sudah merambah ke penggunaan sistem elektronik, seperti salah satu contohnya adalah pelaporan tahunan untuk pajak *(e-filing)*. Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Informatika menyatakan bahwa ini merupakan upaya mewujudkan pemerintahan yang terbuka.[9] Penyelenggaraan pemerintahan dengan keberadaan konvergensi teknologi informasi komunikasi dapat terselenggara dengan lebih efisien dan transparan. Pasal 4 Permenkominfo Tata Cara Pendaftaran Penyelenggara Sistem Elektronik mengatur mengenai pihak penyelenggara sistem elektronik untuk pelayanan publik.

Peran korporasi sudah merambah ke hampir semua struktur sosial. Mulai dari urusan pemerintahan, ekonomi, perdagangan, pendidikan, dan budaya lebih banyak dilakukan oleh korporasi daripada perorangan.[10] Dalam melakukan aktivitasnya untuk mencapai tujuan tertentu, korporasi dapat melakukan perbuatan yang bertentangan dengan ketentuan hukum, yang bahkan memuat sanksi pidana. Perbuatan inilah yang disebut sebagai tindak pidana korporasi atau *corporate crime*.[11] Sahetapy menyatakan kejahatan korporasi bukanlah sesuatu yang baru, namun hanya kemasan, bentuk dan perwujudannya yang berbeda. Kejahatan korporasi sudah ada sejak lebih dari tiga ribu tahun yang lalu atau pada abad 24 Masehi di Mesir. Selain iru, pada masa lampau di Yunani, kejahatan korporasi juga terjadi misalnya ketika Alcmaenoids yang diberi kepercayaan untuk membangun rumah ibadah dengan batu pualam yang diganti semen dengan dilapisi batu pualam.[12] Pertanggungjawaban pidana korporasi belum berlaku secara umum, karena tidak diatur dalam KUHP yang sekarang

---

[8]Lihat di Investor Daily Indonesia, E-Commerce Berpotensi Jadi Pilar Baru Ekonomi RI, <https://id.beritasatu.com/tradeandservices/e-commerce-berpotensi-jadi-pilar-baru-ekonomi-ri/130282>, diakses tanggal 9 Februari 2019

[9]Kementerian Komunikasi dan Informatika, Penerapan Sistem Pemerintahan Berbasis Elektronik, <https://kominfo.go.id/index.php/content/detail/8319/penerapan-sistem-pemerintah-berbasis-elektronik/0/berita_satker>, diakses tanggal 9 Februari 2019

[10]Nani Mulyati, "Pemisahan Pertanggungjawaban Pidana Korporasi Dengan Pertanggungjawaban Pidana Pengurus Korporasi," in *Proceeding Call for Papers Simposium Dan Pelatihan Hukum Pidana Ke-V "Revitalisasi Hukum Pidana Adat Dan Kriminologi Kontemporer"* (Yogyakarta: Genta Publishing, 2018)., h. 553

[11]*Ibid.*

[12]J.E. Sahetapy, *Kejahatan Korporasi*, Eresco, Bandung, 1994., h. 4

berlaku. Namun *hal tersebut* sudah diatur dalam undang-undang tindak pidana khusus maupun undang-*undang khusus* yang memuat ketentuan pidana, misalnya UU tentang Pemberantasan Tindak Pidana *Korupsi*, UU tentang Pemberantasan Tindak Pidana Terorisme, UU tentang Pemberantasan *Tindak Pidana* Pencucian Uang, UU tentang Psikotropika, UU tentang Narkotika, UU tentang *Pengelolaan* dan Perlindungan Lingkungan Hidup, dll.

Ketentuan pidana dalam UU ITE yang mendeklarasikan dirinya sebagai rezim hukum baru, masih terbatas. Perbuatan yang dilarang diatur dalam Pasal 27 sampai dengan Pasal 35, ancaman pidana diatur dalam Pasal 45 sampai dengan Pasal 51. Ada beberapa kewajiban yang diatur dalam UU ITE dan Perubahan UU ITE, namun tidak ada elemen sanksi pidana jika melanggar atau tidak melakukan kewajiban yang disebutkan, hanya terdapat pengaturan pemberian peluang penyelesaian melalui gugatan atas kerugian para pihak akibat tidak dilaksanakannya kewajiban tersebut, seperti Pasal 26 UU ITE jo. Perubahan UU ITE yang sudah disebutkan di atas.

Mengenai subyek hukum dalam ketentuan pidana di UU ITE, menggunakan proposisi 'setiap orang'. Dalam Pasal 1 angka 21 UU ITE dijelaskan: Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum. Dapat dilihat bahwa badan hukum juga diakui sebagai subyek hukum delik dalam UU ITE. Namun terkait kewajiban-kewajiban dalam penyelenggaraan sistem elektronik sayangnya tidak ada ancaman sanksi pidana apabila gagal memenuhinya, terlebih secara sengaja.

Yang dielaborasikan dalam tulisan ini adalah delik dan *liability* korporasi pengelola sistem elektronik terkait penyelenggaraan sistem elektronik di era industri 4.0 dalam hal terjadi kesengajaan atau kelalaian dalam kegagalan pemenuhan kewajiban peraturan perundang-undangan terkait penyelenggaraan sistem elektronik yang aman dan *reliable*, mengingat penyelenggaraan konvergensi teknologi informasi komunikasi terkait perbuatan hukum yang memiliki koridor-koridor khusus yang harus dilaksanakan oleh korporasi penyelenggara atau kontraktor *e-commerce, e-banking, e-governance*, maupun media sosial.

## PEMBAHASAN

### Kewajiban penyelenggara sistem elektronik

Perkembangan teknologi informasi dan komunikasi membawa perubahan yang radikal dalam melakukan transaksi. *Website* telah menjadi sumber informasi utama, dan layanan *web* menjadi *platform* transaksi bisnis yang prioritas. Lebih jauh lagi, keinginan mencapai efisiensi dan efektifitas dalam transaksi, para pelaku bisnis dan juga akademisi mengembangkan sistem pembayaran secara elektronik. Berbagai produk bermunculan, seperti uang tunai digital *(e-money/digital cash)*, cek elektronik *(e-cheques)*, dan kartu kredit.[13] Dilihat dari pelakunya, transaksi elektronik dapat dibagi menjadi antar pelaku bisnis (B2B), antara pelaku bisnis dan konsumen (B2C), antara pelaku bisnis dan pemerintah, (B2G), antar konsumen (C2C), dan antar pemerintah (G2G).[14]

Setiap transaksi mengandung risiko. Risiko dalam transaksi elektronik dapat bersumber dari manusia, alam, atau sistem itu sendiri. Permasalahannya adalah siapa yang mengelola risiko ini dan siapa yang bertanggungjawab apabila risiko terjadi. Neama et al menjelaskan mengenai penyelenggara sistem elektronik yang harus mengembangkan dan menerapkan prinsip kehati-hatian:

---

[13] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw*, Tatanusa Jakarta, 2014, h. 61
[14] *Ibid.*, h. 75

*"Due to such growth, businesses owners should realize that it is vital to improve online services provided to their customers. Currently, many companies are gathering customers' information (e.g., name, address, interest, etc.) through registration, online transactions, or cookies in order to achieve such improvement in provided services..... Privacy and security concerns are the major barriers from adopting e-commerce services."*[15]

Dalam berbagai literatur keamanan informasi, kerahasiaan data *(confidentiality)* yang dipertukarkan, keutuhan data *(integrity)*, dan ketersediaan data *(availability)* merupakan tiga pilar utama dari keamanan informasi.[16] Kerahasiaan data *(confidentiality)* berarti suatu informasi hanya dapat diakses atau diungkapkan oleh orang atau para pihak yang memiliki hak. Ada batasan dalam mengakses atau mengungkap informasi. Keutuhan data *(integrity)* berarti informasi dalam kondisi utuh, tidak diubah, ditambah atau dikurangi oleh orang atau pihak lain tanpa persetujuan dari pemilik atau pemegang hak atas informasi. Ketersediaan data *(availability)* berarti informasi atau dokumen elektronik dapat diakses kembali oleh yang berhak.[17]

UU ITE dipandang sebagai undang-undang yang bersifat administratif. Namun undang-undang yang bersifat administratif sekalipun memiliki ancaman sanksi pidana sebagai *ultimum remedium* apabila terjadi pelanggaran ketentuan undang-undang dan segala upaya untuk menanggulangi sudah dilakukan. UU ITE hadir untuk mengakomodasi kebutuhan para pelaku bisnis di dunia konvergensi teknologi informasi komunikasi atau telematika, dan masyarakat umum untuk mendapatkan kepastian hukum dalam melakukan transaksi elektronik. Beberapa materi yang diatur di dalam UU ITE antara lain: pengakuan informasi/dokumen elektronik sebagai alat bukti yang sah (Pasal 5 dan Pasal 6), *digital signature* atau tanda tangan elektronik (Pasal 11 dan Pasal 12), *certification authority* atau penyelenggaraan sertifikasi elektronik (Pasal 13 dan Pasal 14), dan penyelenggaraan sistem elektronik (Pasal 15 dan Pasal 16).

UU ITE maupun PP Penyelenggaraan Sistem dan Transaksi Elektronik mengamanatkan Sistem Elektronik dibangun secara andal, aman, dan beroperasi sebagaimana mestinya. UU ITE dan PP Penyelenggaraan Sistem dan Transaksi Elektronik mengatur bahwa Penyelenggara Sistem Elektronik harus bertanggung jawab terhadap beroperasinya Sistem Elektronik yang diselenggarakannya. Dalam Pasal 15 UU ITE menyebutkan:

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Dijelaskan dalam penjelasan pasal, andal maksudnya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya. Aman berarti Sistem Elektronik terlindungi secara fisik dan non-fisik. Terlindungi secara fisik antara lain: perlunya server yang terlindungi dari banjir, cukupnya pasokan listrik, berjalan 24 jam kali 7 hari. Ruang penyimpanan data yang memiliki pengaturan hak akses, terlindungi dari kebakaran atau dari panas. Sedangkan terlindungi secara non-fisik maksudnya adanya pengamanan secara *logical*, seperti pertimbangan perlunya tidaknya kode akses, enkripsi

---

[15] Neama, Alaskar, and Alkandari, *Op.Cit.*, h. 1
[16] Josua Sitompul, *Op.Cit.*, h. 82
[17] Kyösti Pennanen, Taina Kaapu, and Minna-Kristiina Paakki, "Trust , Risk , Privacy , and Security in e- Commerce," in *Frontiers of E-Business Research*, 2006., tanpa halaman

data, keberadaan *firewall* atau *Intrusion Detection System* (IDS). Beroperasi sebagaimana mestinya, artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya, antara spesifikasi dengan kenyataan penerapan terdapat kesesuaian.

Lebih lanjut dalam Pasal 16 UU ITE ayat (1) mengatur:

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:
   a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
   b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
   c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
   d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
   e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Seperti yang sudah disinggung pada bagian pendahuluan artikel ini, bahwa terdapat kewajiban-kewajiban bagi penyelenggara sistem elektronik. Dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik disebutkan kewajiban-kewajiban tersebut. Seperti dalam Pasal 4 huruf f, penyelenggaraan terhadap sistem elektronik meliputi aspek pengamanan. Informasi memiliki nilai strategis-ekonomis, sehingga informasi tersebut perlu dilindungi. Namun di dalam praktik, kebocoran informasi dapat saja terjadi, entah karena sistem memiliki galat *(bug)* yang menyebabkan, tidak adanya pengamanan yang layak, sistem yang belum terkelola dengan baik ataupun karena perbuatan melawan hukum seseorang. Kebocoran data informasi tersebut tidak seharusnya disebabkan oleh penyelenggara sistem elektronik. Bagaimana mengupayakan supaya kebocoran ini tidak disebabkan oleh penyelenggara sistem elektronik adalah hal yang harus diupayakan. Keengganan atau penolakan secara eksplisit maupun implisit untuk mengupayakan hal tersebut haruslah dihukum.

Dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik, terdapat beberapa pengaturan mengenai kewajiban penyelenggaraan sistem elektronik. Di dalam Pasal 12 ayat (1) mengatur bahwa penyelenggara sistem elektronik wajib menjamin: tersedianya perjanjian tingkat layanan; tersedianya perjanjian keamanan informasi terhadap jasa layanan Teknologi Informasi yang digunakan; dan keamanan informasi dan sarana komunikasi internal yang diselenggarakan. Selanjutnya dalam Pasal 13 PP tersebut mengatur bahwa penyelenggara sistem elektronik wajib menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan. Lebih lanjut, Pasal 14 PP tersebut mengatur bahwa penyelenggara sistem elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap sistem elektronik. Kemudian Pasal 15 PP tersebut mengatur bahwa penyelenggara sistem elektronik wajib: menjaga rahasia, keutuhan, dan ketersediaan data pribadi yang dikelolanya; menjamin bahwa perolehan, penggunaan, dan pemanfaatan data pribadi berdasarkan persetujuan pemilik data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik data pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik data pribadi pada saat perolehan data. Jika terjadi

kegagalan dalam perlindungan rahasia data pribadi yang dikelolanya, penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut. Pelanggaran terhadap ketentuan-ketentuan tersebut ada ancaman sanksi administratif yang diatur di Pasal 84 PP Penyelenggaraan Sistem dan Transaksi Elektronik.

Peran-peran dalam penyelenggaraan sistem elektronik di media konvergensi teknologi informasi komunikasi dapat dijabarkan sebagai berikut:

- Operator jaringan *(Network operator)*: menyediakan fasilitas-fasilitas teknis untuk transmisi informasi;
- Penyedia akses *(Access provider)*: menyediakan akses ke internet kepada pengguna;
- Mesin pencari *(Search Engines)*: perangkat daring *(online tools)* yang digunakan untuk pencarian laman situs seperti Yahoo!, AltaVista, Google, dsb. Terdapat dua tipe mesin pencari, yaitu mesin pencari otomatis, dan mesin pencari yang mengandalkan review pengguna dan katalog laman situs.
- Penyedia jasa *hosting (Host service provider)*: pihak yang menyediakan layanan dan penyimpanan web atau laman bagi perorangan, termasuk menyewakan laman situs, pembuatan laman situs, dan pengunggahan konten, seperti perangkat lunak *(software)*, teks, grafik, atau suara. Jasa Hosting termasuk pertukaran informasi daring, seperti *bulletin boards* dan *chat rooms*.[18]

Kesemua pihak yang berperan tersebut memiliki kewajiban yang diatur bagi korporasi tempat mereka bekerja.

Pasal 17 UU ITE mengatur secara khusus transaksi elektronik dalam bidang perdagangan *(commerce)* yaitu Transaksi elektronik dapat dilakukan dalam bidang privat dan bidang publik. Yang dimaksud 'lingkup privat' ialah transaksi elektronik dalam lingkup perdata yang dilakukan antara para pihak yang berkepentingan, seperti antara satu orang dengan orang lain, satu perusahaan dengan perusahaan lain, termasuk satu instansi pemerintah dengan instansi pemerintah lain atau dengan pihak lain. Sedangkan yang dimaksud dengan 'lingkup publik' ialah transaksi elektronik yang menyangkut kebijakan publik atau berhubungan dengan masyarakat luas. Transaksi elektronik yang dilakukan dalam rangka menjalankan kebijakan publik seperti pengadaan barang/jasa secara elektronik *(e-Procurement)*, dan penyelenggaraan perizinan secara elektronik adalah dua contoh transaksi elektronik dalam lingkup publik.

Data pribadi perlu dilindungi terhadap penyalahgunaan. Perkembangan pengaturan terhadap perlindungan data pribadi secara umum akan menempatkan Indonesia sejajar dengan negara-negara maju. Hal ini dapat memerkuat dan memerkokoh posisi Indonesia sebagai pusat bisnis dan investasi terpercaya, yang itu adalah strategi kunci dalam perkembangan ekonomi.[19] Rosadi menyebutkan adanya peluang akan kekhawatiran bahwa data pribadi dijual atau digunakan tanpa persetujuan pengguna.[20] *Security* (keamanan) dan *privacy* (privasi) merupakan hal yang utama dalam praktik penyelenggaraan sistem elektronik. Itu juga termasuk karena data pribadi adalah kepentingan hukum yang serius bagi pengguna sistem elektronik.

**Korporasi dan kebijakan pidana dalam konvergensi teknologi informasi komunikasi**

Konvergensi teknologi informasi komunikasi juga berimplikasi pada aturan hukum dan regulasi. Dikatakan hukum merespon kebutuhan manusia akan ketertiban dan keteraturan dalam suatu fenomena yang baru yang muncul. Antisipasi terhadap implikasi ini terdapat tiga pendekatan,

---

[18]Pablo Asbo Baistrocchi, "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce," *Santa Clara High Technology Law Journal Article* 19, no. 1 (2003): 11130., h. 116

[19]Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasional*, Refika Aditama, Bandung, 2015)., h. 14

[20]*Ibid.*, h. 15

yaitu pendekatan legislatif *(Legislative Approach)*, pendekatan regulasi *(Regulatory Approach)* dan pendekatan swa-kramawi *(Self-regulating Approach)*. Ketiganya perlu berjalan bersama-sama atau *co-exist*, untuk mencapai pengaturan yang holistik pada penyelenggaraan konvergensi ini.

Pada dasarnya, kategorisasi konten yang melanggar hukum dalam media konvergensi teknologi informasi komunikasi adalah sebagai berikut:

- *Copyright material.*
  *Creative rights are one of the most affected areas of the law since with the Internet it is extremely easy to disseminate copyrighted work. It occurs when any kind of protected material (text, picture, music) is posted on a Web page without respecting the copyright holder's rights.*
- *Illegal and harmful content.*
  *This category includes material that can be labeled as pornographic, racist, or terrorist.*
- *Private and defamatory material.*
  *This kind of material includes pictures taken in intimate situations, information concerning the family situation, financial or tax statements, or otherwise private or derogatory material infringing various rights of privacy, including those contained in European data protection and anti-defamation laws.*
- *Misrepresentation.*
  *This may happen when false or incorrect information, provided by and disseminated using on-line facilities, causes damage to a third party.*
- *Others: this includes the infringement of other substantive laws such as patents, trademarks, and unfair trade practices.*[21]

Selain itu, UU ITE mengatur mengenai data *interference*, dan ini terdapat ancaman pidananya. Hal tersebut termasuk data *availability, confidentiality*, dan *integrity*. Kesengajaan melakukan data *interference* jelas merupakan tindak pidana. Semua perbuatan yang dilarang dan diancam pidana dalam UU ITE memiliki bentuk kesalahan berupa kesengajaan. Terdapat peluang bagi korporasi penyelenggara yang menyebabkan data *corrupt*, walaupun tidak ada unsur kesengajaan. Selain itu juga ada peluang penyebab kebocoran data adalah sistem elektronik yang dikelola penyelenggara.

Ketiga pilar ini - data *availability, confidentiality*, dan *integrity* - apabila lumpuhnya adalah karena serangan siber, korporasi penyelenggara sistem elektronik belum tentu dapat dipersalahkan mengingat belum tentu ada *mens rea*. Namun penyelenggara wajib membuktikan bahwa telah melakukan pengamanan yang layak, sesuai dengan standar yang ditetapkan Pemerintah dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik yang telah dijelaskan di sub-pembahasan sebelumnya.

Sistem elektronik melibatkan perangkat lunak. Sitompul mengatakan, sama seperti tiada hukum yang tanpa celah, demikian juga tiada perangkat lunak tanpa galat *(bug)*. Galat merupakan kesalahan atau kegagalan dalam pemrograman komputer yang mengakibatkan hasil yang tidak tepat atau tidak sesuai dengan yang diinginkan. Menemukan galat *(bug)* tidak selalu mudah. Itu seperti mencari kebocoran air pada pipa dalam rangkaian instalasi pipa. Namun apabila tidak diperbaiki, akan menimbulkan kerentanan pada sistem elektronik. Jika hal tersebut diketahui oleh orang yang memiliki keahlian, ia dapat masuk ke dalam sistem dan melakukan apa saja termasuk pengrusakan.[22]

---

[21] Pablo Asbo Baistrocchi, *Op.Cit.*, h. 115
[22] Josua Sitompul, *Op.Cit.*, h. 84

Mengingat pekerjaan mencari dan memerbaiki galat *(bug)* merupakan pekerjaan yang tidak mudah, memang mengancam penyelenggara sistem elektronik dengan pidana karena kegagalan sistem yang disebabkan oleh galat *(bug)* merupakan sesuatu yang berlebihan. Namun, apabila penyelenggara sistem elektronik tidak melakukan evaluasi perangkat lunak secara berkala dan tidak berniat memerbaiki untuk upaya pengamanan, dalam hal ini dapat dikatakan sebagai kelalaian yang disadari.

Terdapat beberapa pengembangan pengamanan data yang perlu untuk dilakukan. Seperti contohnya yang dijelaskan oleh de Guise:[23]

*"Given is the plethora of data protection options that may need to be deployed in a modern business:*

- *Backup administrators need to understand storage and virtualization options in use.*
- *Storage administrators need to know how and where backup will supplement replication, snapshots, and redundant array of independent disk (RAID) and be closely aligned to virtualization for performance and protection reasons.*
- *Virtualization administrators need to know what protection, capacity, and performance options are available to them.*

Perlu ada pengelola atau admin yang melakukan *back-up* data, pengelola yang mengerti bagaimana dan kapan *back-up* dilengkapi dengan replikasi, *snapshot*, dan *redundant array of independent disk* (RAID), serta pengelola virtualisasi yang memahami perlindungan, kapasitas data dan pilihan performa yang tersedia bagi pengguna.

Lebih lanjut, de Guise menyatakan untuk mencapai pengamanan data yang layak secara efektif adalah dengan cara mengombinasikan ketiga hal tersebut *back-up*, penyimpanan, dan virtualisasi. Telah banyak pelaku bisnis dalam industry 4.0 yang sudah menerapkannya, khususnya yang sudah mapan.[24]

Korporasi dapat dikatakan sebagai pilar perekonomian nasional - Badan hukum termasuk dalam korporasi, tetapi korporasi tidak selalu berbentuk badan hukum. Pieth dan Ivory menegaskan:

> *"Corporations could, like human beings, hold rights and duties under private law but they could not be regarded as possessing the moral faculties that would enable them to be addressees of the criminal law. It is, however, equally obvious that corporations can cause substantial harm. They have been drivers of industrialization and the globalization of the economy. Their negligence has resulted in severe injury to individuals, groups, and the natural environment and their deliberate abuses of power have highlighted their apparently privileged position relative to other persons and entities."*[25]

Mengingat korporasi juga merupakan pilar perekonomian negara, penjatuhan pidana kepada korporasi bukan sebagai upaya pembalasan atau tindakan retributif, dan pembatasannya harus jelas.*Convention on cybercrime* (CoC) memberikan batasan pertanggungjawaban terhadap penyelenggara jasa yang terlibat dalam transmisi atau komunikasi elektronik. Selain pembatasan pertanggungjawaban, CoC memuat pengaturan kriminalisasi terhadap badan usaha yang melakukan atau terlibat dalam tindak pidana siber. Suatu cybercrime yang dilakukan oleh pribadi kodrati dapat dilakukan untuk kepentingan suatu badan usaha, dan pribadi kodrati tersebut dapat bertindak secara individu atau bertindak sebagai bagian dari organ badan usaha. Dalam hal individu itu merupakan

---

[23]Preston de Guise, *Data Protection Ensuring Data Availability* (Boca Raton London New York: CRC Press Taylor & Francis Group, 2017), https://www.taylorfrancis.com/books/9781351689519.

[24]de Guise., h. 42

[25]Mark Pieth and Radha Ivory, "Emergence and Convergence: Corporate Criminal Liability Principles in Overview," *Ius Gentium Comparative Perspectives on Law and Justice* 9 (2011), https://doi.org/10.1007/978-94-007-0674-3., h. 4

bagian dari organ badan usaha, ia bertindak berdasarkan kuasa untuk merepresentasikan badan usaha; kewenangan untuk mengambil keputusan untuk dan atas nama badan usaha; atau kewenangan untuk melaksanakan kontrol dalam badan usaha. Apabila salah satu dari hal tersebut terpenuhi, maka badan usaha dapat dikenakan pertanggung jawaban secara hukum baik secara pidana, perdata, maupun administrasi.[26]

**Potensi pertanggungjawaban pidana korporasi**

Bermodalkan pengetahuan teknis dan paket data internet atau jaringan internet gratis, setiap orang dapat berperan dalam dunia maya dengan mentransmisikan, mereproduksi, menyebarkan berbagai macam konten atau materi dalam berbagai bentuk atau macam. Contohnya lagu, tulisan, gambar, video, film, semuanya dapat di-*posting* atau diunggah ke laman situs atau *website*, menggunakan peralatan yang sudah umum di dunia teknologi komersil modern. Terkait korporasi penyelenggara sistem elektronik, bukan mem-*posting* atau mengunggah kontennya yang menjadi persoalan, namun konten yang di-*posting* atau diunggah bisa jadi termasuk melanggar hukum.

Disarikan oleh Saputra, terdapat beberapa doktrin terkait pertanggungjawaban pidana korporasi yaitu: Doktrin Identifikasi, Doktrin Pertanggungjawaban Pengganti *(vicarious liability)*, dan Doktrin Pertanggungjawaban yang ketat menurut undang-undang *(strict liability)*.[27]

Doktrin Identifikasi diterapkan di negara-negara Anglo Saxon, salah satu contohnya Inggris. Pertanggungjawaban ini dikenal sebagai *direct-corporate-criminal-liability*. *Mens rea* tidak dikesampingkan dalam doktrin ini. Sikap batin atau perbuatan yang dicela oleh undang-undang dari petinggi korporasi yang memiliki *directing mind* bisa dianggap sebagai sikap korporasi. Hal ini berarti sikap batin yang dimaksud dapat diidentifikasikan sebagai sikap batin korporasi, dengan demikian korporasi dapat dikenakan pertanggungjawaban langsung apabila sikap batin atau perbuatannya melanggar ketentuan pidana.

Pertanggungjawaban pengganti *(vicarious liability)* inti ajarannya adalah pertanggungjawaban tanpa kesalahan pribadi, tetapi pertanggungjawaban muncul atas kesalahan orang atau pihak lain. Menurut doktrin ini, majikan ialah penanggung jawab utama dari perbuatan para buruh atau pekerjanya yang melakukan perbuatan dalam ruang lingkup tugas atau pekerjaannya. Garis bawah untuk doktrin ini, belajar dari contoh kasus Allen V. Whitehead.[28] Kasus melibatkan *Refreshment House* namun disebutkan memelihara prostitusi *(harbouring prostitutes)*, dan mengindikasikan pengetahuan dari pekerja yang bertanggungjawab dan sikap abainya majikan akan hal itu, akhirnya majikan dikenakan pertanggungjawaban pidana atas hal itu berdasarkan Pasal 44 *Metropolitan Police Act* 1893.

Mengenai doktrin *strict liability*, salah satu contoh penganutnya adalah Inggris. Menganut asas *"actus non facit reum nisi mens sit rea"*, doktrin ini menganut prinsip pertanggungjawaban mutlak tanpa harus membuktikan ada atau tidaknya unsur kesalahan pada diri pelaku tindak pidana. Nawawi Arief, memberikan pandangannya atas pertanggungjawaban pidana yang ketat ini. Pertanggungjawaban pidana dapat dikenakan dalam hal korporasi melanggar atau tidak memenuhi kewajiban atau kondisi atau situasi tertentu yang sebagaimana diatur oleh peraturan perundang-undangan, misalnya undang-undang menetapkan suatu perbuatan sebagai delik terhadap korporasi yang beroperasi atau menjalankan bisnis tanpa izin, korporasi pemegang izin yang melanggar syarat-

---

[26] Baca Pasal 12 CoC
[27] Rony Saputra, "Pertanggungjawaban Pidana Korporasi Dalam Tindak Pidana Korupsi," *Jurnal Cita Hukum* 2, no. 2 (2015)., h. 279
[28] King's Bench Division, Allen v Whitehead (1929). <https://www.quitesimplylaw.com/allenvwhite head> diakses 7 Februari 2019

syarat yang ditentukan dalam izin yang diberikan kepadanya, dan korporasi yang mengoperasikan kendaraan tanpa diasuransikan.[29]

Baistrocchi pernah mengungkapkan bahwa dalam menentukan apakah penyedia jasa sistem elektronik[30] dapat dipertanggungjawabkan pidana liabilitasnya, bergantung pada tipe *criminal liability* yang dianut. Untuk tipe *strict liability*, penyedia jasa sistem elektronik akan dikenakan pertanggungjawaban pidana tanpa memandang pengetahuan dan kontrol atas materi yang ditransmisikan atau didistribusikan melalui sistemnya.[31] Tipe ini termasuk sangat restriktif, karena pengelola sistem elektronik dikatakan bertanggungjawab[32] atas materi atau konten meskipun mereka tidak memiliki pengetahuan atau kontrol terhadapnya. Tipe ini secara tidak langsung mewajibkan pengelola sistem elektronik untuk memonitor semua materi atau konten yang di-posting di dalam sistem elektronik yang mereka kelola. Mematuhi kewajiban ini merupakan hal yang kompleks, tugas teknis yang membebani, dan termasuk dalam hal yang terlarang dalam perspektif ekonomi. Maka, mayoritas pengelola sistem elektronik yang masih skala kecil, yang tidak memiliki kapasitas atau niat untuk memenuhi kewajiban, akan menghadapi ancaman potensi bertanggungjawab secara pidana.

Dalam suatu sistem pertanggungjawaban berdasarkan kesalahan, pengelola sistem elektronik dikatakan bertanggungjawab apabila secara sengaja melakukan pelanggaran (juga terhadap hak orang/pihak lain). Menurut Baistrocchi, terdapat dua jenis tingkatan dalam sistem pertanggungjawaban ini: pengetahuan aktual, dan pengetahuan konstruktif. Untuk pengetahuan aktual, apabila pengelola sistem elektronik mengetahui ada konten atau materi dalam sistemnya yang merupakan pelanggaran ketentuan pidana, maka pengelola sistem elektronik dapat dikenakan pertanggungjawaban. Untuk pengetahuan konstruktif, pengelola sistem elektronik akan dikenakan pertanggungjawaban apabila mereka sudah memiliki petunjuk tertentu, atau seharusnya dapat mengasumsi keberadaan konten atau materi tertentu yang melanggar hukum,[33] namun tidak melakukan tindakan sesuai dengan peraturan perundang-undangan. Memang permasalahan yang muncul terkait hal ini adalah membuktikan pengetahuan maupun kelalaian dari pengelola sistem elektronik.

Pandangan bahwa korporasi sebagai persona memungkinkan korporasi dapat dikenakan pertanggungjawaban pidana pengganti *(vicarious liability)* atas perbuatan buruh atau pekerjanya. Di beberapa yurisdiksi, memang mengakui imputasi perbuatan pidana perorangan yang mewakili korporasi kepada perbuatan korporasi.

Selain tiga tipe pertanggungjawaban yang dijelaskan di atas, Pieth dan Ivory menyatakan bahwa telah muncul model tanggung jawab holistik (atau "obyektif") dan agregat. Model holistik, tidak seperti identifikasi dan model pertanggungjawaban pengganti *(vicarious)*, tidak memerlukan imputasi pikiran, tindakan, dan kelalaian manusia untuk menarik pertanggungjawaban perusahaan. Sebaliknya, mereka menganggap korporasi sebagai diri mereka mampu melakukan kejahatan melalui pola internal pengambilan keputusan (budaya perusahaan atau organisasi korporat). Pendekatan agregatif juga memperlakukan korporasi sebagai pelaku utama apabila terdapat tindakan-tindakan yang teragregasi, kelalaian, dan keadaan pikiran para pemangku kepentingan secara individual, terutama pejabat perusahaan dan manajer senior. Ini semacam kompromi antara *vicarious liability* dan holistik.[34]

---

[29] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana* (Bandung: Citra Aditya Bakti, 2003)., h. 237-238

[30] Baistrocchi menggunakan istilah *Intermediary Service Provider (ISP)* untuk penyedia jasa sistem elektronik yang dimaksud pada artikel ini.

[31] Pablo Asbo Baistrocchi, *Op.Cit.*, h. 114

[32] Penggunaan istilah bertanggungjawab di konteks kalimat ini ada dua, *responsible* dan secara konsekuen *liable*.

[33] *Ibid.*

[34] Pieth and Ivory, *Op.Cit.*, h. 5

Sitompul menjelaskan terkait dengan ketentuan pembantuan dalam tindak pidana siber, CoC memberikan batasan pertanggungjawaban terhadap penyelenggara jasa yang terlibat dalam transmisi atau komunikasi elektronik. Misalnya, meski pun transmisi konten *malicious code* memerlukan keterlibatan penyelenggara jasa, mereka yang tidak memiliki tujuan untuk melakukan tindak pidana tersebut tidak dapat dikenakan pertanggungjawaban pidana atas perbuatan yang terjadi melalui layanannya.[35] Oleh karena itu, tidak ada kewajiban bagi penyelenggara jasa untuk memonitor konten secara terus menerus dalam rangka menghindari pertanggungjawaban pidana berdasarkan ketentuan ini. Pengaturan tersebut sesuai dengan *Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)* [selanjutnya disebut EUDC]. Dalam Pasal 12 EUDC diatur mengenai *'mere conduit'*:

> *1) Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:*
>
> *(a.) does not initiate the transmission;*
>
> *(b.) does not select the receiver of the transmission; and*
>
> *(c.) does not select or modify the information contained in the transmission.*
>
> *2) The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.*
>
> *3) This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.*

Pengaturan tersebut mengatur bahwa penyelenggara jasa yang terlibat *e-commerce* hanya sebagai saluran *(intermediary/mere conduit)* tidak dapat dikenakan pertanggungjawaban secara hukum mengenai informasi yang ditransmisikan dengan menggunakan jasanya dengan ketentuan bahwa penyelenggara tersebut memenuhi salah satu kondisi berikut. Pertama, penyelenggara jasa tidak memprakarsai transmisi informasi. Kedua, penyelenggara jasa tidak menentukan siapa yang menjadi penerima informasi. Ketiga, penyelenggara jasa tidak menentukan atau memodifikasi informasi yang ditransmisikan. Penyimpanan informasi elektronik secara otomatis, intermedier, dan temporer dalam proses transmisi informasi dalam rangka memindahkan informasi tersebut termasuk dalam pengecualian pertanggungjawaban pidana.

Lebih lanjut, dalam Pasal 13 EUDC mengena *"caching"* juga diatur bahwa penyelenggara jasa tidak bertanggung jawab terhadap informasi yang tersimpan secara otomatis untuk sementara waktu dan informasi tersebut hanya berupa perantara yang bertujuan untuk mempermudah transmisi informasi kepada penerima jasa berdasarkan permintaan penerima jasa itu sendiri. Berikut kutipan pasalnya:

---

[34] Pieth and Ivory, *Op.Cit.*, h. 5

[35] Josua Sitompul, *Op.Cit.*, h.113

*1) Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:*

*(a) the provider does not modify the information;*

*(b) the provider complies with conditions on access to the information;*

*(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;*

*(d) the provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and*

*(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.*

Penghapusan tanggung jawab ini dimungkinkan dalam hal terpenuhinya salah satu kondisi berikut, Pertama, penyelenggara tidak memodifikasi atau mengubah informasi. Kedua, penyelenggara telah bertindak sesuai dengan ketentuan mengenai akses terhadap informasi. Ketiga, penyelenggara menyimpan informasi sesuai dengan ketentuan pembaruan atau pemutakhiran informasi, yang spesifikasinya diterima secara luas oleh industri. Keempat, penyelenggara jasa tidak melakukan gangguan melalui penggunaan teknologi secara sah untuk menerima atau menggunakan informasi. Terakhir, penyelenggara segera memindahkan atau menghentikan akses terhadap informasi yang telah tersimpan berdasarkan pengetahuan bahwa informasi telah dipindahkan dari jaringan, atau akses terhadap informasi tersebut telah dihentikan, atau berdasarkan perintah pengadilan atau otoritas yang berwenang.

Penyelenggara *hosting* juga tidak bertanggung jawab terhadap informasi yang disimpan padanya berdasarkan permintaan pengguna jasa hosting sepanjang penyelenggara tersebut tidak mengetahui mengenai adanya tindakan yang melawan hukum atau informasi yang melawan hukum. Hal ini diatur di Pasal 14 EUDC:

*1) Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*

*(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*

*(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*

Pengecualiannya ada dua, yang pertama apabila penyelenggara tidak memiliki pengetahuan *actual* terhadap aktifitas ilegal maupun informasi berkonten ilegal. Yang kedua, penyelenggara *hosting* juga tidak bertanggung jawab terhadap informasi yang disimpan itu dalam hal penyelenggara menerima informasi, bertindak segera untuk memindahkan atau menutup akses terhadap informasi tersebut.

EUDC juga tidak membebani penyelenggara jasa untuk memonitor informasi yang mereka transmisikan atau simpan, atau mengharuskan penyelenggara jasa untuk mencari tahu secara aktif mengenai adanya tindakan ilegal. Akan tetapi, dimungkinkan penyelenggara dibebani tanggung jawab untuk melaporkan kepada pihak yang berwenang dalam hal penyelenggara menemui adanya perbuatan yang dilarang yang menggunakan fasilitas yang diberikannya.

Baistrocchi menjelaskan bahwa terdapat dua pendekatan dalam pengenaan pertanggungjawaban pidana terhadap penyelenggara sistem elektronik sebagai intermedier. Dalam pendekatan vertikal, perbedaan tipe pertanggungjawaban korporasi diterapkan dalam berbagai area pengaturan hukum. Pendekatan ini diadopsi oleh Amerika Serikat, contohnya dalam *Act 27 The Digital Millennium Copyright* terkait masalah hak cipta, dan *Act 28 Telecommunications 1996* terkait pertanggungjawaban pidana yang berasal dari pelanggaran ketentuan hukum lainnya.[36]

Dari pemaparan di atas, dapat dilihat bahwa EUDC tidak menganut model *strict liability* untuk pertanggungjawaban pidana korporasi. Pendekatan horizontal digunakan oleh EUDC. Pendekatan horizontal dapat dikatakan lebih diminati karena pengelola sistem elektronik tidak harus memantau konten materi yang diterbitkan oleh pengguna. Jika Uni-Eropa mengadopsi pendekatan vertikal yang menerapkan rezim tanggung jawab hukum yang berbeda terhadap data yang mengalir melalui sistem, pengelola sistem elektronik akan diwajibkan untuk memecahkan kode *bit* yang membentuk data dan menganalisis semua konten (musik, gambar, dll) sebelum di-*posting*kan. Ini akan menjadi beban yang sangat berat untuk diletakkan di pundak pengelola sistem elektronik.

Yang perlu diadopsi oleh Indonesia adalah penggunaan model agregat yang dijelaskan oleh Pieth dan Ivory. Model ini dapat digunakan untuk melihat adanya sikap batin yang tercela melalui agregasi tindakan atau absennya tindakan korporasi. Menggunakan *strict liability* merupakan hal yang berlebihan, *vicarious liability* lebih relevan untuk diterapkan. Ketika terjadi kesulitan dalam membuktikan siapa individu dari pengurus yang melakukan tindakan pelanggaran hukum, pendekatan holistik dapat diterapkan, yaitu menentukan dari pola internal pengambilan keputusan korporasi.

## PENUTUP

Dalam industri 4.0 dan upaya untuk bersaing dalamnya, penyelenggara sistem elektronik harus mengamankan, melakukan *maintenance* dan semua upaya yang diperlukan agar sistem elektronik bekerja sebagaimana mestinya dan *reliable* atau dapat diandalkan. Saat ini, kegagalan pemenuhan kewajiban ini sebagaimana diatur dalam peraturan perundang-undangan, secara sengaja maupun lalai, tidak mengandung elemen sanksi pidana sebagai konsekuensinya. Adapun perlindungan yang diberikan dalam Pasal 26 UU ITE kepada pihak yang dirugikan akibat tindakan atau tidak bertindaknya penyelenggara sistem elektronik hanya dapat ditempuh secara perdata.

Kegagalan penyelenggara sistem elektronik, baik yang sengaja maupun lalai untuk memenuhi kewajiban yang diatur dalam peraturan perundang-undangan, perlu untuk dikriminalisasi. Namun perlu ditekankan bahwa penjatuhan pidana kepada korporasi penyelenggara sistem elektronik bukanlah bersifat retributif. Ini bertujuan untuk memastikan kepatuhan penyelenggara sistem elektronik.

Dalam PP Penyelenggaraan Sistem dan Transaksi Elektronik sudah diatur mengenai sanksi administratif pada Pasal 84 jika terjadi pelanggaran, namun perlu dilihat pada Pasal 15 ayat (1)-

[36] Pablo Asbo Baistrocchi, *Op.Cit.*, h. 117

nya, kegagalan menjaga rahasia, keutuhan dan ketersediaan data pribadi hanya dikenakan sanksi administratif. Padahal data pribadi merupakan kepentingan hukum yang serius bagi pengguna sistem elektronik. Dalam hal ini hukum pidana juga perlu hadir sebagai *ultimum remedium*.

Indonesia perlu menerapkan *vicarious liability* dalam mengenakan pertanggungjawaban pidana terhadap korporasi, juga mengadopsi pendekatan agregat dan holistik untuk mendukung pembuktiannya dalam gagalnya menjalankan kewajiban menyelenggarakan sistem elektronik yang andal dan *reliable*.

Untuk penelitian atau karya ilmiah di masa mendatang, perlu untuk dilaksanakan riset perihal membedakan bilamana pertanggungjawaban dikenakan terhadap korporasi, dan bilamana dikenakan terhadap pengurus korporasi.

## DAFTAR PUSTAKA

### Buku


Arief, Barda Nawawi. *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya Bakti, 2003.

Baistrocchi, Pablo Asbo. "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce." *Santa Clara High Technology Law Journal Article* 19, no. 1 (2003): 11130.

Budhijanto, Danrivanto. *Teori Hukum Konvergensi*. Bandung: Refika Aditama, 2014.

Gilchrist, Alasdair. *Industry 4.0: The Industrial Internet of Things*. Apress, 2016. https://doi.org/10.1017/978-1-4842-2047-4.

Guise, Preston de. *Data Protection Ensuring Data Availability*. Boca Raton London New York: CRC Press Taylor & Francis Group, 2017. https://www.taylorfrancis.com/books/9781351689519.King's Bench Division. Allen v Whitehead (1929).

Makarim, Edmon, and et al. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Jakarta: Raja Grafindo Persada, 2005.

Mulyati, Nani. "Pemisahan Pertanggungjawaban Pidana Korporasi Dengan Pertanggungjawaban Pidana Pengurus Korporasi." In *Proceeding Call for Papers Simposium Dan Pelatihan Hukum Pidana Ke-V "Revitalisasi Hukum Pidana Adat Dan Kriminologi Kontemporer."* Yogyakarta: Genta Publishing, 2018.

Neama, Ghadeer, Rana Alaskar, and Mohammad Alkandari. *"Privacy, Security, Risk, and Trust Concerns in e-Commerce." Proceedings of the 17th International Conference on Distributed Computing and Networking - ICDCN '16*, 2016, 16. https://doi.org/10.1145/2833312.2850445.

Pennanen, Kyösti, Taina Kaapu, and Minna-Kristiina Paakki. "Trust , Risk , Privacy , and Security in e-Commerce." *In Frontiers of E-Business Research*, 2006.

Pieth, Mark, and Radha Ivory. "Emergence and Convergence: Corporate Criminal Liability Principles in Overview." *Ius Gentium Comparative Perspectives on Law and Justice 9* (2011). https://doi.org/10.1007/978-94-007-0674-3.

Rosadi, Sinta Dewi. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasional*. Bandung: Refika Aditama, 2015.

Sahetapy, J.E. *Kejahatan Korporasi*. Bandung: Eresco, 1994.

Saputra, Rony. "Pertanggungjawaban Pidana Korporasi Dalam Tindak Pidana Korupsi." *Jurnal Cita*

*Hukum 2*, no. 2 (2015).

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw*. Jakarta: Tatanusa, 2014.

**Internet**

Investor Daily Indonesia, E-Commerce Berpotensi Jadi Pilar Baru Ekonomi RI, <https://id.beritasatu.com/tradeandservices/e-commerce-berpotensi-jadi-pilar-baru-ekonomi-ri/130282>, diakses tanggal 9 Februari 2019

Kementerian Komunikasi dan Informatika, Penerapan Sistem Pemerintahan Berbasis Elektronik, <https://kominfo.go.id/index.php/content/detail/8319/penerapan-sistem-pemerintah-berbasis-elektronik/0/berita_satker>, diakses tanggal 9 Februari 2019

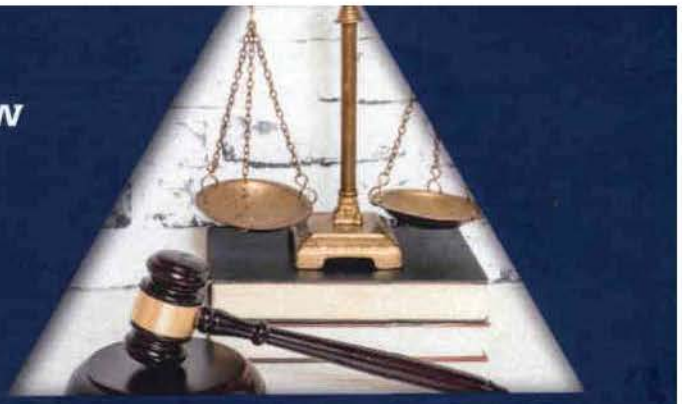
**Peraturan Perundang-undangan**

*Council of Europe, Convention on Cybercrime*, 23.XI.2001, Budapest, Hungaria

Peraturan Menteri Komunikasi dan Informatika No. 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik (Berita Negara RI Tahun 2014 Nomor 1432)

The European Parliament and the Council of the European Union, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce)

MS Centre for Law



# PERSPEKTIF HUKUM BISNIS DI INDONESIA

## Kumpulan Catatan Kritis

Editor :
Martin Suryana,
A. Suhartati Lukito
& Hwian Christianto

GENTA
PUBLISHING

# PERSPEKTIF
# HUKUM BISNIS
## DI INDONESIA

Kumpulan Catatan Kritis

MS Centre for Law

# PERSPEKTIF HUKUM BISNIS DI INDONESIA

## Kumpulan Catatan Kritis

Editor:
Martin Suryana, A. Suhartati Lukito
& Hwian Christianto

GENTA
PUBLISHING

**Perspektif Hukum Bisnis di Indonesia**
Kumpulan Catatan Kritis



Cetakan I, 2019

| | |
|---|---|
| Editor | : Martin Suryana, dkk |
| Layout | : Presylia Lazirosa |
| Desain Cover | : Presylia Lazirosa |
| Pracetak | : Khairul Bari |
| Supervisi | : Nasrullah Ompu Bana |

GENTA
PUBLISHING

Perum Pring Mayang Regency 2 Kav. 4
Jl. Rajawali Gedongan Baru
Banguntapan, Bantul-Yogyakarta
INDONESIA
Telp. (0274) 451654 - 0878 3419 7555
E-mail: redaksigenta@yahoo.com
WA: 0812 3781 8611
**Anggota IKAPI**

**Perspektif Hukum Bisnis di Indonesia**
Kumpulan Catatan Kritis

Yogyakarta: GENTA Publishing 2019
iv + 220 hlm.: 15.5 X 24 cm

ISBN: 978-602-0757-16-2

# KATA PENGANTAR

Dua puluh tahun berkarir sebagai praktisi hukum dan Advokat serta dua belas tahun mendirikan sebuah firma hukum yang bernama "MARTIN SURYANA & ASSOCIATES, ADVOCATES AND LEGAL CONSULTANTS" belum lah cukup sebagai penanda perjalanan karir yang paripurna. Pahit manis, timbul tenggelam, dan pasang surut perjalanan serta pengalaman telah dilalui. Namun pengalaman demi pengalaman akan pupus dengan berjalannya waktu. Kalimat bijak mengatakan *"seorang ahli akan terus dikenang lewat karya dan tulisan-tulisan yang bermanfaat"*.

*"Praise the Lord"*, tidak ada kata yang lebih sempurna selain ucapan syukur kepada Tuhan Yang Maha Besar atas terselesaikannya sebuah karya ilmiah yang merupakan penanda kematangan berkarir dan berprofesi sebagai seorang Advokat dan praktisi hukum. Kumpulan catatan kritis ini bukanlah puncak dari perjalanan karir sebagai seorang Advokat, tetapi justru merupakan awal dari mimpi besar sebagai seorang ahli hukum yang tidak saja cakap di medan pertempuran dunia hukum, melainkan juga mumpuni secara keilmuan di bidang hukum.

Terbitnya buku berjudul **PERSPEKTIF HUKUM BISNIS DI INDONESIA: Kumpulan Catatan Kritis**, merupakan penerbitan perdana yang dilakukan bertepatan dengan hari jadi firma hukum kami yang ke-12 yang jatuh pada tanggal 23 Agustus dan sekaligus *re-branding* MARTIN SURYANA & ASSOCIATES. Bertepatan dengan momentum yang berbahagia tersebut, dengan bangga kami mempersembahkan **MS CENTRE FOR LAW** sebagai awal membangun mimpi besar dan idealisme hukum kami.

Tidak ada yang lebih atau paling hebat diantara kami semua, mulai dari jajaran *Chairman, Senior Associate, Associate, Lawyer,* dan *paralegal* di "MARTIN SURYANA & ASSOCIATES" ingin memberikan karya terbaik kami bagi para client secara khusus dan bagi masyarakat pencari keadilan secara umum. Tulisan-tulisan berupa catatan kritis dari pengalaman profesional kami dapat terwujud bukan saja karena semangat juang kami, namun juga berkat kegigihan serta tangan dingin dari tim editor, yaitu Dr. Hwian Christianto, S.H., M.H., dan Dr. Suhartati, S.H., M.Hum. yang sekaligus merupakan arsitek dan *founder* MS CENTRE FOR LAW.
*Thanks so much for both of you, Guys!*

Terima kasih juga yang tak terhingga untuk semua penulis baik yang berafiliasi pada Martin Suryana & Associates, Advocates and Legal Consultants maupun para akademisi dari Laboratorium Hukum Pidana Fakultas Hukum Universitas Surabaya. Ucapan terima kasih juga diberikan kepada tim paralegal yaitu Louis Sleyvent Eliezer Tappangan, S.H., Chesa Effendi, S.H., dan Rizki Istighfariana Achmadi, S.H. yang telah ikut membantu dalam proses pembuatan buku ini, juga penerbit yang memungkinkan hadirnya buku ini ke tengah para pembaca. Buku ini

dipersembahkan juga bagi kedua orang tua saya, ibu mertua dan almarhum ayah mertua, istri tercinta, kedua buah hati saya, para guru, guru besar, dosen, dan para *mentor* serta *senior* saya yang tidak dapat saya sebutkan satu persatu, yang telah mendidik dan memungkinkan saya dengan segala kekurangan dan kelebihan menjadi seorang Advokat.

*"Tak ada gading yang tak retak"*, tidak ada karya yang maha sempurna. Adagium ini merupakan cerminan dari penerbitan buku ini. Semoga kumpulan catatan kritis ini bermanfaat bagi para client yang kesemuanya bergerak di dunia bisnis maupun para pemerhati hukum, baik di dalam wilayah Indonesia maupun di luar wilayah Indonesia. Setidaknya, tulisan ini dapat memperkaya wawasan hukum bisnis di Indonesia sekaligus diharapkan sebagai sumbangsih pemikiran bagi penyempurnaan pengaturan hukum, khususnya di bidang hukum bisnis di Indonesia.

Salam,

Dr. MARTIN SURYANA, S.H., M.Hum.

# DAFTAR ISI

# LIST OF CONTRIBUTORS

**Dr. A. Suhartati Lukito, S.H., M.Hum.** Menyelesaikan studi S1 dari Fakultas Hukum Universitas Surabaya pada tahun 1999 dengan predikat *Cumlaude*. Pada tahun 2001, ia menyelesaikan pendidikan S2 di Program Pascasarjana Universitas Surabaya dengan predikat *Cumlaude*. Pada tahun 2012 berhasil menyelesaikan pendidikan Doktor Ilmu Hukum di Fakultas Hukum Universitas Airlangga dengan predikat *Cumlaude*. Pada tahun yang sama memperoleh penghargaan Prestasi Akademik dari Ikatan Advokat Indonesia DPC Surabaya, serta penghargaan dari Museum Rekor Indonesia. Pada tahun 2002 mulai bergabung sebagai dosen di Fakultas Hukum Universitas Surabaya. Sesuai dengan fokus pendalaman kompetensi keilmuan dibidang Hukum Pidana Bisnis, sejak tahun 2013 setiap tahun menjadi *invited speaker* di *University of Cambridge*, United Kingdom dalam kegiatan *The Cambridge International Symposium on Economic Crime*. Suhartati juga ikut menjadi salah satu penulis dalam buku referensi internasional yang berjudul *Research Handbook on International Financial Crime* di United Kingdom dan USA. Berbagai karya ilmiah juga telah dipublikasikan dalam jurnal internasional bereputasi (terindeks scopus), jurnal nasional maupun proceeding konferensi internasional.
Suhartati juga menjadi praktisi hukum dan advokat di *Martin Suryana & Associates, Advocates and Legal Consultants*. Selain itu juga menjadi anggota dari *International Bar Association The Criminal Law Committee, The Academic and Professional Development Committee*, anggota Masyarakat Hukum Pidana dan Kriminologi Indonesia (Mahupiki), anggota Perhimpunan Advokat Indonesia DPC Surabaya, Ikatan Advokat Indonesia DPC Surabaya.

**Abdul Rochim, S.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Surabaya. Berpengalaman dibidang Hukum Ketenagakerjaan *(Labour Law)* dan aspek-aspek hukum dibidang perindustrian termasuk segala aspek hukum dibidang perijinan. Tergabung sebagai Konsultan Hukum pada *Martin Suryana & Associates, Advocates and Legal Consultants*.

**Anton Hendrik Samudra, S.H., M.H.** Dosen tetap di Fakultas Hukum Universitas Surabaya. Pendidikan formal Sarjana Hukum pada Fakultas Hukum Universitas Airlangga dan Magister Hukum pada Fakultas Hukum Universitas Airlangga (Unair) Surabaya. S-2 lulus dengan predikat lulusan terbaik program Magister Hukum FH Universitas Airlangga pada tahun 2011. Fokus riset dan pengajaran pada bidang hukum pidana siber. Saat ini menjabat sebagai Ketua Laboratorium Hukum Pidana, dan terlibat dalam Kantor Layanan Hukum dan Biro Bantuan Hukum, Fakultas Hukum, Universitas Surabaya.

**Dr. Elfina Lebrine Sahetapy, S.H., LL.M.,** Menyelesaikan Sarjana Hukum di Fakultas Hukum Universitas Surabaya, 1993, dan menyelesaikan Program Master Criminology and Victimology at Faculty of Law University of Leiden in the Netherlands, 1998. Melanjutkan Program Doktor di

Fakultas Hukum Universitas Brawijaya Malang, 2009. Dosen tetap di Fakultas Hukum Universitas Surabaya sejak 1995. Bernaung di bawah Laboratorium Hukum Pidana dan menjadi pengampu matakuliah Hukum Pidana, Kriminologi Viktimologi dan Sistem Peradilan Pidana Anak. Aktif meneliti dan menulis serta mengikuti International Conference terutama yang berafiliasi dan rutin diadakan oleh International Juvenile Justice Organization (IJJO) dan World Society of Victimology (WSV). Penerima Hibah DIKTI Penelitian 2017 dan 2018, Hibah DIKTI Pengabdian pada Masyarakat 2017. Email: elfina_69@yahoo.com

**Dr. Go Lisanawati, S.H., M.Hum.** adalah seorang dosen dan peneliti dari Fakultas Hukum Universitas Surabaya (UBAYA). Ahli hukum pidana secara khusus Anti Pencucian Uang dan Kejahatan Siber. Giat mengembangkan keahliannya pada bidang *Cyber security* dari dimensi anti pencucian uang. Dr. Go masih aktif menjadi narasumber untuk membahas materi terkait RUU KUHP, RUU Tipikor, dan topik lain serta narasumber seminar nasional dan internasional, mempresentasikan *paper* pada *International conference*, dan juga melakukan kegiatan *visiting Professorship* di Thammasat University, Thailand. Motivasi : *"Accept the challenges, so that you may feel exhilaration of victory" (George S. Patton).*

**Dr. Hwian Christianto, S.H., M.H.** Menyelesaikan Sarjana Hukum di Fakultas Hukum Universitas Airlangga (Unair) Surabaya, Magister Hukum di Program Pascasarjana Fakultas Hukum Universitas Airlangga (Unair) serta Doktor Ilmu Hukum Program Doktor Ilmu Hukum Fakultas Hukum Universitas Gadjah Mada (UGM). Dosen Tetap pada Fakultas Hukum Universitas Surabaya (Ubaya), Surabaya pada Laboratorium Hukum Pidana. Penulis aktif dalam menulis, meneliti, dan mengikuti *training, workshop*, dan konferensi baik yang bersifat nasional maupun internasional terkait isu hukum dan hak asasi manusia. Penerima Hibah Penulisan Buku Ajar DIKTI 2012 dan Insentif Buku Ajar Terbit 2019.

**Irwan Santoso Hadiwidjaja, S.H., M.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Surabaya dan gelar Magister Hukum pada Program Pascasarjana Universitas Airlangga Surabaya. Berpengalaman sebagai Advokat dan Konsultan Hukum serta memiliki keahlian dibidang litigasi maupun non-litigasi. Juga menguasai berbagai aspek hukum dibidang korporasi dan aktif mengikuti berbagai kegiatan ilmiah dan pelatihan hukum dalam skala nasional maupun internasional. Selain itu juga menjadi anggota dalam Perhimpunan Advokat Indonesia (PERADI) DPC Surabaya maupun Ikatan Advokat Indonesia (IKADIN) DPC Surabaya. Tergabung sebagai *Member of Associates pada Martin Suryana & Associates, Advocates and Legal Consultants.*

**Johan Handjojo, S.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Pelita Harapan Surabaya dan saat ini sedang menempuh pendidikan S2 Program Pascasarjana pada Fakultas Hukum Universitas Pelita Harapan Surabaya. Berpengalaman dibidang industri dan Perbankan serta menguasai berbagai aspek Hukum Ekonomi dan Bisnis. Mendalami disiplin ilmu yang berkaitan dengan tindak pidana dibidang Korporasi. Tergabung sebagai Konsultan Hukum pada *Martin Suryana & Associates, Advocates and Legal Consultants.*

**Dr. Martin Suryana, S.H., M.Hum.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Surabaya dengan predikat *Cumlaude*. Gelar Magister Humaniora diperoleh dari Program Pascasarjana Universitas Surabaya dan dinobatkan sebagai Wisudawan Terbaik Universitas Surabaya serta memperoleh predikat *Summa Cumlaude*. Predikat *Cumlaude* juga diperoleh saat dinyatakan lulus pada program Doktor Fakultas Hukum Universitas Airlangga dan sekaligus memperoleh apresiasi berupa piagam penghargaan dari Museum Rekor Dunia Indonesia. Berpengalaman sebagai Advokat dan Konsultan Hukum selama 20 tahun serta memiliki keahlian spesifik dibidang hukum korporasi dan bisnis. Pendiri *Martin Suryana & Associates, Advocates and Legal Consultants*. Dosen pada Fakultas Hukum Universitas Surabaya. Aktif dalam berbagai kegiatan ilmiah, baik sebagai pembicara maupun peserta, dalam skala nasional maupun international, diantaranya *Thirty-Seventh Cambridge International Symposium On Economic Crime* yang diselenggarakan oleh *Law Faculty Jesus College, Cambridge*. Memiliki sertifikasi profesi, yaitu *Certified Liquidator Indonesia* juga sebagai Kurator dan Pengurus. Sebagai anggota Perhimpunan Advokat Indonesia (PERADI), Perkumpulan Profesi Likuidator Indonesia (PPLI), Perhimpunan Kurator dan Pengurus Indonesia (HKPI) dan juga tercatat sebagai *member of International Bar Association (IBA)*.

**Merry Setiawati Tantono, S.H., M.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Surabaya dan gelar Magister Hukum pada Fakultas Hukum Universitas Surabaya. Advokat dan Konsultan Hukum dengan spesialisasi dibidang Hukum Bisnis dan Perusahaan *(Corporate and Bussiness Law)*, dan Hukum Kontrak *(Contract Law)*. Aktif mengikuti kegiatan ilmiah dan pelatihan hukum dalam skala nasional maupun internasional. Pengalaman organisasi, pada tahun 2016 hingga April 2019 sebagai anggota Perhimpunan Profesi Hukum Kristiani Indonesia (PPHKI) Chapter Surabaya. Selain itu juga menjadi anggota dalam Perhimpunan Advokat Indonesia (PERADI) DPC Surabaya maupun Ikatan Advokat Indonesia (IKADIN) DPC Surabaya. Tergabung sebagai *Member of Associates pada Martin Suryana & Associates, Advocates and Legal Consultants*.

**Michelle Kristina, S.H., M.Kn.** Mendapatkan pendidikan Sarjana Hukum pada Fakultas Hukum Universitas Surabaya dan gelar Magister Kenotariatan pada Fakultas Hukum Universitas Surabaya. Saat ini bekerja sebagai Dosen Tetap di Fakultas Hukum Universitas Surabaya. Karya tulis yang telah dibuat diantaranya tentang pemidanaan korporasi yang melakukan korupsi, pendirian korporasi dengan akta yang batal demi hukum, formulasi pertanggungjawaban pidana korporasi, serta korporasi yang didirikan untuk melakukan kejahatan.

**Peter Jeremiah Setiawan, S.H., M.H.** Menyelesaikan studi Sarjana Hukum (2012) dan Magister Ilmu Hukum (2017) pada Fakultas Hukum Universitas Surabaya (UBAYA), masing-masing dengan predikat *cum laude* dan wisudawan teladan pada progam sarjana serta predikat *Summa Cum Laude* pada progam magister. Sejak tahun 2016, aktif dalam konsultasi dan penanganan kasus-kasus hukum, baik perkara pidana maupun perdata di salah satu kantor advokat Surabaya. Saat ini menjadi dosen Fakultas Hukum Universitas Surabaya pada Laboratorium Hukum Pidana dan aktif menulis dengan fokus pada hukum pembuktian dan kejahatan

keuangan. Email: peter.j.setiawan@gmail.com

**Subuh Susilo, S.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Surabaya. Berpengalaman sebagai Advokat dan Konsultan Hukum selama 20 Tahun. Menguasai dan memiliki keahlian dibidang hukum, khususnya dibidang litigasi mapun non-litigasi. Mendalami berbagai aspek dibidang Hukum Korporasi, Hukum Perindustrian, Hukum Ketenagakerjaan, dan Hukum Kontrak. Aktif mengikuti berbagai kegiatan ilmiah dan pelatihan hukum serta berpengalaman menangani kasus-kasus pidana dalam skala besar yang menarik perhatian publik. Selain itu juga menjadi anggota dalam Perhimpunan Advokat Indonesia (PERADI) DPC Surabaya maupun Ikatan Advokat Indonesia (IKADIN) DPC Surabaya. Tergabung sebagai *Senior Associates* pada *Martin Suryana & Associates, Advocates and Legal Consultants.*

**Yuliyati, S.H.** Memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Wijaya Putra Surabaya. Berpengalaman dibidang hak atas kekayaan intelektual *(Intelectual Property Rights).* Aktif mengikuti kegiatan berbagai kegiatan ilmiah dibidang hukum bisnis dan hukum perusahaan. Tergabung sebagai Konsultan Hukum pada *Martin Suryana & Associates, Advocates and Legal Consultants.*

# PERSPEKTIF
# HUKUM BISNIS
## DI INDONESIA

**Kumpulan Catatan Kritis**

Mengingat era globalisasi dan era Revolusi Industri 4.0 yang menghadirkan perkembangan dunia bisnis dan industri yang bergerak dengan pesat, hal ini juga sangat berpengaruh pada perkembangan hukum bisnis di Indonesia. Kejahatan pun muncul dalam berbagai macam bentuk dan modus operandi sehingga membutuhkan pemahaman lebih lanjut tentang tipologi, konsep dan penanganan kejahatan yang telah berkembang tersebut. Buku ini membahas berbagai kajian kritis baik dalam teori maupun praktek hukum dalam hal-hal yang terkait dengan hukum bisnis, secara spesifik yang berkaitan dengan kejahatan ekonomi dan kejahatan korporasi.

Buku ini dapat menjadi referensi bagi para pemerhati hukum, akademisi, praktisi hukum maupun mahasiswa yang tertarik untuk mempelajari tentang hukum bisnis khususnya terkait dengan berbagai tipologi kejahatan ekonomi dan kejahatan korporasi di Indonesia beserta penanggulangannya.

**MS Centre for Law**

GENTA PUBLISHING
Literatur Hukum Indonesia

Perum Pring Mayang Regency 2 Kav. 4
Jl. Rajawali Gedongan Baru
Banguntapan, Bantul-Yogyakarta - INDONESIA
Telp. 0274-451654, 0812 3781 8611
E-mail: redaksigenta@yahoo.com

ISBN 978-602-0757-16-2
9 786020 757162